Notes on the Foundations of Constructive Mathematics

by Joan Rand Moschovakis

October 13, 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 intutionist L. E. J. Brouwer, who believed that the Aristotelian law of excluded middle (A or not A) held only in situations where the decision between the disjuncts could be made effectively. While Brouwer disapproved of formal reasoning, his student A. Heyting developed intuitionistic logic and arithmetic as subtheories of the corresponding classical theories; for this reason, intuitionistic arithmetic is called "Heyting arithmetic." Gödel showed by a translation that these intuitionistic theories are equiconsistent with the classical ones.

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

1.1 The B-H-K Interpretation

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

1. To justify a prime sentence P is to recognize its truth.
2. To justify A & B is to justify A and B.
3. To justify $A \vee B$ is to justify a specific one of A, B.
4. To justify $A \to B$ is to provide a construction which transforms every justification of A into a justification of B.
5. To justify $\neg A$ is to justify $A \to \bot$, where $\bot$ 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 Pp

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

Pp has one *rule of inference*:

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

The *axioms* of **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. $A \,\&\, B \to B$.

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

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

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

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

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

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

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

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

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

- From B conclude $A \to B$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

End of Handout 1 (corrected). Handout 2 will begin with a completed version of this page 5. For n=1 to 10, your solutions to the new exercises in Handout n are due at the beginning of the $n + 1$st class. Solutions will then be posted on the class homepage. Solutions to starred exercises will usually be discussed in class.