465 (transformation incompleteness) The user's variable is i and the implementer's variable is j , both of type $0, 1, 2$. The operations are:

$initialize = i'=0$

$step =$ **if** $j>0$ **then** $i:= i+1.\ j:= j-1$ **else** ok **fi**

The user can look at i but not at j . The user can $initialize$, which starts i at 0 and starts j at any of 3 values. The user can then repeatedly $step$ and observe that i increases 0 or 1 or 2 times and then stops increasing, which effectively tells the user what value j started with.

(a) Show that there is no data transformer to replace j with binary variable b so that

$initialize$	is transformed to	$i'=0$
$step$	is transformed to	**if** $b \wedge i<2$ **then** $i' = i+1$ **else** ok **fi**

The transformed $initialize$ starts b either at $\top$, meaning that i will be increased, or at $\bot$, meaning that i will not be increased. Each use of the transformed $step$ tests b to see if we might increase i , and checks $i<2$ to ensure that the increased value of i will not exceed 2 . If i is increased, b is again assigned either of its two values. The user will see i start at 0 and increase 0 or 1 or 2 times and then stop increasing, exactly as in the original specification.

(b) Use the data transformer $b=(j>0)$ to transform $initialize$ and $i+j=k \Rightarrow step$, where k is a constant, $k: 0, 1, 2$.

(a)§ Let D be a function of three variables with a binary result.

$$D: (0, 1, 2)\to(0, 1, 2)\to bin\to bin$$

For showing a contradiction, let D be such that

(0) $\quad \forall b\cdot\ \exists j\cdot\ D\ i\ j\ b$

(1) $\quad \forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b'\ \wedge\ initialize \quad\Leftarrow\quad i'{=}0$

(2) $\quad \forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b'\ \wedge\ step \quad\Leftarrow\quad \textbf{if}\ b \wedge i{<}2\ \textbf{then}\ i' = i{+}1\ \textbf{else}\ ok\ \textbf{fi}$

(0) says that $D\ i\ j\ b$ is a transformer for replacing variable j with variable b. (1) says that $D\ i\ j\ b$ transforms *initialize* to something refined by $i'{=}0$. (2) says that $D\ i\ j\ b$ transforms *step* to something refined by $\textbf{if}\ b \wedge i{<}2\ \textbf{then}\ i' = i{+}1\ \textbf{else}\ ok\ \textbf{fi}$. Our task is to show that (0), (1), and (2) together are inconsistent.

(0) can be restated without quantifiers as follows:

(3) $\quad (D\ i\ 0\ \top \vee D\ i\ 1\ \top \vee D\ i\ 2\ \top) \wedge (D\ i\ 0\ \bot \vee D\ i\ 1\ \bot \vee D\ i\ 2\ \bot)$

Now start with (1).

$$\begin{array}{lll}
 & i'{=}0\ \Rightarrow\ \forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b'\ \wedge\ initialize & \text{expand } initialize\\
= & i'{=}0\ \Rightarrow\ \forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b'\ \wedge\ i'{=}0 & \text{expand } Di'j'b'\text{, use context } i'{=}0\\
= & i'{=}0\ \Rightarrow\ \forall j\cdot\ D\ i\ j\ b \Rightarrow D\ 0\ 0\ b' \vee D\ 0\ 1\ b' \vee D\ 0\ 2\ b' & \text{use (3) with } i{=}0\\
= & i'{=}0\ \Rightarrow\ \forall j\cdot\ D\ i\ j\ b \Rightarrow \top & \text{base, identity, base}\\
= & \top &
\end{array}$$

So we can forget about (1).

