455 A theory provides three names: *set* , *flip* , and *ask* . It is presented by an implementation. Let u: *bin* be the user's variable, and let v: *bin* be the implementer's variable. The axioms are

$$set \;=\; v{:=}\ \top$$
$$flip \;=\; v{:=}\ \neg v$$
$$ask \;=\; u{:=}\ v$$

(a)√ Replace v with w: *nat* according to the data transformer $v \;=\; even\ w$.

(b) Replace v with w: *nat* according to the data transformer $(w{=}0 \Rightarrow v) \wedge (w{=}1 \Rightarrow \neg v)$. Is anything wrong?

(c) Replace v with w: *nat* according to $(v \Rightarrow w{=}0) \wedge (\neg v \Rightarrow w{=}1)$. Is anything wrong?

After trying the question, scroll down to the solution.

(a)√ Replace v with w: *nat* according to the data transformer $v = even\ w$.

§ see book Section 7.2

(b) Replace v with w: *nat* according to the data transformer $(w{=}0 \Rightarrow v) \land (w{=}1 \Rightarrow \neg v)$. Is anything wrong?

§ Operation *set* becomes

$$\forall v\cdot (w{=}0 \Rightarrow v) \land (w{=}1 \Rightarrow \neg v) \Rightarrow \exists v'\cdot (w'{=}0 \Rightarrow v') \land (w'{=}1 \Rightarrow \neg v') \land (v{:=}\ \top)$$
$$= \quad u'{=}u \land w'{\ne}1$$

Operation *flip* becomes

$$\forall v\cdot (w{=}0 \Rightarrow v) \land (w{=}1 \Rightarrow \neg v) \Rightarrow \exists v'\cdot (w'{=}0 \Rightarrow v') \land (w'{=}1 \Rightarrow \neg v') \land (v{:=}\ \neg v)$$
$$= \quad u'{=}u \land (w{\ne}0 \Rightarrow w'{\ne}1) \land (w{\ne}1 \Rightarrow w'{\ne}0)$$

Operation *ask* becomes

$$\forall v\cdot (w{=}0 \Rightarrow v) \land (w{=}1 \Rightarrow \neg v) \Rightarrow \exists v'\cdot (w'{=}0 \Rightarrow v') \land (w'{=}1 \Rightarrow \neg v') \land (u{:=}\ v)$$
$$= \quad (w{\ne}0 \Rightarrow w'{\ne}0 \land \neg u') \land (w{\ne}1 \Rightarrow w'{\ne}1 \land u')$$
$$= \quad (w{=}0 \land w'{\ne}1 \land u') \lor (w{=}1 \land w'{\ne}0 \land \neg u')$$

Something is wrong. Although $(w{=}0 \Rightarrow v) \land (w{=}1 \Rightarrow \neg v)$ is a data transformer, it is a rather weak one because when w is neither 0 nor 1 it doesn't constrain v . So the result is that *ask* is transformed into something that's unimplementable.

(c) Replace v with w: *nat* according to $(v \Rightarrow w{=}0) \land (\neg v \Rightarrow w{=}1)$. Is anything wrong?

§ Operation *set* becomes

$$\forall v\cdot (v \Rightarrow w{=}0) \land (\neg v \Rightarrow w{=}1) \Rightarrow \exists v'\cdot (v' \Rightarrow w'{=}0) \land (\neg v' \Rightarrow w'{=}1) \land (v{:=}\ \top)$$
$$= \quad w{:}\ 0,1 \Rightarrow (w{:=}\ 0)$$

Operation *flip* becomes

$$\forall v\cdot (v \Rightarrow w{=}0) \land (\neg v \Rightarrow w{=}1) \Rightarrow \exists v'\cdot (v' \Rightarrow w'{=}0) \land (\neg v' \Rightarrow w'{=}1) \land (v{:=}\ \neg v)$$
$$= \quad w{:}\ 0,1 \Rightarrow (w{:=}\ 1{-}w)$$

Operation *ask* becomes

$$\forall v\cdot (v \Rightarrow w{=}0) \land (\neg v \Rightarrow w{=}1) \Rightarrow \exists v'\cdot (v' \Rightarrow w'{=}0) \land (\neg v' \Rightarrow w'{=}1) \land (u{:=}\ v)$$
$$= \quad w{:}\ 0,1 \Rightarrow (u{:=}\ w{=}0)$$

Something is wrong. We have been transforming with something that isn't a transformer; it's too strong.

$$\forall w\cdot \exists v\cdot (v \Rightarrow w{=}0) \land (\neg v \Rightarrow w{=}1)$$
$$= \quad \forall w\cdot w{=}0 \lor w{=}1$$
$$= \quad \bot$$

The last line isn't a theorem, so neither is the first. Nothing constrains the implementation to start in a state where $w{=}0 \lor w{=}1$. If it starts with $w{=}2$, then *set* might not set w to 0 , after which *ask* will give the wrong answer.