Equational Propositional Logic

David Gries [1] and Fred B. Schneider [2]
Computer Science, Cornell University

September 1994

Abstract

We formalize equational propositional logic, prove that it is sound and complete, and compare the equational-proof style with the more traditional Hilbert style.

Keywords: Logic, equational reasoning, soundness, completeness.

1 Introduction

Equational calculations have been used extensively over the past 15–20 years by researchers in the formal development of programs. The equational style makes it possible to develop and present calculations in a rigorous manner, without complexity and detail overwhelming (in contrast to other proof styles). Undergraduate text [4] formalizes this equational style for a propositional logic and a predicate logic and then uses the style in presenting the topics typically found in undergraduate discrete-math courses. Logic becomes a tool, rather than simply an object of study as it has been in the past.

In this paper, we prove that equational propositional logic **E** of [4] is sound (with respect to the conventional model of evaluation of boolean expressions) and complete. Proofs in **E** can be presented in either the Hilbert style or the equational style. We explain both styles and argue that the equational style is superior.

2 Preliminaries

We use conventional notation for propositional (boolean) expressions, with a few modifications. The single unary operator is $\neg$ (not). The binary operators

[1] Supported by the NSF under grant CDA-9214957 and ARPA under ONR grant N00014-91-J-4123.

[2] Supported by ONR under contract N00014-91-J-1219, AFOSR under grant F49620-94-1-0198, NSF under grant CCR-8701103, and ARPA/NSF grant CCR-9014363.

Table 1: Table of Precedences

(a)	$[x := e]$ (textual substitution)	(highest precedence)
(b)	$= \;\; \neq$	(conjunctional)
(c)	$\vee \;\; \wedge$	
(d)	$\Rightarrow \;\; \Leftarrow \;\; \not\Rightarrow \;\; \not\Leftarrow$	
(e)	$\equiv \;\; \not\equiv$	(lowest precedence)

Nonassociative infix operators associate to the left, except $\Rightarrow$, which associates to the right.

A slash / through an operator denote its negation —e.g. $b \not\equiv c$ is an abbreviation for $\neg(b \equiv c)$.

are $\equiv$ or $=$ (equality), $\vee$ (or, disjunction), $\wedge$ (and, conjunction), $\Rightarrow$ (implication), and $\Leftarrow$ (consequence). Operators $\equiv$, $=$, $\Rightarrow$, and $\Leftarrow$ may have a slash through them to denote their negation —e.g. $b \not\equiv c$ is equivalent to $\neg(b \equiv c)$. Precedences for these operators are given in Table 1.

We use two symbols for equality: $=$ and $\equiv$. We regard $=$ as *conjunctional*: $b = c = d$ is shorthand for $b = d \;\wedge\; c = d$. Operation $\equiv$, on the other hand, is used associatively[3]: $b \equiv c \equiv d$ is equivalent to $(b \equiv c) \equiv d$ and to $b \equiv (c \equiv d)$.

Throughout, we allow the implicit replacement of $=$ for $\equiv$ and vice versa as needed, the only restriction being that a replacement not change the meaning of an expression. This can be ensured by introducing parentheses around every subexpression before making the replacement —i.e. $((b) = (c))$ and $((b) \equiv (c))$ are interchangeable.

Let E and R be expressions and x be a variable. The notation $E[x := R]$ denotes *textual substitution*: $E[x := R]$ is an expression that is the same as E but with all occurrences of x replaced by "(R)". Textual substitution can be defined recursively on the structure of expressions; we leave this definition to the reader.

For x a list $x_1, \ldots, x_n$ of distinct variables and R a list $R_1, \ldots, R_n$ of expressions, $E[x := R]$ denotes the *simultaneous textual substitution* in E of the variables of x by the corresponding expressions of R.

[3] Equivalence of booleans is indeed associative, a fact that has not been used much in past. For example, Rosser [5] uses equivalence only conjunctionally. The implicit use of associativity (and symmetry) of $\equiv$ can simplify manipulations quite a bit, just as the implicit use of associativity and symmetry of $+$ simplifies numerical calculations.

[4] Walter Potter has shown that Symmetry of $\vee$ can be proved from the other axioms.