Now start with the left side of (2).

$$\begin{array}{lll}
 & \forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b'\ \wedge\ step & \text{expand } step\\
= & \forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b'\ \wedge\ \textbf{if}\ j{>}0\ \textbf{then}\ i{:=}\ i{+}1.\ \ j{:=}\ j{-}1\ \textbf{else}\ ok\ \textbf{fi} & \text{expand } \textbf{if fi}\text{, } ok\\
= & \forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b'\ \wedge\ (j{>}0 \wedge i'{=}i{+}1 \wedge j'{=}j{-}1\ \vee\ j{=}0 \wedge i'{=}i \wedge j'{=}j) & \text{expand } \exists j'\cdot\\
= & \forall j\cdot\ D\ i\ j\ b \Rightarrow\ \ \ D\ i'\ 0\ b' \wedge (j{>}0 \wedge i'{=}i{+}1 \wedge 0{=}j{-}1\ \vee\ j{=}0 \wedge i'{=}i \wedge 0{=}j) & \\
 & \qquad\qquad\qquad \vee\ D\ i'\ 1\ b' \wedge (j{>}0 \wedge i'{=}i{+}1 \wedge 1{=}j{-}1\ \vee\ j{=}0 \wedge i'{=}i \wedge 1{=}j) & \\
 & \qquad\qquad\qquad \vee\ D\ i'\ 2\ b' \wedge (j{>}0 \wedge i'{=}i{+}1 \wedge 2{=}j{-}1\ \vee\ j{=}0 \wedge i'{=}i \wedge 2{=}j) & \text{simplify}\\
= & \forall j\cdot\ D\ i\ j\ b \Rightarrow\ \ \ D\ i'\ 0\ b' \wedge (i'{=}i{+}1 \wedge j{=}1\ \vee\ i'{=}i \wedge j{=}0) & \\
 & \qquad\qquad\qquad \vee\ D\ i'\ 1\ b' \wedge i'{=}i{+}1 \wedge j{=}2 & \\
 & \qquad\qquad\qquad \vee\ D\ i'\ 2\ b' \wedge i'{=}i{+}1 \wedge j{=}3 & \text{expand } \forall j\cdot
\end{array}$$

$$
\begin{aligned}
=\quad & (D\ i\ 0\ b \Rightarrow\ \ D\ i'\ 0\ b' \land (i'=i+1 \land 0=1\ \lor\ i'=i \land 0=0)\\
& \qquad\qquad \lor\ D\ i'\ 1\ b' \land i'=i+1 \land 0=2\\
& \qquad\qquad \lor\ D\ i'\ 2\ b' \land i'=i+1 \land 0=3)\\
& \land\ (D\ i\ 1\ b \Rightarrow\ \ D\ i'\ 0\ b' \land (i'=i+1 \land 1=1\ \lor\ i'=i \land 1=0)\\
& \qquad\qquad \lor\ D\ i'\ 1\ b' \land i'=i+1 \land 1=2\\
& \qquad\qquad \lor\ D\ i'\ 2\ b' \land i'=i+1 \land 1=3)\\
& \land\ (D\ i\ 2\ b \Rightarrow\ \ D\ i'\ 0\ b' \land (i'=i+1 \land 2=1\ \lor\ i'=i \land 2=0)\\
& \qquad\qquad \lor\ D\ i'\ 1\ b' \land i'=i+1 \land 2=2\\
& \qquad\qquad \lor\ D\ i'\ 2\ b' \land i'=i+1 \land 2=3) && \text{simplify}\\
=\quad & (D\ i\ 0\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i)\\
& \land (D\ i\ 1\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i+1)\\
& \land (D\ i\ 2\ b\ \Rightarrow\ D\ i'\ 1\ b' \land i'=i+1)
\end{aligned}
$$

This must be refined by **if** $b \land i<2$ **then** $i' = i+1$ **else** *ok* **fi** . Two cases. First case.

