

# Notes on the Foundations of Constructive Mathematics

by Joan Rand Moschovakis

December 27, 2004

## 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 intuitionist 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  $\&$ ,  $\vee$ ,  $\rightarrow$ ,  $\neg$ ,  $\forall$ ,  $\exists$  a distinct meaning. Classically, all the propositional connectives can be defined from  $\&$  and  $\neg$ , while  $\exists$  can be defined from  $\forall$  and  $\neg$ , so  $\vee$ ,  $\rightarrow$  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 $\mathbf{Pp}$

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

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

$\mathbf{Pp}$  has one *rule of inference*:

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

The *axioms* of  $\mathbf{Pp}$  are all formulas of the following forms:

- X1.  $A \rightarrow (B \rightarrow A)$ .
- X2.  $(A \rightarrow B) \rightarrow ((A \rightarrow (B \rightarrow C)) \rightarrow (A \rightarrow C))$ .
- X3.  $A \rightarrow (B \rightarrow A \& B)$ .
- X4.  $A \& B \rightarrow A$ .

- X5.  $A \& B \rightarrow B$ .  
 X6.  $A \rightarrow A \vee B$ .  
 X7.  $B \rightarrow A \vee B$ .  
 X8.  $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$ .  
 X9.  $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$ .  
 X10.  $\neg A \rightarrow (A \rightarrow B)$ .

*Definition.* A *proof* in  $\mathbf{Pp}$  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  $\mathbf{Pp}$ . We write  $\vdash_{\mathbf{Pp}} E$  (or in this section just  $\vdash E$ ) to denote that  $E$  is a theorem of  $\mathbf{Pp}$ .

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

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

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

- From  $B$  conclude  $A \rightarrow B$ .

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  $\mathbf{Pp}$  of a formula  $E$  from a collection  $\Gamma$  of formulas is a finite sequence of formulas, each of which is an axiom or a member of  $\Gamma$  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  $\mathbf{Pp}$  from  $\Gamma$ , 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  $\Gamma' = \{G_1, \dots, G_n\}$  of  $\Gamma$  such that  $\Gamma' \vdash E$  (also written  $G_1, \dots, G_n \vdash E$ ). If  $n = 0$  (so  $\Gamma'$  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  $\mathbf{Pp}$ )* If  $\Gamma, A \vdash B$  then  $\Gamma \vdash (A \rightarrow B)$ .

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

If  $n = 1$  then  $E_1$  is an axiom, a member of  $\Gamma$ , or  $A$ . In the first two cases we construct a new deduction  $F_1, F_2, F_3$  of  $(A \rightarrow E_1)$  from  $\Gamma$  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  $(A \rightarrow A)$  in  $\mathbf{Pp}$ .

Assuming the theorem holds for deductions of length  $< n$  where  $n > 1$ , consider a given deduction  $E_1, \dots, E_n$  from  $\Gamma, A$ . If  $E_n$  is an axiom or a member of  $\Gamma$ , 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  $(E_j \rightarrow E_n)$ , then by the induction hypothesis there are deductions  $F_1, \dots, F_r$  of  $(A \rightarrow E_j)$  from  $\Gamma$ , and  $F_{r+1}, \dots, F_{r+s}$  of  $(A \rightarrow E_k)$  from  $\Gamma$ . Extend the deduction  $F_1, \dots, F_{r+s}$  by three lines to obtain a deduction of  $(A \rightarrow E_n)$  from  $\Gamma$ .

*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,  $\Gamma, \Delta$  are collections of formulas and  $A, B$  are formulas; note that  $\Gamma, \Delta$  may overlap.

*Theorem 2.2. In  $\mathbf{Pp}$ :*

- (a) If  $\Gamma \vdash (A \rightarrow B)$  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  $\vdash (A \rightarrow B) \& (B \rightarrow C) \rightarrow (A \rightarrow C)$ . 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  $\mathbf{Pp}$  of  $(A \rightarrow B) \& (B \rightarrow C) \rightarrow (A \rightarrow C)$ .

1.  $(A \rightarrow B) \& (B \rightarrow C) \vdash (A \rightarrow B)$ . [by Thm. 2.2(a) from X4]
2.  $(A \rightarrow B) \& (B \rightarrow C) \vdash (B \rightarrow C)$ . [by Thm. 2.2(a) from X5]
3.  $(B \rightarrow C) \vdash (A \rightarrow (B \rightarrow C))$ . [by Thm. 2.2(a) from X1]
4.  $(A \rightarrow B), (A \rightarrow (B \rightarrow C)) \vdash (A \rightarrow C)$ . [by Thm. 2.2(a) twice, from X2]
5.  $(A \rightarrow B), (B \rightarrow C) \vdash (A \rightarrow C)$ . [by Thm. 2.2(b) from 3,4]
6.  $(A \rightarrow B) \& (B \rightarrow C), (B \rightarrow C) \vdash (A \rightarrow C)$ . [by Thm. 2.2(b) from 1,5]
7.  $(A \rightarrow B) \& (B \rightarrow C) \vdash (A \rightarrow C)$ . [by Thm. 2.2(b) from 2,6]
8.  $\vdash (A \rightarrow B) \& (B \rightarrow C) \rightarrow (A \rightarrow C)$ . [by Thm. 2.1 from 7]

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

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  $\mathbf{Pp}$  has the *single substitution property*: If  $\Gamma \vdash E$ , and if  $\Gamma', E'$  come from  $\Gamma, E$  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  $P_1, \dots, P_n$ . Let  $A_1, \dots, A_n$  be (not necessarily distinct) formulas of  $\mathcal{L}(\mathbf{Pp})$ . If  $E'$  comes from  $E$  by simultaneously replacing each occurrence of  $P_i$  in  $E$  by an occurrence of  $A_i$ , for  $i = 1, \dots, n$ , 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  $P_1, \dots, P_{n+m}$  includes all the proposition letters occurring in  $A_1, \dots, A_n$ . 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  $P_1, \dots, P_n$  occurs in any of  $B_1, \dots, B_n$ . 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  $\mathbf{Pp}$ )* If  $\Gamma \vdash E$ , and if  $\Gamma', E'$  come from  $\Gamma, E$  respectively by simultaneously replacing every occurrence of  $P_i$  by an occurrence of  $A_i$ , for  $i = 1, \dots, n$ , then  $\Gamma' \vdash E'$ .

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

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

*Exercise 2.5\**. Suppose that  $E, F$  are formulas of  $\mathcal{L}(\mathbf{Pp})$  such that for every substitution instance  $(E' \rightarrow F')$  of  $(E \rightarrow F)$ : if  $\vdash_{\mathbf{cPp}} E'$  then  $\vdash_{\mathbf{cPp}} F'$ . Show that  $\vdash_{\mathbf{cPp}} (E \rightarrow F)$ . [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  $\mathbf{cPp}$  is *derivable* in  $\mathbf{cPp}$ . The corresponding statement for  $\mathbf{Pp}$  is false; in fact, the collection of admissible, nonderivable rules of  $\mathbf{Pp}$  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 $\mathbf{Np}$

We have just observed that a few derived rules can save much time and effort in constructing (outlines of) formal proofs and derivations in  $\mathbf{Pp}$ . One can go still further and abandon all axiom schemas in favor of rules as in the following *natural deduction* system  $\mathbf{Np}$  (essentially from Kleene [1952]), which differs from  $\mathbf{N-IPC}$  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  $\mathbf{Np}$  of a formula  $E$  from assumptions  $\Gamma$  is a finite tree with a formula attached to each node (in particular, formulas from  $\Gamma$  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  $\Gamma$  of  $E$* .
- (ii) If  $\mathcal{D}_1, \mathcal{D}_2$  and  $\mathcal{D}_3$  are *deductions from  $\Gamma$*  (and possibly the additional assumptions shown inside square brackets), of their last formulas (shown explicitly), then new *deductions from  $\Gamma$*  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*.

$$\begin{array}{c} \mathcal{D}_1 \quad \mathcal{D}_2 \\ \&I \quad \frac{A \quad B}{A \& B} \end{array} \quad \begin{array}{c} \mathcal{D}_1 \\ \&E_r \quad \frac{A \& B}{A} \end{array} \quad \begin{array}{c} \mathcal{D}_1 \\ \&E_l \quad \frac{A \& B}{B} \end{array}$$

$$\begin{array}{c} \mathcal{D}_1 \\ \vee I_r \quad \frac{A}{A \vee B} \end{array} \quad \begin{array}{c} \mathcal{D}_1 \\ \vee I_l \quad \frac{B}{A \vee B} \end{array} \quad \begin{array}{c} [A] \quad [B] \\ \mathcal{D}_1 \quad \mathcal{D}_2 \quad \mathcal{D}_3 \\ \vee E \quad \frac{A \vee B \quad C \quad C}{C} \end{array}$$

$$\begin{array}{c}
[A] \\
\mathcal{D}_1 \\
\hline
\rightarrow \text{I} \frac{B}{A \rightarrow B}
\end{array}
\quad
\rightarrow \text{E} \frac{\mathcal{D}_1 \quad \mathcal{D}_2}{\frac{A \rightarrow B}{B} \quad A}$$

$$\begin{array}{c}
[A] \quad [A] \\
\mathcal{D}_1 \quad \mathcal{D}_2 \\
\hline
\neg \text{I} \frac{B \quad \neg B}{\neg A}
\end{array}
\quad
\neg \text{E}_i \frac{\mathcal{D}_1 \quad \mathcal{D}_2}{\frac{A \quad \neg A}{B}}$$

If  $\Gamma$  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  $\mathbf{NPp}$  of  $E$  from  $\Gamma$ . If  $\Gamma$  is empty then  $\mathcal{D}$  is a *proof of  $E$*  in  $\mathbf{NPp}$ .

It follows from the definition that if  $\mathcal{D}$  is a deduction from  $\Gamma$  of  $E$ , and  $\Gamma'$  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  $\Delta$  of  $E$ .

## 2.4 Equivalence of $\mathbf{Pp}$ with $\mathbf{NPp}$

*Theorem 2.4.* If  $E$  is a formula, and  $\Gamma$  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  $\Gamma, E$  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  $\mathbf{NPp}$  of each axiom  $E$  of  $\mathbf{Pp}$ . As an example, observe that

$$\frac{A}{B \rightarrow A} \rightarrow \text{I}$$

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

$$\frac{\frac{[A]}{B \rightarrow A} \rightarrow \text{I}}{A \rightarrow (B \rightarrow A)} \rightarrow \text{I}$$

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

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

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

*Exercise 2.7.* Construct labelled  $\mathbf{NPp}$ -proofs of Axioms X9 and X10 of  $\mathbf{Pp}$ .

