Supplement of "Necessary Feasibility Analysis for Mixed-Criticality Real-Time Embedded Systems"

Hoon Sung Chwa, Hyeongboo Baek, and Jinkyu Lee

Proof of Lemma 8

Lemma 8. Target the scenario of S1–S4 with given $t^{\text{end}} > 0$ and J_k^*, and target a single mode change instant t^* belonging to $[t_a^*(J_k^*), t_b^*(J_k^*)]$ (defined in Lemma 5). Consider a job of $\tau_i \in \tau^{\texttt{HI}}$ potentially belonging to CG2, J_i^q, whose release time and deadline are $r_i^q = \lfloor \frac{t^*}{T_i} \rfloor \cdot T_i$ and $d_i^q = r_i^q + D_i$, respectively. Considering J_i^q, we have three cases for calculating $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$. In Case 1, there is no job of τ_i in CG2; J_i^q does not belong to CG2. In Cases 2 and 3, J_i^q is the job of τ_i that belongs to CG2, but the job's execution requirement amounts to its LO and HI WCET, respectively. Case 3 consists of Subcases 3A and 3B, in which J_i^q does trigger and does not trigger the mode change, respectively. Then, $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$ for every $\tau_i \in \tau^{\texttt{HI}}$ should satisfy the following constraints.

- Case 1: If $r_i^q = t^*$, $d_i^q \le t^*$ or $d_i^q > t^{\text{end}}$, $\texttt{OP}_i^-(t^*) = \texttt{OP}_i^+(t^*) = 0$ holds.
- Case 2: Otherwise, if $r_i^q < r_k^*$ (recall r_k^* is J_k^*'s release time),
  (i) $\texttt{LB}^- \le \texttt{OP}_i^-(t^*) \le \texttt{UB}^-$,
  (ii) $\texttt{LB}^+ \le \texttt{OP}_i^+(t^*) \le \texttt{UB}^+$, and
  (iii) $\texttt{OP}_i^+(t^*) + \texttt{OP}_i^-(t^*) = C_i^{\texttt{LO}}$ hold, where
  $\texttt{UB}^- = \min(t^* - r_i^q, C_i^{\texttt{LO}})$, $\texttt{UB}^+ = \min(d_i^q - t^*, C_i^{\texttt{LO}})$,
  $\texttt{LB}^- = C_i^{\texttt{LO}} - \texttt{UB}^+$ and $\texttt{LB}^+ = C_i^{\texttt{LO}} - \texttt{UB}^-$.
- Case 3: Otherwise (i.e., $r_i^q \ge r_k^*$),

  (Subcase 3A) if $t^* - r_i^q \ge C_i^{\texttt{LO}}$ and $d_i^q - t^* \ge C_i^{\texttt{HI}} - C_i^{\texttt{LO}}$ hold and the job of τ_i triggers the mode change,
  (i) $\texttt{OP}_i^-(t^*) = C_i^{\texttt{LO}}$ and
  (ii) $\texttt{OP}_i^+(t^*) = C_i^{\texttt{HI}} - C_i^{\texttt{LO}}$ hold;

  (Subcase 3B) otherwise (i.e., the job of τ_i does not trigger the mode change),
  (i) $\texttt{LB2}^- \le \texttt{OP}_i^-(t^*) \le \texttt{UB2}^-$,
  (ii) $\texttt{LB2}^+ \le \texttt{OP}_i^+(t^*) \le \texttt{UB2}^+$, and
  (iii) $\texttt{OP}_i^+(t^*) + \texttt{OP}_i^-(t^*) = C_i^{\texttt{HI}}$ hold, where
  $\texttt{UB2}^- = \min(t^* - r_i^q, C_i^{\texttt{LO}} - 1)$, $\texttt{UB2}^+ = \min(d_i^q - t^*, C_i^{\texttt{HI}})$,
  $\texttt{LB2}^- = C_i^{\texttt{HI}} - \texttt{UB2}^+$ and $\texttt{LB2}^+ = C_i^{\texttt{HI}} - \texttt{UB2}^-$.