Table 2: Axioms of Logic **E**

(1) **Associativity of $\equiv$:** $((p \equiv q) \equiv r) \ \equiv \ (p \equiv (q \equiv r))$

(2) **Symmetry of $\equiv$:** $p \equiv q \equiv q \equiv p$

(3) **Identity of $\equiv$:** $true \equiv q \equiv q$

(4) **Definition of $false$:** $false \equiv \neg true$

(5) **Distributivity of $\neg$ over $\equiv$:** $\neg(p \equiv q) \ \equiv \ \neg p \equiv q$

(6) **Definition of $\not\equiv$:** $(p \not\equiv q) \ \equiv \ \neg(p \equiv q)$

(7) **Associativity of $\vee$:** $(p \vee q) \vee r \ \equiv \ p \vee (q \vee r)$

(8) **Symmetry of $\vee$ [4]:** $p \vee q \ \equiv \ q \vee p$

(9) **Idempotency of $\vee$:** $p \vee p \ \equiv \ p$

(10) **Distributivity of $\vee$ over $\equiv$:** $p \vee (q \ \equiv \ r) \ \equiv \ p \vee q \ \equiv \ p \vee r$

(11) **Excluded Middle:** $p \vee \neg p$

(12) **Golden rule:** $p \wedge q \ \equiv \ p \ \equiv \ q \ \equiv \ p \vee q$

(13) **Implication:** $p \Rightarrow q \ \equiv \ p \vee q \ \equiv \ q$

(14) **Consequence:** $p \Leftarrow q \ \equiv \ q \Rightarrow p$

(15) **Anti-implication:** $p \not\Rightarrow q \ \equiv \ \neg(p \Rightarrow q)$

(16) **Anti-consequence:** $p \not\Leftarrow q \ \equiv \ \neg(p \Leftarrow q)$

3 Propositional logic E

The inference rules of logic **E** are given by the following four inference-rule schema. Instantiating E, P, Q, and R with expressions and r with a variable in any of these schema results in an inference rule.

$$\textbf{Leibniz: } \frac{P = Q}{E[r := P] = E[r := Q]} \qquad \textbf{Substitution: } \frac{P}{P[r := Q]}$$

$$\textbf{Transitivity: } \frac{P = Q, \ Q = R}{P = R} \qquad \textbf{Equanimity: } \frac{P, \ P \ \equiv \ Q}{Q}$$

The axioms of logic **E** are given in Table 2. Note that these are expressions, not schemas. Rule Substitution can be used to generate as theorems instances of these expressions in which variables are replaced by particular expressions.

A *theorem* of logic **E** is either an axiom or the conclusion of an inference rule whose premises are (previously proved) theorems [5]. Text [4] contains proofs of many theorems of **E**, and we will refer to them when necessary in this article. Also, we use symmetry and associativity of operators transparently, without mention.

4 Equational versus Hilbert-style proofs

A Hilbert-style proof consists of a sequence of expressions; each expression is a theorem because of one of the following:

- It is an axiom. To its right appears a reference to the axiom.
- It is the conclusion of an inference rule whose premises appear previously in the sequence, are axioms, or are previously proved theorems. To its right appears the name of the inference rule and references to the premises.

As an example, we give a proof of a law of absorption, $p \wedge (p \vee q) \equiv p$.

1	$p \equiv p \vee p$	Idempotency of $\vee$ (9)
2	$p \vee q \equiv p \vee p \vee q$	Leibniz, 1
3	$p \wedge q \equiv p \equiv q \equiv p \vee q$	Golden rule (12)
4	$p \wedge (p \vee q) \equiv p \equiv p \vee q \equiv p \vee p \vee q$	Substitution, 3
5	$p \wedge (p \vee q) \equiv p$	Equanimity, 2, 4

This proof suffers, as do most Hilbert-style proofs, because no motivation is given for each line —there appears to be no rhyme or reason for each step. How did we know to start with axiom Idempotency? Why was the second expression written? There are two inherent difficulties with such proofs: (i) they build up to the final theorem in a bottom-up fashion, giving little pieces without saying how the pieces will fit together, and (ii) there is little structure to the proof. It is difficult to develop such proofs and to understand them.

We now present a proof in the equational style for the same theorem. The proof consists of a series of applications of inference rule Leibniz, linked implicitly by Transitivity. For example, the last three lines of the following proof indicate that $(p \vee q \equiv p \vee p \vee q) = (p \vee q \equiv p \vee q)$ is a theorem because it is the conclusion of an instance of Leibniz whose premise is Idempotency of $\vee$ (9), $p \vee p \equiv p$.