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

## 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  $\rightarrow$  cannot be replaced by  $\leftrightarrow$ .

*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  $\neg$ I rule of **NPp** to conclude  $A \vdash \neg\neg A$ . Then use  $\rightarrow$  I.

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

$$\frac{\frac{\frac{[A]}{A \vee B} \vee I_r \quad \neg(A \vee B) \quad \neg I}{\neg A} \quad \neg I \quad \frac{\frac{[B]}{A \vee B} \vee I_l \quad \neg(A \vee B) \quad \neg I}{\neg B} \quad \& I}{(\neg A \& \neg B)} \& I$$

$$\frac{[A \vee B] \quad \frac{\frac{[A] \quad \frac{\neg A \& \neg B}{\neg A} \& E_r}{\neg(A \vee B)} \neg E_i \quad \frac{[B] \quad \frac{\neg A \& \neg B}{\neg B} \& E_l}{\neg(A \vee B)} \neg E_i}{\neg(A \vee B)} \vee E}{\neg(A \vee B)} \neg I, \text{ cancelling } A \vee B \text{ (twice)}$$

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

$$\frac{A \rightarrow B \quad \frac{[A \& \neg B] \quad \& E_r}{A} \rightarrow E \quad \frac{[A \& \neg B] \quad \& E_l}{\neg B} \& E_l}{\neg(A \& \neg B)} \neg I$$

*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  $\neg$ -elimination rule  $\neg E_i$  to the following rule expressing the classical *law of double negation*:

$$\neg E_c \frac{\mathcal{D} \quad \neg\neg A}{A}$$

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 $\mathbf{Pd}$

Again taking Kleene [1952] as a guide, we begin with a Hilbert-style formal system  $\mathbf{Pd}$  which contains  $\mathbf{Pp}$  as a subsystem. Formal theorems of  $\mathbf{Pp}$  (such as the parts of Theorem 2.5) will hold in  $\mathbf{Pd}$  for all formulas  $A, B$  of the extended language. The Deduction Theorem for  $\mathbf{Pd}$  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  $a_1, a_2, a_3, \dots$ , and countably infinitely many distinct predicate letters of arity  $n$  for each  $n = 0, 1, 2, 3, \dots$ . The 0-ary predicate letters are the proposition letters  $P_1, P_2, \dots$  of  $\mathcal{L}(\mathbf{Pp})$ . The unary predicate letters are  $P_1(\cdot), P_2(\cdot), \dots$ , the binary ones are  $P_1(\cdot, \cdot), P_2(\cdot, \cdot), \dots$ , and in general the  $n$ -ary ones are  $P_i(\cdot, \dots, \cdot)$  for  $i = 1, 2, \dots$  where  $\cdot, \dots, \cdot$  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  $P(\cdot, \dots, \cdot)$  is an  $n$ -ary predicate letter and  $t_1, \dots, t_n$  are terms, then  $P(t_1, \dots, t_n)$  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  $(A \ \& \ B)$ ,  $(A \vee B)$ ,  $(A \rightarrow B)$  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,  $x, y, z, w, x_1, y_1, \dots$  will be used as metavariables for individual variables, and  $A, B, C, \dots$  as metavariables for formulas. Anticipating applications (e.g. to arithmetic) where the terms may be more complicated, we use  $t, u, v, t_1, \dots$  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  $\mathbf{Pd}$  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  $\forall a_1 (\exists a_2 (P_1(a_1, a_2) \rightarrow \exists a_1 P_2(a_1, a_2))) \ \& \ P_1(a_1)$ , 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  $x \mapsto y \mapsto x$  leads from  $A(x)$  to  $A(y)$  and back to  $A(x)$ . (Note that distinct metavariables  $x, y, z, w, x_1, \dots$  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  $C \rightarrow \forall xA(x)$ .

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

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

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

*Definition.* A *deduction* (or *derivation*) in **Pd** of a formula  $E$  from a collection  $\Gamma$  of formulas is a finite sequence of formulas, each of which is an axiom by X1 - X12, or a member of  $\Gamma$ , 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  $E_1, \dots, E_n$  is a deduction from  $\Gamma$  and  $G \in \Gamma$ , then for each  $k = 1, \dots, n$  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  $\Gamma$ , 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  $\Gamma$ , with respect to a variable  $x$  which occurs free in at least one assumption from  $\Gamma$  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  $\Gamma$  exists in which  $x_1, \dots, x_k$  are varied, we sometimes write  $\Gamma \vdash_{\mathbf{Pd}}^{x_1, \dots, x_k} E$  (or in this subsection just  $\Gamma \vdash^{x_1, \dots, x_k} E$ ).

*Exercise 2.11.* Construct a deduction in **Pd** of  $\exists xA(x)$  from  $\forall xA(x)$ , 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  $(\exists xA(x) \rightarrow C)$  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  $x_1, \dots, x_k$  are varied, then  $\Gamma, A \vdash B$  by a deduction in which only  $x_1, \dots, x_k$  are varied.

(b) If  $\Gamma, A \vdash B$  by a deduction  $E_1, \dots, E_k$  in which  $B$  does not depend on  $A$  and only  $x_1, \dots, x_n$  are varied, then some subsequence of  $E_1, \dots, E_k$  is a deduction of  $B$  from  $\Gamma$  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  $x_1, \dots, x_k$  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  $y_1, \dots, y_m$  is varied, and  $x$  does not occur free in any assumption from  $\Gamma$  on which the conclusion  $A(x)$  depends, then  $\Gamma \vdash_{\mathbf{Pd}} \forall xA(x)$  by a deduction in which none of  $y_1, \dots, y_m$  is varied.

*Exercise 2.14.* [This is part of the proof of Theorem 2.7.] Prove that in **Pp**:

- (a)  $(A \rightarrow (C \rightarrow D)) \vdash (A \& C \rightarrow D)$  and
- (b)  $(A \& C \rightarrow D) \vdash (A \rightarrow (C \rightarrow D))$ .

*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  $x_1, \dots, x_m$  are varied, then  $\Gamma \vdash_{\mathbf{Pd}} (A \rightarrow B)$  by a deduction in which no variables except  $x_1, \dots, x_m$  (and possibly only some of these) are varied.

*Proof.* Fix  $\Gamma$  and  $A$ , and suppose  $E_1, \dots, E_n$  is a given deduction of  $B$  from  $\Gamma, A$  in which all variables occurring free in  $A$  are held constant and only  $x_1, \dots, x_m$  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  $\Gamma$  then  $(A \rightarrow E_1)$  is derivable from  $\Gamma$  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  $E_1, \dots, E_n$  from  $\Gamma, A$  in which all variables free in  $A$  are held constant, and only  $x_1, \dots, x_m$  are varied. If  $E_n$  is an axiom or a member of  $\Gamma$ , proceed as in the basis, observing that no variables are varied in the resulting deduction of  $(A \rightarrow E_n)$  from  $\Gamma$ . 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  $x_1, \dots, x_m$  were varied in the (independent) deductions  $F_1, \dots, F_r$  of  $(A \rightarrow E_j)$  and  $F_{r+1}, \dots, F_{r+s}$  of  $(A \rightarrow E_k)$  from  $\Gamma$  provided by the induction hypothesis. If  $y$  is another variable occurring free in some formula of  $\Gamma$  which appears as assumption  $F_i$  for some  $1 \leq i \leq r$ , then none of  $F_{i+1}, \dots, F_r$  was justified by applying R2 or R3 (with  $y$  as the variable) to any formula depending on  $F_i$ , and none of  $F_{r+1}, \dots, F_{r+s}$  depends on any of  $F_1, \dots, F_r$ . Hence  $y$  is not varied in  $F_1, \dots, F_{r+s}$ . Since the new steps  $F_{r+s+1}, F_{r+s+2}, F_{r+s+3}$  use only propositional logic, no variables other than  $x_1, \dots, x_m$  are varied in the resulting deduction of  $(A \rightarrow E_n)$  from  $\Gamma$ .

*Rule 2.* If  $E_n$  comes from some  $E_j$  with  $j < n$  by R2, then  $E_n$  is of the form  $(C \rightarrow \forall x D(x))$  where  $E_j$  is  $(C \rightarrow D(x))$  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  $F_1, \dots, F_r$  of  $(A \rightarrow E_j)$  from  $\Gamma$  in which no variables other than  $x_1, \dots, x_m$  are varied. By the result of Exercise 2.14 this deduction can be extended to  $F_1, \dots, F_{r+s}$ , using only X1-X10 and R1 in the new part, so that  $F_{r+s}$  is  $(A \& C \rightarrow D(x))$ . Since  $x$  is not free in  $A \& C$ , by R2 from  $F_{r+s}$  we conclude  $(A \& C \rightarrow \forall x D(x))$ , which is  $F_{r+s+1}$ . More propositional steps lead to  $(A \rightarrow (C \rightarrow \forall x D(x)))$ , which is  $(A \rightarrow E_n)$ . In the resulting deduction no variables have been varied which were not already varied in  $E_1, \dots, E_n$ .

*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  $\Gamma$  in which no variables other than  $x_1, \dots, x_m$  are varied. Extend this to a deduction of  $(A \rightarrow E_n)$  from  $\Gamma$  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  $(\exists x D(x) \rightarrow C)$  where  $E_j$  is  $(D(x) \rightarrow C)$ , 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  $G_1, \dots, G_r$  of  $(A \rightarrow E_j)$  from  $\Gamma$  in which no variables other than  $x_1, \dots, x_m$  are varied. Then  $G_1, \dots, G_r$  can be extended by propositional steps to  $G_1, \dots, G_{r+s}$  where  $G_{r+s}$  is  $(D(x) \rightarrow (A \rightarrow C))$ . Since  $x$  is not free in  $(A \rightarrow C)$ , by R3 from  $G_{r+s}$  we can conclude  $(\exists x D(x) \rightarrow (A \rightarrow C))$ , from which  $(A \rightarrow E_n)$  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  $\Gamma$  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  $\Gamma$  of  $E$ .
- (ii) If  $\mathcal{D}_1, \mathcal{D}_2$  and  $\mathcal{D}_3$  are deductions from  $\Gamma$  (and possibly the additional assumptions shown inside square brackets), of their last formulas (shown explicitly), then new deductions from  $\Gamma$  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  $A(x)$ .

$$\begin{array}{c} \mathcal{D}_1 \\ \forall I \frac{A(x)}{\forall x A(x)} \end{array} \quad \begin{array}{c} \mathcal{D}_1 \\ \forall E \frac{\forall x A(x)}{A(t)} \end{array}$$

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

If  $\Gamma$  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  $\Gamma$ . If  $\Gamma$  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  $\Gamma$  of  $E$ , and  $\Gamma'$  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  $\Delta$ .