Proof: (Case 1) If $r_i^q = t^*$ (or $d_i^q \le t^*$), J_i^q belongs to CG3 (or CG1) and there is no job of τ_i in CG2. Also, if $d_i^q > t^{\text{end}}$, the scenario of S2 does not generate J_i^q.

(Case 2) If $r_i^q < r_k^*$ (i.e., the release time of J_i^q less than that of J_k^*), J_i^q's execution requirement is $C_i^{\texttt{LO}}$ by the definition of J_k^* and S4, yielding $\texttt{OP}_i^-(t^*) + \texttt{OP}_i^+(t^*) = C_i^{\texttt{LO}}$. J_i^q can be executed in $[r_i^q, t^*]$ and $[t^*, d_i^q]$ (i.e., before and after the mode change), for at most the interval length, i.e., $(t^* - r_i^q)$ and $(d_i^q - t^*)$ time units, respectively, yielding upper bounds of $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$. Considering J_i^q's execution requirement equals to $C_i^{\texttt{LO}}$, we can derive upper bounds of $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$ as $\texttt{UB}^-$ and $\texttt{UB}^+$. If we use $\texttt{OP}_i^-(t^*) + \texttt{OP}_i^+(t^*) = C_i^{\texttt{LO}}$, we can derive lower bounds of $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$ as $\texttt{LB}^-$ and $\texttt{LB}^+$, from $\texttt{UB}^+$ and $\texttt{UB}^-$.

(Case 3) This case implies that J_i^q's execution requirement is $C_i^{\texttt{HI}}$ (by the definition of J_k^* and S4), yielding $\texttt{OP}_i^-(t^*) + \texttt{OP}_i^+(t^*) = C_i^{\texttt{HI}}$.

(Subcase 3A) This subcase implies that J_i^q triggers the mode change, which requires J_i^q to execute for $C_i^{\texttt{LO}}$ in $[r_i^q, t^*]$ and for $(C_i^{\texttt{HI}} - C_i^{\texttt{LO}})$ in $[t^*, d_i^q]$. Therefore, the conditions (i) and (ii) for Subcase 3A hold.

(Subcase 3B) This subcase implies that J_i^q does not trigger the mode change. Therefore, there is a limit for the maximum of $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$, which is $(C_i^{\texttt{LO}} - 1)$ and $C_i^{\texttt{HI}}$, respectively. While the latter is straightforward, the former holds because executing for $C_i^{\texttt{LO}}$ before the mode change implies that J_i^q triggers the mode change, which contradicts the supposition of Subcase 3B. Applying the same idea as Case 2, we can derive upper bounds of $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$ as $\texttt{UB2}^-$ and $\texttt{UB2}^+$, and then derive lower bounds of $\texttt{OP}_i^-(t^*)$ and $\texttt{OP}_i^+(t^*)$ as $\texttt{LB2}^-$ and $\texttt{LB2}^+$, from $\texttt{UB2}^+$ and $\texttt{UB2}^-$. □

Proof of Lemma 10

Lemma 10. If Alg. 1 returns FALSE, Theorem 1 (and Lemma 9) judges that for given t^* it is impossible to satisfy both Eqs. (5) and (6) subject to Lemma 8 and the constraint in Lemma 9.

Proof: Suppose that Alg. 1 returns FALSE but Lemma 9 cannot judge that a mode change cannot occur at given $t^* \in [t_a^*(J_k^*), t_b^*(J_k^*)]$ without any deadline miss of jobs invoked by τ in $[0, t^{\text{end}}]$. We now derive contradiction.

