"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 a0 and a1:

(a0) I have a proof that <u>true</u> (holds)
(a1) <u>true</u> (holds) .

Then, a0 and a1 are equivalent. (Since —by definition— the proof that <u>true</u> (holds) is empty, it is impossible not to have it.)

Consider statements b0 and b1:

(b0) I have a proof that <u>false</u> (holds)
(b1) <u>false</u> (holds) .

Then b0 and b1 are equivalent. (Since —by definition— the proof that <u>false</u> (holds) does not exist, it is impossible to have it.)

From the above we conclude by case analysis the equivalence of c0 and c1:

(c0) 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.

<u>Remark</u> 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)

(f1) I have a proof that, if I have a proof that A holds, then B (holds) .

Then f0 and f1 are equivalent. (If I don't have a proof that A (holds), f0 and f1 are both "vacuously" <u>true</u>; if I do have a proof that A (holds), both f0 and f1 reduce to "I have a proof that B (holds)".)

<u>Remark</u> As a result it is semantically irrelevant 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 g0 and g1:

(g0) I have a proof that $A \vee B$ (holds)

(g1) 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 <u>not</u> equivalent: g1 implies g0, 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 summarized as follows:

(a) $[\underline{true}] \equiv \underline{true}$
(b) $[\underline{false}] \equiv \underline{false}$
(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