*Example.* Here is a proof in **NPd** of  $\forall x A(x) \rightarrow \forall y A(y)$  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  $\forall I$ .

$$\frac{\frac{\frac{[\forall x A(x)]}{A(y)} \quad \forall E}{\forall y A(y)} \quad \forall I}{\forall x A(x) \rightarrow \forall y A(y)} \rightarrow I$$

*Exercise 2.15.* Construct a proof in **NPd** of  $\exists x A(x) \rightarrow \exists y A(y)$  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 $\mathbf{Pd}$ with $\mathbf{NPd}$ , and the Replacement Theorem for $\mathbf{Pd}$

*Theorem 2.8.* If  $E$  is a formula, and  $\Gamma$  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  $\Gamma, E$  simultaneously, by complete induction on the length of a given  $\mathbf{Pd}$ -deduction of  $E$  from  $\Gamma$  in which no variable is varied. The proof of Theorem 2.4  $\Rightarrow$  provides  $\mathbf{NPd}$ -proof schemas for the propositional axioms X1-X10 of  $\mathbf{Pd}$ . It is easy to construct  $\mathbf{NPd}$ -proof schemas for X11 and X12, using the  $\rightarrow$  rules with  $\forall E$  and  $\exists I$  (which have the same restrictions as X11 and X12 of  $\mathbf{Pd}$ ). The rules require more care.

Suppose  $F_1, \dots, F_n, F_{n+1}$  is a deduction in  $\mathbf{Pd}$  from  $\Gamma$  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  $\mathbf{Pd}$ -deduction of length  $\leq n$ , so for each  $j \leq n$  and each  $\Delta$ : If  $G_1, \dots, G_j$  is a deduction in  $\mathbf{Pd}$  from  $\Delta$  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  $F_j \rightarrow F_{n+1}$ . By the induction hypothesis there are  $\mathbf{NPd}$ -deductions  $\mathcal{D}_1, \mathcal{D}_2$  of  $F_i, F_j$  respectively from  $\Gamma$ . Combine these using  $\rightarrow E$  to get an  $\mathbf{NPd}$ -deduction of  $F_{n+1}$  from  $\Gamma$ .

*Case 2.*  $F_{n+1}$  is  $(C \rightarrow \forall xA(x))$ , 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  $(C \rightarrow A(x))$ , and  $x$  is not free in any assumption from  $\Gamma$  on which  $F_i$  depends (otherwise  $x$  would be varied by the use of R2). Then by Lemma 2.6(b) some subsequence of  $F_1, \dots, F_i$  is a  $\mathbf{Pd}$ -deduction of  $(C \rightarrow A(x))$  from a subcollection  $\Gamma'$  of  $\Gamma$  in which  $x$  does not occur free. By the induction hypothesis there is an  $\mathbf{NPd}$ -deduction  $\mathcal{D}_1$  of  $F_i$  from  $\Gamma'$ . Extend it as follows to an  $\mathbf{NPd}$ -deduction of  $F_{n+1}$  from  $\Gamma'$  (hence also from  $\Gamma$ ). The use of  $\forall I$  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  $\Gamma'$ .

$$\frac{\frac{\mathcal{D}_1}{(C \rightarrow A(x))} \quad [C]}{A(x)} \rightarrow E}{\frac{A(x)}{\forall xA(x)} \forall I} \rightarrow I, \text{ cancelling } C$$

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

$$\frac{\frac{\mathcal{D}_1}{(A(x) \rightarrow C)} \quad [A(x)]}{\frac{[\exists xA(x)]}{C} \exists E, \text{ cancelling } A(x); \text{ no free } x \text{ in } \Gamma' \text{ or } C} \rightarrow E}{\frac{C}{(\exists xA(x) \rightarrow C)} \rightarrow I, \text{ cancelling } \exists xA(x)}$$

*Proof of (b)  $\Rightarrow$  (a).* Assume  $\mathcal{D}$  is an  $\mathbf{NPd}$ -deduction from  $\Gamma$  of  $E$ , and assume the induction hypothesis holds for the subdeduction(s) from  $\Gamma$  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  $\rightarrow$  rules. If the last inference was by a quantifier rule, there are four possibilities.

*Case 1.*  $E$  is  $\forall xA(x)$ , 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  $\Gamma'$  be the collection of all assumptions from  $\Gamma$  which are open in  $\mathcal{D}_1$ , so  $x$  is not free in  $\Gamma'$  and  $\mathcal{D}_1$  is a **NPd**-deduction from  $\Gamma'$  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  $\Gamma'$  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  $\exists xA(x)$  from  $\Gamma$ , 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  $\Gamma'$  be the collection of all assumptions from  $\Gamma$  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  $\Gamma'$ . 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  $\Gamma'$ , we can use R3 to conclude  $\Gamma' \vdash_{\mathbf{Pd}} (\exists xA(x) \rightarrow C)$  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  $(A \leftrightarrow B), (A \vee C) \vdash_{\mathbf{NPd}} (B \vee C)$ :

$$\frac{\frac{\frac{A \leftrightarrow B}{(A \rightarrow B)} \&E_r \quad [A]}{B} \rightarrow E \quad \frac{[C]}{B \vee C} \vee I_l}{\frac{A \vee C}{B \vee C} \vee E, \text{cancelling } A \text{ and } C} \vee I_r$$

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  $\forall x(A(x) \leftrightarrow B(x)) \vdash_{\mathbf{Pd}} (\exists xA(x) \leftrightarrow \exists xB(x))$  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  $x_1, \dots, x_k$  all occur free in  $E$ , then  $E \vdash_{\mathbf{Pd}}^{x_1, \dots, x_k} \forall x_1 \dots \forall x_k E$ .

*Definition.* If  $E(x_1, \dots, x_k)$  is a formula of  $\mathcal{L}(\mathbf{Pd})$  with exactly the distinct variables  $x_1, \dots, x_k$  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  $\forall x_1 \dots \forall x_k E(x_1, \dots, x_k)$ .

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  $x_1, \dots, x_k$  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

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

## 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  $\mathbf{Pd}$  (or equivalently, in  $\mathbf{NPd}$ ), for all formulas  $A(x), B(x), C$  such that  $x$  is not free in  $C$ :

- (a)  $\vdash (\forall xA(x) \vee C) \rightarrow \forall x(A(x) \vee C)$ .
- (b)  $\vdash (\exists xA(x) \vee \exists xB(x)) \leftrightarrow \exists x(A(x) \vee B(x))$ .
- (c)  $\vdash \forall x(A(x) \& B(x)) \leftrightarrow (\forall xA(x) \& \forall xB(x))$ .
- (d)  $\vdash \exists x(A(x) \& B(x)) \rightarrow (\exists xA(x) \& \exists xB(x))$ .
- (e)  $\vdash \forall x(A(x) \rightarrow C) \leftrightarrow (\exists xA(x) \rightarrow C)$ .
- (f)  $\vdash \forall x(C \rightarrow A(x)) \leftrightarrow (C \rightarrow \forall xA(x))$ .
- (g)  $\vdash \exists x(A(x) \rightarrow C) \rightarrow (\forall xA(x) \rightarrow C)$ .
- (h)  $\vdash \exists x(C \rightarrow A(x)) \rightarrow (C \rightarrow \exists xA(x))$ .
- (i)  $\vdash (\exists xC \leftrightarrow C)$  and  $\vdash (\forall xC \leftrightarrow C)$ .

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

$$\frac{\frac{\frac{[\forall xA(x)]}{A(x)} \forall E}{\forall xA(x) \vee C} \vee I_r \quad \frac{[C]}{A(x) \vee C} \vee I_l}{\frac{A(x) \vee C}{\forall x(A(x) \vee C)} \vee E, \text{cancelling } \forall xA(x), C} \forall I, \text{ no free } x \text{ in } \forall xA(x) \vee C$$

*Proof of (e).* Here is an informal argument that  $\forall x(A(x) \rightarrow C) \vdash_{\mathbf{NPd}} (\exists xA(x) \rightarrow C)$ . 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  $\mathbf{Pd}$  of  $(A(x) \rightarrow C)$  from  $\forall x(A(x) \rightarrow C)$  in which no variable is varied. Extend this deduction using R3, so  $\forall x(A(x) \rightarrow C) \vdash_{\mathbf{Pd}} (\exists xA(x) \rightarrow C)$  with all variables held constant. Now use Theorem 2.8. [Alternatively, use the proof tree 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  $(\exists xA(x) \rightarrow C) \vdash_{\mathbf{NPd}} \forall x(A(x) \rightarrow C)$ :

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

*Exercise 2.19.* Prove (f) of Theorem 2.10.

*Exercise 2.20.* Prove (g) of Theorem 2.10.

The proof theory of  $\mathbf{Pp}$  and  $\mathbf{Pd}$  has been studied extensively, building on work of Gödel [1932] and Gentzen [1934-35] which established constructively that  $\mathbf{Pp}$  (like  $\mathbf{cPp}$ ) is decidable, although  $\mathbf{Pp}$  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  $\mathbf{cPp}$  into  $\mathbf{Pp}$ , and of  $\mathbf{cPd}$  into  $\mathbf{Pd}$ , showing that in each case the intuitionistic 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  $\vdash_{\mathbf{Pp}} \neg\neg A \rightarrow A$  does not hold for all formulas  $A$  of  $\mathbf{Pp}$ , we need an interpretation with respect to which  $\mathbf{Pp}$  is *sound* (so every theorem of  $\mathbf{Pp}$  is verified by the semantics), and an instance of  $\neg\neg A \rightarrow A$  which is not verified by the semantics. For similar reasons, we need a semantics for  $\mathbf{Pd}$ . 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  $\mathbf{Pp}$  and then the full interpretation for  $\mathbf{Pd}$ .

