RDCS423 Tutorial Problems and Solutions #3 - Time Constraint Projection, Propagation and Real-Time Logic

1. Suppose we have a time constraint imposed on the invoker of a remote object as TC_{in} and a time constraint imposed by the invokee TC_{out}. Let the service to be invoked succeed TC_{in} by exactly γ time units.

   If $TC_{in} = \langle t^{in}_\alpha, t^{in}_\beta \rangle$ and $TC_{out} = \langle t^{out}_\alpha, t^{out}_\beta \rangle$ using *meet* convex interval relations, show the relationship between t^{in}_x's and t^{out}_x's holds.

2. With the following time constraints TC_1 and TC_2:

   TC_1 : T_{begin} : $1.0 \rightarrow 1.6$ $\quad T_{end}$: $1.4 \rightarrow 2.0$ $\quad C_{ld}$: $0.2 \rightarrow 0.6$
   TC_2 : T_{begin} : $0.2 \rightarrow 2.2$ $\quad T_{end}$: $1.0 \rightarrow 3.0$ $\quad C_{ld}$: $0.8 \rightarrow 1.8$

   draw the time constraint laxity windows for both constraints and propagate TC_1 onto TC_2. What can be said about occurrence windows for $TC_1 \prec TC_2$ and $TC_1 \succ TC_2$? What regions define where TC_1 and TC_2 have a non-null intersection, and an accurate knowledge is required of all constraint begin and end times?

3. Given the following system specification:

   A control panel with a button that when pushed must generate an action SAMPLE which must execute within 10 time units. The computation time of this SAMPLE action is at least 5 time units.

   Produce a set of RTL axioms corresponding to the specification and reduce them to determine if this specification is realisable or not.

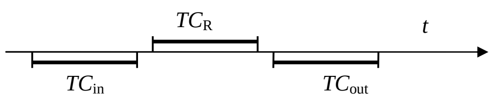
4. In addition to the system specification of the previous question, add the safety assertion:

   If the transmitted information is displayed within 8 time units of the completion of action SAMPLE, then within 15 time units of pressing button 1, the requested information will be displayed.

   Now augment the set of RTL axioms and reduce them to determine if the safety assertion is consistent with the system specification.

Solutions:

1.



$TC_{in}\ \Re_{in}\ TC_R\ \Re_{out}\ TC_{out}$ is satisfied in this case with $\Re_{in} = \Re_{out} = \Uparrow$

$TC_{in} \Uparrow TC_R \Rightarrow t^{in}_\beta = t^R_\alpha$

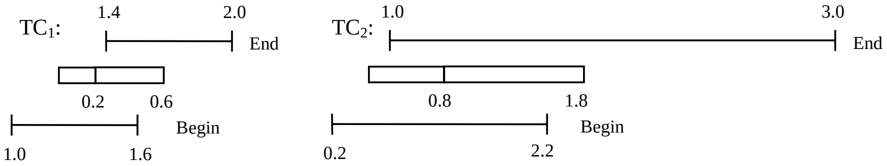
$\|TC_R\| = \gamma \Rightarrow t^R_\beta = t^R_\alpha + \gamma$

$t^R_\beta = t^{in}_\beta + \gamma$

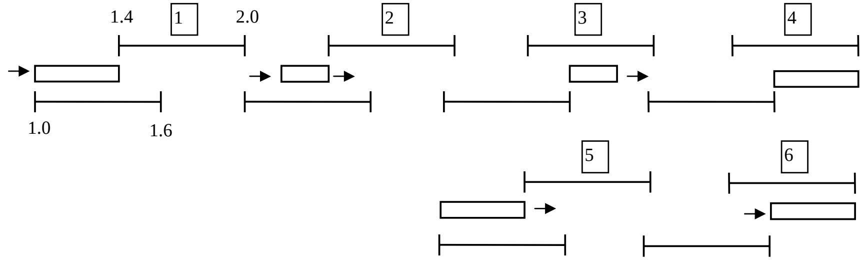
$TC_R \Uparrow TC_{out} \Rightarrow t^R_\beta = t^{out}_\alpha \Rightarrow t^{out}_\alpha = t^{in}_\beta + \gamma$

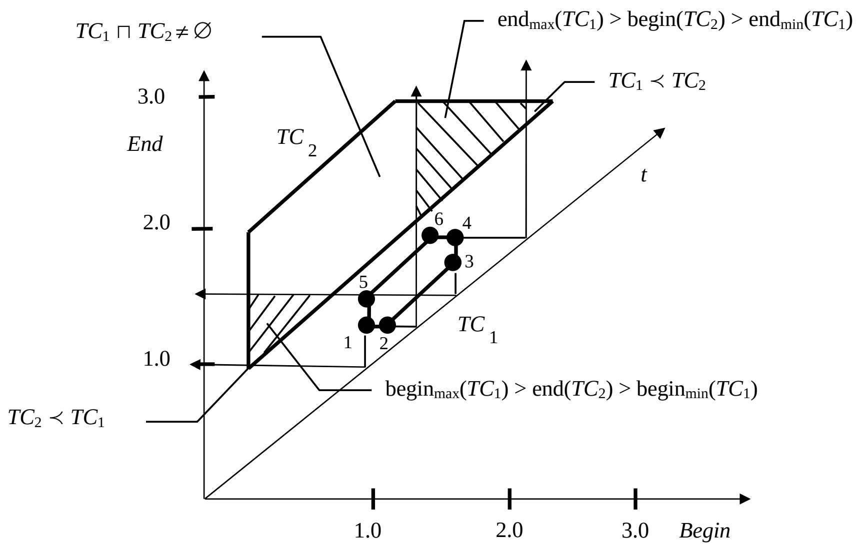
i.e. the service to be invoked succeeds TC_{in} by exactly γ time units.

