Essential Exercise 5.17

We shall prove the following four results jointly:

R1 if $sec[\![C]\!](X)$

$q_0 \neq q_\bullet$

$(q, y := a\{X'\}, q') \in edges_s(q_0 \rightsquigarrow q_\bullet)[\![C]\!](X)$

then $X' \cup fv(a) \Rightarrow \{y\}$

$X \subseteq X'$

R2 if $w = true$ where $(w, d') = sec_2[\![GC]\!](d, X)$

$q_0 \neq q_\bullet$

$(q, y := a\{X'\}, q') \in E$ where $(E, d') = edges_{s2}(q_0 \rightarrow q_\bullet)[\![GC]\!](d, X)$

then $X' \cup fv(a) \Rightarrow \{y\}$

$X \subseteq X'$

R3 if $sec[\![C]\!](X)$

$q_0 \neq q_\bullet$

$(q, A[a_1] := a_2\{X'\}, q') \in edges_s(q_0 \rightsquigarrow q_\bullet)[\![C]\!](X)$

then $X' \cup fv(a_1) \cup fv(a_2) \Rightarrow \{A\}$

$X \subseteq X'$

R4 if $w = true$ where $(w, d') = sec_2[\![GC]\!](d, X)$

$q_0 \neq q_\bullet$

$(q, A[a_1] := a_2\{X'\}, q') \in E$ where $(E, d') = edges_{s2}(q_0 \rightarrow q_\bullet)[\![GC]\!](d, X)$

then $X' \cup fv(a_1) \cup fv(a_2) \Rightarrow \{A\}$

$X \subseteq X'$

While this looks like a lot of work all cases are extremely similar (-1)

5.17 continued

Proving R1, R2, R3, R4 jointly means that we perform a proof by mathematical induction on the size of the syntactic component (C for R1, R3 and GC for R2, R4).

(This is sometimes called mutual structural induction.)

Basically this means that we need to consider 8 cases: 6 for the commands and 2 for the guarded commands.

During the proofs we need to simultaneously inspect:
Definitions 5.4 and 5.5 for $edges_S$ and $edges_{S2}$
Definitions 5.12 and 5.13 for sec and sec_2
(This would be easiest if you have a page on your desk with each set of definitions - otherwise one may easily get lost.)

Case C is $x := a$

Only R1 applies and it is immediate that $X' = X$, $y = x$ and that $X' \cup fv(a) \rightrightarrows \{x\}$.

Case C is $A[a_1] := a_2$

Only R3 applies and it is immediate that $X' = X$ and that $X' \cup fv(a_1) \cup fv(a_2) \rightrightarrows \{A\}$.

Case C is skip

Immediate as neither R1, R2, R3 nor R4 applies.

5.17 continued'

Case C is $C_1 ; C_2$

Both R1 and R3 may apply. Any edge in the program graph for C must come from either C_1 or C_2 and our induction hypothesis for C_1 and C_2 then give us the result.

Case C is if GC fi

Both R1 and R3 may apply. Our induction hypothesis established R2 and R4 for GC and this gives us the result.

Case C is do GC od

Both R1 and R3 may apply. Our induction hypothesis established R2 and R4 for GC and this gives us the result. (Because the edge $(q_0, \neg d, q_0)$ in $edges_S(q_0 \to q_0)[\![C]\!](X)$ is not an assignment.)

Case GC is $b \to C$

Both R2 and R4 may apply. Our induction hypothesis established R1 and R3 for C and we observe that the set $X \cup fv(b) \cup fv(d)$ is used both for $edges_S$ and for sec; hence this gives us the result. (Because the edge $(q_0, b \wedge \neg d, q)$ is not an assignment.)

Case GC is $GC_1 [\!] GC_2$

Both R2 and R4 may apply. Our induction hypothesis established R2 and R4 for both GC_1 and GC_2 and we observe that the set X is used both for the two occurrences of $edges_{S2}$ and for sec_2 and that furthermore the d's match up; hence this gives us the result.

End of 5.17