[5] In [4], only the first three inference rules are given, and Equanimity is accounted for in the definition of theorem. Here, we have added Equanimity so that the more conventional definition of a theorem could be used.

$$\begin{array}{ll}
 & p \wedge (p \vee q) \ \equiv\ p \\
= & \quad \langle \text{Golden rule, with } q := p \vee q \,\rangle \\
 & p \vee q \ \equiv\ p \vee p \vee q \\
= & \quad \langle \text{Idempotency of } \vee \ (9),\ p \vee p \ \equiv\ p \rangle \\
 & p \vee q \ \equiv\ p \vee q \ \text{—Reflexivity of } \equiv \ (3.5) \text{ of [4]}
\end{array}$$

In the equational style,

$$\begin{array}{ll}
 & E[r := P] \\
= & \quad \langle\, P \ \equiv\ Q \,\rangle \\
 & E[r := Q]
\end{array}$$

indicates a use of inference rule Leibniz with premise $P \equiv Q$.

Substitution is most frequently used to create a theorem that is a premise of Leibniz. For example, the premise of Leibniz used in the first hint is the Golden rule with the textual substitution $q := p \vee q$. Substitution is often used without mention when it is obvious. For example, the last line of the proof above claims that $p \vee q \ \equiv\ p \vee q$ is theorem Reflexivity of $\equiv$. Well, it is really Reflexivity, $q \equiv q$, with the textual substitution $q := p \vee q$.

Inference rule Transitivity is used to conclude that the first expression of an equational proof is equivalent to the last (or vice versa). Often, this is what we want to prove: we prove some expression $P = Q$ by transforming P to Q (or Q to P) by a series of substitutions of equals for equals. In the proof above, one application of Transitivity yields the theorem $p \wedge (p \vee q) \ \equiv\ p \ \equiv\ p \vee q \ \equiv\ p \vee q$.

Finally, inference rule Equanimity is used in the above proof to conclude that the first expression $p \wedge (p \vee q) \ \equiv\ p$ is a theorem because it is equivalent to the last expression, which is a theorem. By convention, the implicit use of Equanimity is triggered by the last line being *true* or by a comment of the form "— . . . ", indicating that the last line is a previously proved theorem.

This equational proof is easy to read and remember because definite strategies are used in its construction. In developing the proof, we first noted that $\wedge$ and $\vee$ are juxtaposed in the first line, which is the expression to be proved. Removing this juxtaposition (using the Golden rule) simplified the expression. Next, the occurrence of $p \vee p$ cried out for removal using Idempotency. Finally, the instance of Reflexivity was easily recognized.

In the equational style of proof, the aim of each step is to change the expression using Leibniz, and the only task is to determine which equality (equivalence) to use. The shape of the expression and the already existing theorems give guidance. Consequently, proofs in this style are relatively easy to construct (and then to remember). Further, a number of simple but useful principles and strategies for developing proofs have been articulated (see [3, 4]), making it possible to teach the development of equational proofs.

The equational style has several other advantages over the Hilbert style. None of the inference rules need be mentioned explicitly in an equational proof, since each is used only in a particular way and only in a particular part of the proof. (Each step is an application of Leibniz, with perhaps a use of Substitution to generate the premise.) This reduces the amount of writing in presenting a proof and the amount of reading in understanding it.

The equational style is also more concise than the Hilbert style because expressions do not have to be repeated as often. For example, suppose a proof first proves $P \equiv Q$ using Leibniz, then $Q \equiv R$ using Leibniz, and finally $P \equiv R$ using Transitivity. In the Hilbert style, each of P , Q , and R appears twice; in the equational style, each appears only once. As expressions become longer, this advantage becomes more important.

Translating equational proofs into the Hilbert style

A proof in the equational style can be translated mechanically into the Hilbert style. We illustrate this with an example. A proof of the form

$$\begin{array}{ll}
 & P0 \\
= & \quad \langle \text{reference to a theorem } F0 \text{, with } x0 := E0 \rangle \\
 & P1 \\
= & \quad \langle \text{reference to a theorem } F1 \text{, with } x1 := E1 \rangle \\
 & P2 \qquad \text{—reference to theorem } P2
\end{array}$$

is translated into

1	$F0[x0 := E0]$	Substitution, reference to theorem $F0$
2	$P0 = P1$	Leibniz, 1
3	$F1[x1 := E1]$	Substitution, reference to theorem $F1$
4	$P1 = P2$	Leibniz, 3
5	$P0 = P2$	Transitivity, 2, 4
6	$P0$	Equanimity, reference to theorem $P2$, 5

Thus, each step of the equational proof gives rise to a line of the Hilbert-style proof that uses Leibniz, with a preceding line (if necessary) that uses inference rule Substitution. And, for each two consecutive steps of the equational proof, there is a line of the Hilbert-style proof that uses inference rule Transitivity to establish that the first and last expressions are equal. In addition, if the last line of the equational proof is a theorem (it is either *true* or contains a reference to that theorem), then the last line of the Hilbert-style proof contains the *first* expression of the equational proof, substantiated using inference rule Equanimity.

