Notre Dame Journal of Formal Logic
Volume 49, Number 4, 2008

Intuitionistic Logic according to Dijkstra's Calculus of Equational Deduction

Jaime A. Bohórquez V.

Abstract Dijkstra and Scholten have proposed a formalization of classical predicate logic on a novel deductive system as an alternative to Hilbert's style of proof and Gentzen's deductive systems. In this context we call it *CED* (*Calculus of Equational Deduction*). This deductive method promotes logical equivalence over implication and shows that there are easy ways to prove predicate formulas without the introduction of hypotheses or metamathematical tools such as the deduction theorem. Moreover, syntactic considerations (in Dijkstra's words, "letting the symbols do the work") have led to the "calculational style," an impressive array of techniques for elegant proof constructions. In this paper, we formalize *intuitionistic* predicate logic according to *CED* with similar success. In this system (*I-CED*), we prove Leibniz's principle for intuitionistic logic and also prove that any (intuitionistic) valid formula of predicate logic can be proved in *I-CED*.

1 Introduction

Computing science has had a major influence on developments in mathematics, in particular, the modern emphasis on formal logic. Its influence on the development of logic is still continuing and profoundly affects the way logic is presented.

The characteristic "theorem-proof" style of traditional mathematical reasoning, in which theorems are first formulated, and then verified, by mathematical proof, has only a minor role in the computing scientists' world. Instead, their skills are characterized by "goal followed-by-construction." This practice could be seen as a particular and more demanding case of the "theorem-proof" approach. The "goal" part in the computing scientist's view could be thought of as specifying an existence theorem of which the only acceptable proof must be a completely formal and constructive one; moreover, its deductive steps must be precisely detailed as to be

Received January 23, 2008; accepted May 2, 2008; printed September 25, 2008
2000 Mathematics Subject Classification: Primary, 03F50; Secondary, 03B20
Keywords: intuitionistic logic, calculational style, equational deduction
 10.1215/00294527-2008-017

executable by a machine. Thereby, the mathematician's (rightful) demand for rigor is not at all diminished; it is an integral part of the process. In short, the hallmark of computing science is "correct by construction" [1] regarding the goal's specification.

The computing scientist demands simplicity and conciseness of expression. This is the cornerstone of Dijkstra's development of *calculational logic* which emphasizes the use of equational reasoning rather than the traditional emphasis on logical implication. Calculational logic is innovative because it takes us beyond the limitations of "natural" modes of reasoning [8]. It was devised as an informal but rigorous method of proof by Dijkstra and Scholten [8], formalized by Gries and Schnider ([9], [10], [11]), and subsequently improved by Tourlakis ([16], [17]) and Lifschitz [12]. Bijlsma and Nederpelt [4] clarified several ideas and misconceptions related to this novel approach to logic. Applications of calculational logic to the teaching of Discrete Mathematics and Algorithm Design can be found in [9], [2], and [6].

The end product, *calculus of equational deduction* (or *CED*) becomes an alternative formalization of classical predicate logic based on logical equivalence, rather than on implication, and on textual substitution of logically equivalent subexpressions, rather than on modus ponens. Encouraged by the fact that "with the right choice of inference rules, proving predicate formulas is easy even without introducing assumptions or the use of auxiliary derivable objects and tools such as sequents or the deduction theorem," Hoare and Lifschitz [12] independently proposed these *surprisingly powerful*, so-called Leibniz inference rules for *CED*:

$$\text{LEIBNIZ RULES} \qquad \frac{E(p/A) \qquad A \equiv B}{E(p/B)} \qquad\qquad \frac{E(p/B) \qquad A \equiv B}{E(p/A)} \tag{1}$$

where A and B are free for a propositional symbol p in $E(p)$.

Actually, these are the only rules needed to derive arbitrary valid formulas of classical propositional logic from a small set of axiom schemas. This is done by means of a *calculational proof format*, a syntactic tool introduced by Dijkstra and Scholten [8] on the basis of ideas due to Feijen.

This proof format can be formalized as a chain of derivations (that we shall call a *deductive chain*), encoding a nonnull sequence of applications of rules (1). Each link of the chain is a triplet of formulas with three elements: an *initial*, a *final*, and the *hint*. For every pair of consecutive links in a deductive chain, we have that the final element of the first link coincides with the initial element of the second link. Obviously, every hint is an equivalence. Two formulas in a deductive chain have special names: the first element of the first triplet is the *source* of the deductive chain, and the final element of the last triplet is the *destination*. The hints that are different from instances of the axiom schemas (to be described later) are the *hypotheses* of the chain. This formalization follows Lifschitz [12] very closely.

Deductive chains are represented as follows: the horizontal bar in a Leibniz rule is replaced by $\Leftrightarrow$, and the hint $A \equiv B$, according to rules (1), is written to the right of the arrow in braces $\{\}$. The general format for a link of the deductive chain is of the form

$$\begin{array}{ll} & E(p/A) \\ \Leftrightarrow & \{A \equiv B\} \\ & E(p/B) \end{array}$$

where $E(p/A)$ and $E(p/B)$ are the members and $A \equiv B$ is the hint.

Accordingly, a deductive chain has a representation that looks like this:

$$\begin{array}{ll} & P_1 \\ \Leftrightarrow & \{ E_1 \} \\ & P_2 \\ \Leftrightarrow & \{ E_2 \} \\ & \vdots \\ \Leftrightarrow & \{ E_{n-1} \} \\ & P_n . \end{array}$$

It should be clear that if there exists a deductive chain with source P, destination Q, and set of hypotheses Γ, then

$$Q \text{ is derivable from } \Gamma \cup \{ P \}.$$

Similarly, we can also assert that

$$P \text{ is derivable from } \Gamma \cup \{ Q \} \quad \text{and} \quad P \equiv Q \text{ and } Q \equiv P \text{ are derivable from } \Gamma.$$

The first claim is easily proved by reversing the order of the members in the given deductive chain. The result will be a deductive chain, since every application of any of the Leibniz rules will turn into an application of the other one of these rules. To prove the second claim, replace every member R of the chain with $P \equiv R$. Once again, the result will be a deductive chain whose source $P \equiv P$ is provable in *CED* (as will be clear soon) and whose destination is $P \equiv Q$. The proof for the case of $Q \equiv P$ is similar.

Remark 1.1 Observe that we were able to define and reason about deductive chains based only on the capabilities of the "replacement of equivalent subexpressions" given by Leibniz rules. We did this without appealing explicitly to any axiom system except for the supposition that the reflexivity of logical equivalence could be proved as a theorem. Actually, its commutativity is implicitly assumed considering the symmetry of rules (1) and the very concept of the deductive chain accounts for the derivability of its transitivity, as may be seen from our last claim. From an algebraic point of view, and considering the relative novelty and power of calculational logic, it becomes evident that the congruence properties of logical equivalence have not been fully exploited.

The purpose of this article is to show that the elegance and "proof effectiveness" of the calculus of equational deduction can be extended to the intuitionistic predicate logic.

In Section 2 we present equational axiom schemas for intuitionistic predicate logic, based on *CED*, that we shall refer to as *I-CED*. Moreover, to further improve our derivations, we derive complementary inference rules and introduce notational and methodological conventions that extend the *I-CED* proof format with the modus ponens rule. To illustrate the proof methodology of *I-CED*, we present, in Section 3, deductive chains to prove a few theorems needed in Section 4, and also for our proofs of the completeness of *I-CED*. In Section 4 we prove a metatheorem for intuitionistic predicate logic (Leibniz's principle) about replacement of equivalents in implications and conjunctions.

2 Equational Axiomatization for Intuitionistic Logic

In the language of *CED*, *terms* and *atomic formulas* are defined as in predicate logic (without equality). By $\top$ (true) and $\bot$ (false), we denote the obvious 0-ary constant predicates. The following logical binary connectives are listed in order of decreasing binding power (those listed as a pair have the same precedence): $\vee$ and $\wedge$ denote disjunction and conjunction, respectively; $\rightarrow$ denotes implication; $\equiv$ denotes equivalence as we have just seen. As usual, the symbols $\forall$ and $\exists$ denote the universal and the existential quantifier, respectively; their scope, when necessary, is delineated by a pair of parentheses. *Formulas* are built from atomic formulas, $\bot$ and $\top$, using the above-mentioned connectives, and $\forall$ and $\exists$.