#### 3.1 Kripke Semantics for $\mathbf{Pp}$

We first provide a Kripke semantics, based on finite rooted trees, with respect to which  $\mathbf{Pp}$  is *sound* and *complete*. Using the decidability of  $\mathbf{Pp}$ , this interpretation is constructive. From the classical viewpoint, on the other hand, the decidability of  $\mathbf{Pp}$  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  $\Gamma$  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  $\Gamma$ . A class  $\Delta$  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*  $\langle \rangle \in T$ , and if  $\langle n_1, \dots, n_{k+1} \rangle \in T$  then  $\langle n_1, \dots, n_k \rangle \in T$ . In the second case,  $\langle n_1, \dots, n_k \rangle$  is called the *immediate predecessor* of  $\langle n_1, \dots, n_{k+1} \rangle$  in  $T$ , and  $\langle n_1, \dots, n_{k+1} \rangle$  is an *immediate successor* of  $\langle n_1, \dots, n_k \rangle$  in  $T$ . More generally, for each  $i \leq k$ ,  $\langle n_1, \dots, n_i \rangle$  is a *predecessor* of  $\langle n_1, \dots, n_{k+1} \rangle$  in  $T$  and  $\langle n_1, \dots, n_{k+1} \rangle$  is a *successor* of  $\langle n_1, \dots, n_k \rangle$ .

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  $\langle n_1, \dots, n_k \rangle \in T$  has only finitely many immediate successors in  $T$  (possibly none). Note that a finitary tree may be finite or infinite.

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

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

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

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

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

where  $p_i$  is the  $i$ th 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  $P_1, \dots, P_n$  of proposition letters is a pair

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

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

The *forcing relation*  $\Vdash$  on  $\mathcal{K}$  is completely determined by  $\kappa$  and the structure of  $(\mathbb{K}, \leq)$ . If  $u \in \mathbb{K}$  and  $E$  is a formula such that  $\mathbf{psf}(E) \subseteq \{P_1, \dots, P_n\}$ , 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.  $u \Vdash (A \rightarrow B)$  if, for each  $v \in \mathbb{K}$  with  $u \leq v$ : if  $v \Vdash A$  then  $v \Vdash B$ .
5.  $u \Vdash (\neg A)$  if, for each  $v \in \mathbb{K}$  with  $u \leq v$ , it is *not* the case that  $v \Vdash A$ .

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

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

*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  $u \in \mathbb{K}$ . 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  $F_1, \dots, F_m$  such that  $\mathbf{psf}(F_i) \subseteq \{P_1, \dots, P_n\}$  for each  $i = 1, \dots, m$ , then for every propositional Kripke model  $\mathcal{K}$  over  $\{P_1, \dots, P_n\}$ :  $\mathcal{K} \Vdash E$ .

*Proof,* by complete induction on the length  $m$  of  $F_1, \dots, F_m$ , where  $F_m$  is  $E$ . If  $m = 1$  then  $E$  is an axiom of **Pp**. For example, if  $E$  is  $A \rightarrow (B \rightarrow A)$  by X1, then for every  $u \in \mathbb{K}$ : 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  $u \leq v \in \mathbb{K}$  and  $u \Vdash (A \rightarrow C)$  and  $v \Vdash (B \rightarrow C)$ , then for every  $w \in \mathbb{K}$  with  $v \leq w$  such that  $w \Vdash (A \vee B)$ :

- (a)  $w \Vdash (A \rightarrow C)$  and  $w \Vdash (B \rightarrow C)$  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  $u \leq v \in \mathbb{K}$ , then  $v \not\Vdash A$  and so  $u \Vdash (A \rightarrow B)$  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  $(F_j \rightarrow E)$ . 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  $\mathcal{K} \not\Vdash E$ ). 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  $\mathbb{K}_1 = \{\langle \rangle, \langle 0 \rangle\}$ , let  $\kappa_1(\langle 0 \rangle) = \{P_1\}$  and  $\kappa_1(\langle \rangle) = \emptyset$ . Then  $\langle \rangle \not\Vdash P_1$ , but also  $\langle \rangle \not\Vdash \neg P_1$  since  $\langle \rangle \leq \langle 0 \rangle \in \mathbb{K}_1$  and  $\langle 0 \rangle \Vdash P_1$ . Note that this is also a countermodel to  $\neg \neg P_1 \rightarrow P_1$ , showing that the converse of Theorem 2.5(b) is unprovable in **Pp**.

*Example.* Let  $\mathcal{K}_2 = ((\mathbb{K}_2, \leq), \kappa_2)$  where  $\mathbb{K}_2 = \mathbb{K}_1 = \{\langle \rangle, \langle 0 \rangle\}$ , 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  $\neg(P_1 \ \& \ \neg P_2) \rightarrow (P_1 \rightarrow P_2)$ , showing that the converse of Theorem 2.5(g) is unprovable in **Pp**.

*Example.* A three-node countermodel to  $(P_1 \rightarrow (P_2 \vee P_3)) \rightarrow (P_1 \rightarrow P_2) \vee (P_1 \rightarrow P_3)$  is  $\mathcal{K}_3 = ((\mathbb{K}_3, \leq), \kappa_3)$  where  $\mathbb{K}_3 = \{\langle \rangle, \langle 0 \rangle, \langle 1 \rangle\}$  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  $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$ , 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  $\Gamma, \Delta$  are collections of formulas of  $\mathcal{L}(\mathbf{Pp})$ , then  $\Gamma$  is  $\Delta$ -saturated if

- (i)  $\Gamma$  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  $\Gamma$  is a  $\Delta$ -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  $\Delta$ -saturated set is a deductively closed subset of  $\Delta$ .

*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  $\Gamma_0$  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  $\Gamma$  is  $\mathbf{sf}(E)$ -saturated,  $\Delta \subseteq \Gamma$ , and  $\Gamma \not\vdash_{\mathbf{Pp}} C$ .

*Proof of (a).* List all the subformulas  $F_1, \dots, F_k$  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  $\Gamma_0^i$  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  $F_1, \dots, F_k$  but neither belongs to any  $\Gamma_0^i$ , 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  $\mathbf{Pp}$  as well as for  $\mathbf{Np}$  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  $F_1, \dots, F_k$  at least one of  $A, B$  must be a member of  $\Gamma$ . So  $\Gamma$  is  $\mathbf{sf}(E)$ -saturated.

*Remark.* Lemma 3.3 holds constructively because the relation  $\{C_1, \dots, C_j\} \vdash_{\mathbf{Pp}} D$  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  $\Gamma_0$  be an  $\mathbf{sf}(E)$ -saturated subset of  $\mathbf{sf}(E)$  given by Lemma 3.3(a). Let  $\Gamma_1, \dots, \Gamma_m$  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  $\langle i_1, \dots, i_n \rangle$  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  $\Gamma_0$ , and each node  $u = \langle i_1, \dots, i_n \rangle$  above  $\langle \rangle$  represents an increasing sequence  $\langle \Gamma_{i_1}, \dots, \Gamma_{i_n} \rangle$  of  $\mathbf{sf}(E)$ -saturated supersets of  $\Gamma_0$ , with every possible such sequence included. We say that  $\Gamma_0$  is *attached to* the root  $\langle \rangle$ , and  $\Gamma_{i_n}$  is *attached to* the node  $\langle i_1, \dots, i_n \rangle$  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  $\langle i_1, \dots, i_n \rangle \in K$ :

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

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  $u = \langle i_1, \dots, i_n \rangle$  of  $\mathbf{K}$ , representing the increasing sequence  $\langle \Gamma_{i_0}, \Gamma_{i_1}, \dots, \Gamma_{i_n} \rangle$  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  $(A \rightarrow B)$  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 $\mathbf{Pp}$

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

- (a)  $P \vee \neg P$ .
- (b)  $\neg P \vee \neg \neg P$ .
- (c)  $\neg \neg P \rightarrow P$ .
- (d)  $(P \rightarrow Q) \rightarrow (\neg P \vee Q)$ .
- (e)  $\neg(P \& \neg Q) \rightarrow (P \rightarrow Q)$ .
- (f)  $\neg(P \& Q) \rightarrow (\neg P \vee \neg Q)$ .
- (g)  $(\neg P \rightarrow \neg Q) \rightarrow (Q \rightarrow P)$ .
- (h)  $(P \rightarrow Q \vee R) \rightarrow (P \rightarrow Q) \vee (P \rightarrow R)$ .
- (i)  $(\neg P \rightarrow Q \vee R) \rightarrow (\neg P \rightarrow Q) \vee (\neg P \rightarrow R)$ .
- (j)  $((P \rightarrow Q) \rightarrow P) \rightarrow P$  (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  $\mathcal{K}_4 = ((\mathbf{K}_4, \leq), \kappa_4)$  where  $\mathbf{K}_4 = \mathbf{K}_3 = \{\langle \rangle, \langle 0 \rangle, \langle 1 \rangle\}$  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  $\mathbf{Pp}$ , 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  $\mathbf{Pp}$ )* 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  $\Delta_0, \dots, \Delta_m$  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  $\mathcal{H}^j \subseteq \{\Delta_0, \dots, \Delta_m\}$  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  $\mathbf{H}^j$  whose root  $\langle \rangle$  represents  $\Delta_j$ , where  $\langle i_1, \dots, i_n \rangle \in \mathbf{H}^j$  if and only if  $\Delta_{i_1}, \dots, \Delta_{i_n} \in \mathcal{H}^j$  and  $\Delta_j \subsetneq \Delta_{i_1} \subsetneq \dots \subsetneq \Delta_{i_n}$ . Let  $\mathbf{H}_1^j, \mathbf{H}_2^j, \dots, \mathbf{H}_{k_j}^j$  be all the trees of this kind, with root representing  $\Delta_j$ . Define  $\kappa^j(\langle \rangle) = \Delta_j \cap \mathbf{psf}(E)$  and for  $n > 0$  define  $\kappa^j(\langle i_1, \dots, i_n \rangle) = \Delta_{i_n} \cap \mathbf{psf}(E)$ . Then for each  $1 \leq j \leq m$ , for each  $1 \leq l \leq k_j$ , the structure  $\mathcal{H}_l^j = ((\mathbf{H}_l^j, \leq), \kappa^j)$  is a propositional Kripke model over  $\mathbf{psf}(E)$ . By the proof of Theorem 3.4, if  $\not\vdash_{\mathbf{Pp}} E$  then some  $\mathcal{H}_l^j$  is a countermodel to  $E$ .

To check whether a given  $\mathbf{H}_l^j$  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  $\mathbf{H}_l^j$  to check. If some  $\mathbf{H}_l^j$  is a countermodel to  $E$ , then  $\not\vdash_{\mathbf{Pp}} E$  by Theorem 3.2. Otherwise,  $\vdash_{\mathbf{Pp}} E$ , and a proof of  $E$  can be found by recursively enumerating all the proofs in  $\mathbf{Pp}$ .