5 Soundness of E

The standard interpretation of boolean expressions concerns evaluating expressions in states, where a state is a mapping of all identifiers in the expression to the values **t** or **f**. For a state s, the value $s[\![P]\!]$ of an expression P in state s is given by:

(17) $s[\![true]\!] = \mathbf{t}$

(18) $s[\![false]\!] = \mathbf{f}$

(19) $s[\![x]\!] = s.x$ (for variable x, $s.x$ denotes the value of x in state s)

(20) $s[\![\neg P]\!] = \neg s[\![P]\!]$

(21) $s[\![P \circ Q]\!] = s[\![P]\!] \circ s[\![Q]\!]$ (for any binary operator $\circ$)

In addition, for c and d constants (either **t** or **f**), the expressions $\neg c$, $c \wedge d$, $c \vee d$, etc., have their usual values, as shown in the following truth table.

b	c	$\neg b$	$b \equiv c$	$b \not\equiv c$	$b \vee c$	$b \wedge c$	$b \Rightarrow c$	$b \Leftarrow c$	$b \not\Rightarrow c$	$b \not\Leftarrow c$
t	**t**	**f**	**t**	**f**	**t**	**t**	**t**	**t**	**f**	**f**
t	**f**	**f**	**f**	**t**	**t**	**f**	**f**	**t**	**t**	**f**
f	**t**	**t**	**f**	**t**	**t**	**f**	**t**	**f**	**f**	**t**
f	**f**	**t**	**t**	**f**	**f**	**f**	**t**	**t**	**f**	**f**

Logic **E** is sound with respect the standard interpretation. To see this, first check that each axiom is valid. (This task we leave to the reader.) Second, for each inference rule, prove that if its premises are valid then so is its conclusion. These proofs appear in Appendix I.

6 Completeness of E

In [1], Church defines and proves complete a logic P_1 whose expressions are constructed from variables, implication operator $\Rightarrow$, and constant *false*. P_1 has inference rules Substitution and Modus Ponens and three axioms:

P$_1$ **Substitution:** $\dfrac{P}{P[r := Q]}$

P$_1$ **Modus Ponens:** $\dfrac{P,\ P \Rightarrow Q}{Q}$

$\mathbf{P}_1$ Axiom 0: $p \Rightarrow (q \Rightarrow p)$

$\mathbf{P}_1$ Axiom 1: $(s \Rightarrow (p \Rightarrow q)) \Rightarrow ((s \Rightarrow p) \Rightarrow (s \Rightarrow q))$

$\mathbf{P}_1$ Axiom 2: $((p \Rightarrow \mathit{false}) \Rightarrow \mathit{false}) \Rightarrow p$

We prove that the three axioms of P_1 are theorems of **E**.

P_1 Axiom 0 is theorem (4.1) of [4].

P_1 Axiom 1.

$$\begin{array}{ll}
 & (s \Rightarrow (p \Rightarrow q)) \Rightarrow ((s \Rightarrow p) \Rightarrow (s \Rightarrow q)) \\
= & \quad \langle \text{Shunting (3.65) of [4]}, \ p \wedge q \Rightarrow r \ \equiv \\
 & \qquad p \Rightarrow (q \Rightarrow r)\text{, twice} \rangle \\
 & (s \wedge p \Rightarrow q) \Rightarrow (s \wedge (s \Rightarrow p) \Rightarrow q) \\
= & \quad \langle \text{(3.66) of [4]}, \ x \wedge (x \Rightarrow y) \ \equiv \ x \wedge y \rangle \\
 & (s \wedge p \Rightarrow q) \Rightarrow (s \wedge p \Rightarrow q) \\
= & \quad \langle \text{Reflexivity of } \Rightarrow \text{ (3.71) of [4]} \rangle \\
 & \mathit{true}
\end{array}$$

P_1 Axiom 2.