The supposition implies that there is no task $\tau_k \in \tau^{\texttt{HI}}$ that satisfies the inequality of $\texttt{DiffLO} + \texttt{DiffHI} \le \texttt{DiffOP}$ in Alg. 1. The supposition also implies that there exists at least $t^* \in [t_a^*(J_k^*), t_b^*(J_k^*)]$ that satisfies Eqs. (5) and (6) subject to Lemma 8 and the constraint in Lemma 9; let t' denote such t^*, and τ_k denote the task that satisfies the constraint (i.e., the task whose job triggers the mode change). Then, $\texttt{OP}_k^-(t') = C_k^{\texttt{LO}}$ and $\texttt{OP}_k^+(t') = C_k^{\texttt{HI}} - C_k^{\texttt{LO}}$ holds by Subcase 3A of Lemma 8. Let δ_i^- and δ_i^+ for $\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}$ denote the difference between $\max \texttt{OP}_i^-(t')$ and the actual $\texttt{OP}_i^-(t')$, and the difference between $\max \texttt{OP}_i^+(t')$ and the actual $\texttt{OP}_i^+(t')$, respectively. Then, for $\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}$ belonging to Subcase 3B of Lemma 8, the following holds: $\delta_i^- + \delta_i^+ = \texttt{UB2}^{-\prime} - \texttt{OP}_i^-(t') + \texttt{UB2}^+ - \texttt{OP}_i^+(t') = \texttt{UB2}^{-\prime} + \texttt{UB2}^+ - C_i^{\texttt{HI}} = \texttt{UB2}^{-\prime} + C_i^{\texttt{HI}} - \texttt{LB2}^- - C_i^{\texttt{HI}}$, which is $\texttt{UB2}^{-\prime} - \texttt{LB2}^-$. The same holds for $\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}$ belonging to Case 2 of Lemma 8.

Then, the following inequality holds from Eq. (5):

$$\sum_{\tau_i \in \tau} \texttt{DBF}_i^{\texttt{LO}}(t') + \texttt{SumOP}^- - \sum_{\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}} \delta_i^- \le m \cdot t'$$
$$\Rightarrow \sum_{\tau_i \in \tau} \texttt{DBF}_i^{\texttt{LO}}(t') + \texttt{SumOP}^- - m \cdot t' \le \sum_{\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}} \delta_i^-.$$

Similarly, we can derive the following inequality holds from Eq. (6):

$$\sum_{\tau_i \in \tau^{\texttt{HI}}} \texttt{DBF}_i^{\texttt{HI}}\big(t^{\text{end}} - \lceil t'/T_i \rceil \cdot T_i\big) + \texttt{SumOP}^+ - m \cdot (t^{\text{end}} - t') \le \sum_{\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}} \delta_i^+.$$

Note that the LHSes of the above two inequalites are the same as DiffLO and DiffHI without the max operation. Considering δ_i^- and δ_i^+ are non-negative for every $\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}$ by their definitions, if we combine the above two inequalities, the LHS is $\texttt{DiffLO} + \texttt{DiffHI}$, and the RHS is $\sum_{\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}} (\delta_i^- + \delta_i^+) = \sum_{\tau_i \in \tau^{\texttt{HI}} \setminus \{\tau_k\}} \big(\max \texttt{OP}_i^-(t') - \min \texttt{OP}_i^-(t')\big)$, which is equal to DiffOP. Therefore, the supposition of non-existence of $\tau_k \in \tau^{\texttt{HI}}$ that satisfies $\texttt{DiffLO} + \texttt{DiffHI} \le \texttt{DiffOP}$ contradicts. □

PROOF OF LEMMA 11

Lemma 11. If Eq. (5) is violated with any t^*, it is also violated with some t^* which is smaller than $\big(\sum_{\tau_i\in\tau}(T_i-D_i)\cdot C_i^{\mathtt{LO}}/T_i+\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{LO}}\big)/\big(m-\sum_{\tau_i\in\tau}C_i^{\mathtt{LO}}/T_i\big)$. Also, if Eq. (6) is violated with any $(t^{\text{end}}-t^*)$, it is also violated with some $(t^{\text{end}}-t^*)$ which is smaller than $\big(\sum_{\tau_i\in\tau^{\mathtt{HI}}}(T_i-D_i)\cdot C_i^{\mathtt{HI}}/T_i+C_i^{\mathtt{HI}}\big)/\big(m-\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{HI}}/T_i\big)$.