2.



TC_1 constraint laxity window turning points:

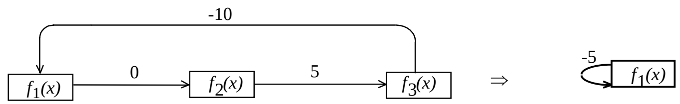




3. Form the RTL axioms for the specification:

$$\forall x:\ @\ (\Omega\text{BUTTON1},\ x)\ \le\ @\ (\uparrow\text{SAMPLE},\ x)$$
$$\wedge\ @\ (\downarrow\text{SAMPLE},\ x)\ \le\ @\ (\Omega\text{BUTTON1},\ x)\ +\ 10$$
$$\forall y:\ @\ (\uparrow\text{SAMPLE},\ y)\ +\ 5\ \le\ @\ (\downarrow\text{SAMPLE},\ y)$$

Form the RTL constraint graph and reduce:



Yielding a single negative cycle $\rightarrow$ the system specification is realizable.

4. Form the RTL axioms for the safety assertion:

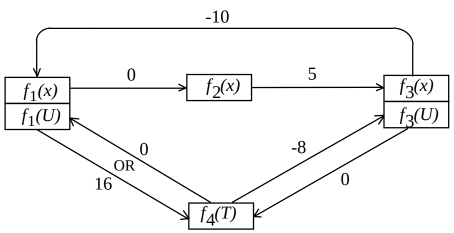
$$\forall u\ \forall t:\ @\ (\downarrow\text{SAMPLE},\ u)\ \le\ @\ (\Omega\ \text{DISPLAY},\ t)$$
$$\wedge\ @\ (\Omega\ \text{DISPLAY},\ t)\ \le\ @\ (\downarrow\text{SAMPLE},\ u)+\ 8$$
$$\rightarrow\ @\ (\Omega\ \text{BUTTON1},\ u)\ <\ @\ (\Omega\ \text{DISPLAY},\ t)$$
$$\wedge\ @\ (\Omega\ \text{DISPLAY},\ t)\ \le\ @\ (\Omega\ \text{BUTTON1},\ u)+\ 15$$

The negated form of the safety assertion ($\neg\{P\}$) is given by:

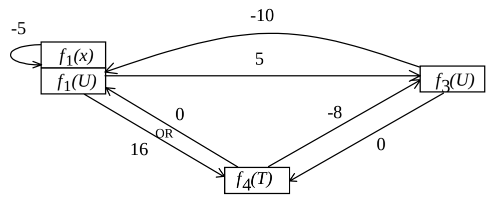
$$\exists u\ \exists t:\ @\ (\downarrow\text{SAMPLE},\ u)\ \le\ @\ (\Omega\ \text{DISPLAY},\ t)$$
$$\wedge\ @\ (\Omega\ \text{DISPLAY},\ t)\ \le\ @\ (\downarrow\text{SAMPLE},\ u)+\ 8$$
$$\wedge\ \{\ @\ (\Omega\ \text{DISPLAY},\ t)\ \le\ @\ (\Omega\ \text{BUTTON1},\ u)$$
$$\vee\ @\ (\Omega\ \text{BUTTON1},\ u)\ +\ 16\ \le\ @\ (\Omega\ \text{DISPLAY},\ t)\ \}$$

and note the use of: $\neg\{@(E_1, i)\ \le\ @(E_2, j)\}\ =\ @(E_2, j) + 1\ \le\ @(E_1, i)$

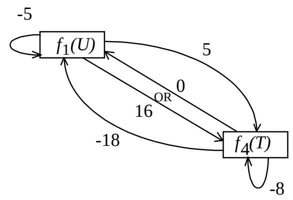
Map to uninterpreted integer functions and form the RTL constraint graph:



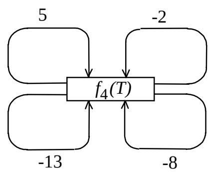
Eliminate $f_2(x)$ trivially and eliminate $f_3(x)$ with substitution $x \rightarrow U$:



$f_1(x)$ has a negative cycle - ok to eliminate $f_1(x)$ and $f_3(U)$:



Eliminate $f_1(U)$:



There is only one positive cycle in a cycle involving one element of a disjunction in the reduced RTL constraint graph, so {S} $\wedge$ $\neg$(P) is satisfiable -> the safety assertion {P} is not consistent with the system specification so it cannot be met..