*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  $\not\vdash_{\mathbf{Pp}} A$  and  $\not\vdash_{\mathbf{Pp}} B$  then  $\not\vdash_{\mathbf{Pp}} (A \vee B)$ . Theorem 3.6 (which is constructive except for the use of Markov's Principle) then justifies (a).

Assume  $\not\vdash_{\mathbf{Pp}} A$  and  $\not\vdash_{\mathbf{Pp}} B$ . By Theorem 3.4, there are propositional Kripke countermodels  $\mathcal{K}_1 = ((K_1, \leq), \kappa_1)$  to  $A$  and  $\mathcal{K}_2 = ((K_2, \leq), \kappa_2)$  to  $B$ . Construct a new model  $\mathcal{K} = ((K, \leq), \kappa)$  as follows. The elements of  $K$  will be  $\langle \rangle$  and all sequences of the forms  $\langle 1 \rangle * u$  where  $u \in K_1$ , and  $\langle 2 \rangle * u$  where  $u \in K_2$ .  $\kappa(\langle \rangle)$  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  $R_1, \dots, R_s$  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  $R_1, \dots, R_s$  is an  $(s + 3)$ -tuple

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

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,  $\delta$  is a function with domain  $K$  such that

- (i) for each  $u \in K$  there is at least one  $d \in \delta(u)$ , and
- (ii) if  $u, v \in K$  with  $u \leq v$  then  $\delta(u) \subseteq \delta(v) \subseteq D$ ,

and for each  $1 \leq i \leq s$ :  $\chi_i$  is an  $(n_i + 1)$ -ary function from  $K \times D^{n_i}$  to  $\{0, 1\}$  such that for  $u, v \in K$  and all  $x_1, \dots, x_{n_i} \in D$ :

- (iii) if  $\chi_i(u, x_1, \dots, x_{n_i}) = 1$  then  $x_1, \dots, x_{n_i} \in \delta(u)$ , and
- (iv) if  $u \leq v$  and  $\chi_i(u, x_1, \dots, x_{n_i}) = 1$  then  $\chi_i(v, x_1, \dots, x_{n_i}) = 1$ .

*Remarks.* There are good reasons for using characteristic functions  $\chi_i$  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  $\chi_i(u, x_1, \dots, x_{n_i}) = 0$  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  $\mathcal{K} = ((K, \leq), D, \delta, \chi_1, \dots, \chi_s)$  is a Kripke model over  $R_1, \dots, R_s$ , then every function  $\phi$  from  $\{a_1, a_2, \dots\}$  to  $D$  is a possible *assignment of values in  $D$*  to the distinct individual variables  $a_1, a_2, \dots$  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  $R_1, \dots, R_s$  (but with all the individual variables  $a_1, a_2, \dots$ ). For each formula  $E$  in  $\mathcal{L}'(\mathbf{Pd})$  and each  $u \in K$ , we define  $u \Vdash_\phi E$  by induction on the logical form of  $E$ .

1. If  $E$  is prime,  $E$  is  $R_i(y_1, \dots, y_{n_i})$  for some  $1 \leq i \leq s$ , where  $y_1, \dots, y_{n_i}$  are (not necessarily distinct) individual variables. Then  $u \Vdash_\phi R_i(y_1, \dots, y_{n_i})$  if (and only if)  $\chi_i(u, \phi(y_1), \dots, \phi(y_{n_i})) = 1$ .
2.  $u \Vdash_\phi (A \& B)$  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.  $u \Vdash_\phi (A \rightarrow B)$  if  $\phi(y) \in \delta(u)$  for every variable  $y$  free in  $(A \rightarrow B)$ , and for each  $v \in \mathbf{K}$  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  $v \in \mathbf{K}$  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  $v \in \mathbf{K}$  with  $u \leq v$  and every assignment  $\psi$  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  $\psi$  to the individual variables which agrees with  $\phi$  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  $\phi$  and  $\psi$  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  $\mathcal{K} = ((\mathbf{K}, \leq), \mathbf{D}, \delta, \chi_1, \dots, \chi_s)$  is a Kripke model over  $R_1, \dots, R_s$ , then for every formula  $E$  in the restricted language  $\mathcal{L}'(\mathbf{Pd})$  with only the predicate letters  $R_1, \dots, R_s$ , and every assignment  $\phi$  of elements of  $\mathbf{D}$  to the individual variables, for each  $u, v \in \mathbf{K}$ :

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

*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  $u, v \in \mathbf{K}$  with  $u \leq v$ , and  $u \Vdash_\phi \forall x A(x)$ . Suppose  $w \in \mathbf{K}$  and  $v \leq w$ , and let  $\psi$  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  $\mathbf{K}$  and  $u \Vdash_\phi \exists x A(x)$ , so there is an assignment  $\psi$  which agrees with  $\phi$  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  $R_1, \dots, R_s$  are distinct predicate letters including all those which occur in a formula  $E$  of  $\mathcal{L}(\mathbf{Pd})$ , and  $\mathcal{K} = ((\mathbf{K}, \leq), \mathbf{D}, \delta, \chi_1, \dots, \chi_s)$  over  $R_1, \dots, R_s$  is a Kripke model over  $R_1, \dots, R_s$ , then  $E$  is *valid in  $\mathcal{K}$*  (written  $\mathcal{K} \Vdash E$ ) if  $\langle \rangle \Vdash_\phi E$  for every assignment  $\phi$  of elements of  $\mathbf{D}$  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  $R_1, \dots, R_s$  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  $F_1, \dots, F_m$  in which no predicate letters but  $R_1, \dots, R_s$  may occur, then the universal closure  $\forall E$  of  $E$  is valid in every Kripke model  $\mathcal{K}$  over  $R_1, \dots, R_s$ . 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  $F_1, \dots, F_m$ , where  $F_m$  is  $E$ . Let  $\mathcal{K}$  be a Kripke model over a list  $R_1, \dots, R_s$  of distinct predicate letters including all those occurring in  $F_1, \dots, F_m$ . We must show that  $\langle \rangle \Vdash_\phi \forall E$  for every assignment  $\phi$  of elements of  $\mathbf{D}$  to the individual variables, or equivalently that  $u \Vdash_\phi E$  for every  $u \in \mathbf{K}$  and every assignment  $\phi$  such that

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

If  $m = 1$  then  $E$  is an axiom of  $\mathbf{Pd}$ . The arguments for X1 - X10 are as for  $\mathbf{Pp}$ . If  $E$  is an axiom by X11 then  $E$  is  $\forall x A(x) \rightarrow A(y)$  where  $y$  is a variable free for  $x$  in  $A(x)$ . Suppose  $u \in \mathbf{K}$ , and  $\phi$  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  $A(y) \rightarrow \exists x A(x)$  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  $u \in K$  and  $\phi$  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  $\psi$  agree with  $\phi$  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  $(F_j \rightarrow E)$ , then  $\forall F_i$  and  $\forall F_j$  are valid in  $\mathcal{K}$  by the induction hypothesis. If  $u \in K$  and  $\phi$  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  $C \rightarrow A(x)$  where  $x$  is not free in  $C$ ,  $\forall F_i$  is valid in  $\mathcal{K}$  by the induction hypothesis, and  $E$  is  $C \rightarrow \forall x A(x)$ . Suppose  $u \in K$  and  $\phi$  is an assignment of elements of  $D$  to the variables satisfying  $(\star)$ , and suppose  $u \Vdash_\phi C$ . Then for every  $v \in K$  with  $u \leq v$ , and every  $\psi$  which agrees with  $\phi$  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  $A(x) \rightarrow C$  where  $x$  is not free in  $C$ ,  $\forall F_j$  is valid in  $\mathcal{K}$ , and  $E$  is  $\exists x A(x) \rightarrow C$ . If  $u \in K$  and  $\phi$  satisfies  $(\star)$  and  $u \Vdash_\phi \exists x A(x)$ , then for some assignment  $\psi$  which agrees with  $\phi$  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  $\mathcal{K}_1 = ((K_1, \leq), D, \delta, \chi_1, \chi_2)$  to  $(P_1 \rightarrow \exists x P_2(x)) \rightarrow \exists x (P_1 \rightarrow P_2(x))$ , 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  $K_1 = \{\langle \rangle, \langle 0 \rangle\}$  and the domain of individuals is  $D = \{d_0, d_1\}$ , 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  $\chi_1, \chi_2$  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  $\phi$  to the variables:  $\langle \rangle \Vdash_\phi (P_1 \rightarrow \exists x P_2(x))$  since  $\langle \rangle \not\Vdash_\phi P_1$  and  $\langle 0 \rangle \Vdash_\phi \exists x P_2(x)$ , but  $\langle \rangle \not\Vdash_\phi \exists x (P_1 \rightarrow P_2(x))$  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  $\mathcal{K}_1 \not\Vdash (P_1 \rightarrow \exists x P_2(x)) \rightarrow \exists x (P_1 \rightarrow P_2(x))$ .

*Example.* Here is a Kripke countermodel to  $\forall x \neg \neg P_1(x) \rightarrow \neg \neg \forall x P_1(x)$ , showing that this formula is unprovable in **Pd**. Let  $D = \{d_0, d_1, d_2, \dots\}$  and let  $K$  be the tree consisting of all finite sequences of 0s (so  $K = \{\langle \rangle, \langle 0 \rangle, \langle 0, 0 \rangle, \dots\}$ ). If  $u$  is a sequence of 0s of length  $n$ , define  $\delta(u) = \{d_0, \dots, d_n\}$  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  $u \in K$  there is exactly one  $d_i \in \delta(u)$  for which  $\chi_1(u, d_i) = 0$ , and
- (d) for each  $d_i \in D$  there is some  $u \in K$  such that  $\chi_1(u, d_i) = 1$ .

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

*Exercise 3.10.* Show that the converse of Theorem 2.10(g) is unprovable in **Pd** by constructing a Kripke countermodel to  $(\forall x P_1(x) \rightarrow P_2) \rightarrow \exists x (P_1(x) \rightarrow P_2)$ , 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  $\mathcal{K} = ((K, \leq), D, \delta, \chi_1, \dots, \chi_s)$  over  $R_1, \dots, R_s$  has *constant domain*  $D$  if  $\delta(u) = D$  for every  $u \in K$ . In this case, we may write  $\mathcal{K} = ((K, \leq), D, \chi_1, \dots, \chi_s)$  and the definition of  $\Vdash_\phi$  can be simplified accordingly.