As propositional axiom schemas for intuitionistic logic in *I-CED* (for any formulas P, Q, and R), we take $\top$ to be an identity element for equivalence:

$$(P \equiv \top) \equiv P, \tag{2}$$

for conjunction and disjunction, those corresponding to the defining properties of a distributive lattice, that is, respectively, commutativity, associativity, idempotence, one absorption and one (complementary) distributivity. In addition, $\top$ and $\bot$ are taken to be, respectively, identity elements for conjunction and disjunction,

$$P \wedge Q \equiv Q \wedge P \quad \text{and} \quad P \vee Q \equiv Q \vee P \tag{3}$$

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R) \quad \text{and} \quad (P \vee Q) \vee R \equiv P \vee (Q \vee R) \tag{4}$$

$$P \wedge P \equiv P \quad \text{and} \quad P \vee P \equiv P \tag{5}$$

$$P \vee (P \wedge Q) \equiv P \tag{6}$$

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R) \tag{7}$$

$$\top \wedge P \equiv P \quad \text{and} \quad \bot \vee P \equiv P, \tag{8}$$

and for implication,

$$P \rightarrow Q \equiv (P \vee Q \equiv Q) \qquad \text{(defining axiom)} \tag{9}$$

$$(P \equiv Q) \equiv (P \rightarrow Q) \wedge (Q \rightarrow P) \qquad \text{(mutual implication)} \tag{10}$$

$$P \rightarrow (Q \rightarrow R) \equiv P \wedge Q \rightarrow R \qquad \text{(coupling)} \tag{11}$$

$$P \wedge (P \rightarrow Q) \equiv P \wedge Q \qquad \text{(compression).} \tag{12}$$

The only inference for propositional intuitionistic logic in *I-CED* is (1).

As axioms for the *intuitionistic predicate calculus* in *I-CED*, we take all formulas of the following groups:

All instances of (2) – (12); (13)

$$\forall x\, P \wedge P(x/t) \equiv \forall x\, P \qquad \text{(where } t \text{ is free for } x \text{ in } P(x)\text{);} \tag{14}$$

$$\exists x\, P \vee P(x/t) \equiv \exists x\, P \qquad \text{(where } t \text{ is free for } x \text{ in } P(x)\text{);} \tag{15}$$

$$\forall x\, P \equiv P \qquad \text{(provided } x \text{ is not free in } P\text{);} \tag{16}$$

$$\exists x\, P \equiv P \qquad \text{(provided } x \text{ is not free in } P\text{);} \tag{17}$$

$$\forall x (P \rightarrow Q) \rightarrow (\forall x\, P \rightarrow \forall x\, Q); \tag{18}$$

$$\forall x (P \rightarrow Q) \rightarrow (\exists x\, P \rightarrow \exists x\, Q); \tag{19}$$

All *generalizations* of axioms of the preceding groups. (20)

By a generalization of P we mean any formula of the form $\forall x_1 \ldots \forall x_k (P)$, where $k \geq 1$ and $x_1, \ldots, x_k$ are variables not necessarily different. As inference rules for predicate intuitionistic logic in *I-CED*, in addition to inference rules (1), we have the usual generalization rule,

$$\frac{P}{\forall x\, P} \quad . \tag{21}$$

Remark 2.1 Observe that practically all axioms are equational.[1] Axiom schemas (9) and (10) suggest that we could have expressed implication axioms in terms of equivalence, or conversely. However, our goal in this paper is, besides providing a formal analysis of the viability of applying Dijkstra's calculus of equational deduction to intuitionistic logic, to help develop a methodology similar to the one developed for classical logic that can be used by the working mathematician (or computer scientist) for discovering and presenting proofs in this logic. For this reason, we prefer expressiveness and easy handling of proofs rather than conciseness and economy in terms of number of axioms.

It is clear that this deductive system is intuitionistically sound, if for any "forcing frame" on the language of *I-CED*, $\top$ is forced by every state. Forcing an equivalence in a state is understood as forcing the conjunction of the associated implications in that same state [13]. Its completeness is proved in the Appendix.

As we have announced before, reflexivity of equivalence

$$P \equiv P \tag{22}$$

is actually a theorem in *I-CED* that can be proved in one step using axiom schema (5) and the first Leibniz rule:

$$\frac{P \wedge P \equiv P \qquad P \wedge P \equiv P}{P \equiv P} \quad . \tag{23}$$

In terms of the proof format introduced above, this deduction will be written as

$$\begin{array}{ll} & P \wedge P \equiv P \\ \Leftrightarrow & \{P \wedge P \equiv P\} \\ & P \equiv P . \end{array}$$

Since $\top \equiv \top$ and $(\top \equiv \top) \equiv \top$ are, respectively, instances of (22) and (2),

$$\top \tag{24}$$

can be obtained as a corollary through the following deductive chain:

$$\begin{array}{ll} & \top \\ \Leftrightarrow & \{(\top \equiv \top) \equiv \top\} \\ & \top \equiv \top . \end{array}$$

As the destination formula is provable in *I-CED*, so is the source formula.

As another example, here is a deductive chain with source $P \equiv Q$, destination $Q \equiv P$, and the empty set of hypotheses,

$$\begin{array}{ll} & P \equiv Q \\ \Leftrightarrow & \{(10)\} \\ & (P \to Q) \wedge (Q \to P) \\ \Leftrightarrow & \{\text{first part of (3)}\} \\ & (Q \to P) \wedge (P \to Q) \\ \Leftrightarrow & \{(10)\} \\ & Q \equiv P , \end{array}$$

which proves commutativity of equivalence,

$$(P \equiv Q) \equiv (Q \equiv P)\,. \tag{25}$$

To improve readability, from here on, we will replace hint formulas by references explaining why they are provable in *I-CED*, and we will sometimes combine several derivations into one step. Due to the numerous applications of the commutative and associative properties of $\wedge$ and $\vee$, we will not mention their use every time they are needed.

The proof power of *I-CED* is readily illustrated by the derivation[2] of the following inference rules from Leibniz rules (1), axiom (2), and Theorem (24),

$$\frac{\top \qquad P \equiv \top}{P} \qquad\qquad \frac{P \qquad (P \equiv \top) \equiv P}{P \equiv \top} \tag{26}$$

which proves the following metatheorem. (We use the usual "turnstile" notation "$\vdash$" as part of the metalanguage to denote provability in *I-CED*.)

Theorem 2.2 *If P is a formula in I-CED, then*

$$\vdash P \quad \textit{if and only if} \quad \vdash P \equiv \top\,.$$

Consequently, to prove that P is a theorem in *I-CED*, it is enough to establish $P \equiv \top$. Conversely, if P is a theorem in *I-CED*, so is $P \equiv \top$. Furthermore, as a corollary, since transitivity of equivalence can be expressed as a derived inference rule from (1),

Transitivity
$$\frac{P \equiv Q \qquad Q \equiv R}{P \equiv R}\,, \tag{27}$$

by (25), and replacing Q by $\top$, and we obtain the following corollary.

Corollary 2.3 *In I-CED, if $\vdash P$ and $\vdash R$ then $\vdash P \equiv R$. In other words, all theorems in I-CED are equivalent.*

Moreover, Theorem 2.2 allows us to derive a few complementary inference rules that contribute to the simplification of our proof activities, such as rule $\wedge$-Int:

$\wedge$-Int
$$\frac{P \qquad Q}{P \wedge Q}\,. \tag{28}$$

To prove a conjunction, this rule allows a *system* of deductive chains in which each conjunct is proved by means of a separate deductive chain.

The derivation of rule $\wedge$-Int is given by the following calculation:

$$\begin{array}{ll} & P \wedge Q \\ \Leftrightarrow & \{P \equiv \top\} \\ & \top \wedge Q \\ \Leftrightarrow & \{Q \equiv \top\} \\ & \top \wedge \top \\ \Leftrightarrow & \{\text{idempotence of } \wedge \text{ and } (8)\} \\ & \top\,, \end{array}$$

in view of the fact that, by Theorem 2.2, hints $P \equiv \top$ and $Q \equiv \top$ can be, respectively, derived from P and Q.

