

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:

$initialize = i'=0$

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

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 $\mathbf{if } b \wedge i<2 \mathbf{ then } i' = i+1 \mathbf{ else } ok \mathbf{ fi}$

The transformed $initialize$ starts b either at \top , meaning that i will be increased, or at \perp , 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.

$$D: (0, 1, 2) \rightarrow (0, 1, 2) \rightarrow \text{bin} \rightarrow \text{bin}$$

For showing a contradiction, let D be such that

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

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

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

(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 **if** $b \wedge i < 2$ **then** $i' = i+1$ **else ok fi**. Our task is to show that (0), (1), and (2) together are inconsistent.

(0) can be restated without quantifiers as follows:

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

Now start with (1).

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

So we can forget about (1).

Now start with the left side of (2).

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

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

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

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

Last case:

$$\begin{aligned}
& \neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \Rightarrow (D i 0 b \Rightarrow D i' 0 b' \wedge i' = i) \\
& \quad \wedge (D i 1 b \Rightarrow D i' 0 b' \wedge i' = i + 1) \\
& \quad \wedge (D i 2 b \Rightarrow D i' 1 b' \wedge i' = i + 1) \\
& \hspace{15em} \text{portation, distribution} \\
= & \quad (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \wedge D i 0 b \Rightarrow D i' 0 b' \wedge i' = i) \\
& \wedge (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \wedge D i 1 b \Rightarrow D i' 0 b' \wedge i' = i + 1) \\
& \wedge (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \wedge D i 2 b \Rightarrow D i' 1 b' \wedge i' = i + 1) \\
& \hspace{15em} \text{context, base} \\
= & \quad (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \wedge D i 0 b \Rightarrow D i 0 b) \\
& \wedge (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \wedge D i 1 b \Rightarrow \perp) \\
& \wedge (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \wedge D i 2 b \Rightarrow \perp) \\
& \hspace{15em} \text{context, base} \\
& \hspace{15em} \text{indirect} \\
= & \quad (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \Rightarrow \neg D i 1 b) \\
& \wedge (\neg(b \wedge i < 2) \wedge i' = i \wedge b' = b \Rightarrow \neg D i 2 b) \\
& \hspace{15em} \text{indirect} \\
(5) \quad = & \quad (\neg b \wedge i' = i \wedge \neg b' \Rightarrow \neg D i 1 \perp) \\
& \wedge (\neg b \wedge i' = i \wedge \neg b' \Rightarrow \neg D i 2 \perp) \\
& \wedge (i = 2 \wedge i' = 2 \wedge b' = b \Rightarrow \neg D 2 1 b) \\
& \wedge (i = 2 \wedge i' = 2 \wedge b' = b \Rightarrow \neg D 2 2 b) \\
& \hspace{15em} \text{context, distribution}
\end{aligned}$$

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.

$$\begin{aligned}
(3a) \quad & D i 0 \top \vee D i 1 \top \vee D i 2 \top \\
(3b) \quad & D i 0 \perp \vee D i 1 \perp \vee D i 2 \perp \\
(4a) \quad & b \wedge i < 2 \wedge i' = i + 1 \Rightarrow \neg D i 0 \top \\
(4b) \quad & b \wedge i < 2 \wedge i' = i + 1 \wedge D i 1 \top \Rightarrow D (i + 1) 0 b' \\
(4c) \quad & b \wedge i < 2 \wedge i' = i + 1 \wedge D i 2 \top \Rightarrow D (i + 1) 1 b' \\
(5a) \quad & \neg b \wedge i' = i \wedge \neg b' \Rightarrow \neg D i 1 \perp \\
(5b) \quad & \neg b \wedge i' = i \wedge \neg b' \Rightarrow \neg D i 2 \perp \\
(5c) \quad & i = 2 \wedge i' = i \wedge b' = b \Rightarrow \neg D 2 1 b \\
(5d) \quad & i = 2 \wedge i' = i \wedge b' = b \Rightarrow \neg D 2 2 b
\end{aligned}$$