Proof: Simply applying the inequality in [17], [21] that upper-bounds the demand bound function for SC task systems, we can derive the following inequality from Eq. (3): $\sum_{\tau_i\in\tau}\mathtt{DBF}_i^{\mathtt{LO}}(t)\le t\cdot\sum_{\tau_i\in\tau}C_i^{\mathtt{LO}}/T_i+\sum_{\tau_i\in\tau}(T_i-D_i)\cdot C_i^{\mathtt{LO}}/T_i$. Also, we use $\mathtt{OP}_i^-(t^*)\le C_i^{\mathtt{LO}}$.

Using the above inequalities, if Eq. (5) is violated, the following holds:

$$\begin{aligned} m\cdot t^* &< \sum_{\tau_i\in\tau}\mathtt{DBF}_i^{\mathtt{LO}}(t^*)+\sum_{\tau_i\in\tau^{\mathtt{HI}}}\mathtt{OP}_i^-(t^*)\\ &\le t^*\cdot\sum_{\tau_i\in\tau}C_i^{\mathtt{LO}}/T_i+\sum_{\tau_i\in\tau}(T_i-D_i)\cdot C_i^{\mathtt{LO}}/T_i+\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{LO}}\\ \Rightarrow t^*\cdot\big(m-\sum_{\tau_i\in\tau}C_i^{\mathtt{LO}}/T_i\big) &< \sum_{\tau_i\in\tau}(T_i-D_i)\cdot C_i^{\mathtt{LO}}/T_i+\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{LO}}\\ \Rightarrow t^* &< \frac{\sum_{\tau_i\in\tau}(T_i-D_i)\cdot C_i^{\mathtt{LO}}/T_i+\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{LO}}}{m-\sum_{\tau_i\in\tau}C_i^{\mathtt{LO}}/T_i}. \end{aligned}$$

Using the same technique, we can derive an upper bound for $(t^{\text{end}}-t^*)$. First, we also derive the following inequality from Eq. (4) by applying [17], [21]: $\sum_{\tau_i\in\tau^{\mathtt{HI}}}\mathtt{DBF}_i^{\mathtt{HI}}(t)\le t\cdot\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{HI}}/T_i+\sum_{\tau_i\in\tau^{\mathtt{HI}}}(T_i-D_i)\cdot C_i^{\mathtt{HI}}/T_i$. Using this inequality and $\mathtt{OP}_i^+(t^*)\le C_i^{\mathtt{HI}}$, if Eq. (6) is violated, the following holds:

$$\begin{aligned} m\cdot(t^{\text{end}}-t^*) &< \sum_{\tau_i\in\tau^{\mathtt{HI}}}\mathtt{DBF}_i^{\mathtt{HI}}\Big(t^{\text{end}}-\Big\lceil\frac{t^*}{T_i}\Big\rceil\cdot T_i\Big)+\sum_{\tau_i\in\tau^{\mathtt{HI}}}\mathtt{OP}_i^+(t^*)\\ &\le \sum_{\tau_i\in\tau^{\mathtt{HI}}}\mathtt{DBF}_i^{\mathtt{HI}}(t^{\text{end}}-t^*)+\sum_{\tau_i\in\tau^{\mathtt{HI}}}\mathtt{OP}_i^+(t^*)\\ &\le (t^{\text{end}}-t^*)\cdot\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{HI}}/T_i+\sum_{\tau_i\in\tau^{\mathtt{HI}}}(T_i-D_i)\cdot C_i^{\mathtt{HI}}/T_i+C_i^{\mathtt{HI}}\\ &\Rightarrow (t^{\text{end}}-t^*)\cdot\big(m-\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{HI}}/T_i\big)\\ &< \sum_{\tau_i\in\tau^{\mathtt{HI}}}(T_i-D_i)\cdot C_i^{\mathtt{HI}}/T_i+C_i^{\mathtt{HI}}\\ \Rightarrow t^{\text{end}}-t^* &< \frac{\sum_{\tau_i\in\tau^{\mathtt{HI}}}(T_i-D_i)\cdot C_i^{\mathtt{HI}}/T_i+C_i^{\mathtt{HI}}}{m-\sum_{\tau_i\in\tau^{\mathtt{HI}}}C_i^{\mathtt{HI}}/T_i}. \end{aligned}$$