*Exercise 3.11.* Show that  $\forall x(A(x) \vee B) \rightarrow \forall xA(x) \vee B$  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  $\forall x(P_1(x) \vee P_2) \rightarrow \forall xP_1(x) \vee P_2$ , 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  $\not\Vdash_{\mathbf{Pd}} \forall x(P_1(x) \vee P_2) \rightarrow \forall xP_1(x) \vee P_2$ . 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  $\mathcal{K} = ((K, \leq), D, \delta, \chi_1, \dots, \chi_s)$  is a Kripke model over  $R_1, \dots, R_s$  and  $u \in K$ , then  $\mathcal{K}^u = ((K^u, \leq^u), D, \delta^u, \chi_1^u, \dots, \chi_s^u)$  is the *submodel of  $\mathcal{K}$*  defined as follows:

- (i)<sup>u</sup> for each finite sequence  $v$  of natural numbers,  $v \in K^u$  if and only if  $u * v \in K$ ,
- (ii)<sup>u</sup> if  $v, w \in K^u$ , then  $v \leq^u w$  if and only if  $u * v \leq u * w$  in  $K$ ,
- (iii)<sup>u</sup> if  $v \in K^u$  then  $\delta^u(v) = \delta(u * v)$ , and
- (iv)<sup>u</sup> if  $v \in K^u$  then for each  $1 \leq i \leq s$  and all  $x_1, \dots, x_{n_i} \in D$ :

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

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

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

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

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

for every assignment  $\phi$  to  $a_1, a_2, \dots$ , every  $u \in K$  and every formula  $E(y_1, \dots, y_k)$  (with exactly the distinct variables  $y_1, \dots, y_k$  free) of the language  $\mathcal{L}'(\mathbf{Pd})$  restricted to  $R_1, \dots, R_s$ , 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  $\forall xA(x)$  by  $\forall x(P(x) \rightarrow A(x))$ , and every subformula of  $E$  of the form  $\exists yB(y)$  by  $\exists y(P(y) \ \& \ B(y))$ ).

*Theorem 3.12. (de Jongh’s Observation)* A closed formula  $E$  is Kripke-valid if and only if  $\exists xP(x) \rightarrow E^P$  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  $\exists xP(x) \rightarrow E^P$  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  $\phi$  to the individual variables,  $\langle \rangle \Vdash_\phi^+ (\exists xP(x) \rightarrow E^P)$  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  $\mathcal{K} = ((\mathbf{K}, \leq), \mathbf{D}, \chi_1, \dots, \chi_s, \chi_{s+1})$  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  $\chi_{s+1}$ . Suppose  $u \in \mathbf{K}$  and  $\phi$  is an assignment to the individual variables such that  $u \Vdash_{\phi} \exists x P(x)$  in  $\mathcal{K}$ . For each  $v \in \mathbf{K}$  define  $\delta(v) = \{d \in \mathbf{D} \mid \chi_{s+1}(v, d) = 1\}$ . Then  $\mathcal{K}^- = ((\mathbf{K}, \leq), \mathbf{D}, \delta, \chi_1, \dots, \chi_s)$  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  $V = \{a_1, a_2, \dots\}$  of individual variables of  $\mathcal{L}(\mathbf{Pd})$ . Let  $R_1, \dots, R_s$  be any distinct predicate letters of  $\mathcal{L}(\mathbf{Pd})$ , where  $R_i$  is  $n_i$ -ary ( $1 \leq i \leq s$ ). Then  $\mathcal{L}(V_0, \{R_1, \dots, R_s\})$  is the *sublanguage* of  $\mathcal{L}(\mathbf{Pd})$  consisting of all formulas involving only variables from  $V_0$  and relation symbols from  $\{R_1, \dots, R_s\}$ .

*Definition.* Let  $V_0 \subseteq W \subseteq V_1$  be inhabited subsets of  $V$ . Let  $R_1, \dots, R_s$  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  $\mathcal{L}'(V_j) = \mathcal{L}(V_j, \{R_1, \dots, R_s\})$ . Then a collection  $\Gamma$  of formulas of  $\mathcal{L}'(V_1)$  is  *$\mathcal{L}'(V_0)$ -saturated with witnesses in  $W$*  if

- (i)  $\Gamma$  is consistent.
- (ii) If  $A \vee B$  is a formula of  $\mathcal{L}'(V_0)$  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  $\mathcal{L}'(V_0)$  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  $\mathcal{L}'(V_1)$  congruent to  $A(x)$  and some  $y \in W$  which is free for  $x$  in  $A'(x)$ .

If  $V_0 = W = V_1$ , so  $\Gamma$  is a collection of formulas of  $\mathcal{L}'(V_1)$  which is  $\mathcal{L}'(V_1)$ -saturated with witnesses in  $V_1$ , we say  $\Gamma$  is  *$\mathcal{L}'(V_1)$ -saturated*.

*Convention.* For the rest of this section, “ $\Gamma \vdash E$ ” abbreviates “ $\Gamma \vdash_{\mathbf{Pd}} E$  with all variables free in  $\Gamma$  held constant,” and “ $\Gamma \not\vdash E$ ” abbreviates “there is no derivation of  $E$  from  $\Gamma$  in  $\mathbf{Pd}$  with all variables held constant.”

*Exercise 3.13.* Show that if  $\Gamma$  is an  $\mathcal{L}'(V_0)$ -saturated collection of formulas of  $\mathcal{L}'(V_1)$  with witnesses in  $W$  (where  $V_0 \subseteq W \subseteq V_1$ ), and if  $E$  is a formula of  $\mathcal{L}'(V_0)$  which has a congruent  $E'$  in  $\mathcal{L}'(V_1)$  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  $\Gamma$  is an  $\mathcal{L}'(V_1)$ -saturated collection of formulas of  $\mathcal{L}'(V_1)$ , then for all formulas  $E, E'$  of  $\mathcal{L}'(V_1)$ :

- (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  $R_1, \dots, R_s$  be distinct predicate letters of  $\mathcal{L}(\mathbf{Pd})$ , where  $R_i$  is  $n_i$ -ary. Let  $V_0 \subset V_1 \subseteq V$  where  $V_0$  is inhabited and  $V_1 - V_0$  is countably infinite, let  $\mathcal{L}'(V_j) = \mathcal{L}(V_j, \{R_1, \dots, R_s\})$  for  $j = 0, 1$ , and suppose  $C$  is a formula of  $\mathcal{L}'(V_0)$  and  $\Delta$  a collection of formulas of  $\mathcal{L}'(V_0)$  such that  $\Delta \not\vdash C$ . Then

- (a) There is a  $\Gamma \subseteq \mathcal{L}'(V_1)$  which is  $\mathcal{L}'(V_0)$ -saturated with witnesses in  $V_1$ , such that  $\Delta \subseteq \Gamma$  and  $\Gamma \not\vdash C$ .
- (b) There is a  $\Gamma^* \subseteq \mathcal{L}'(V_1)$  which is  $\mathcal{L}'(V_1)$ -saturated, such that  $\Delta \subseteq \Gamma^*$  and  $\Gamma^* \not\vdash C$ .

*Proof of (a).* Let  $F_1, F_2, F_3, \dots$  be an enumeration of the formulas of  $\mathcal{L}'(V_0)$  without repetition. Define an increasing sequence  $\{\Gamma_i\}$  of consistent subsets of  $\mathcal{L}'(V_1)$  as follows. Let  $\Gamma_0 = \Delta$ , so  $\Gamma_0 \not\vdash C$  by assumption. If  $i \geq 0$  and  $\Gamma_i \subseteq \mathcal{L}'(V_1)$  has already been defined such that  $\Gamma_i \not\vdash C$ , consider  $F_{i+1}$  and define  $\Gamma_{i+1}$  by cases:

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

*Case 2.*  $\Gamma_i \cup \{F_{i+1}\} \not\vdash C$ , and  $F_{i+1}$  is of the form  $\exists xA(x)$ . 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  $\Gamma_i \cup \{F_{i+1}\} \vdash A(y) \rightarrow C$  by the Deduction Theorem for  $\mathbf{Pd}$ , so  $\Gamma_i \cup \{F_{i+1}\} \vdash \exists yA(y) \rightarrow C$  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  $\Gamma_{i+1} \not\vdash C$ .

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

Finally, let  $\Gamma = \bigcup_{i \geq 0} \Gamma_i$ . Observe that  $\Gamma \not\vdash C$  and  $\Delta \subseteq \Gamma \subseteq \mathcal{L}'(V_1)$  by construction. We need to prove that  $\Gamma$  satisfies (ii) and (iii) of the definition of  $\mathcal{L}'(V_0)$ -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  $\mathcal{L}'(V_0)$ , say  $A$  is  $F_{j+1}$  and  $B$  is  $F_{k+1}$ . If  $\Gamma_j \cup \{A\} \not\vdash C$  then  $A \in \Gamma$  by construction. If  $\Gamma_k \cup \{B\} \not\vdash C$  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  $\Gamma$ .

For (iii), suppose  $F_{i+1}$  is  $\exists xA(x)$  where  $\Gamma \vdash \exists xA(x)$ . Then  $\Gamma \cup \{\exists xA(x)\} \not\vdash C$ , so  $\Gamma_i \cup \{F_{i+1}\} \not\vdash C$ , so  $A(y) \in \Gamma$  for some  $y \in V_1$  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  $\{V_j^*\}$  so that  $V_0 = V_0^*$ ,  $V_1 = \bigcup_{j \in \omega} V_j^*$  and for  $j = 0, 1, 2, \dots$ :  $V_j^* \subseteq V_{j+1}^*$  and  $V_{j+1}^* - V_j^*$  is infinite. Using (a), define by induction on  $j$  an increasing sequence  $\{\Gamma_j^*\}$  of subsets of  $\mathcal{L}'(V_1)$  such that  $\Delta \subseteq \Gamma_0^*$  and for each  $j = 0, 1, \dots$ :  $\Gamma_j^*$  is a subset of  $\mathcal{L}'(V_{j+1}^*)$  which is  $\mathcal{L}'(V_j^*)$ -saturated with witnesses in  $V_{j+1}^*$ , and  $\Gamma_j^* \not\vdash C$ . Let  $\Gamma^* = \bigcup_{j \geq 0} \Gamma_j^*$ . Then  $\Delta \subseteq \Gamma^*$  by construction,  $\Gamma^* \not\vdash C$ , and  $\Gamma^*$  is  $\mathcal{L}'(V_1)$ -saturated because  $V_1 = \bigcup_{j \geq 0} V_{j+1}^*$  and  $\Gamma_0^* \subseteq \Gamma_1^* \subseteq \dots \subseteq \Gamma^* \subseteq \mathcal{L}'(V_1) = \bigcup_{j \geq 0} \mathcal{L}'(V_j^*)$ .