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

$$\begin{aligned}
(3a0) \quad & D 0 0 \top \vee D 0 1 \top \vee D 0 2 \top \\
(3a1) \quad & D 1 0 \top \vee D 1 1 \top \vee D 1 2 \top \\
(3a2) \quad & D 2 0 \top \vee D 2 1 \top \vee D 2 2 \top \\
(3b0) \quad & D 0 0 \perp \vee D 0 1 \perp \vee D 0 2 \perp \\
(3b1) \quad & D 1 0 \perp \vee D 1 1 \perp \vee D 1 2 \perp \\
(3b2) \quad & D 2 0 \perp \vee D 2 1 \perp \vee D 2 2 \perp \\
(4a0) \quad & \neg D 0 0 \top \\
(4a1) \quad & \neg D 1 0 \top \\
(4b0\top) \quad & D 0 1 \top \Rightarrow D 1 0 \top \\
(4b0\perp) \quad & D 0 1 \top \Rightarrow D 1 0 \perp \\
(4b1\top) \quad & D 1 1 \top \Rightarrow D 2 0 \top \\
(4b1\perp) \quad & D 1 1 \top \Rightarrow D 2 0 \perp \\
(4c0\top) \quad & D 0 2 \top \Rightarrow D 1 1 \top \\
(4c0\perp) \quad & D 0 2 \top \Rightarrow D 1 1 \perp \\
(4c1\top) \quad & D 1 2 \top \Rightarrow D 2 1 \top \\
(4c1\perp) \quad & D 1 2 \top \Rightarrow D 2 1 \perp
\end{aligned}$$

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

$$\begin{aligned}
(4b1\perp) & D 1 1 \top \Rightarrow D 2 0 \perp \\
(4c0\top) & D 0 2 \top \Rightarrow D 1 1 \top \\
(4c0\perp) & \neg D 0 2 \top \\
(4c1\top) & \neg D 1 2 \top \\
(4c1\perp) & \neg D 1 2 \top \\
(5a0) & \neg D 0 1 \perp \\
(5a1) & \neg D 1 1 \perp \\
(5a2) & \neg D 2 1 \perp \\
(5b0) & \neg D 0 2 \perp \\
(5b1) & \neg D 1 2 \perp \\
(5b2) & \neg D 2 2 \perp \\
(5c\top) & \neg D 2 1 \top \\
(5d\top) & \neg D 2 2 \top
\end{aligned}$$

Now I use all the newly known values to simplify.

$$\begin{aligned}
(3a0) & \perp \vee \perp \\
(3a1) & D 1 1 \top \vee \perp \\
(3a2) & D 2 0 \top \\
(3b0) & D 0 0 \perp \\
(3b1) & D 1 0 \perp \\
(3b2) & D 2 0 \perp \\
(4a0) & \neg D 0 0 \top \\
(4a1) & \neg D 1 0 \top \\
(4b0\top) & \neg D 0 1 \top \\
(4b0\perp) & \perp \Rightarrow \top \\
(4b1\top) & D 1 1 \top \Rightarrow \top \\
(4b1\perp) & D 1 1 \top \Rightarrow \top \\
(4c0\top) & D 0 2 \top \Rightarrow D 1 1 \top \\
(4c0\perp) & \neg D 0 2 \top \\
(4c1\top) & \neg D 1 2 \top \\
(4c1\perp) & \neg D 1 2 \top \\
(5a0) & \neg D 0 1 \perp \\
(5a1) & \neg D 1 1 \perp \\
(5a2) & \neg D 2 1 \perp \\
(5b0) & \neg D 0 2 \perp \\
(5b1) & \neg D 1 2 \perp \\
(5b2) & \neg D 2 2 \perp \\
(5c\top) & \neg D 2 1 \top \\
(5d\top) & \neg D 2 2 \top
\end{aligned}$$

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 $i+j=k \Rightarrow \text{step}$, where k is a constant, $k: 0, 1, 2$.