$$
\begin{aligned}
& b \land i<2 \land i'=i+1\ \Rightarrow\ \ (D\ i\ 0\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i)\\
& \qquad\qquad\qquad\qquad\quad \land (D\ i\ 1\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i+1)\\
& \qquad\qquad\qquad\qquad\quad \land (D\ i\ 2\ b\ \Rightarrow\ D\ i'\ 1\ b' \land i'=i+1) && \text{portation, distribution}\\
=\quad & (b \land i<2 \land i'=i+1 \land D\ i\ 0\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i)\\
& \land (b \land i<2 \land i'=i+1 \land D\ i\ 1\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i+1)\\
& \land (b \land i<2 \land i'=i+1 \land D\ i\ 2\ b\ \Rightarrow\ D\ i'\ 1\ b' \land i'=i+1) && \text{context, indirect proof}\\
=\quad & \neg(b \land i<2 \land i'=i+1 \land D\ i\ 0\ b)\\
& \land (b \land i<2 \land i'=i+1 \land D\ i\ 1\ b\ \Rightarrow\ D\ i'\ 0\ b')\\
& \land (b \land i<2 \land i'=i+1 \land D\ i\ 2\ b\ \Rightarrow\ D\ i'\ 1\ b') && \text{context, duality, inclusion}
\end{aligned}
$$

(4)
$$
\begin{aligned}
=\quad & (b \land i<2 \land i'=i+1 \Rightarrow \neg\, D\ i\ 0\ \top)\\
& \land (b \land i<2 \land i'=i+1 \land D\ i\ 1\ \top\ \Rightarrow\ D\ (i+1)\ 0\ b')\\
& \land (b \land i<2 \land i'=i+1 \land D\ i\ 2\ \top\ \Rightarrow\ D\ (i+1)\ 1\ b')
\end{aligned}
$$

Last case:

$$
\begin{aligned}
& \neg(b \land i<2) \land i'=i \land b'=b\ \ \Rightarrow\ \ (D\ i\ 0\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i)\\
& \qquad\qquad\qquad\qquad\qquad\quad \land (D\ i\ 1\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i+1)\\
& \qquad\qquad\qquad\qquad\qquad\quad \land (D\ i\ 2\ b\ \Rightarrow\ D\ i'\ 1\ b' \land i'=i+1)\\
& && \text{portation, distribution}\\
=\quad & (\neg(b \land i<2) \land i'=i \land b'=b \land D\ i\ 0\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i)\\
& \land (\neg(b \land i<2) \land i'=i \land b'=b \land D\ i\ 1\ b\ \Rightarrow\ D\ i'\ 0\ b' \land i'=i+1)\\
& \land (\neg(b \land i<2) \land i'=i \land b'=b \land D\ i\ 2\ b\ \Rightarrow\ D\ i'\ 1\ b' \land i'=i+1) && \text{context, base}\\
=\quad & (\neg(b \land i<2) \land i'=i \land b'=b \land D\ i\ 0\ b\ \Rightarrow\ D\ i\ 0\ b) && \text{context, base}\\
& \land (\neg(b \land i<2) \land i'=i \land b'=b \land D\ i\ 1\ b\ \Rightarrow\ \bot) && \text{indirect}\\
& \land (\neg(b \land i<2) \land i'=i \land b'=b \land D\ i\ 2\ b\ \Rightarrow\ \bot) && \text{indirect}\\
=\quad & (\neg(b \land i<2) \land i'=i \land b'=b \Rightarrow \neg\, D\ i\ 1\ b)\\
& \land (\neg(b \land i<2) \land i'=i \land b'=b \Rightarrow \neg\, D\ i\ 2\ b) && \text{context, distribution}
\end{aligned}
$$

(5)
$$
\begin{aligned}
=\quad & (\neg b \land i'=i \land \neg b' \Rightarrow \neg\, D\ i\ 1\ \bot)\\
& \land (\neg b \land i'=i \land \neg b' \Rightarrow \neg\, D\ i\ 2\ \bot)\\
& \land (i=2 \land i'=2 \land b'=b \Rightarrow \neg\, D\ 2\ 1\ b)\\
& \land (i=2 \land i'=2 \land b'=b \Rightarrow \neg\, D\ 2\ 2\ b)
\end{aligned}
$$

The task now is to show that (3), (4), and (5) together are inconsistent. That is, we need to show that the following together are inconsistent.

