A regrettable cover

On the cover of "A Logical Approach to Discrete Math" by David Gries and Fred B. Schneider we find a theorem and its formal proof. Regrettably, the nice idea of putting a theorem and its proof on the cover has been poorly executed, for the proof is clumsy. I copy from the cover:

"Theorem:

$(\forall x|: P \Rightarrow Q) \equiv \{x|P\} \subseteq \{x|Q\}$

Proof:

$\{x|P\} \subseteq \{x|Q\}$

$=$ ⟨Def. of Subset $\subseteq$, with v not occurring free in P or Q⟩

$(\forall v|\ v \in \{x|P\} :\ v \in \{x|Q\})$

$=$ ⟨$v \in \{x|R\} \equiv R[x:=v]$, twice⟩

$(\forall v|\ P[x:=v] :\ Q[x:=v])$

$=$ ⟨Trading; Dummy renaming⟩

$(\forall x|: P[x:=v][v:=x] \Rightarrow$
$Q[x:=v][v:=x])$

$=$ ⟨$R[x:=v][v:=x] \equiv R$ if v does not occur free in R, twice⟩

$(\forall x|: P \Rightarrow Q)$ "

In the book, dummy renaming is covered by -p.150-

"(8.21) <u>Axiom, Dummy renaming</u>: Provided

$\neg$ occurs ('y', 'R,P')

$$(* x | R : P) = (* y | R[x:=y] : P[x:=y])$$.

In the quoted proof, (8.21) is used to introduce the substitution $[v:=x]$, instead of using it to eliminate the substitution $[x:=v]$: the proof could have ended with

$$
\begin{aligned}
& (\forall v | P[x:=v] : Q[x:=v]) \\
= & \quad \langle \text{Trading; Dummy renaming} \rangle \\
& (\forall x | : P \Rightarrow Q)
\end{aligned}
$$.

The proof on the cover missed that "substituting equals for equals" can be used in either direction. But the whole "dummy renaming" is avoidable, for dummy v should not have been introduced in the first place: The one and only variable that by definition does not occur free in expressions $\{x|P\}$ or $\{x|Q\}$ is x ! So, here is a simpler proof:

$$
\begin{aligned}
& \{x|P\} \subseteq \{x|Q\} \\
= & \quad \{ \text{Def. of } \subseteq \} \\
& \langle \forall x : x \in \{x|P\} : x \in \{x|Q\} \rangle \\
= & \quad \{ x \in \{x|R\} \equiv R, \text{ twice; trading} \} \\
& \langle \forall x :: P \Rightarrow Q \rangle
\end{aligned}
$$.

By the standards of the book there is nothing fancy about this proof. I quote from

p. 199:

"Theorem (11.7) formalizes the connection between sets and predicates: a predicate is a representation for the set of argument-values for which it is *true*,

$$(11.7) \qquad x \in \{x \mid R\} \equiv R$$

Note that x is used with two different meanings in the LHS of (11.7). The leftmost occurrence of x is free, as are free occurrences of x in the RHS. All occurrences of x in $\{x \mid R\}$ are bound."

With the same four steps, the quoted proof occurs inside the book on p. 207.

Acknowledgement Wim H.J. Feijen en Rutger M. Dijkstra have independently drawn my attention to the cover's clumsiness.

Nuenen, 30 December 1993

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