Our next goal is to enhance Feijen's proof format (described above) with modus ponens rule. Modus ponens rule

$$\frac{P \qquad P \to Q}{Q} \tag{29}$$

is derivable in *I-CED*, as shown by the deductive chain

$$\begin{array}{ll} & Q \\ \Leftrightarrow & \{\text{first part of (8)}\} \\ & \top \wedge Q \\ \Leftrightarrow & \{P \equiv \top\} \\ & P \wedge Q \\ \Leftrightarrow & \{(12)\} \\ & P \wedge (P \Rightarrow Q) \\ \Leftrightarrow & \{P \equiv \top\} \\ & \top \wedge (P \Rightarrow Q) \\ \Leftrightarrow & \{\text{first part of (8)}\} \\ & P \Rightarrow Q \\ \Leftrightarrow & \{P \Rightarrow Q \equiv \top\} \\ & \top, \end{array}$$

in view of the fact that, by Theorem 2.2, hints $P \equiv \top$ and $P \to Q \equiv \top$ can be, respectively, derived from P and $P \to Q$.

Consequently, the deductive system *I-CED**, obtained from *I-CED* by adding rules (29) and (28) to Leibniz inference rules, is a conservative extension of *I-CED*; in other words, it has the same theorems as *I-CED*. The definition of a deductive chain and other related concepts, introduced in Section 1, apply to the extended system without changes; the only difference is that for applications of modus ponens, the horizontal bar of such rule will be replaced in the proof format by a $\Rightarrow$ (instead of a $\Leftrightarrow$, as we did in applications of Leibniz rules) with the hint written to the right of this single arrow.

For instance, the deductive chain,

$$\begin{array}{ll} & P \vee \bot \\ \Leftrightarrow & \{\text{second part of (8): identity of } \vee\} \\ & P \\ \Rightarrow & \{P \to P \vee Q\} \\ & P \vee Q, \end{array}$$

establishes the provability of $P \vee \bot \to P \vee Q$, since it is easy to prove $P \to P \vee Q$ in *I-CED*, as we will see below.

In this extended notation, bidirectional deductive chains are distinguished by the absence of the sign $\Rightarrow$ in them. Note that now hints are not necessarily equivalences. Just as in the less general setting of Section 1, if there exists a deductive chain with source P, destination Q, and set of hypotheses Γ, then Q is derivable from $\Gamma \cup \{P\}$ in *I-CED** (and consequently in *I-CED*).

In fact, we can also assert that $P \to Q$ is derivable from Γ. To prove this claim, reduce such chain to an equivalent system of bidirectional deductive chains preserving global source and destination; then, replace every member R in such bidirectional deductive chains with $P \to R$. The (global) source of such system of chains turns into $P \rightarrow P$, which is easily provable in *I-CED*. Applications of Leibniz rules (1) turn into applications of the same rules. The (global) destination turns into $P \rightarrow Q$.

Another inference rule derivable in *I-CED* is

$$\frac{P \rightarrow Q \qquad Q \rightarrow P}{P \equiv Q} \tag{30}$$

which methodologically corresponds to proofs by mutual implication or "ping-pong arguments" as they are called in [8]. Dijkstra advised to avoid the ping-pong arguments as much as possible but also to learn to recognize situations in which they are appropriate.

The following deductive chain demonstrates the derivability of rule (30):

$$\begin{array}{ll} & P \rightarrow Q \\ \Leftrightarrow & \{(9)\} \\ & P \vee Q \equiv Q \\ \Leftrightarrow & \{P \vee Q \equiv P\} \\ & P \equiv Q \end{array}$$

in view of the fact that the hint $P \vee Q \equiv P$ can be derived from $Q \rightarrow P$ using axiom schemas (9) and (3).

Remark 2.4 After realizing that the "algebraic content" of Dijkstra's axiomatization of classical propositional logic corresponded to Stone's concept of Boolean ring ([5], [15])—with disjunction and equivalence, respectively, playing the role of duals of conjunction and "symmetric difference"—the concept of Heyting algebra (or pseudo-Boolean algebra, as they call it in [14]) was a suitable inspiration to propose the axiomatization for *I-CED*.

3 The Proof Methodology of *I-CED*

We now proceed to establish the provability of some (classes of) formulas in *I-CED* by exhibiting in every case an appropriate system of deductive chains whose hypotheses are already known to be provable. This will illustrate the usefulness of Feijen's proof format (these proofs will be needed for our proof of the completeness of *I-CED*).

Abbreviations $\neg P$ stands for $P \equiv \bot$.

We plan to prove the following theorem schemas:

$$\neg\top \equiv \bot \tag{31}$$

$$\bot \rightarrow P \tag{32}$$

$$P \rightarrow P \qquad \text{(reflexivity of } \rightarrow) \tag{33}$$

$$P \wedge Q \rightarrow P \qquad (\wedge\text{−weakening}) \tag{34}$$

$$P \rightarrow P \vee Q \qquad (\vee\text{−weakening}) \tag{35}$$

$$P \wedge (P \equiv Q) \equiv P \wedge Q \qquad \text{(compaction)} \tag{36}$$

$$P \wedge (P \equiv Q) \equiv Q \wedge (P \equiv Q) \qquad \text{(interchange)} \tag{37}$$

$$(P \rightarrow Q) \wedge (P \rightarrow R) \equiv (P \rightarrow Q \wedge R) \tag{38}$$

$$P \rightarrow Q \equiv (P \wedge Q \equiv P) \tag{39}$$

$$\bot \wedge P \equiv \bot \qquad \text{(zero of } \wedge) \tag{40}$$

$$P \wedge \neg P \equiv \bot \qquad \text{(contradiction)} \tag{41}$$

$$(P \to R) \wedge (Q \to R) \equiv P \vee Q \to R \tag{42}$$
$$(P \to Q) \wedge (R \to S) \to (P \wedge R \to Q \wedge S) \tag{43}$$
$$(P \equiv Q) \wedge (Q \equiv R) \to (P \equiv R) \qquad \text{(transitivity of } \equiv\text{)} \tag{44}$$
$$(P \equiv Q) \wedge (R \equiv S) \to (P \vee R \equiv Q \vee S) \tag{45}$$
$$(P \equiv Q) \wedge (R \equiv S) \to (P \wedge R \equiv Q \wedge S) \tag{46}$$
$$\forall x (P \wedge Q) \equiv \forall x P \wedge \forall x Q \qquad \text{(conjunctivity)} \tag{47}$$

Remark 3.1 Associativity of equivalence is one the jewels of the axiomatization of classical logic in *CED*. However, the soundness of *I-CED* implies that this property is not provable in this system since otherwise (using the previous abbreviation) we could prove $P \equiv \neg\neg P$, which is well known as a constructively invalid formula:

$$\begin{array}{ll} & (P \equiv \bot) \equiv \neg P \\ \Leftrightarrow & \{\text{wrong step!}\} \\ & P \equiv (\bot \equiv \neg P) \\ \Leftrightarrow & \{\text{previous abbreviation}\} \\ & P \equiv \neg\neg P. \end{array}$$

Nevertheless, we will manage very well without it.

The pairwise equivalence of the following theorem schemas will be used in Section 4.

Theorem 3.2 *If P, Q, R are arbitrary formulas, then the following are pairwise equivalent in I-CED:*

(a) $P \to (Q \equiv R)$;
(b) $P \to Q \equiv P \to R$;
(c) $P \wedge Q \equiv P \wedge R$;
(d) $(P \wedge Q \to R) \wedge (P \wedge R \to Q)$.

We prove this theorem in the Appendix.

Below we show how the provability of six of the previous schemas are established by deductive chains. Proofs of the other eleven are given in the Appendix.

Proof of (32)

$$\begin{array}{ll} & \bot \to P \\ \Leftrightarrow & \{(9)\} \\ & \bot \vee P \equiv P \\ \Leftrightarrow & \{(8)\text{: identity of } \vee\} \\ & P \equiv P \\ \Leftrightarrow & \{(22)\text{: reflexivity of } \equiv\text{; Theorem 2.2}\} \\ & \top\,. \end{array}$$

This deductive chain proves $\bot \to P \equiv \top$. By Theorem 2.2, we conclude that the source is provable in *I-CED*. (For the coming deductions, we will not repeat this explanation anymore.)

