424 Prove the following definitions implement simple data-stack theory (Subsection 7.0.2).

$$stack = [nil], [stack; X]$$
$$push = \langle s: stack \cdot \langle x: X \cdot [s; x]\rangle\rangle$$
$$pop = \langle s: stack \cdot s\ 0\rangle$$
$$top = \langle s: stack \cdot s\ 1\rangle$$

After trying the question, scroll down to the solution.

§ Consider the implementation to be four axioms, named by their left sides. Now I prove each of the axioms of simple data-stack theory. First, $stack \neq null$ by contradiction.

$$\begin{array}{lll}
 & stack = null & \text{conjoin } stack \text{ axiom} \\
= & stack = null \ \wedge \ stack \ = \ [nil], [stack; X] & \text{context, then specialize} \\
\Rightarrow & null \ = \ [nil], [null; X] & \text{both } ; \text{ and } [\ ] \text{ distribute over } , \\
= & null \ = \ [nil], null & null \text{ is identity for } , \\
= & null \ = \ [nil] & \text{transparency} \\
\Rightarrow & \cent\, null \ = \ \cent\, [nil] & \text{size axioms; note that } [nil] \text{ is an element} \\
 & & \text{because all } 0 \text{ of its items are elements} \\
= & 0 = 1 & \text{arithmetic axiom} \\
= & \bot &
\end{array}$$

Let s: $stack$ and x: X . Then

$$\begin{array}{lll}
 & push\ s\ x :\ stack & \text{use } push \text{ and } stack \text{ axioms} \\
= & \langle s\colon stack\cdot \langle x\colon X\cdot [s; x]\rangle\rangle\ s\ x :\ [nil], [stack; X] & \text{apply} \\
= & [s; x]\colon\ [nil], [stack; X] & \text{generalization} \\
\Leftarrow & [s; x]\colon\ [stack; X] & \\
= & \top & \\
 & pop\ (push\ s\ x) = s & \text{use } pop \text{ and } push \text{ axioms} \\
= & \langle s\colon stack\cdot s\ 0\rangle\ \langle s\colon stack\cdot \langle x\colon X\cdot [s; x]\rangle\rangle\ s\ x = s & \text{apply} \\
= & \langle s\colon stack\cdot s\ 0\rangle\ [s; x] = s & \text{apply} \\
= & [s; x]\ 0 = s & \text{index} \\
= & \top & \\
 & top\ (push\ s\ x) = x & \text{use } top \text{ and } push \text{ axioms} \\
= & \langle s\colon stack\cdot s\ 1\rangle\ \langle s\colon stack\cdot \langle x\colon X\cdot [s; x]\rangle\rangle\ s\ x = x & \text{apply} \\
= & \langle s\colon stack\cdot s\ 1\rangle\ [s; x] = x & \text{apply} \\
= & [s; x]\ 1 = x & \text{index} \\
= & \top &
\end{array}$$

The last step, indexing, requires x to be an item, so this implementation requires X to be a bunch of items.