(3a) $D\ i\ 0\ \top \lor D\ i\ 1\ \top \lor D\ i\ 2\ \top$

(3b) $D\ i\ 0\ \bot \lor D\ i\ 1\ \bot \lor D\ i\ 2\ \bot$

(4a) $b \land i<2 \land i'=i+1 \Rightarrow\ \neg\, D\ i\ 0\ \top$

(4b) $b \land i<2 \land i'=i+1 \land D\ i\ 1\ \top \Rightarrow\ D\ (i+1)\ 0\ b'$

(4c) $b \land i<2 \land i'=i+1 \land D\ i\ 2\ \top \Rightarrow\ D\ (i+1)\ 1\ b'$

(5a) $\neg b \land i'=i \land \neg b'\ \Rightarrow\ \neg\, D\ i\ 1\ \bot$

(5b) $\neg b \land i'=i \land \neg b'\ \Rightarrow\ \neg\, D\ i\ 2\ \bot$

(5c) $i=2 \land i'=i \land b'=b\ \Rightarrow\ \neg\, D\ 2\ 1\ b$

(5d)	$i{=}2 \land i'{=}i \land b'{=}b \;\Rightarrow\; \neg D\ 2\ 2\ b$

(4) and (5) were refinements, so they are implicitly universally quantified over i, b, i', b' . Instantiating them gives us the following.

(3a0)	$D\ 0\ 0\ \top \lor D\ 0\ 1\ \top \lor D\ 0\ 2\ \top$
(3a1)	$D\ 1\ 0\ \top \lor D\ 1\ 1\ \top \lor D\ 1\ 2\ \top$
(3a2)	$D\ 2\ 0\ \top \lor D\ 2\ 1\ \top \lor D\ 2\ 2\ \top$
(3b0)	$D\ 0\ 0\ \bot \lor D\ 0\ 1\ \bot \lor D\ 0\ 2\ \bot$
(3b1)	$D\ 1\ 0\ \bot \lor D\ 1\ 1\ \bot \lor D\ 1\ 2\ \bot$
(3b2)	$D\ 2\ 0\ \bot \lor D\ 2\ 1\ \bot \lor D\ 2\ 2\ \bot$
(4a0)	$\neg D\ 0\ 0\ \top$
(4a1)	$\neg D\ 1\ 0\ \top$
(4b0⊤)	$D\ 0\ 1\ \top \Rightarrow D\ 1\ 0\ \top$
(4b0⊥)	$D\ 0\ 1\ \top \Rightarrow D\ 1\ 0\ \bot$
(4b1⊤)	$D\ 1\ 1\ \top \Rightarrow D\ 2\ 0\ \top$
(4b1⊥)	$D\ 1\ 1\ \top \Rightarrow D\ 2\ 0\ \bot$
(4c0⊤)	$D\ 0\ 2\ \top \Rightarrow D\ 1\ 1\ \top$
(4c0⊥)	$D\ 0\ 2\ \top \Rightarrow D\ 1\ 1\ \bot$
(4c1⊤)	$D\ 1\ 2\ \top \Rightarrow D\ 2\ 1\ \top$
(4c1⊥)	$D\ 1\ 2\ \top \Rightarrow D\ 2\ 1\ \bot$
(5a0)	$\neg D\ 0\ 1\ \bot$
(5a1)	$\neg D\ 1\ 1\ \bot$
(5a2)	$\neg D\ 2\ 1\ \bot$
(5b0)	$\neg D\ 0\ 2\ \bot$
(5b1)	$\neg D\ 1\ 2\ \bot$
(5b2)	$\neg D\ 2\ 2\ \bot$
(5c⊤)	$\neg D\ 2\ 1\ \top$
(5c⊥)	$\neg D\ 2\ 1\ \bot$ which is the same as (5a2)
(5d⊤)	$\neg D\ 2\ 2\ \top$
(5d⊥)	$\neg D\ 2\ 2\ \bot$ which is the same as (5b2)

Now I leave out the two redundant lines, and use all the known values to simplify the (3) and (4b) and (4c) lines.