□

CORRECTED RESULTS OF MC-NFT FOR CONSTRAINED- DEADLINE TASK SETS IN [15], AND ADDITIONAL RESULTS FOR MC-NFT, MC-NFT*, MC-NFT-S AND MC-NFT*-S

Fig. 9 plots the detection ratio by the four proposed necessary feasibility tests while varying $\min(U^{\mathtt{LO}},U^{\mathtt{HI}})$ from $[0.40,0.45)$ to $[0.95,1.0]$ on a uniprocessor platform (i.e., $m=1$). We have the following observations. First, all the proposed tests exhibit high capability in finding infeasible task sets in that MC-NFT, MC-NFT*, MC-NFT-S, and MC-NFT*-S find 4,551 (12.3%), 5,195 (14.1%), 3,041 (8.2%) and 4,096 (11.1%) total infeasible task sets, respectively, among 36,935 task sets of interests. Such high capability can be interpreted as the benefit of dealing with unique issues pertaining to MC task systems. In particular, higher capability for constrained-deadline task sets (than that for implicit-deadline task sets) mainly comes from accurate calculation on the execution contribution of HI to the subintervals and precise constraints thereof, in that we generate a constrained-deadline task set by reducing the relative deadline of tasks in the corresponding implicit-deadline task set. Second, all the proposed tests find more infeasible task sets as $\min(U^{\mathtt{LO}},U^{\mathtt{HI}})$ increases; for example, using MC-NFT*, 3.0% and 75.5% of the task sets are proven infeasible with $\min(U^{\mathtt{LO}},U^{\mathtt{HI}})$ in $[0.4,0.45)$ and $[0.95,1.0]$, respectively. This is due to the difficulty in meeting all job deadlines of a task set with high $\min(U^{\mathtt{LO}},U^{\mathtt{HI}})$. Third, MC-NFT and MC-NFT* are shown to outperform MC-NFT-S and MC-NFT*-S, respectively, for all values of $\min(U^{\mathtt{LO}},U^{\mathtt{HI}})$. This is because MC-NFT and MC-NFT* (i) derive a tighter bound on the demand of HI jobs by considering the relationship between the mode change instant and each HI job's execution window, and (ii) test many choices of J_k^* (while MC-NFT-S and MC-NFT*-S test one choice of J_k^*). Nevertheless, MC-NFT-S and MC-NFT*-S have the same time complexity as in the SC task system case, while finding some infeasible task sets. Fourth, MC-NFT* and MC-NFT*-S outperform MC-NFT and MC-NFT-S, respectively, to some extent (by up to 6.8% and 7.0% detection ratio, respectively) for all ranges of $\min(U^{\mathtt{LO}},U^{\mathtt{HI}})$. Such an improvement can be interpreted as the benefit of considering another job release pattern favorable to finding infeasible MC task sets, compared to the synchronous one.

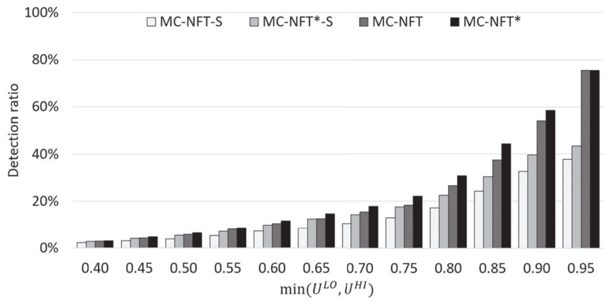

Fig. 9. Detection ratio of the four proposed necessary feasibility tests for constrained-deadline task sets with different ranges of $\min(U^{\mathtt{LO}},U^{\mathtt{HI}})$ when $m=1$, $n=4$, $\mathsf{CP}=0.5$ and $\mathsf{CF}=2$

Recall that there is no clear dominance relation between MC-NFT and MC-NFT* in terms of capability in finding infeasible task sets as stated in Lemma 14. Thus, these two tests can be used to complement each other in discovering a more infeasible task sets. By combining the results of MC-NFT and MC-NFT*, 5,608 (15.2%) total infeasible tasks sets were proven infeasible, which finds 1.1% more infeasible task sets than the maximum performance of the two tests.