$$\begin{array}{ll}
 & ((p \Rightarrow \mathit{false}) \Rightarrow \mathit{false}) \Rightarrow p \\
= & \quad \langle \text{(3.74) of [4]}, \ \neg p \ \equiv \ p \Rightarrow \mathit{false}\text{, twice} \rangle \\
 & \neg\neg p \Rightarrow p \\
= & \quad \langle \text{Double negation (3.12) of [4]} \rangle \\
 & p \Rightarrow p \\
= & \quad \langle \text{Reflexivity of } \Rightarrow \text{ (3.71) of [4]} \rangle \\
 & \mathit{true}
\end{array}$$

Moreover, Substitution of P_1 is an inference rule of **E**, and Modus Ponens is a derived inference rule[6] of **E**. To prove that Modus Ponens is a derived rule of **E**, we assume that $P \Rightarrow Q$ and P are theorems of E and prove that Q is a theorem. To do this, we first prove $\mathit{true} \equiv P$ (assuming P is a theorem).

$$\begin{array}{ll}
 & P \quad \text{—A given theorem} \\
= & \quad \langle \text{Identity of } \equiv \text{ (3)}, \ \mathit{true} \equiv q \equiv q \rangle \\
 & \mathit{true} \ \equiv \ P
\end{array}$$

$$\begin{array}{ll}
 & P \Rightarrow Q \quad \text{—A given theorem} \\
= & \quad \langle \ \mathit{true} \ \equiv \ P \text{ (proved above)} \rangle \\
 & \mathit{true} \Rightarrow Q \\
= & \quad \langle \text{Left identity of } \Rightarrow \text{ (3.73) of [4]}, \ \mathit{true} \Rightarrow p \ \equiv \ p \rangle \\
 & Q
\end{array}$$

[6] A derived inference rule is a rule that does not add theorems to the logic but simply allows some proofs to be shortened.

Since P_1 is complete, any valid expression that contains only variables, $\Rightarrow$, and *false* is a theorem of P_1. The above discussion shows that it is a theorem of **E** as well.

It remains to show that every valid expression that contains other operators and/or *false* is a theorem of **E**. To this end, we prove in Appendix II that the following definitions are theorems of **E**. (In [1], these expressions appear as abbreviations, e.g. P_1 views *true* as an abbreviation of $\mathit{false} \Rightarrow \mathit{false}$.)

$\mathbf{P}_1$ Definition of *true*: $\mathit{true} \equiv \mathit{false} \Rightarrow \mathit{false}$
$\mathbf{P}_1$ Definition of $\neg$: $\neg p \equiv p \Rightarrow \mathit{false}$
$\mathbf{P}_1$ Definition of $\nLeftarrow$: $p \nLeftarrow q \equiv \neg(q \Rightarrow p)$
$\mathbf{P}_1$ Definition of $\vee$: $p \vee q \equiv (p \Rightarrow q) \Rightarrow q$
$\mathbf{P}_1$ Definition of $\wedge$: $p \wedge q \equiv (p \nLeftarrow q) \nLeftarrow q$
$\mathbf{P}_1$ Definition of $\equiv$: $(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$
$\mathbf{P}_1$ Definition of $\not\equiv$: $(p \not\equiv q) \equiv (p \nLeftarrow q) \vee (q \nLeftarrow p)$
$\mathbf{P}_1$ Definition of $\Leftarrow$: $p \Leftarrow q \equiv q \Rightarrow p$
$\mathbf{P}_1$ Definition of $\nRightarrow$: $p \nRightarrow q \equiv q \nLeftarrow p$

Now consider a valid expression Q (say) that contains operators other than $\Rightarrow$ and/or *true*. The definitions given above, which are theorems of **E**, can be used (with Leibniz) to remove those other operators and *true* from Q, resulting in an equivalent, valid expression Q' that contains only variables, $\Rightarrow$, and *false*. The following informal use of our equational style, extended to allow implication in the left column, shows that Q is a theorem of **E**.

Q is valid
$=$ $\langle Q \equiv Q' \rangle$
Q' is valid
$\Rightarrow$ $\langle$Logic P_1 is complete$\rangle$
Q' is a theorem of P_1
$\Rightarrow$ $\langle$Every theorem of P_1 is a theorem of **E**$\rangle$
Q' is a theorem of **E**
$=$ $\langle Q \equiv Q'$; use inference rule Equanimity$\rangle$
Q is a theorem of **E**

Hence, every valid expression is a theorem of **E**, and **E** is complete.

