"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 \textbf{true} (holds)
(a1) \textbf{true} (holds).

Then, a0 and a1 are equivalent. (Since —by definition— the proof that \textbf{true} (holds) is empty, it is impossible not to have it.)

Consider statements b0 and b1:

(b0) I have a proof that \textbf{false} (holds)
(b1) \textbf{false} (holds).

Then b0 and b1 are equivalent. (Since —by definition— the proof that \textbf{false} (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)

(\( c_1 \)) I have a proof that \( A \) (holds).

Consider statements \( d_0 \) and \( d_1 \):

(\( d_0 \)) I have a proof that \( A \land B \) (holds)
(\( d_1 \)) I have a proof that \( A \) (holds) and I have a proof that \( B \) (holds).

Then \( d_0 \) and \( d_1 \) are equivalent. (Well, that is what "\( \land \)" (= "and") means.)

This last law can be generalized to universal quantification. Consider statements \( e_0 \) and \( e_1 \) (in which the range for \( n \) is implicitly understood):

(\( e_0 \)) I have a proof that, for all \( n \), \( A \cdot n \) (holds)
(\( e_1 \)) For all \( n \), I have a proof that \( A \cdot n \) (holds).

Then \( e_0 \) and \( e_1 \) are equivalent.

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

Consider the statements \( f_0 \) and \( f_1 \):

(\( f_0 \)) If I have a proof that \( A \) (holds)
then I have a proof that B (holds)
(g1) I have a proof that, if I have a proof
that A holds, then B (holds).

Then \( p_0 \) and \( p_1 \) are equivalent. (If I don't
have a proof that A (holds), \( p_0 \) and \( p_1 \)
are both "vacuously" true; if I do have a
proof that A (holds), both \( p_0 \) and \( p_1 \)
reduce 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 \( A \lor B \) (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-
rized as follows:

(a) \[ \text{true} \] \equiv \text{true} \\
(b) \[ \text{false} \] \equiv \text{false} \\
(c) \[ [A] \] \equiv [A] \\
(d) \[ A \land B \] \equiv [A] \land [B] \\
(e) \[ \langle \forall n :: A.n \rangle \] \equiv \langle \forall n :: [A.n] \rangle \\
(f) \[ A \implies B \] \equiv \[ [A] \implies B \] \\
(g) \[ A \lor B \] \equiv \[ [A] \lor [B] \]

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]).


Austin, 15 October 1995

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