(3a0)	$\bot \lor D\ 0\ 1\ \top \lor D\ 0\ 2\ \top$
(3a1)	$\bot \lor D\ 1\ 1\ \top \lor D\ 1\ 2\ \top$
(3a2)	$D\ 2\ 0\ \top \lor \bot \lor \bot$
(3b0)	$D\ 0\ 0\ \bot \lor \bot \lor \bot$
(3b1)	$D\ 1\ 0\ \bot \lor \bot \lor \bot$
(3b2)	$D\ 2\ 0\ \bot \lor \bot \lor \bot$
(4a0)	$\neg D\ 0\ 0\ \top$
(4a1)	$\neg D\ 1\ 0\ \top$
(4b0⊤)	$D\ 0\ 1\ \top \Rightarrow \bot$
(4b0⊥)	$D\ 0\ 1\ \top \Rightarrow D\ 1\ 0\ \bot$
(4b1⊤)	$D\ 1\ 1\ \top \Rightarrow D\ 2\ 0\ \top$
(4b1⊥)	$D\ 1\ 1\ \top \Rightarrow D\ 2\ 0\ \bot$
(4c0⊤)	$D\ 0\ 2\ \top \Rightarrow D\ 1\ 1\ \top$
(4c0⊥)	$D\ 0\ 2\ \top \Rightarrow \bot$
(4c1⊤)	$D\ 1\ 2\ \top \Rightarrow \bot$
(4c1⊥)	$D\ 1\ 2\ \top \Rightarrow \bot$
(5a0)	$\neg D\ 0\ 1\ \bot$
(5a1)	$\neg D\ 1\ 1\ \bot$

(5a2) $\neg D\ 2\ 1\ \bot$
(5b0) $\neg D\ 0\ 2\ \bot$
(5b1) $\neg D\ 1\ 2\ \bot$
(5b2) $\neg D\ 2\ 2\ \bot$
(5c$\top$) $\neg D\ 2\ 1\ \top$
(5d$\top$) $\neg D\ 2\ 2\ \top$

Simplifying,

(3a0) $D\ 0\ 1\ \top \vee D\ 0\ 2\ \top$
(3a1) $D\ 1\ 1\ \top \vee D\ 1\ 2\ \top$
(3a2) $D\ 2\ 0\ \top$
(3b0) $D\ 0\ 0\ \bot$
(3b1) $D\ 1\ 0\ \bot$
(3b2) $D\ 2\ 0\ \bot$
(4a0) $\neg D\ 0\ 0\ \top$
(4a1) $\neg D\ 1\ 0\ \top$
(4b0$\top$) $\neg D\ 0\ 1\ \top$
(4b0$\bot$) $D\ 0\ 1\ \top \Rightarrow D\ 1\ 0\ \bot$
(4b1$\top$) $D\ 1\ 1\ \top \Rightarrow D\ 2\ 0\ \top$
(4b1$\bot$) $D\ 1\ 1\ \top \Rightarrow D\ 2\ 0\ \bot$
(4c0$\top$) $D\ 0\ 2\ \top \Rightarrow D\ 1\ 1\ \top$
(4c0$\bot$) $\neg D\ 0\ 2\ \top$
(4c1$\top$) $\neg D\ 1\ 2\ \top$
(4c1$\bot$) $\neg D\ 1\ 2\ \top$
(5a0) $\neg D\ 0\ 1\ \bot$
(5a1) $\neg D\ 1\ 1\ \bot$
(5a2) $\neg D\ 2\ 1\ \bot$
(5b0) $\neg D\ 0\ 2\ \bot$
(5b1) $\neg D\ 1\ 2\ \bot$
(5b2) $\neg D\ 2\ 2\ \bot$
(5c$\top$) $\neg D\ 2\ 1\ \top$
(5d$\top$) $\neg D\ 2\ 2\ \top$

Now I use all the newly known values to simplify.