Acknowledgements. We gratefully acknowledge the help of referees Wim Feijen and Lex Bijlsma and issue-editor Roland Backhouse.

References

[1] Church, A. *Introduction to Mathematical Logic.* Princeton University Press, Princeton, 1956.

[2] Dijkstra, E.W., and C.S. Scholten. *Predicate Calculus and Program Semantics.* Springer-Verlag, New York, 1990.

[3] van Gasteren, A.J.M. *On the Shape of Mathematical Arguments.* Doctoral thesis, Technical University Eindhoven, December 1988. LNCS 445, Springer Verlag, New York, 1990.

[4] Gries, D., and F.B. Schneider. *A Logical Approach to Discrete Math.* Springer-Verlag, New York, 1993.

[5] Rosser, B. *Logic for Mathematicians.* McGraw-Hill, New York, 1953.

Appendix I: Soundness of E

We prove that the inference rules of **E** preserve validity. We begin with a lemma that shows that textual substitution has the anticipated semantics. Write $(s; r : v)$ for the state that is the same as s except that at variable r its value is v. Then, evaluating $E[r := F]$ in a state s yields the same value as evaluating E in the state $(s; r{:}s[\![F]\!])$.

(22) **Lemma.** $s[\![E[r := F]]\!] = (s; r{:}s[\![F]\!])[\![E]\!]$.

Proof. The proof is by induction on the structure of expression E.

Case *true* **.**

$$\begin{array}{ll} & (s; r{:}s[\![F]\!])[\![true]\!] \\ = & \quad \langle \text{Definition (17) of } s[\![\cdots]\!] \rangle \\ & \mathbf{t} \\ = & \quad \langle \text{Definition (17) of } s[\![\cdots]\!] \rangle \\ & s[\![true]\!] \\ = & \quad \langle \text{Textual substitution} \rangle \\ & s[\![true[r := F]]\!] \end{array}$$

Case *false* **.** Similar to the case *true*.

Case r **.**

$$\begin{array}{ll} & (s; r{:}s[\![F]\!])[\![r]\!] \\ = & \quad \langle \text{Definition (19) of } s[\![\cdots]\!] \rangle \\ & (s; r{:}s[\![F]\!]).r \\ = & \quad \langle \text{Definition of } (s; r{:}v) \rangle \end{array}$$

$$\begin{array}{ll}
 & s\llbracket F\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket r[r:=F]\rrbracket
\end{array}$$

Case x (for x a variable different from r).

$$\begin{array}{ll}
 & (s;r\!:s\llbracket F\rrbracket)\llbracket x\rrbracket \\
= & \quad \langle \text{Definition (19) of } s\llbracket\cdots\rrbracket \rangle \\
 & (s;r\!:s\llbracket F\rrbracket).x \\
= & \quad \langle \text{Definition of } (s;r\!:v) \rangle \\
 & s\llbracket x\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket x[r:=F]\rrbracket
\end{array}$$

Case $\neg P$.

$$\begin{array}{ll}
 & (s;r\!:s\llbracket F\rrbracket)\llbracket \neg P\rrbracket \\
= & \quad \langle \text{Definition (20) of } s\llbracket\cdots\rrbracket \rangle \\
 & \neg(s;r\!:s\llbracket F\rrbracket)\llbracket P\rrbracket \\
= & \quad \langle \text{Inductive hypothesis — } P \text{ is a} \\
 & \quad\quad \text{proper subexpression of } \neg P \rangle \\
 & \neg s\llbracket P[r:=F]\rrbracket \\
= & \quad \langle \text{Definition (20) of } s\llbracket\cdots\rrbracket \rangle \\
 & s\llbracket(\neg(P[r:=F])\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket(\neg P)[r:=F]\rrbracket
\end{array}$$

Case $P \circ Q$. Similar to the above case.

(23) **Theorem.** Inference rule Substitution preserves validity.

Proof. We assume that P is valid and prove that $P[r:=F]$ is valid by showing that it evaluates to $\mathbf{t}$ in every state s .

$$\begin{array}{ll}
 & s\llbracket P[r:=F]\rrbracket \\
= & \quad \langle \text{Lemma (22)} \rangle \\
 & (s;r\!:s\llbracket F\rrbracket)\llbracket P\rrbracket \\
= & \quad \langle \text{Assumption that } P \text{ is valid} \rangle \\
 & \mathbf{t}
\end{array}$$

(24) **Theorem.** Inference rule Leibniz preserves validity.