Proof of (36)

$$
\begin{array}{ll}
 & P \wedge (P \equiv Q) \\
\Leftrightarrow & \{(10)\text{: mutual implication}\} \\
 & P \wedge (P \rightarrow Q) \wedge (Q \rightarrow P) \\
\Leftrightarrow & \{(12)\text{: compression}\} \\
 & P \wedge Q \wedge (Q \rightarrow P) \\
\Leftrightarrow & \{(11), (5), \text{and commutativity of } \wedge\} \\
 & P \wedge Q\,.
\end{array}
$$

Proof of (38) By ping-pong argument.

Ping:

$$
\begin{array}{ll}
 & (P \rightarrow Q) \wedge (P \rightarrow R) \rightarrow (P \rightarrow Q \wedge R) \\
\Leftrightarrow & \{(11)\text{: coupling; idempotence of } \wedge\} \\
 & P \wedge (P \rightarrow Q) \wedge P \wedge (P \rightarrow R) \rightarrow Q \wedge R \\
\Leftrightarrow & \{(12)\text{ (twice); idempotence of } \wedge\} \\
 & P \wedge Q \wedge R \rightarrow Q \wedge R \\
\Leftrightarrow & \{(34), (4)\text{; Theorem } 2.2\} \\
 & \top\,.
\end{array}
$$

Pong: By *ping* and rule ($\wedge$-Int), it is enough to prove

$$(P \rightarrow Q \wedge R) \rightarrow (P \rightarrow Q) \text{ and } (P \rightarrow Q \wedge R) \rightarrow (P \rightarrow R)$$

separately. The following deductive chain proves the first of them:

$$
\begin{array}{ll}
 & (P \rightarrow Q \wedge R) \rightarrow (P \rightarrow Q) \\
\Leftrightarrow & \{(11)\text{: coupling}\} \\
 & (P \rightarrow Q \wedge R) \wedge P \rightarrow Q \\
\Leftrightarrow & \{(12)\text{: compression; idempotence of } \wedge\} \\
 & P \wedge Q \wedge R \rightarrow Q \\
\Leftrightarrow & \{(34), (4)\text{; Theorem } 2.2\} \\
 & \top.
\end{array}
$$

The proof of the second formula is similar.

Proof of (39) By ping-pong argument.

Ping: Since

$$
\begin{array}{ll}
 & (P \rightarrow Q) \rightarrow (P \wedge Q \equiv P) \\
\Leftrightarrow & \{(10)\} \\
 & (P \rightarrow Q) \rightarrow (P \wedge Q \rightarrow P) \wedge (P \rightarrow P \wedge Q)
\end{array}
$$

by (38) and rule ($\wedge$-Int), it is sufficient to prove

(a) $(P \rightarrow Q) \rightarrow (P \wedge Q \rightarrow P)$ and
(b) $(P \rightarrow Q) \rightarrow (P \rightarrow P \wedge Q)$.

We prove (b). The proof of (a) is similar.

$$\begin{array}{ll} & (P \to Q) \to (P \to P \wedge Q) \\ \Leftrightarrow & \{(11)\text{: coupling}\} \\ & (P \to Q) \wedge P \to P \wedge Q \\ \Leftrightarrow & \{(12)\text{ compression}\} \\ & P \wedge Q \to P \wedge Q \\ \Leftrightarrow & \{(33)\text{; Theorem 2.2}\} \\ & \top. \end{array}$$

Pong:

$$\begin{array}{ll} & (P \wedge Q \equiv P) \to (P \to Q) \\ \Leftrightarrow & \{(11)\text{: coupling}\} \\ & (P \wedge Q \equiv P) \wedge P \to Q \\ \Leftrightarrow & \{(36)\text{: compaction; idempotence of } \wedge\} \\ & P \wedge Q \to Q \\ \Leftrightarrow & \{(34)\text{; Theorem 2.2}\} \\ & \top. \end{array}$$

Proof of (40)

$$\begin{array}{ll} & \bot \wedge P \equiv \bot \\ \Leftrightarrow & \{(39)\} \\ & \bot \to P \\ \Leftrightarrow & \{(32)\text{; Theorem 2.2}\} \\ & \top\,. \end{array}$$

Proof of (41)

$$\begin{array}{ll} & P \wedge \neg P \\ \Leftrightarrow & \{\text{Abbreviation: } \neg P \equiv (P \equiv \bot)\} \\ & P \wedge (P \equiv \bot) \\ \Leftrightarrow & \{(36)\text{: compaction}\} \\ & P \wedge \bot \\ \Leftrightarrow & \{(40)\text{: zero of } \wedge\} \\ & \bot\,. \end{array}$$

4 Leibniz's Principle

Dijkstra [7] proved in *CED*, for classical predicate logic, what might be called *Leibniz's principle*, a stronger replacement law than Leibniz inference rules. Actually, this principle is intuitionistically valid; in fact, it is provable in *I-CED*. It may be expressed as follows.

Theorem 4.1 (Leibniz's Principle) *Every instance of*

$$(A \equiv B) \to (E(p/A) \equiv E(p/B)) \tag{48}$$

is a theorem in I-CED, if A, B are free for a propositional symbol p in $E(p)$.

We prove this theorem in the Appendix.

Gries and Schnider [9] proved several rephrasings and applications of this principle in classical propositional logic and we can prove a few of them in *I-CED*. By

Theorem 3.2, it can also be stated as follows:

$$(A \equiv B) \wedge E(p/A) \equiv (A \equiv B) \wedge E(p/B), \tag{49}$$

where A, B are free for a propositional symbol p in $E(p)$. Theorem 3.2 gives another useful rephrasing of this principle:

$$(A \equiv B) \rightarrow E(p/A) \equiv (A \equiv B) \rightarrow E(p/B). \tag{50}$$

The following are easy, but interesting, consequences of Leibniz's principle based on axiom schema (2) and definition of negation, since they provide powerful simplifying identities, potentially useful for devising theorem-proving techniques based on term rewriting.

Corollary 4.2 (Replacement by Boolean constants) *Every instance of the following schemas is a theorem in I-CED.*

(i) $A \wedge E(p/A) \equiv A \wedge E(p/\top)$,
(ii) $\neg A \wedge E(p/A) \equiv \neg A \wedge E(p/\bot)$,
(iii) $A \rightarrow E(p/A) \equiv A \rightarrow E(p/\top)$,
(iv) $\neg A \rightarrow E(p/A) \equiv \neg A \rightarrow E(p/\bot)$,

whenever A is free for a propositional symbol p in $E(p)$.

Appendix: Proofs

Proofs of Formulas from Section 3

Proof of (31)

$$\begin{array}{ll} & \neg\top \\ \Leftrightarrow & \{\text{notation: definition of } \neg\} \\ & \top \equiv \bot \\ \Leftrightarrow & \{(2)\text{: identity of } \equiv\} \\ & \bot\,. \end{array}$$

Proof of (33)

$$\begin{array}{ll} & P \rightarrow P \\ \Leftrightarrow & \{(9)\} \\ & P \vee P \equiv P \\ \Leftrightarrow & \{(5)\text{: idempotence of } \vee\} \\ & P \equiv P \\ \Leftrightarrow & \{(22)\text{: reflexivity of } \equiv\text{; Theorem 2.2}\} \\ & \top\,. \end{array}$$

Proof of (34)

$$\begin{array}{ll} & P \wedge Q \rightarrow P \\ \Leftrightarrow & \{(9)\} \\ & (P \wedge Q) \vee P \equiv P \\ \Leftrightarrow & \{(6)\text{: absorption}\} \\ & P \equiv P \\ \Leftrightarrow & \{(22)\text{: reflexivity of } \equiv\text{; Theorem 2.2}\} \\ & \top\,. \end{array}$$

Proof of (35)

$$
\begin{aligned}
& P \to P \vee Q \\
\Leftrightarrow \quad & \{(9);\ (4)\} \\
& P \vee P \vee Q \equiv P \vee Q \\
\Leftrightarrow \quad & \{(5)\text{: idempotence of } \vee\} \\
& P \vee Q \equiv P \vee Q \\
\Leftrightarrow \quad & \{(22)\text{: reflexivity of } \equiv\text{; Theorem 2.2}\} \\
& \top\,.
\end{aligned}
$$

Proof of (37)

$$
\begin{aligned}
& P \wedge (P \equiv Q) \\
\Leftrightarrow \quad & \{(36)\text{: compaction}\} \\
& P \wedge Q \\
\Leftrightarrow \quad & \{(36)\text{, commutativity of } \wedge \text{ and } \equiv\} \\
& Q \wedge (Q \equiv P)\,.
\end{aligned}
$$

Proof of (42) By ping-pong argument.