(3a0) $\bot \vee \bot$
(3a1) $D\ 1\ 1\ \top \vee \bot$
(3a2) $D\ 2\ 0\ \top$
(3b0) $D\ 0\ 0\ \bot$
(3b1) $D\ 1\ 0\ \bot$
(3b2) $D\ 2\ 0\ \bot$
(4a0) $\neg D\ 0\ 0\ \top$
(4a1) $\neg D\ 1\ 0\ \top$
(4b0$\top$) $\neg D\ 0\ 1\ \top$
(4b0$\bot$) $\bot \Rightarrow \top$
(4b1$\top$) $D\ 1\ 1\ \top \Rightarrow \top$
(4b1$\bot$) $D\ 1\ 1\ \top \Rightarrow \top$
(4c0$\top$) $D\ 0\ 2\ \top \Rightarrow D11\top$
(4c0$\bot$) $\neg D\ 0\ 2\ \top$
(4c1$\top$) $\neg D\ 1\ 2\ \top$
(4c1$\bot$) $\neg D\ 1\ 2\ \top$

(5a0) $\neg D\ 0\ 1\ \bot$
(5a1) $\neg D\ 1\ 1\ \bot$
(5a2) $\neg D\ 2\ 1\ \bot$
(5b0) $\neg D\ 0\ 2\ \bot$
(5b1) $\neg D\ 1\ 2\ \bot$
(5b2) $\neg D\ 2\ 2\ \bot$
(5c⊤) $\neg D\ 2\ 1\ \top$
(5d⊤) $\neg D\ 2\ 2\ \top$

We could go one more round of simplifying and then make the one remaining substitution, but I already see the inconsistency: line (3a0). So I am finished. I could go back and shorten the proof to just those steps that contributed to finding the inconsistency, but that would leave the reader wondering how I found it.

(b) Use the data transformer $b=(j>0)$ to transform *initialize* and $i+j=k \Rightarrow step$, where k is a constant, k: 0, 1, 2 .

§ Transforming *initialize*

$$\forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b' \land initialize \qquad \text{expand } initialize$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow \exists j'\cdot\ b'=(j'>0) \land i'=0 \qquad \text{expand } \exists j'\cdot$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow \quad b'=(0>0) \land i'=0$$
$$\lor\ b'=(1>0) \land i'=0$$
$$\lor\ b'=(2>0) \land i'=0 \qquad \text{simplify}$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow \neg b' \land i'=0\ \lor\ b' \land i'=0 \qquad \text{factor, excluded middle}$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow i'=0 \qquad \text{expand } \forall j\cdot$$
$$= (b=(0>0) \Rightarrow i'=0) \land (b=(1>0) \Rightarrow i'=0) \land (b=(2>0) \Rightarrow i'=0) \qquad \text{simplify}$$
$$= (\neg b \Rightarrow i'=0) \land (b \Rightarrow i'=0) \land (b \Rightarrow i'=0) \qquad \text{idempotent, case analysis, case idempotent}$$
$$= i'=0$$

