387 Prove that the following definitions implement the simple data-stack theory.

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

§ 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.

$stack = null$ — conjoin *stack* axiom
$=$ $stack = null \wedge stack = [nil], [stack; X]$ — context, then specialize
$\Longrightarrow$ $null = [nil], [null; X]$ — [ ] distributes over ,
$=$ $null = [nil], null$ — *null* is identity for ,
$=$ $null = [nil]$ — transparency
$\Longrightarrow$ $\not\subset null = \not\subset [nil]$ — size axioms; note that $[nil]$ is an element because all 0 of its items are elements
$=$ $0 = 1$ — arithmetic axiom
$=$ $\bot$

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

$push\ s\ x :\ stack$ — use *push* and *stack* axioms
$=$ $\langle s: stack \rightarrow \langle x: X \rightarrow [s; x]\rangle\rangle\ s\ x :\ [nil], [stack; X]$ — apply
$=$ $[s; x]:\ [nil], [stack; X]$ — generalization
$\Longleftarrow$ $[s; x]:\ [stack; X]$
$=$ $\top$



$pop\ (push\ s\ x) = s$ — use *pop* and *push* axioms
$=$ $\langle s: stack \rightarrow s\ 0\rangle\ \langle s: stack \rightarrow \langle x: X \rightarrow [s; x]\rangle\rangle\ s\ x = s$ — apply
$=$ $\langle s: stack \rightarrow s\ 0\rangle\ [s; x] = s$ — apply
$=$ $[s; x]\ 0 = s$ — index
$=$ $\top$



$top\ (push\ s\ x) = x$ — use *top* and *push* axioms
$=$ $\langle s: stack \rightarrow s\ 1\rangle\ \langle s: stack \rightarrow \langle x: X \rightarrow [s; x]\rangle\rangle\ s\ x = x$ — apply
$=$ $\langle s: stack \rightarrow s\ 1\rangle\ [s; x] = x$ — apply
$=$ $[s; x]\ 1 = x$ — index
$=$ $\top$



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