Ping:

$$
\begin{aligned}
& (P \to R) \wedge (Q \to R) \to (P \vee Q \to R) \\
\Leftrightarrow \quad & \{(11)\text{: coupling}\} \\
& (P \to R) \wedge (Q \to R) \wedge (P \vee Q) \to R \\
\Leftrightarrow \quad & \{(7)\text{: } \wedge \text{ distributes over } \vee\} \\
& ((P \to R) \wedge (Q \to R) \wedge P) \vee ((P \to R) \wedge (Q \to R) \wedge Q) \to R \\
\Leftrightarrow \quad & \{(12)\text{: compression; (5): idempotence of } \wedge \text{ (twice)}\} \\
& (P \wedge R \wedge (Q \to R)) \vee ((P \to R) \wedge Q \wedge R) \to R \\
\Leftrightarrow \quad & \{(7)\text{: } \wedge \text{ distributes over } \vee\} \\
& R \wedge (P \wedge (Q \to R)) \vee ((P \to R) \wedge Q) \to R \\
\Leftrightarrow \quad & \{(34)\text{: } \wedge\text{-weakening; Theorem 2.2}\} \\
& \top\,.
\end{aligned}
$$

Pong: By (38) and rule ($\wedge$-Int), it is sufficient to prove

(a) $(P \vee Q \to R) \to (P \to R)$ and
(b) $(P \vee Q \to R) \to (Q \to R)$.

We prove (a). Proofs of (a) and (b) are symmetrical.

$$
\begin{aligned}
& (P \vee Q \to R) \to (P \to R) \\
\Leftrightarrow \quad & \{(11)\text{: coupling}\} \\
& (P \vee Q \to R) \wedge P \to R,
\end{aligned}
$$

and then

$$
\begin{array}{ll}
 & (P \vee Q \to R) \wedge P \\
\Rightarrow & \{(35)\text{: } \vee\text{-weakening}\} \\
 & ((P \vee Q \to R) \wedge P) \vee ((P \vee Q \to R) \wedge Q) \\
\Leftrightarrow & \{(7)\text{: } \wedge \text{ distributes over } \vee\} \\
 & (P \vee Q \to R) \wedge (P \vee Q) \\
\Leftrightarrow & \{(12)\text{: compression}\} \\
 & (P \vee Q) \wedge R \\
\Rightarrow & \{(34)\text{: } \wedge\text{-weakening}\} \\
 & R\,.
\end{array}
$$

Proof of (43)

$$
\begin{array}{ll}
 & (P \to Q) \wedge (R \to S) \to (P \wedge R \to Q \wedge S) \\
\Leftrightarrow & \{(11)\text{: coupling}\} \\
 & (P \to Q) \wedge (R \to S) \wedge P \wedge R \to Q \wedge S \\
\Leftrightarrow & \{(12)\text{: compression (twice)}\} \\
 & P \wedge Q \wedge R \wedge S \to Q \wedge S \\
\Leftrightarrow & \{(34)\text{: } \wedge\text{-weakening; Theorem 2.2}\} \\
 & \top\,.
\end{array}
$$

Proof of (44) By (38) and rule ($\wedge$-Int), it is enough to prove

(a) $(P \equiv Q) \wedge (Q \equiv R) \to (P \to R)$ and
(b) $(P \equiv Q) \wedge (Q \equiv R) \to (R \to P)$.

We prove (a). Proofs of (a) and (b) are symmetrical.

$$
\begin{array}{ll}
 & (P \equiv Q) \wedge (Q \equiv R) \to (P \to R) \\
\Leftrightarrow & \{(11)\text{: coupling}\} \\
 & (P \equiv Q) \wedge (Q \equiv R) \wedge P \to R \\
\Leftrightarrow & \{(36)\text{: compaction}\} \\
 & P \wedge Q \wedge (Q \equiv R) \to R \\
\Leftrightarrow & \{(36)\text{: compaction}\} \\
 & P \wedge Q \wedge R \to R \\
\Leftrightarrow & \{(34)\text{: } \wedge\text{-weakening}\} \\
 & \top\,.
\end{array}
$$

Proof of (45) By (10), (38), and rule ($\wedge$-Int), it is enough to prove

(a) $(P \equiv Q) \wedge (R \equiv S) \to (P \vee R \to Q \vee S)$ and
(b) $(P \equiv Q) \wedge (R \equiv S) \to (Q \vee S \to P \vee R)$.

We prove (a). Proofs of (a) and (b) are symmetrical.

$$
\begin{array}{ll}
 & (P \equiv Q) \wedge (R \equiv S) \rightarrow (P \vee R \rightarrow Q \vee S) \\
\Leftrightarrow & \{(11)\text{: coupling}\} \\
 & (P \equiv Q) \wedge (R \equiv S) \wedge (P \vee R) \rightarrow Q \vee S \\
\Leftrightarrow & \{(7)\text{: } \wedge \text{ distributes over } \vee\} \\
 & ((P \equiv Q) \wedge (R \equiv S) \wedge P) \vee ((P \equiv Q) \wedge (R \equiv S) \wedge R) \rightarrow Q \vee S \\
\Leftrightarrow & \{(37)\text{: interchange (twice)}\} \\
 & ((P \equiv Q) \wedge (R \equiv S) \wedge Q) \vee ((P \equiv Q) \wedge (R \equiv S) \wedge S) \rightarrow Q \vee S \\
\Leftrightarrow & \{(7)\text{: } \wedge \text{ distributes over } \vee\} \\
 & (P \equiv Q) \wedge (R \equiv S) \wedge (Q \vee S) \rightarrow Q \vee S \\
\Leftrightarrow & \{(34)\text{: } \wedge\text{-weakening; Theorem 2.2}\} \\
 & \top .
\end{array}
$$

Proof of (46) This proof is similar and simpler than (45). We skip it.

Proof of (47) By ping-pong argument.

Ping: By (34) and (21), the following formulas are theorems in *I-CED*:

$$\forall x(P \wedge Q \rightarrow P) \qquad \forall x(P \wedge Q \rightarrow Q). \tag{51}$$

Therefore,

$$
\begin{array}{ll}
 & \forall x(P \wedge Q) \\
\Leftrightarrow & \{(5)\text{: idempotence of } \wedge\} \\
 & \forall x(P \wedge Q) \wedge \forall x(P \wedge Q) \\
\Rightarrow & \{(51), (18), (43)\text{: monotonicity of } \wedge\} \\
 & \forall x P \wedge \forall x Q .
\end{array}
$$

Pong: By (14), (39), (21), and (43), the following formula is a theorem in *I-CED*:

$$\forall x(\forall x P \wedge \forall x Q \rightarrow P \wedge Q). \tag{52}$$

Therefore,

$$
\begin{array}{ll}
 & \forall x P \wedge \forall x Q \\
\Leftrightarrow & \{(16) : x \text{ is not free in } \forall x(P \wedge Q)\} \\
 & \forall x(\forall x P \wedge \forall x Q) \\
\Rightarrow & \{(52), (18)\} \\
 & \forall x(P \wedge Q).
\end{array}
$$

Proof of Theorem 3.2 By Transitivity rule, it is enough to prove that (a), (b), (c) are each pairwise equivalent to (d).