Transforming $i+j=k \Rightarrow step$

$$\forall j\cdot\ D\ i\ j\ b \Rightarrow \exists j'\cdot\ D\ i'j'b' \land (i+j=k \Rightarrow step)$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow \exists j'\cdot\ b'=(j'>0) \land (i+j=k \Rightarrow \textbf{if } j>0 \textbf{ then } i:=i+1.\ j:=j-1 \textbf{ else } ok \textbf{ fi})$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow \exists j'\cdot\ b'=(j'>0) \land (i+j=k \Rightarrow (\quad j>0 \land i'=i+1 \land j'=j-1$$
$$\lor\ j=0 \land i'=i \land j'=j))$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow \quad b'=(0>0) \land (i+j=k \Rightarrow (j>0 \land i'=i+1 \land 0=j-1\ \lor\ j=0 \land i'=i \land 0=j))$$
$$\lor\ b'=(1>0) \land (i+j=k \Rightarrow (j>0 \land i'=i+1 \land 1=j-1\ \lor\ j=0 \land i'=i \land 1=j))$$
$$\lor\ b'=(2>0) \land (i+j=k \Rightarrow (j>0 \land i'=i+1 \land 2=j-1\ \lor\ j=0 \land i'=i \land 2=j))$$
$$= \forall j\cdot\ b=(j>0) \Rightarrow \quad \neg b' \land (i+j=k \Rightarrow i'=i+1 \land j=1\ \lor\ j=0 \land i'=i)$$
$$\lor\ b' \land (i+j=k \Rightarrow i'=i+1 \land j=2)$$
$$\lor\ b' \land (i+j=k \Rightarrow i'=i+1 \land j=3)$$
$$= \quad (b=(0>0) \Rightarrow \quad \neg b' \land (i+0=k \Rightarrow i'=i+1 \land 0=1\ \lor 0=0 \land i'=i)$$
$$\lor\ b' \land (i+0=k \Rightarrow i'=i+1 \land 0=2)$$
$$\lor\ b' \land (i+0=k \Rightarrow i'=i+1 \land 0=3)$$
$$\land\ (b=(1>0) \Rightarrow \quad \neg b' \land (i+1=k \Rightarrow i'=i+1 \land 1=1\ \lor\ 1=0 \land i'=i)$$
$$\lor\ b' \land (i+1=k \Rightarrow i'=i+1 \land 1=2)$$
$$\lor\ b' \land (i+1=k \Rightarrow i'=i+1 \land 1=3))$$
$$\land\ (b=(2>0) \Rightarrow \quad \neg b' \land (i+2=k \Rightarrow i'=i+1 \land 2=1\ \lor\ 2=0 \land i'=i)$$
$$\lor\ b' \land (i+2=k \Rightarrow i'=i+1 \land 2=2)$$
$$\lor\ b' \land (i+2=k \Rightarrow i'=i+1 \land 2=3))$$
$$= \quad (\neg b \Rightarrow\ \neg b' \land (i=k \Rightarrow i'=i)\ \lor\ \ b' \land i \ne k) \qquad \text{material}$$
$$\land\ (b \Rightarrow\ \neg b' \land (i+1=k \Rightarrow i'=i+1)\ \lor\ b' \land i+1 \ne k) \qquad \text{implication}$$
$$\land\ (b \Rightarrow\ \neg b' \land i+2 \ne k\ \lor\ b' \land (i+2=k \Rightarrow i'=i+1)\ \lor\ b' \land i+2 \ne k) \qquad \text{3 times}$$

$$
\begin{aligned}
= \quad & \ (\neg b \Rightarrow \neg b' \wedge (i \ne k \vee i'=i) \ \vee \ b' \wedge i \ne k) \\
& \wedge\ (b \Rightarrow \neg b' \wedge (i+1 \ne k \vee i'=i+1) \ \vee \ b' \wedge i+1 \ne k) \\
& \wedge\ (b \Rightarrow \neg b' \wedge i+2 \ne k \ \vee \ b' \wedge (i+2 \ne k \vee i'=i+1) \ \vee \ b' \wedge i+2 \ne k) \qquad \text{distribute 3 times} \\
= \quad & \ (\neg b \Rightarrow \neg b' \wedge i \ne k \ \vee \ \neg b' \wedge i'=i \ \vee \ b' \wedge i \ne k) \\
& \wedge\ (b \Rightarrow \neg b' \wedge i+1 \ne k \ \vee \ \neg b' \wedge i'=i+1 \ \vee \ b' \wedge i+1 \ne k) \\
& \wedge\ (b \Rightarrow \neg b' \wedge i+2 \ne k \ \vee \ b' \wedge i+2 \ne k \ \vee \ b' \wedge i'=i+1 \ \vee \ b' \wedge i+2 \ne k) \\
= \quad & \ (\neg b \wedge i=k \Rightarrow \neg b' \wedge i'=i) \\
& \wedge\ (b \wedge i+1=k \Rightarrow \neg b' \wedge i'=i+1) \\
& \wedge\ (b \wedge i+2=k \Rightarrow b' \wedge i'=i+1) \\
= \quad & \textbf{if } b \textbf{ then } b'=(i+2=k) \wedge i'=i+1 \textbf{ else } i'=i \textbf{ fi}
\end{aligned}
$$

