Inspired by Peter Auer's proof

When proofs are constructed from strengthening (or weakening) transformations common form of the proof of $[R]$ show

(0) $[R \Leftarrow true]$ or $[false \Leftarrow \neg R]$.

Though the last form has a special name - "proof by contradiction" - the distinction is not profound because a strengthening sequence from R to $true$ can be translated mechanically into a strengthening sequence from $false$ to $\neg R$ (viz. the reverse sequence of the negated elements).

Strengthening sequences are formally the easier to construct, the weaker the starting element, and the stronger the final element. This note is devoted to the observation that it suffices to take from (0) the weaker of the consequents and the stronger of the antecedents:

(1) $[R \Leftarrow \neg R]$.

Formulation (1) is an optimum in the sense that of all implications equivalent to R it is the one with the weakest consequent and the strongest antecedent. Furthermore, we draw attention to the fact that, whereas the implications of (0) are each other's contrapositive, implication (1) is its own contrapositive. Finally we remark that, whereas the $\Leftarrow$'s in (0) can be replaced by $\equiv$'s , (1) remains an implication: when proved, the consequent (true) is strictly weaker than the antecedent (false).

Had the original proof obligation been an implication - i.e. of the form $[P \Leftarrow Q]$ - (1) would have yielded the rephrasing

(2) $\quad [P \vee \neg Q \ \Leftarrow\ \neg P \wedge Q]$;

compared with the original $[P \Leftarrow Q]$, the consequent has been weakened by the disjunction with the negated antecedent, the antecedent has been strengthened by the conjunction with the negated consequent.

* * *

The above observation has been triggered by the following proof by Peter Auer (of Vienna), that $[X \Rightarrow X;X]$ when it has been given that

(i) $\quad [X \Rightarrow J]$

(ii) $\quad J$ is the identity element of ;

(iii) $\quad$; distributes in both directions over $\vee$ (from which ;'s monotonicity follows) .

Auer's proof went as follows (here the

unary $\neg$ is the only logical operator with higher binding power than $;$), proving $[X \Rightarrow X;X \vee \neg X]$:

$$
\begin{array}{ll}
 & X \\
= & \quad \{ J \text{ is identity element of } ; \} \\
 & X; J \\
\Rightarrow & \quad \{ ; \text{ monotonic and } [J \Rightarrow X \vee \neg X] \} \\
 & X;(X \vee \neg X) \\
= & \quad \{ ; \text{ distributes over } \vee \} \\
 & X;X \;\vee\; X;\neg X \\
\Rightarrow & \quad \{ [X \Rightarrow J] \text{ and } ; \text{ monotonic} \} \\
 & X;X \;\vee\; J;\neg X \\
= & \quad \{ J \text{ is identity element of } ; \} \\
 & X;X \;\vee\; \neg X
\end{array}
$$

Pedernales Falls State Park
29 March 1991

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