(a) $\equiv$ (d):

$$
\begin{array}{ll}
 & P \rightarrow (Q \equiv R) \\
\Leftrightarrow & \{(10)\text{: mutual implication}\} \\
 & P \rightarrow (Q \rightarrow R) \wedge (R \rightarrow Q) \\
\Leftrightarrow & \{(38)\} \\
 & (P \rightarrow (Q \rightarrow R)) \wedge (P \rightarrow (R \rightarrow Q)) \\
\Leftrightarrow & \{(11)\text{: coupling (twice)}\} \\
 & (P \wedge Q \rightarrow R) \wedge (P \wedge R \rightarrow Q).
\end{array}
$$

(b) $\equiv$ (d):

$$
\begin{aligned}
& P \to Q \equiv P \to R \\
\Leftrightarrow \quad & \{(10)\text{: mutual implication}\} \\
& ((P \to Q) \to (P \to R)) \wedge ((P \to R) \to (P \to Q)) \\
\Leftrightarrow \quad & \{(11), (12)\text{: coupling and compression (twice)}\} \\
& (P \wedge Q \to R) \wedge (P \wedge R \to Q).
\end{aligned}
$$

(c) $\equiv$ (d):

$$
\begin{aligned}
& P \wedge Q \equiv P \wedge R \\
\Leftrightarrow \quad & \{(10)\text{: mutual implication}\} \\
& (P \wedge Q \to P \wedge R) \wedge (P \wedge R \to P \wedge Q) \\
\Leftrightarrow \quad & \{(38)\} \\
& (P \wedge Q \to R) \wedge (P \wedge R \to Q) \wedge (P \wedge Q \to P) \wedge (P \wedge R \to P) \\
\Leftrightarrow \quad & \{(34)\text{: } \wedge\text{-weakening; Theorem 2.2 (twice)}\} \\
& (P \wedge Q \to R) \wedge (P \wedge R \to Q) \wedge \top \wedge \top \\
\Leftrightarrow \quad & \{\text{identity of } \equiv \text{ (twice)}\} \\
& (P \wedge Q \to R) \wedge (P \wedge R \to Q).
\end{aligned}
$$

Proof of the Completeness Theorem

Proposition 3 *Every intuitionistically valid formula is provable in I-CED.*

We will prove this fact by relating *I-CED* to another formalization of intuitionistic predicate logic which is defined and proved to be complete, for instance, the system *BM* (for Bell and Machover), Chapter 9 of [3]. The language of *BM* is a subset of the language of *I-CED*. Its formulas are built from atomic formulas using negation, conjunction, disjunction, implication, and the universal and existential quantifiers. We will show that *I-CED* is a "conservative extension" of *BM* in the sense that both systems prove the same theorems considering an adequate translation.

The propositional axiom schemas of *BM* are

$$P \to (Q \to P) \tag{53}$$
$$(P \to (Q \to R)) \to ((P \to Q) \to (P \to R)) \tag{54}$$
$$P \to (Q \to P \wedge Q) \tag{55}$$
$$P \wedge Q \to P \tag{56}$$
$$P \wedge Q \to Q \tag{57}$$
$$P \to P \vee Q \tag{58}$$
$$Q \to P \vee Q \tag{59}$$
$$(P \to R) \to ((Q \to R) \to (P \vee Q \to R)) \tag{60}$$
$$(P \to Q) \to ((P \to \neg Q) \to \neg P) \tag{61}$$
$$\neg P \to (P \to Q) \tag{62}$$

The inference rule of *BM* is modus ponens.

The axioms of the *intuitionistic predicate calculus* in *BM* are all formulas in the following groups:

All instances of (53) – (62); (63)

$\forall x(P \to Q) \to (\forall x P \to \forall x Q)$; (64)

$\forall x(P \to Q) \to (\exists x P \to \exists x Q)$; (65)

$P \to \forall x P$ (provided x is not free in P); (66)

$\exists x P \to P$ (provided x is not free in P); (67)

$\forall x P \to P(x/t)$ (where t is free for x in $P(x)$); (68)

$P(x/t) \to \exists x P$ (where t is free for x in $P(x)$); (69)

All *generalizations* of axioms of the preceding groups. (70)

Remember that by a generalization of P we mean any formula of the form $\forall x_1 \ldots \forall x_k(P)$, where $k \geq 1$ and $x_1, \ldots, x_k$ are variables not necessarily different.

To prove the completeness of *I-CED*, we will define a translation α from the language of *I-CED* into the language of *BM* and will prove the following claims.

Claim 1 If P is an intuitionistically valid formula in the language of *I-CED*, then αP is intuitionistically valid too.

Claim 2 If P is provable in *BM*, then P is provable in *I-CED*.

Claim 3 For any formula P in the language of *I-CED*, $\alpha P \equiv P$ is provable in *I-CED*.

Since *BM* is complete, the completeness of *I-CED* follows from Claims 1–3.

The translation α is defined as follows:

1. $\alpha P = P$ if P is atomic,
2. $\alpha\top = R \to R$, for some propositional symbol R,
3. $\alpha\bot = \neg\alpha\top$,
4. $\alpha(P \equiv Q) = (\alpha P \to \alpha Q) \wedge (\alpha Q \to \alpha P)$,
5. $\alpha(P \wedge Q) = \alpha P \wedge \alpha Q$,
6. $\alpha(P \vee Q) = \alpha P \vee \alpha Q$,
7. $\alpha\forall x(P) = \forall x \alpha P$,
8. $\alpha\exists x(P) = \exists x \alpha P$.

Claim 1 follows from the fact that αP is semantically equivalent to P, which is easy to check by structural induction, since, as we mentioned before, for any forcing frame on the language of *I-CED*, $\top$ is forced by every state, and forcing an equivalence in a state is understood as forcing the conjunction of the associated implications in that same state.

In order to verify Claim 2, we first prove in *I-CED*, *BM*'s axioms (53) – (62), and (64) – (69).

Proof of (53)

$$
\begin{array}{ll}
 & P \to (Q \to P) \\
\Leftrightarrow & \{(11)\text{: coupling}\} \\
 & P \wedge Q \to P \\
\Leftrightarrow & \{(34)\text{; Theorem } 2.2\} \\
 & \top\,.
\end{array}
$$

Proof of (54)

$$
\begin{aligned}
& (P \to (Q \to R)) \to ((P \to Q) \to (P \to R)) \\
\Leftrightarrow\ & \{(11)\text{: coupling}\} \\
& (P \to (Q \to R)) \wedge (P \to Q) \to (P \to R) \\
\Leftrightarrow\ & \{(11)\text{: coupling}\} \\
& (P \wedge Q \to R) \wedge (P \to Q) \to (P \to R) \\
\Leftrightarrow\ & \{(11)\text{: coupling}\} \\
& (P \wedge Q \to R) \wedge (P \to Q) \wedge P \to R \\
\Leftrightarrow\ & \{(12)\text{: compression}\} \\
& (P \wedge Q \to R) \wedge P \wedge Q \to R \\
\Leftrightarrow\ & \{(12)\text{: compression}\} \\
& P \wedge Q \wedge R \to R \\
\Leftrightarrow\ & \{(34)\text{; Theorem 2.2}\} \\
& \top\,.
\end{aligned}
$$

Proof of (55)

$$
\begin{aligned}
& P \to (Q \to P \wedge Q) \\
\Leftrightarrow\ & \{(11)\text{: coupling}\} \\
& P \wedge Q \to P \wedge Q \\
\Leftrightarrow\ & \{(33)\text{: reflexivity of } \to\text{; Theorem 2.2}\} \\
& \top\,.
\end{aligned}
$$

Proof of (56) (56) coincides with theorem schema (34).
Proof of (57) It is an easy consequence of (34) and commutativity of $\wedge$.
Proof of (58) (58) coincides with theorem schema (35).
Proof of (59) It is an easy consequence of (35) and commutativity of $\vee$.