It's not part of the Exercise, but I'll try using $b=(j>0)$ to transform *step* without $i+j=k$.

$$
\begin{aligned}
& \forall j\cdot D\ i\ j\ b \Rightarrow \exists j'\cdot D\ i' j' b' \wedge step \\
= \quad & \forall j\cdot b=(j>0) \Rightarrow \exists j'\cdot b'=(j'>0) \wedge \textbf{if } j>0 \textbf{ then } i:=i+1.\ j:=j-1 \textbf{ else } ok \textbf{ fi} \\
= \quad & \forall j\cdot b=(j>0) \Rightarrow \exists j'\cdot b'=(j'>0) \wedge (j>0 \wedge i'=i+1 \wedge j'=j-1 \ \vee \ j=0 \wedge i'=i \wedge j'=j) \\
= \quad & \forall j\cdot b=(j>0) \Rightarrow \quad b'=(0>0) \wedge (j>0 \wedge i'=i+1 \wedge 0=j-1 \ \vee \ j=0 \wedge i'=i \wedge 0=j) \\
& \qquad\qquad\qquad \vee\ b'=(1>0) \wedge (j>0 \wedge i'=i+1 \wedge 1=j-1 \ \vee \ j=0 \wedge i'=i \wedge 1=j) \\
& \qquad\qquad\qquad \vee\ b'=(2>0) \wedge (j>0 \wedge i'=i+1 \wedge 2=j-1 \ \vee \ j=0 \wedge i'=i \wedge 2=j) \\
= \quad & \forall j\cdot b=(j>0) \Rightarrow \quad \neg b' \wedge (i'=i+1 \wedge j=1 \ \vee \ j=0 \wedge i'=i) \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge j=2 \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge j=3 \\
= \quad & \ (b=(0>0) \Rightarrow \quad \neg b' \wedge (i'=i+1 \wedge 0=1 \ \vee 0=0 \wedge i'=i) \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge 0=2 \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge 0=3) \\
& \wedge\ (b=(1>0) \Rightarrow \quad \neg b' \wedge (i'=i+1 \wedge 1=1 \ \vee \ 1=0 \wedge i'=i) \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge 1=2 \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge 1=3) \\
& \wedge\ (b=(2>0) \Rightarrow \quad \neg b' \wedge (i'=i+1 \wedge 2=1 \ \vee \ 2=0 \wedge i'=i) \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge 2=2 \\
& \qquad\qquad\qquad \vee\ b' \wedge i'=i+1 \wedge 2=3) \\
= \quad & \ (\neg b \Rightarrow \neg b' \wedge i'=i) \\
& \wedge\ (b \Rightarrow \neg b' \wedge i'=i+1) \\
& \wedge\ (b \Rightarrow b' \wedge i'=i+1) \\
= \quad & (\neg b \Rightarrow \neg b' \wedge i'=i) \wedge \neg b \\
= \quad & \neg b \wedge \neg b' \wedge i'=i
\end{aligned}
$$

which is unimplementable. So that's why we needed $i+j=k$.