Proof. Assume $P=Q$ is valid: $s\llbracket P=Q\rrbracket=\mathbf{t}$, for all states s . Equivalently, according to (21), $s\llbracket P\rrbracket = s\llbracket Q\rrbracket$ for all s . We have to prove that $E[r:=P] = E[r:=Q]$ is valid, i.e. for all states s , $s\llbracket E[r:=P]\rrbracket = s\llbracket E[r:=Q]\rrbracket$. The proof is by induction on the structure of E .

Case *true* **.**

$$\begin{array}{ll}
 & s\llbracket true[r := P]\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket true\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket true[r := Q]\rrbracket
\end{array}$$

Case *false* **.** Similar to the case *true* .

Case r **.**

$$\begin{array}{ll}
 & s\llbracket r[r := P]\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket P\rrbracket \\
= & \quad \langle \text{Assumption } s\llbracket P\rrbracket = s\llbracket Q\rrbracket \rangle \\
 & s\llbracket Q\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket r[r := Q]\rrbracket
\end{array}$$

Case x **(for** x **a variable different from** r **).**

$$\begin{array}{ll}
 & s\llbracket x[r := P]\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket x\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket x[r := Q]\rrbracket
\end{array}$$

Case $\neg R$ **.**

$$\begin{array}{ll}
 & s\llbracket (\neg R)[r := P]\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket \neg(R[r := P])\rrbracket \\
= & \quad \langle \text{Definition (20) of } s\llbracket \cdots \rrbracket \rangle \\
 & \neg s\llbracket R[r := P]\rrbracket \\
= & \quad \langle \text{Inductive hypothesis — } R \text{ is a} \\
 & \quad\quad \text{proper subexpression of } \neg R \rangle \\
 & \neg s\llbracket R[r := Q]\rrbracket \\
= & \quad \langle \text{Definition (20) of } s\llbracket \cdots \rrbracket \rangle \\
 & s\llbracket \neg(R[r := Q])\rrbracket \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & s\llbracket (\neg R)[r := Q]\rrbracket
\end{array}$$

Case $R0 \circ R1$ **.** Similar to the above case.

(25) **Theorem.** Inference rule Transitivity preserves validity.

Proof. Suppose $P = Q$ and $Q = R$ are valid. We show that $P = R$ is valid by proving that it evaluates to $\mathbf{t}$ in every state.

$$\begin{array}{ll}
& s\llbracket P = R \rrbracket \\
= & \quad \langle \text{Definition (21) of } s\llbracket \ldots \rrbracket \,\rangle \\
& s\llbracket P \rrbracket = s\llbracket R \rrbracket \\
= & \quad \langle\, s\llbracket P \rrbracket = s\llbracket Q \rrbracket \text{, since } P = Q \text{ is valid;} \\
& \qquad s\llbracket Q \rrbracket = s\llbracket R \rrbracket \text{, since } Q = R \text{ is valid} \rangle \\
& s\llbracket Q \rrbracket = s\llbracket Q \rrbracket \\
= & \quad \langle \text{Definition of } = \text{ (see truth table on page 7)} \rangle \\
& \mathbf{t}
\end{array}$$

(26) **Theorem.** Inference rule Equanimity preserves validity.

Proof. Suppose P and $P \equiv Q$ are valid. The following shows that $s\llbracket Q \rrbracket = \mathbf{t}$ in an arbitrary state s, so Q is valid. For arbitrary state s, we have

$$\begin{array}{ll}
& s\llbracket Q \rrbracket \\
= & \quad \langle\, P \equiv Q \text{ is valid} \rangle \\
& s\llbracket P \rrbracket \\
= & \quad \langle\, P \text{ is valid} \rangle \\
& \mathbf{t}
\end{array}$$

Appendix II: Proofs of the P_1 definitions

We prove that the axioms and abbreviations of P_1 are theorems of **E**. References are made to theorems of **E** proved in [4].

P_1 Definition of *true*, $true \equiv false \Rightarrow false$.

$$\begin{array}{ll}
& false \Rightarrow false \\
= & \quad \langle \text{Idempotency of } \wedge \text{ (3.38) of [4]} \rangle \\
& (false \Rightarrow false) \wedge (false \Rightarrow false) \\
= & \quad \langle \text{Mutual implication (3.80) of [4]} \rangle \\
& false \equiv false \text{ —Reflexivity of } \equiv \text{ (3.5) of [4]}
\end{array}$$

P_1 Definition of $\neg$, $\neg p \equiv p \Rightarrow false$. This is theorem (3.74) of [4].

