315 In a language with array element assignment, the program

$$x:= i.\ \ i:= A\ i.\ \ A\ i:= x$$

was written with the intention to swap the values of i and $A\ i$. Assume that all variables and array elements are of type nat , and that i has a value that is an index of A .

(a) In variables x , i , and A , specify that i and $A\ i$ should be swapped, the rest of A should be unchanged, but x might change.

(b) Find the exact precondition for which the program refines the specification of part (a).

(c) Find the exact postcondition for which the program refines the specification of part (a).

After trying the question, scroll down to the solution.

(a) In variables x , i , and A , specify that i and $A\,i$ should be swapped, the rest of A should be unchanged, but x might change.

§ $i' = A\,i \;\land\; A' = i{\to}i \mid A$

(b) Find the exact precondition for which the program refines the specification of part (a).

§ $\forall x', i', A'\cdot\; i' = A\,i \;\land\; A' = i{\to}i \mid A \;\Leftarrow\; (x{:=}\,i.\;\; i{:=}\,Ai.\;\; A{:=}\,i{\to}x \mid A)$

expand final asmt

$=\;\; \forall x', i', A'\cdot\; i' = A\,i \;\land\; A' = i{\to}i \mid A \;\Leftarrow\; (x{:=}\,i.\;\; i{:=}\,A\,i.\;\; x'{=}x \land i'{=}i \land A' = i{\to}x \mid A)$

substitution law twice

$=\;\; \forall x', i', A'\cdot\; i' = A\,i \;\land\; A' = i{\to}i \mid A \;\Leftarrow\; x'{=}i \;\land\; i' = A\,i \;\land\; A' = A\,i \to i \mid A$ 1-pt × 3

$=\;\; A\,i = A\,i \;\land\; A\,i \to i \mid A \;=\; i{\to}i \mid A$ reflexivity and identity

$=\;\; A\,i \to i \mid A \;=\; i{\to}i \mid A$ case idempotent

$=\;\; \textbf{if } A\,i = i \textbf{ then } A\,i \to i \mid A \;=\; i{\to}i \mid A \textbf{ else } A\,i \to i \mid A \;=\; i{\to}i \mid A \textbf{ fi}$ context, reflexive

$=\;\; \textbf{if } A\,i = i \textbf{ then } \top \textbf{ else } A\,i \to i \mid A \;=\; i{\to}i \mid A \textbf{ fi}$ One Case Law

$=\;\; A\,i = i \;\lor\; A\,i \to i \mid A \;=\; i{\to}i \mid A$ list equality

$=\;\; A\,i = i \;\lor\; \forall j\cdot\; (A\,i \to i \mid A)j \;=\; (i{\to}i \mid A)j$ split domain of j

$=\;\; A\,i = i \;\lor\; (\; (A\,i \to i \mid A)i \;=\; (i{\to}i \mid A)i$
$\qquad \land\; \forall j\cdot\; j{\ne}i \;\Rightarrow\; (A\,i \to i \mid A)j \;=\; (i{\to}i \mid A)j \;)$

The left disjunct $Ai = i$ gives us the context $Ai \ne i$ in the right disjunct. Use it to simplify $(A\,i \to i \mid A)i$. Also simplify $(i{\to}i \mid A)i$.

$=\;\; A\,i = i \;\lor\; (\; Ai \;=\; i$
$\qquad \land\; \forall j\cdot\; j{\ne}i \;\Rightarrow\; (A\,i \to i \mid A)j \;=\; (i{\to}i \mid A)j \;)$ absorption

$=\;\; A\,i = i$

So i and $A\,i$ will be swapped if and only if they have the same value to start with, making the swap useless.

(c) Find the exact postcondition for which the program refines the specification of part (a).

§ $\forall x, i, A\cdot\; i' = A\,i \;\land\; A' = i{\to}i \mid A \;\Leftarrow\; x'{=}i \;\land\; i' = A\,i \;\land\; A' = Ai{\to}i \mid A$

context to drop first $i' = A\,i$; x doesn't appear; one-pt for i ; context to replace last $A\,i$

$=\;\; \forall A\cdot\; A' = x'{\to}x' \mid A \;\Leftarrow\; i' = A\,x' \;\land\; A' = i'{\to}x' \mid A$ case idempotent

$=\;\; \textbf{if } x'{=}i' \textbf{ then } \forall A\cdot\; A' = x'{\to}x' \mid A \;\Leftarrow\; i' = A\,x' \;\land\; A' = i'{\to}x' \mid A$ context: replace i'
$\qquad \textbf{else } \forall A\cdot\; A' = x'{\to}x' \mid A \;\Leftarrow\; i' = A\,x' \;\land\; A' = i'{\to}x' \mid A \textbf{ fi}$ context: replace A'

$=\;\; \textbf{if } x'{=}i' \textbf{ then } \forall A\cdot\; A' = x'{\to}x' \mid A \;\Leftarrow\; i' = A\,x' \;\land\; A' = x'{\to}x' \mid A$ specialization
$\qquad \textbf{else } \forall A\cdot\; i'{\to}x' \mid A = x'{\to}x' \mid A \;\Leftarrow\; i' = A\,x' \;\land\; A' = i'{\to}x' \mid A \textbf{ fi}$

$=\;\; x'{\ne}i' \;\Rightarrow\; (\forall A\cdot\; i'{\to}x' \mid A = x'{\to}x' \mid A \;\Leftarrow\; i' = A\,x' \;\land\; A' = i'{\to}x' \mid A)$

$=\;\; x'{\ne}i' \;\Rightarrow\; (\forall A\cdot\; x' = A\,i' \;\land\; A\,x' = x' \;\Leftarrow\; i' = A\,x' \;\land\; A' = i'{\to}x' \mid A)$ context

$=\;\; x'{\ne}i' \;\Rightarrow\; (\forall A\cdot\; \bot \;\Leftarrow\; i' = A\,x' \;\land\; A' = i'{\to}x' \mid A)$

note that $x'{\ne}i' \;\land\; A' = i'{\to}x' \mid A \;\Rightarrow\; A'x' = A\,x'$

$=\;\; x'{\ne}i' \;\Rightarrow\; (\forall A\cdot\; \bot \;\Leftarrow\; i'{=}A'x' \;\land\; A' = i'{\to}x' \mid A)$

$=\;\; x'{\ne}i' \land i'{=}A'x' \;\Rightarrow\; \lnot(\exists A\cdot\; A' = i'{\to}x' \mid A)$

$=\;\; x'{\ne}i' \land i'{=}A'x' \;\Rightarrow\; \lnot(A'i'{=}x')$

$=\;\; x'{=}i' \lor A'x'{\ne}i' \lor A'i'{\ne}x'$

If, in the end, we see $x'{=}i'$ or $A'x'{\ne}i'$ or $A'i'{\ne}x'$ we know they were swapped (well, we won't see $A'i'{\ne}x'$ because of the final assignment, so really it's just the first two possibilities).