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

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

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

*Theorem 3.15. (Completeness for Pd)* Suppose  $E$  is a formula of  $\mathcal{L}(V, \{R_1, \dots, R_s\})$  such that  $\not\vdash_{\mathbf{Pd}} E$ . Then there is a Kripke model  $\mathcal{K} = ((K, \leq), V, \delta, \chi_1, \dots, \chi_s)$  over  $R_1, \dots, R_s$ , with domain  $V$ , such that  $\langle \rangle \not\vdash_\phi E$  where  $\phi(y) = y$  for every  $y \in V$ , and  $\phi(x) \in \delta(\langle \rangle)$  for every  $x$  free in  $E$ .

*Proof.* Define an increasing sequence  $V_0 \subseteq V_1 \subseteq \dots$  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  $V = \bigcup_{j \geq 0} V_j$ . For each  $j \geq 0$  let  $F_1^j, F_2^j, \dots$  be an enumeration without repetitions of all the formulas of  $\mathcal{L}'(V_j) = \mathcal{L}(V_j, \{R_1, \dots, R_s\})$ . Since  $\not\vdash E$ , by (b) of the Saturation Lemma there is an  $\mathcal{L}'(V_0)$ -saturated  $\Gamma_0 \subseteq \mathcal{L}'(V_0)$  such that  $\Gamma_0 \not\vdash E$ .

$(K, \leq)$  is defined inductively, with nodes  $u = \langle n_1, \dots, n_k \rangle$  representing chains  $\Gamma_0 \subseteq \dots \subseteq \Gamma_k$  where each  $\Gamma_j$  is an  $\mathcal{L}'(V_j)$ -saturated collection of formulas of  $\mathcal{L}'(V_j)$ , and we say  $\Gamma_k$  is *attached to* the node  $u$ . First attach  $\Gamma_0$  to the root  $\langle \rangle$  of  $K$ . For each node  $u$  of length  $k$  with  $\Gamma_k$  attached, enumerate all the finite sequences  $F_{i_1}^{k+1}, \dots, F_{i_r}^{k+1}, F_{i_{r+1}}^{k+1}$  of formulas of  $\mathcal{L}'(V_{k+1})$  such that  $r \geq 1$  and  $\{F_{i_1}^{k+1}, \dots, F_{i_r}^{k+1}\} \cap \Gamma_k = \emptyset$  and  $\Gamma_k \cup \{F_{i_1}^{k+1}, \dots, F_{i_r}^{k+1}\} \not\vdash F_{i_{r+1}}^{k+1}$ . For each  $m$ : If  $F_{i_1}^{k+1}, \dots, F_{i_r}^{k+1}, F_{i_{r+1}}^{k+1}$  is the  $m^{\text{th}}$  such sequence, by (b) of the Saturation Lemma there is an  $\mathcal{L}'(V_{k+1})$ -saturated  $\Gamma_{k+1}$  such that  $\Gamma_k \cup \{F_{i_1}^{k+1}, \dots, F_{i_r}^{k+1}\} \subseteq \Gamma_{k+1}$  and  $\Gamma_{k+1} \not\vdash F_{i_{r+1}}^{k+1}$ . Attach this  $\Gamma_{k+1}$  to  $u * \langle m \rangle$ .

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



Suppose  $\phi$  is an assignment to the variables which maps  $V_k$  into  $V_k$  and  $C(x_1, \dots, x_m)$  is a formula of  $\mathcal{L}'(V_k)$  with only the distinct variables  $x_1, \dots, x_m$  free. We call  $\phi$  *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  $\mathbf{K}$  with  $\Gamma_k$  attached,  $\phi(y) \in V_k$  for every  $y \in V_k$ , and  $\phi(x_i) = z_i$  for  $1 \leq i \leq m$ . Then for every formula  $C(x_1, \dots, x_m)$  of  $\mathcal{L}'(V_k)$  in which  $\phi$  is free and only the distinct variables  $x_1, \dots, x_m$  occur free:

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

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  $C(x_1, \dots, x_m)$ , and let  $u$  be a node of length  $k$  with  $\Gamma_k$  attached and  $\phi$  be an assignment free in  $C$  such that  $\phi(y) \in V_k$  for all  $y \in V_k$ , 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  $z, x \in V_k$  and  $\phi$  is an assignment, then  $\phi[z/x]$  is a standard abbreviation for the assignment  $\psi$  such that  $\psi(x) = z$  and  $\psi(y) = \phi(y)$  for all  $y \neq x$ .

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

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

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

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

By the claim,  $\langle \rangle \not\vdash_{\phi} E$  if  $\phi(x) = x$  for every  $x \in V$ , since  $E \notin \Gamma_0$  by construction. So the Kripke semantics is complete for  $\mathbf{Pd}$ .

*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  $A \rightarrow B$ .

Note the nonconstructive steps in the proof of the Soundness Theorem for  $\mathbf{Pd}$ . 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  $\mathbf{Pd}$  of  $E$ . Hence by Markov's Principle, if  $\Vdash E$  then  $\vdash_{\mathbf{Pd}} E$ .

### 3.6 Applications of Kripke Semantics for $\mathbf{Pd}$

*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  $\mathbf{Pd}$ :

- (a)  $\neg\neg\forall x(\neg P(x) \vee \neg\neg P(x))$ .
- (b)  $\forall x(\neg\neg P(x) \rightarrow P(x))$ .
- (c)  $\forall x(\neg\neg P(x) \rightarrow P(x)) \rightarrow \forall x(P(x) \vee \neg P(x))$ .
- (d)  $\forall x\neg\neg P(x) \rightarrow \neg\neg\forall x P(x)$ .
- (e)  $\neg\neg\exists x P(x) \rightarrow \exists x\neg\neg P(x)$ .
- (f)  $\forall x(P(x) \vee \neg P(x)) \ \& \ \neg\forall x\neg P(x) \rightarrow \exists x P(x)$ .
- (g)  $\forall x(Q(x) \vee R) \rightarrow (\forall x Q(x) \vee R)$ .
- (h)  $(\forall x Q(x) \rightarrow R) \rightarrow \exists x(Q(x) \rightarrow R)$ .
- (i)  $(R \rightarrow \exists x Q(x)) \rightarrow \exists x(R \rightarrow Q(x))$ .
- (j)  $(\neg R \rightarrow \exists x Q(x)) \rightarrow \exists x(\neg R \rightarrow Q(x))$ .

*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  $\mathcal{K}_5 = ((\mathbf{K}_5, \leq), \{d_0\}, \chi)$  where  $\mathbf{K}_5 = \mathbf{K}_1 = \{\langle \rangle, \langle 0 \rangle\}$ , 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  $\mathbf{Pp}$ , intuitionistic predicate logic  $\mathbf{Pd}$  is not (recursively) decidable, so we have no analogue of Theorem 3.6. The completeness of Kripke semantics for  $\mathbf{Pd}$  does give classical proofs of some interesting admissible rules of  $\mathbf{Pd}$ , 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  $\mathcal{L}'(\mathbf{V}) = \mathcal{L}(\mathbf{V}, \{R_1, \dots, R_s\})$  and  $\mathcal{K}$  is a Kripke model over  $R_1, \dots, R_s$  with domain  $\mathbf{D}$  such that  $\langle \rangle \Vdash_\phi B$  for some assignment  $\phi$  of elements of  $\mathbf{D}$  to  $\mathbf{V}$ , then  $\langle \rangle \Vdash_\psi B$  for every assignment  $\psi$  of elements of  $\mathbf{D}$  to  $\mathbf{V}$ , so  $\mathcal{K} \Vdash B$ .

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

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

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

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

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

*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  $\mathbf{Pd}$ , two of which do not hold for classical predicate logic  $\mathbf{cPd}$ . None of these rules is derivable in  $\mathbf{Pd}$ .

*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  $\mathbf{Pd}$ ).

*Proof* of (b). Assume  $\vdash_{\mathbf{Pd}} \exists x A(x)$ , so by soundness  $\Vdash \exists x A(x)$ , and suppose  $\not\vdash_{\mathbf{Pd}} A(x)$ . Then by completeness there is a Kripke model  $\mathcal{K} = ((\mathbf{K}, \leq), \mathbf{D}, \delta, \chi_1, \dots, \chi_s)$  over  $R_1, \dots, R_s$  and an assignment  $\phi$  of elements of  $\mathbf{D}$  to the individual variables such that  $\phi(x) \in \delta(\langle \rangle)$  and  $\langle \rangle \not\vdash_{\phi} A(x)$ . Without loss of generality, suppose  $\phi(x) = d_0$ . Apply Lemma 3.17(c) with  $m = 1$  to get a new model  $\mathcal{K}' = ((\mathbf{K}', \leq), \mathbf{D}, \delta', \chi'_1, \dots, \chi'_s)$  such that  $\delta'(\langle \rangle) = \{d_0\}$  and  $\mathcal{K} = \mathcal{K}'^{(1)}$  (see the definition of submodel in section 3.4). Let  $\Vdash'$  be the forcing relation on  $\mathcal{K}'$ .

By Lemma 3.10,  $\langle 1 \rangle \Vdash'_{\phi} A(x)$ , so by monotonicity  $\langle \rangle \Vdash'_{\phi} A(x)$ . 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  $\mathcal{K}_0 = ((\{\langle \rangle\}, \leq), \mathbf{D}, \chi_1, \dots, \chi_s)$  where  $\mathbf{D} = \{d_0\}$ . The only assignment of elements of  $\mathbf{D}$  to the individual variables is the constant function  $\phi$  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  $\not\vdash_{\mathbf{Pd}} \exists x \neg A(x)$ , 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 rules of  $\mathbf{Pd}$  is complete  $\Pi_2^0$ , so no simple syntactical characterization is possible. Is there any reasonable syntactical characterization of this class? The question is apparently still 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 $\mathbf{Pd}[=]$

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  $\mathbf{Pd}[=]$  are all formulas of  $\mathcal{L}(\mathbf{Pd}[=])$  of the forms X1-X12 (the axiom schemas of  $\mathbf{Pd}$ ), XE1 and XE2 (asserting that equality is an equivalence relation), and XE3 (allowing the substitution of equals for equals in prime formulas not involving  $=$ ). In XE1 and XE2,  $x, y$  and  $z$  are distinct variables. For XE3,  $P(z)$  may be any prime formula of  $\mathcal{L}(\mathbf{Pd})$ ,  $x$  and  $y$  are distinct variables free for

$z$  in  $P(z)$ , and  $P(x)$ ,  $P(y)$  are the results of substituting  $x$  and  $y$  respectively for all free occurrences of  $z$  in  $P(z)$ .