§ Transforming *initialize*

$$\begin{aligned}
& \forall j \cdot D i j b \Rightarrow \exists j' \cdot D i' j' b' \wedge \text{initialize} && \text{expand } \textit{initialize} \\
= & \forall j \cdot b=(j>0) \Rightarrow \exists j' \cdot b'=(j'>0) \wedge i'=0 && \text{expand } \exists j' \cdot
\end{aligned}$$

$$\begin{aligned}
&= \forall j. b=(j>0) \Rightarrow b'=(0>0) \wedge i'=0 \\
&\quad \vee b'=(1>0) \wedge i'=0 \\
&\quad \vee b'=(2>0) \wedge i'=0 && \text{simplify} \\
&= \forall j. b=(j>0) \Rightarrow \neg b' \wedge i'=0 \vee b' \wedge i'=0 && \text{factor, excluded middle} \\
&= \forall j. b=(j>0) \Rightarrow i'=0 && \text{expand } \forall j. \\
&= (b=(0>0) \Rightarrow i'=0) \wedge (b=(1>0) \Rightarrow i'=0) \wedge (b=(2>0) \Rightarrow i'=0) && \text{simplify} \\
&= (\neg b \Rightarrow i'=0) \wedge (b \Rightarrow i'=0) \wedge (b \Rightarrow i'=0) && \text{idempotent, case analysis, case idempotent} \\
&= i'=0
\end{aligned}$$