Proof of (60)

$$
\begin{aligned}
& (P \to R) \to ((Q \to R) \to (P \vee Q \to R)) \\
\Leftrightarrow\ & \{(11)\text{: coupling}\} \\
& (P \to R) \wedge (Q \to R) \to (P \vee Q \to R) \\
\Leftrightarrow\ & \{(42)\} \\
& (P \vee Q \to R) \to (P \vee Q \to R) \\
\Leftrightarrow\ & \{(33)\text{: reflexivity of } \to\text{; Theorem 2.2}\} \\
& \top\,.
\end{aligned}
$$

Proof of (61)

$$
\begin{aligned}
& (P \to Q) \to ((P \to \neg Q) \to \neg P) \\
\Leftrightarrow\ & \{(11)\text{: coupling}\} \\
& (P \to Q) \wedge (P \to \neg Q) \to \neg P \\
\Leftrightarrow\ & \{(38)\} \\
& (P \to Q \wedge \neg Q) \to \neg P \\
\Leftrightarrow\ & \{(41)\text{: contradiction}\} \\
& (P \to \bot) \to \neg P \\
\Leftrightarrow\ & \{(32)\text{; } (8)\text{: identity of } \wedge\text{; Theorem 2.2}\} \\
& (\bot \to P) \wedge (P \to \bot) \to \neg P \\
\Leftrightarrow\ & \{(10)\text{; notation: definition of } \neg\} \\
& \neg P \to \neg P \\
\Leftrightarrow\ & \{(33)\text{: reflexivity of } \to\text{; Theorem 2.2}\} \\
& \top\,.
\end{aligned}
$$

Proof of (62)

$$
\begin{array}{ll}
 & \neg P \to (P \to Q) \\
\Leftrightarrow & \{(11)\text{: coupling}\} \\
 & \neg P \wedge P \to Q \\
\Leftrightarrow & \{(41)\text{: contradiction}\} \\
 & \bot \to Q \\
\Leftrightarrow & \{(32)\text{; Theorem 2.2}\} \\
 & \top\,.
\end{array}
$$

Proof of (64) (64) coincides with axiom schema (18).
Proof of (65) (65) coincides with axiom schema (19).

Proof of (66) We suppose x is not free in P.

$$
\begin{array}{ll}
 & P \\
\Leftrightarrow & \{(16)\} \\
 & \forall x\, P \\
\Rightarrow & \{(33)\text{: reflexivity of} \to\} \\
 & \forall x\, P\,.
\end{array}
$$

Proof of (67) We suppose x is not free in P.

$$
\begin{array}{ll}
 & \exists x\, P \\
\Leftrightarrow & \{(17)\} \\
 & P \\
\Rightarrow & \{(33)\text{: reflexivity of} \to\} \\
 & P\,.
\end{array}
$$

Proof of (68) Assuming t free for x in $P(x)$,

$$
\begin{array}{ll}
 & \forall x\, P \to P(x/t) \\
\Leftrightarrow & \{(39)\} \\
 & \forall x\, P \wedge P(x/t) \;\equiv\; \forall x\, P \\
\Leftrightarrow & \{(14)\} \\
 & \top\,.
\end{array}
$$

Proof of (69) Assuming t free for x in $P(x)$,

$$
\begin{array}{ll}
 & P(x/t) \to \exists x\, P \\
\Leftrightarrow & \{(9)\} \\
 & P(x/t) \vee \exists x\, P \;\equiv\; \exists x\, P \\
\Leftrightarrow & \{(15)\} \\
 & \top\,.
\end{array}
$$

Now we can prove Claim 2 by induction on the proof of P in *BM*. We have proved axioms (53)–(62) and (64)–(69) of *BM* as theorems of *I-CED*. Furthermore, we have proved that modus ponens is a derived inference rule in *I-CED*; besides this, requirements (63) and (70) of *BM* are compatible with (13) and (21) in *I-CED*.

Claim 3 is proved by structural induction. If P is an atomic formula then $\alpha P \equiv P$ is an instance of (22). If P is $\top$ then $\alpha P \equiv (R \to R)$ so the equivalence to prove is $(R \to R) \equiv \top$. This formula follows from (33), Theorem 2.2, and (2). Similarly, if P is $\bot$, then $\alpha P \equiv \neg(R \to R)$ so that the equivalence to prove is $\neg(R \to R) \equiv \bot$.

This follows from (33), Theorem 2.2, and (31). Assume now that $\alpha P \equiv P$ and $\alpha Q \equiv Q$ are provable in *I-CED*. We need to verify that

$$\alpha(P \equiv Q) \equiv (P \equiv Q), \tag{71}$$

$$\alpha(P \wedge Q) \equiv (P \wedge Q), \tag{72}$$

and

$$\alpha(P \vee Q) \equiv (P \vee Q) \tag{73}$$

are provable in *I-CED* too.

Proof of (71)

$$\begin{array}{ll} & \alpha(P \equiv Q) \\ = & \{\text{definition of } \alpha\} \\ & (\alpha P \to \alpha Q) \wedge (\alpha Q \to \alpha P) \\ \Leftrightarrow & \{\text{induction hypothesis}\} \\ & (P \to Q) \wedge (Q \to P) \\ \Leftrightarrow & \{(10)\} \\ & P \equiv Q. \end{array}$$

(The expressions connected with the equal sign represent the same formula; these transitions do not correspond to derivation steps.)

Proof of (72)

$$\begin{array}{ll} & \alpha(P \wedge Q) \\ = & \{\text{definition of } \alpha\} \\ & \alpha P \wedge \alpha Q \\ \Leftrightarrow & \{\text{induction hypothesis}\} \\ & P \wedge Q. \end{array}$$

The proof of (73) is similar to the one of (72).

Finally, assuming that $\alpha P \equiv P$ is provable in *I-CED*, we need to check that $\forall x P \equiv \alpha \forall x P$ and that $\exists x P \equiv \alpha \exists x P$ are provable in *I-CED* too. Actually, these two formulas can be written as $\forall x P \equiv \forall x \alpha P$ and $\exists x P \equiv \exists x \alpha P$, respectively. We prove the first of them; the proof of the other one is similar. By (21) and our assumption, we can suppose that $\forall x(\alpha P \equiv P)$ is provable in *I-CED*. Then

$$\begin{array}{ll} & \forall x(\alpha P \equiv P) \\ \Leftrightarrow & \{(10)\} \\ & \forall x((\alpha P \to P) \wedge (P \to \alpha P)) \\ \Leftrightarrow & \{(47)\} \\ & \forall x(\alpha P \to P) \wedge \forall x(P \to \alpha P) \\ \Rightarrow & \{(18), (43)\} \\ & (\forall x \alpha P \to \forall x P) \wedge (\forall x P \to \forall x \alpha P) \\ \Leftrightarrow & \{(10)\} \\ & \forall x \alpha P \equiv \forall x P; \end{array}$$

by modus ponens rule, we obtain $\forall x \alpha P \equiv \forall x P$ as planned.

Proof of Leibniz's Principle We prove it by structural induction. Suppose A and B are formulas free for propositional variable p. If E is a logical constant, an atomic formula, or a propositional variable different from p, then (48) reduces to $(A \equiv B) \to (E \equiv E)$. This formula follows from (32) using (33) and Theorem 2.2. If E coincides with p, then (48) reduces to $(A \equiv B) \to (A \equiv B)$, which is an instance of (33). Assume now that $(A \equiv B) \to (Q(p/A) \equiv Q(p/B))$ and $(A \equiv B) \to (R(p/A) \equiv R(p/B))$. First, we need to verify that

$$(A \equiv B) \to ((Q(p/A) \equiv R(p/A)) \equiv (Q(p/B) \equiv R(p/B))), \tag{74}$$

$$(A \equiv B) \to (Q(p/A) \wedge R(p/A) \equiv Q(p/B) \wedge R(p/B)), \tag{75}$$

and

$$(A \equiv B) \to (Q(p/A) \vee R(p/A) \equiv Q(p/B) \vee R(p/B)) \tag{76}$$

are provable in *I-CED*.

Proof of (74) By (38) and rule ($\wedge$-Int), it is sufficient to prove

(a) $(A \equiv B) \to ((Q(p/A) \equiv R(p/A)) \to (Q(p/B) \equiv R(p/B)))$ and
(b) $(A \equiv B) \to ((Q(p/B) \equiv R(p/B)) \to (Q(p/A) \equiv R(p/A)))$.