P_1 Definition of $\not\Leftarrow$, $p \not\Leftarrow q \equiv \neg(q \Rightarrow p)$.

$$\begin{array}{ll}
& \neg(q \Rightarrow p) \\
= & \quad \langle \text{Definition of Consequence (3.58) of [4]} \rangle \\
& \neg(p \Leftarrow q) \\
= & \quad \langle \text{Definition of } \not\Leftarrow \text{ (see Table 1)} \rangle \\
& p \not\Leftarrow q
\end{array}$$

P_1 Definition of $\vee$, $p \vee q \equiv (p \Rightarrow q) \Rightarrow q$.

$$\begin{array}{ll}
 & (p \Rightarrow q) \Rightarrow q \\
= & \quad \langle \text{Implication (3.59) from [4], } p \Rightarrow q \equiv \neg p \vee q \text{, twice} \rangle \\
 & \neg(\neg p \vee q) \vee q \\
= & \quad \langle \text{De Morgan (3.47b) of [4]} \rangle \\
 & (\neg\neg p \wedge \neg q) \vee q \\
= & \quad \langle \text{Double negation (3.12) of [4]} \rangle \\
 & (p \wedge \neg q) \vee q \\
= & \quad \langle \text{Absorption (3.44b) of [4]} \rangle \\
 & p \vee q
\end{array}$$

P_1 Definition of $\wedge$, $p \wedge q \equiv (p \not\Leftarrow q) \not\Leftarrow q$.

$$\begin{array}{ll}
 & (p \not\Leftarrow q) \not\Leftarrow q \\
= & \quad \langle \text{Definition of } \not\Leftarrow \text{ in } \mathrm{P}_1 \text{ (proved above), twice} \rangle \\
 & \neg(q \Rightarrow \neg(q \Rightarrow p)) \\
= & \quad \langle \text{Implication (3.59) of [4], } p \Rightarrow q \equiv \neg p \vee q \text{, twice} \rangle \\
 & \neg(\neg q \vee \neg(\neg q \vee p)) \\
= & \quad \langle \text{De Morgan (3.47b) of [4]; Double negation (3.12) of [4], twice} \rangle \\
 & q \wedge (\neg q \vee p) \\
= & \quad \langle \text{Absorption (3.44a) of [4]} \rangle \\
 & q \wedge p
\end{array}$$

P_1 Definition of $\equiv$, $(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$. This is theorem Mutual implication (3.80) of [4].

P_1 Definition of $\not\equiv$, $(p \not\equiv q) \equiv (p \not\Leftarrow q) \vee (q \not\Leftarrow p)$.

$$\begin{array}{ll}
 & (p \not\Leftarrow q) \vee (q \not\Leftarrow p) \\
= & \quad \langle \text{Definition of } \not\Leftarrow \text{ in } \mathrm{P}_1 \text{ (proved above), twice} \rangle \\
 & \neg(q \Rightarrow p) \vee \neg(p \Rightarrow q) \\
= & \quad \langle \text{De Morgan (3.47a) of [4]} \rangle \\
 & \neg((q \Rightarrow p) \wedge (p \Rightarrow q)) \\
= & \quad \langle \text{Mutual implication (3.80) of [4]} \rangle \\
 & \neg(p \equiv q) \\
= & \quad \langle \text{Definition of } \not\equiv \text{ (see Table 1)} \rangle \\
 & (p \not\equiv q)
\end{array}$$

P_1 Definition of $\Leftarrow$, $p \Leftarrow q \equiv q \Rightarrow p$. This is axiom (3.58) of [4].

P_1 Definition of $\not\Rightarrow$, $p \not\Rightarrow q \equiv q \not\Leftarrow p$.

$$\begin{array}{ll}
 & q \not\Leftarrow p \\
= & \quad \langle \text{Definition of } \not\Leftarrow \text{ (see Table 1)} \rangle
\end{array}$$

$$
\begin{array}{ll}
 & \neg(q \Leftarrow p) \\
= & \quad \langle \text{Consequence (14)} \rangle \\
 & \neg(p \Rightarrow q) \\
= & \quad \langle \text{Definition of } \not\Rightarrow \text{ (15)} \rangle \\
 & p \not\Rightarrow q
\end{array}
$$