Transforming $i+j=k \Rightarrow \text{step}$

$$\begin{aligned}
&\forall j. D i j b \Rightarrow \exists j'. D i' j' b' \wedge (i+j=k \Rightarrow \text{step}) \\
&= \forall j. b=(j>0) \Rightarrow \exists j'. b'=(j'>0) \wedge (i+j=k \Rightarrow \text{if } j>0 \text{ then } i:=i+1. j:=j-1 \text{ else ok fi}) \\
&= \forall j. b=(j>0) \Rightarrow \exists j'. b'=(j'>0) \wedge (i+j=k \Rightarrow (j>0 \wedge i'=i+1 \wedge j'=j-1 \\
&\quad \vee j=0 \wedge i'=i \wedge j'=j)) \\
&= \forall j. b=(j>0) \Rightarrow b'=(0>0) \wedge (i+j=k \Rightarrow (j>0 \wedge i'=i+1 \wedge 0=j-1 \vee j=0 \wedge i'=i \wedge 0=j)) \\
&\quad \vee b'=(1>0) \wedge (i+j=k \Rightarrow (j>0 \wedge i'=i+1 \wedge 1=j-1 \vee j=0 \wedge i'=i \wedge 1=j)) \\
&\quad \vee b'=(2>0) \wedge (i+j=k \Rightarrow (j>0 \wedge i'=i+1 \wedge 2=j-1 \vee j=0 \wedge i'=i \wedge 2=j)) \\
&= \forall j. b=(j>0) \Rightarrow \neg b' \wedge (i+j=k \Rightarrow i'=i+1 \wedge j=1 \vee j=0 \wedge i'=i) \\
&\quad \vee b' \wedge (i+j=k \Rightarrow i'=i+1 \wedge j=2) \\
&\quad \vee b' \wedge (i+j=k \Rightarrow i'=i+1 \wedge j=3) \\
&= (b=(0>0) \Rightarrow \neg b' \wedge (i+0=k \Rightarrow i'=i+1 \wedge 0=1 \vee 0=0 \wedge i'=i) \\
&\quad \vee b' \wedge (i+0=k \Rightarrow i'=i+1 \wedge 0=2) \\
&\quad \vee b' \wedge (i+0=k \Rightarrow i'=i+1 \wedge 0=3)) \\
&\wedge (b=(1>0) \Rightarrow \neg b' \wedge (i+1=k \Rightarrow i'=i+1 \wedge 1=1 \vee 1=0 \wedge i'=i) \\
&\quad \vee b' \wedge (i+1=k \Rightarrow i'=i+1 \wedge 1=2) \\
&\quad \vee b' \wedge (i+1=k \Rightarrow i'=i+1 \wedge 1=3)) \\
&\wedge (b=(2>0) \Rightarrow \neg b' \wedge (i+2=k \Rightarrow i'=i+1 \wedge 2=1 \vee 2=0 \wedge i'=i) \\
&\quad \vee b' \wedge (i+2=k \Rightarrow i'=i+1 \wedge 2=2) \\
&\quad \vee b' \wedge (i+2=k \Rightarrow i'=i+1 \wedge 2=3)) \\
&= (\neg b \Rightarrow \neg b' \wedge (i=k \Rightarrow i'=i) \vee b' \wedge i \neq k) && \text{material} \\
&\wedge (b \Rightarrow \neg b' \wedge (i+1=k \Rightarrow i'=i+1) \vee b' \wedge i+1 \neq k) && \text{implication} \\
&\wedge (b \Rightarrow \neg b' \wedge i+2 \neq k \vee b' \wedge (i+2=k \Rightarrow i'=i+1) \vee b' \wedge i+2 \neq k) && \text{3 times} \\
&= (\neg b \Rightarrow \neg b' \wedge (i \neq k \vee i'=i) \vee b' \wedge i \neq k) \\
&\wedge (b \Rightarrow \neg b' \wedge (i+1 \neq k \vee i'=i+1) \vee b' \wedge i+1 \neq k) \\
&\wedge (b \Rightarrow \neg b' \wedge i+2 \neq k \vee b' \wedge (i+2 \neq k \vee i'=i+1) \vee b' \wedge i+2 \neq k) && \text{distribute 3 times} \\
&= (\neg b \Rightarrow \neg b' \wedge i \neq k \vee \neg b' \wedge i'=i \vee b' \wedge i \neq k) \\
&\wedge (b \Rightarrow \neg b' \wedge i+1 \neq k \vee \neg b' \wedge i'=i+1 \vee b' \wedge i+1 \neq k) \\
&\wedge (b \Rightarrow \neg b' \wedge i+2 \neq k \vee b' \wedge i+2 \neq k \vee b' \wedge i'=i+1 \vee b' \wedge i+2 \neq k) \\
&= (\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) \\
&= \text{if } b \text{ then } b'=(i+2=k) \wedge i'=i+1 \text{ else } i'=i \text{ fi}
\end{aligned}$$

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

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

$$\begin{aligned}
& \vee b' \wedge i'=i+1 \wedge j=3 \\
= & (b=(0>0) \Rightarrow \neg b' \wedge (i'=i+1 \wedge 0=1 \vee 0=0 \wedge i'=i) \\
& \vee b' \wedge i'=i+1 \wedge 0=2 \\
& \vee b' \wedge i'=i+1 \wedge 0=3) \\
& \wedge (b=(1>0) \Rightarrow \neg b' \wedge (i'=i+1 \wedge 1=1 \vee 1=0 \wedge i'=i) \\
& \vee b' \wedge i'=i+1 \wedge 1=2 \\
& \vee b' \wedge i'=i+1 \wedge 1=3) \\
& \wedge (b=(2>0) \Rightarrow \neg b' \wedge (i'=i+1 \wedge 2=1 \vee 2=0 \wedge i'=i) \\
& \vee b' \wedge i'=i+1 \wedge 2=2 \\
& \vee b' \wedge i'=i+1 \wedge 2=3) \\
= & (\neg b \Rightarrow \neg b' \wedge i'=i) \\
& \wedge (b \Rightarrow \neg b' \wedge i'=i+1) \\
& \wedge (b \Rightarrow b' \wedge i'=i+1) \\
= & (\neg b \Rightarrow \neg b' \wedge i'=i) \wedge \neg b \\
= & \neg b \wedge \neg b' \wedge i'=i
\end{aligned}$$

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