We prove (a). Proofs of (a) and (b) are symmetrical.

$$\begin{array}{ll} & (A \equiv B) \to ((Q(p/A) \equiv R(p/A)) \to (Q(p/B) \equiv R(p/B))) \\ \Leftrightarrow & \{(11)\text{: coupling}\} \\ & (A \equiv B) \wedge (Q(p/A) \equiv R(p/A)) \to (Q(p/B) \equiv R(p/B)) \end{array}$$

and then

$$\begin{array}{ll} & (A \equiv B) \wedge (Q(p/A) \equiv R(p/A)) \\ \Rightarrow & \{\text{inductive hypothesis; } (46)\} \\ & (Q(p/A) \equiv Q(p/B)) \wedge (R(p/A) \equiv R(p/B)) \wedge (Q(p/A) \equiv R(p/A)) \\ \Rightarrow & \{(44)\text{: transitivity of } \equiv\} \\ & (Q(p/B) \equiv R(p/A)) \wedge (R(p/A) \equiv R(p/B)) \\ \Rightarrow & \{(44)\text{: transitivity of } \equiv\} \\ & Q(p/B) \equiv R(p/B). \end{array}$$

Proof of (75)

$$\begin{array}{ll} & A \equiv B \\ \Rightarrow & \{\text{inductive hypothesis; } (5), (43)\} \\ & (Q(p/A) \equiv Q(p/B)) \wedge (R(p/A) \equiv R(p/B)) \\ \Rightarrow & \{(46)\} \\ & Q(p/A) \wedge R(p/A) \equiv Q(p/B) \wedge R(p/B). \end{array}$$

Proof of (76)

$$\begin{array}{ll} & A \equiv B \\ \Rightarrow & \{\text{inductive hypothesis; } (5), (43)\} \\ & (Q(p/A) \equiv Q(p/B)) \wedge (R(p/A) \equiv R(p/B)) \\ \Rightarrow & \{(45)\} \\ & Q(p/A) \vee R(p/A) \equiv Q(p/B) \vee R(p/B). \end{array}$$

Finally, assuming $(A \equiv B) \to (Q(p/A) \equiv Q(p/B))$ is provable in *I-CED*, and that A, B are free for a propositional variable in $Q(p)$, we need to show that

$$(A \equiv B) \to (\forall x\, Q(p/A) \equiv \forall x\, Q(p/B)) \tag{77}$$

and

$$(A \equiv B) \to (\exists x\, Q(p/A) \equiv \exists x\, Q(p/B)). \tag{78}$$

We prove (78). The proof of (77) is similar. From our assumption and the generalization rule (21), we have that $\forall x((A \equiv B) \to (Q(p/A) \equiv Q(p/B)))$ is also provable in *I-CED*, and since

$$\begin{array}{ll} & \forall x((A \equiv B) \to (Q(p/A) \equiv Q(p/B))) \\ \Rightarrow & \{(18)\} \\ & \forall x(A \equiv B) \to \forall x(Q(p/A) \equiv Q(p/B)) \\ \Leftrightarrow & \{(16);\ A,\ B \text{ are free for } x \text{ by assumption}\} \\ & (A \equiv B) \to \forall x(Q(p/A) \equiv Q(p/B)), \end{array}$$

we have that

$$(A \equiv B) \to \forall x(Q(p/A) \equiv Q(p/B)) \tag{79}$$

is also provable in *I-CED*. Therefore,

$$\begin{array}{ll} & A \equiv B \\ \Rightarrow & \{(79)\} \\ & \forall x(Q(p/A) \equiv Q(p/B)) \\ \Leftrightarrow & \{(10)\} \\ & \forall x((Q(p/A) \to Q(p/B)) \wedge (Q(p/B) \to Q(p/A))) \\ \Leftrightarrow & \{(47)\} \\ & \forall x(Q(p/A) \to Q(p/B)) \wedge \forall x(Q(p/B) \to Q(p/A)) \\ \Rightarrow & \{(19), (43)\} \\ & (\exists x\, Q(p/A) \to \exists x\, Q(p/B)) \wedge (\exists x\, Q(p/B) \to \exists x\, Q(p/A)) \\ \Leftrightarrow & \{(10)\} \\ & \exists x\, Q(p/A) \equiv \exists x\, Q(p/B), \end{array}$$

as we wanted to prove.

Notes

1. We could have given "more equational" versions for axiom schemas (18) and (19) related with axiom schema (10), but for the sake of briefness we chose not to do it.

2. An inference rule is *derivable* in a deductive system Σ if the conclusion (of any instance) of such rule is derivable from its premises in Σ.

References

[1] Backhouse, R., "Mathematics and Programming. A Revolution in the Art of Effective Reasoning," 2001. http://www.cs.nott.ac.uk/~rcb/inaugural.pdf 362

[2] Backhouse, R., *Program Construction: Calculating Implementations from Specifications*, John Wiley and Sons, Inc., Hoboken, 2003. 362

[3] Bell, J. L., and M. Machover, *A Course in Mathematical Logic*, North-Holland Publishing Co., Amsterdam, 1977. Zbl 0359.02001. MR 0472455. 376

[4] Bijlsma, L., and R. Nederpelt, "Dijkstra-Scholten predicate calculus: Concepts and misconceptions," *Acta Informatica*, vol. 35 (1998), pp. 1007–1036. Zbl 0917.68142. MR 1661953. 362

[5] Birkhoff, G., *Lattice Theory*, 3d edition, vol. 25 of *American Mathematical Society Colloquium Publications*, American Mathematical Society, Providence, 1979. Zbl 0505.06001. MR 598630. 368

[6] Bohorquez, J., and C. Rocha, "Towards the effective use of formal logic in the teaching of discrete math," 6th International Conference on Information Technology Based Higher Education and Training (ITHET), 2005. 362

[7] Dijkstra, E. W., "Boolean connectives yield punctual expressions," EWD 1187 in *The Writings of Edsger W. Dijkstra*, 2000. 371

[8] Dijkstra, E. W., and C. S. Scholten, *Predicate Calculus and Program Semantics*, Texts and Monographs in Computer Science, Springer-Verlag, New York, 1990. Zbl 0698.68011. MR 1028545. 362, 368

[9] Gries, D., and F. B. Schneider, *A Logical Approach to Discrete Math*, Texts and Monographs in Computer Science, Springer-Verlag, New York, 1993. Zbl 0861.03001. MR 1247233. 362, 371

[10] Gries, D., and F. B. Schneider, "Equational propositional logic," *Information Processing Letters*, vol. 53 (1995), pp. 145–52. Zbl 0875.03034. MR 1315198. 362

[11] Gries, D., and F. B. Schneider, "Formalizations of Substitution of Equals for Equals," Technical Report TR98-1686, Cornell University-Computer Science, Ithaca, 1998. 362

[12] Lifschitz, V., "On calculational proofs (First St. Petersburg Conference on Days of Logic and Computability, 1999)," *Annals of Pure and Applied Logic*, vol. 113 (2002), pp. 207–24. Zbl 0992.03069. MR 1875744. 362

[13] Nerode, A., "Some lectures on intuitionistic logic," pp. 12–59 in *Logic and Computer Science (Montecatini Terme, 1988)*, edited by A. Dold, B. Eckmann, and F. Takens, vol. 1429 of *Lecture Notes in Mathematics*, Springer, Berlin, 1990. Zbl 0703.03001. MR 1074800. 365

[14] Rasiowa, H., and R. Sikorski, *The Mathematics of Metamathematics*, 3d edition, Monografie Matematyczne, Tom 41. PWN-Polish Scientific Publishers, Warsaw, 1970. Zbl 0122.24311. MR 0344067. 368

[15] Simmons, G. F., *Introduction to Topology and Modern Analysis*, Robert E. Krieger Publishing Co. Inc., Melbourne, 1983. Reprint of the 1963 original. Zbl 0495.46001. MR 695310. 368

[16] Tourlakis, G., "A basic formal equational predicate logic," Technical Report CS1998-09, York University-Computer Science, Toronto,1998. 362

[17] Tourlakis, G., "On the soundness and completeness of equational predicate logics," *Journal of Logic and Computation*, vol. 11 (2001), pp. 623–53. Zbl 1006.03007. MR 1864606. 362

Acknowledgments

The author thanks Vladimir Lifschitz and Camilo Rocha for suggestions to improve the presentation of this paper. He also thanks Jorge Villalobos and Michael Katelman for their advice about writing and stylistic matters concerning this note.

Escuela Colombiana de Ingeniería
AK 45 # 205 - 59
Bogotá
COLOMBIA
jaime.bohorquez@escuelaing.edu.co