

"I have a proof that...."

This is about an observation of a type that I don't particularly like to make, but once the observation has been made, it had better be recorded. In the following, A and B stand for propositions for which I may have a proof.

Consider statements a_0 and a_1 :

- (a_0) I have a proof that true (holds)
 (a_1) true (holds) .

Then, a_0 and a_1 are equivalent. (Since -by definition- the proof that true (holds) is empty, it is impossible not to have it.)

Consider statements b_0 and b_1 :

- (b_0) I have a proof that false (holds)
 (b_1) false (holds) .

Then b_0 and b_1 are equivalent. (Since -by definition- the proof that false (holds) does not exist, it is impossible to have it.)

From the above we conclude by case analysis the equivalence of c_0 and c_1 :

- (c_0) I have a proof that I have a proof

that A (holds)

(c1) I have a proof that A (holds) .

Consider statements $d0$ and $d1$:

(d0) I have a proof that $A \wedge B$ (holds)

(d1) I have a proof that A (holds) and I have a proof that B (holds) .

Then $d0$ and $d1$ are equivalent. (Well, that is what " $\wedge$ " (= "and") means.)

This last law can be generalized to universal quantification. Consider statements $e0$ and $e1$ (in which the range for n is implicitly understood):

(e0) I have a proof that, for all n , $A.n$ (holds)

(e1) For all n , I have a proof that $A.n$ (holds) .

Then $e0$ and $e1$ are equivalent.

Remark As a result it is semantically irrelevant that the sentence "I have a proof of $A.n$ for all n " is syntactically ambiguous. (End of Remark.)

Consider the statements $f0$ and $f1$:

(f0) If I have a proof that A (holds)

then I have a proof that B (holds)
 (f_1) I have a proof that, if I have a proof
 that A holds, then B (holds) .

Then f_0 and f_1 are equivalent. (If I don't
 have a proof that A (holds), f_0 and f_1
 are both "vacuously" true ; if I do have a
 proof that A (holds), both f_0 and f_1 re-
 duce to "I have a proof that B (holds)".)

Remark As a result it is semantically irrel-
 evant that the sentence "I have a proof that
 B holds if I have a proof of A ." is
 syntactically ambiguous. (End of Remark.)

But consider now statements g_0 and g_1 :

(g_0) I have a proof that $A \vee B$ (holds)

(g_1) I have a proof that A (holds) or I
 have a proof that B (holds) or I
 have both proofs.

In this case, the two statements are not
 equivalent: g_1 implies g_0 , but it is in
 general not the other way round.

* * *

Let us now do away with all the above
 verbosity and abbreviate "I have a proof
 that A (holds)" to " $[A]$ ". Our laws
 about having proofs can then be summa-

alized as follows:

- (a) $[\underline{\text{true}}] \equiv \underline{\text{true}}$
- (b) $[\underline{\text{false}}] \equiv \underline{\text{false}}$
- (c) $[[A]] \equiv [A]$
- (d) $[A \wedge B] \equiv [A] \wedge [B]$
- (e) $[\langle \forall n :: A.n \rangle] \equiv \langle \forall n :: [A.n] \rangle$
- (f) $[A] \Rightarrow [B] \equiv [[A] \Rightarrow B]$
- (g) $[A \vee B] \leftarrow [A] \vee [B]$

The moral of the story is that "I have a proof that..." has all the algebraic properties of the "everywhere" operator, i.e. of universal quantification over a non-empty domain (see [DS90]).

[DS90] Dijkstra, Edsger W. and Scholten, Carel S.,
 "Predicate Calculus and Program Semantics",
 Springer-Verlag, New York, 1990.

Austin, 15 October 1995

prof. dr. Edsger W. Dijkstra
 Department of Computer Sciences
 The University of Texas at Austin
 Austin, TX 78712-1188
 USA