Homework 7

Non-compositional Verification

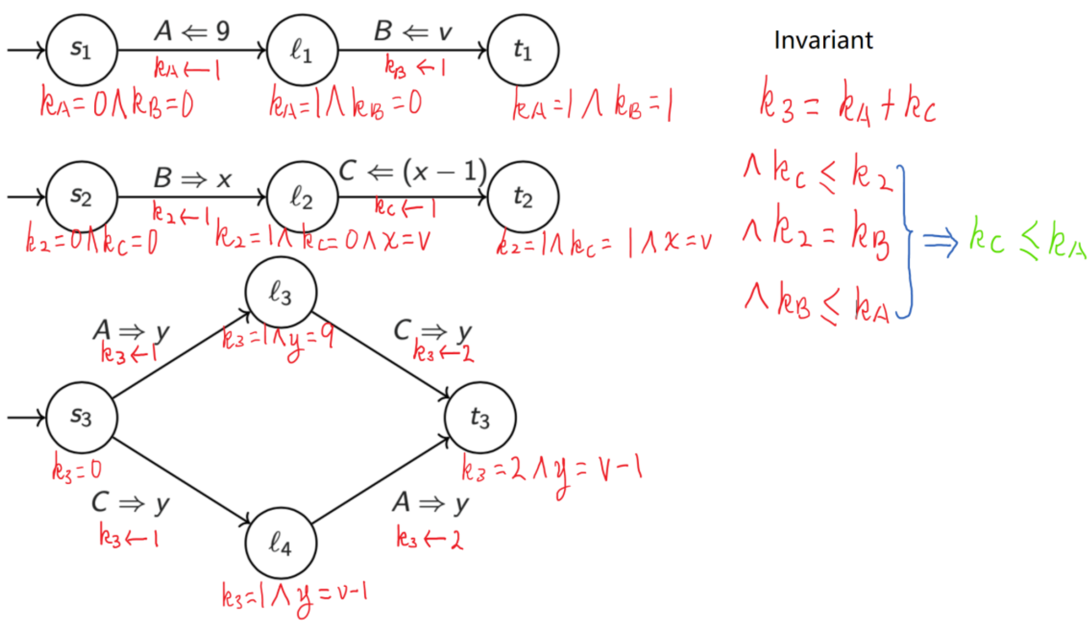

Diagram for assertion network and communication invariants

Explanation of auxiliary variables

AFR method is used to prove that $\{True\}P_1||P_2||P_3\{y = v - 1\}$ holds.

Firstly, three variables corresponding to the three channels are defined, which are k_A, k_B, k_C respectively. $k_{channel} = 0$ is defined as the default state while $k_{channle} = 1$ implies that certain value has been sent into the channel.

Also, we defined k_2 to indicate whether process 2 has already received a variable from B.

Finally, k_3 is defined to record the "stage" of process 3 where $k_3 = k_A + k_C$.

Communication invariant

$$I: \boldsymbol{k_3 = k_A + k_C \wedge k_C \leq k_2 \wedge k_2 = k_B \wedge k_B \leq k_A}$$

Notice that $\boldsymbol{k_c \leq k_2 \wedge k_2 = k_b \wedge k_B \leq k_A}$ implies that $k_C \leq k_A$, which is useful for discharging proof obligation.

Termination

1. prove $x \geq 0$-convergence

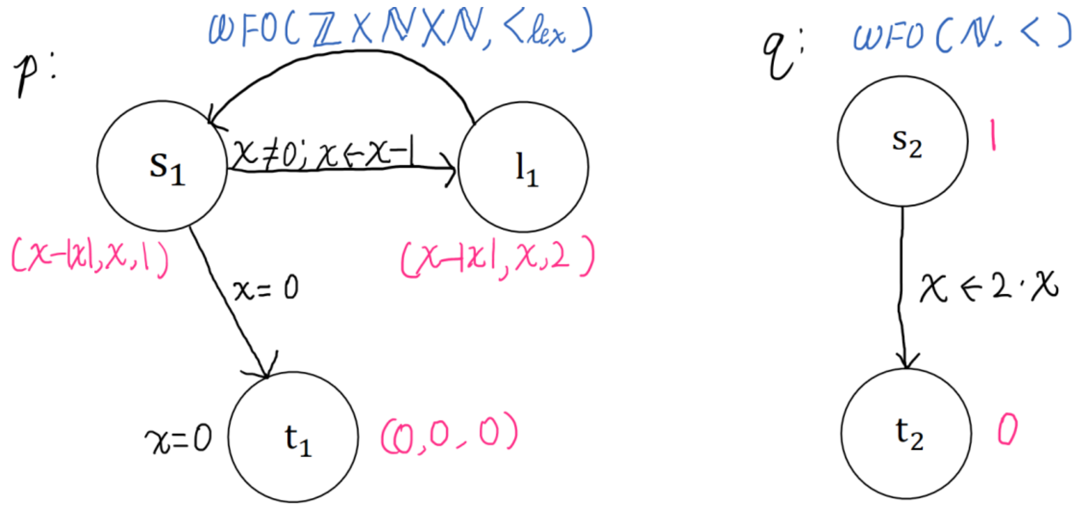

Diagram for assertion network, well founded set and ranking function

For $x \geq 0$, the program is convergent.

This program terminates when $x = 0$ at t_1.

2. Is this program $\top$-convergent?

No, because for $x < 0$, this program will stay in the loop $s \leftrightarrow l_1$ forever and x will keep going far away the terminate state therefore it never converges.

2. Is this program $\perp$-convergent?

No, because for $x \geq 0$, this program will converge.