XE1.  $x = x$ .

XE2.  $x = y \rightarrow (x = z \rightarrow y = z)$ .

XE3.  $x = y \rightarrow (P(x) \rightarrow P(y))$ .

The rules of inference of  $\mathbf{Pd}[=]$  are R1-R3 extended to  $\mathcal{L}(\mathbf{Pd}[=])$ . A *deduction* (or *derivation*) in  $\mathbf{Pd}[=]$  of a formula  $E$  from a collection  $\Gamma$  of formulas is a finite sequence of formulas, each of which is an axiom by X1-X12 or XE1-XE3, or a member of  $\Gamma$ , 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  $\mathbf{Pd}$ , and a *proof* is a deduction from no assumptions.

*Remarks.* Alternatively, we could have replaced  $P(z)$  in XE3 by an arbitrary formula  $A(z)$  of  $\mathcal{L}(\mathbf{Pd}[=])$ , and omitted XE2 (which would then be provable). We choose this axiomatization because it separates the axioms XE1-2 (from which it is easy to prove that  $=$  is an equivalence relation) from the schema XE3 comprising the *equality axioms* (such as  $x = y \rightarrow (R_i(w, x) \rightarrow R_i(w, y))$  and  $x = y \rightarrow (R_i(x, w) \rightarrow R_i(y, w))$ ) for the other predicate symbols of the language. We follow Kleene [1952] in choosing open equality axioms, from which their universal closures can easily be proved. However, we treat XE1-3 as axiom schemas rather than particular axioms.

*Lemma 4.1.* The Deduction Theorem holds for  $\mathbf{Pd}[=]$ .

*Proof.* Exactly as for  $\mathbf{Pd}$ , with the new axioms XE1-3 treated using X1 and R1 as usual.

*Lemma 4.2.*  $\mathbf{Pd}[=]$  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)  $\vdash_{\mathbf{Pd}[=]} \forall x \forall y (x = y \rightarrow y = x)$ .
- (c)  $\vdash_{\mathbf{Pd}[=]} \forall x \forall y \forall z (x = y \ \& \ y = z \rightarrow x = z)$ .

*Theorem 4.3. (The Replacement Property of Equality)* For every formula  $A(z)$  of  $\mathcal{L}(\mathbf{Pd}[=])$  and any distinct variables  $x, y$  which are free for  $z$  in  $A(z)$ :

$$\vdash_{\mathbf{Pd}[=]} \forall x \forall y (x = y \rightarrow (A(x) \leftrightarrow A(y))).$$

*Proof,* by induction on the logical form of  $A(z)$ . Lemma 4.1 is useful for the case that  $A(z)$  is  $s = z$  or  $z = s$  or  $z = z$ , where  $s$  is a term in which  $z$  does not occur free (i.e.  $s$  is a variable other than  $z$ ). XE3 takes care of the other prime formulas, and Theorem 4.3 helps with the inductive cases.

A natural deduction system  $\mathbf{NPd}[=]$  equivalent to  $\mathbf{Pd}[=]$  can be obtained by extending the rules of inference of  $\mathbf{NPd}$  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  $=$ :

$$= \text{I} \quad \cdot \quad x = x \qquad = \text{E} \quad \frac{\mathcal{D}_1 \quad \mathcal{D}_2}{\frac{A(s) \quad s = t}{A(t)}}$$

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  $\mathbf{NPd}[=]$ -deductions from  $\Gamma$  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  $\Gamma$*  of its last formula.

*Theorem 4.4.*  $\mathbf{NPd}[=]$  and  $\mathbf{Pd}[=]$  are equivalent in the sense that if  $E$  is a formula, and  $\Gamma$  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)  $\Gamma \vdash_{\mathbf{NPd}[=]} E$ .

*Corollary 4.5.* The Replacement Theorem holds for  $\mathbf{Pd}[=]$

## 4.2 Kripke Semantics for $\mathbf{Pd}[=]$

A *Kripke model*  $\mathcal{K}_= = ((K, \leq), D, \delta, \chi_1, \dots, \chi_s, \chi_=)$  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  $u \in K$ , 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 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 $\mathbf{HA}$

Heyting arithmetic  $\mathbf{HA}$  is related to Peano arithmetic  $\mathbf{PA}$  as  $\mathbf{Pd}$  is related to  $\mathbf{cPd}$ , that is,  $\mathbf{HA}$  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  $\mathbf{HA}$  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.

*Formulas* are built from prime formulas as for  $\mathcal{L}(\mathbf{Pd})$ , using  $\&$ ,  $\vee$ ,  $\rightarrow$ ,  $\neg$ ,  $\forall$  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  $\mathbf{HA}$  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.

$$\text{X13. } A(0) \ \& \ \forall x(A(x) \rightarrow A(x')) \rightarrow A(x).$$

$$\text{X14. } (a' = b') \rightarrow (a = b).$$

$$\text{X15. } \neg(a' = 0).$$

$$\text{X16. } (a = b) \rightarrow ((a = c) \rightarrow (b = c)).$$

$$\text{X17. } (a = b) \rightarrow (a' = b').$$

$$\text{X18. } (a + 0) = a.$$

$$\text{X19. } (a + b') = (a + b)'$$

$$\text{X20. } (a \cdot 0) = 0.$$

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

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  $\Gamma$  is a finite sequence  $F_1, \dots, F_n$  of formulas each of which is an axiom by one of the schemas X1-X13, or one of the particular arithmetical axioms X14-X21, 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  $\Gamma$  in  $\mathbf{HA}$* , and if  $\vdash_{\mathbf{HA}} E$  then  $E$  is a *theorem* (or *provable formula*) of  $\mathbf{HA}$ . 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  $\mathbf{Pd}$ , as does the proof of the Deduction Theorem.

Observe that the universal closures of X14-X21 are provable by the method of Exercise 2.13, and hence *every* formula obtained by replacing  $a, b, c$  in X14-X21 by (not necessarily distinct) individual variables  $x, y, z$  is provable. After proving Lemma 4.7 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.

*Important Remark.* This standard axiomatization follows Kleene [1952], even preserving Kleene's numbers for the arithmetical axioms (though not for the logical axioms and rules). Note that X18-X19 and X20-X21 are the primitive recursive definitions of  $+$  and  $\cdot$  respectively.

All other primitive recursive functions such as  $a^b$  can be defined from these, in the sense that one can find a formula  $A(a, b, c)$  of  $\mathcal{L}(\mathbf{HA})$  for which  $A(a, 0, 0')$  and  $A(a, b, c) \rightarrow A(a, b', (c \cdot a))$  and  $A(a, b, c) \rightarrow (A(a, b, d) \rightarrow (c = d))$  are provable in  $\mathbf{HA}$ . Thus it is possible to add a function symbol for exponentiation, and its primitive recursive definition, to  $\mathbf{HA}$  without increasing the class of provable formulas of the original language; such an extension of a theory is called an *inessential* or *conservative* extension. Kleene's precise formal development of the theory of partial and general recursive functions along these lines has never been improved on, and will be used rather than repeated here.

*Lemma 4.6.* The Deduction Theorem holds for  $\mathbf{HA}$ .

*Lemma 4.7.*  $\mathbf{HA}$  proves that  $=$  is an equivalence relation. If  $x, y, z$  are distinct variables, then

- (a)  $\vdash_{\mathbf{HA}} \forall x(x = x)$ .
- (b)  $\vdash_{\mathbf{HA}} \forall x \forall y(x = y \rightarrow y = x)$ .
- (c)  $\vdash_{\mathbf{HA}} \forall x \forall y \forall z(x = y \ \& \ y = z \rightarrow x = z)$ .

*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  $((x+0) = x) \rightarrow (((x+0) = x) \rightarrow (x = x))$  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  $(x = y) \rightarrow ((x = x) \rightarrow (y = x))$  is an instance of the schema corresponding to X16, and use (a). For (c), use (b) with X16.

*Lemma 4.8.* 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 4.7(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 4.7(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 4.7(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  $\exists z(y = z')$ .

## 4.4 Kripke Semantics for HA

Since **HA** is an applied predicate logic with equality in which prime formulas are decidable (by Lemma 4.8(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  $\gamma_1$  from  $D$  to  $D$ , and two binary functions  $\gamma_2, \gamma_3$  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  $\mathcal{K} = ((K, \leq), D, \delta, 0_{\mathcal{K}}, \gamma_1, \gamma_2, \gamma_3)$  is a *normal Kripke model for  $\mathcal{L}(\mathbf{HA})$*  if  $(K, \leq)$  is a tree,  $\delta$  is a monotone function from  $K$  into the class of all subsets of  $D$  such that  $D = \bigcup_{u \in K} \delta(u)$ , and  $0_{\mathcal{K}}, \gamma_1, \gamma_2, \gamma_3$  satisfy (i) - (iv). Each assignment  $\phi$  of values in  $D$  to the individual variables determines a *valuation function*  $\Phi$  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  $\phi$  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 - X21 at each node. The definition is justified by a soundness theorem, and completeness holds by the remarks in Section 4.2.

*Theorem 4.9. (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 4.10. (Completeness for HA)*. If  $E$  is a formula of  $\mathcal{L}(\mathbf{HA})$  such that  $\not\vdash_{\mathbf{HA}} E$ , then there is a normal Kripke model  $\mathcal{K}$  for **HA** such that  $\mathcal{K} \not\Vdash E$ .

The *numerals* of  $\mathcal{L}(\mathbf{HA})$  are the terms  $0, 0', 0'', \dots$  representing the natural numbers  $0, 1, 2, \dots$  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  $\omega_{\mathcal{K}}$ .

*Corollary 4.11.* 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  $\vdash_{\mathbf{HA}} \neg B \rightarrow \exists x A(x)$  then  $\vdash_{\mathbf{HA}} \exists x (\neg B \rightarrow A(x))$ .
- (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**.)

---

*End of the half-course.* I thank Cristofer Anagnostopoulos, Anastasia Fasouli, Konstantina Garoufi, Alexandra Sirokofsky, Nikos Theodorou, Giorgos Tsoதாக and Nick Vaporis for their participation and patience with the text-in-progress. Without them, these notes would not exist. I am greatly indebted to Garyfallia Vafeiadou and Giorgos Stavrinos for their continued interest in intuitionistic logic and mathematics. And I thank Costas Dimitracopoulos and MIIAA for giving me the chance to teach the subject I know best.

If any reader of these notes finds errors, please e-mail me: joan@math.ucla.edu. New sections will be added to the posted version as they are written.