Abstract

The development of complex real-time distributed embedded systems is challenging since the functional requirements also include the timing requirements. While it is well-understood how to decompose system level untimed functional requirements into component and subsystem level functional requirements, the same can not be said about timing requirements.

This work proposes an early stage hierarchical time-budgeting methodology to bridge the above gap. The main emphasis of this methodology is on the systematic derivation of component level timing (constraints) from system level timing requirements. We model the component timing requirements using parameters and synthesize constraints over these parameters. The computed constraint provides flexibility in selecting a parameter valuation as the *component's time-budget*.

For specifying the requirements we have used Parametric Temporal Logic (PLTL) which extends linear temporal logic with parametric operators like $\Box_{\leq y}$ and $\Diamond_{\leq x}$. One of the main steps in the component time-budgeting involves checking the validity of a PLTL formula. Due to the presence of parameters, the validity checking problem reduces to a constraint computation problem, such that any satisfying assignment of the computed constraint makes the formula valid.

To check whether the constraint is trivial, a *parameter abstraction* operation over PLTL formulae has been defined. Based on this operation, a set of parameter-free formulae is obtained from the given formula and the triviality check is reduced to verifying the satisfiability/validity of any formula from this set. For the non-trivial case, we have developed two separate algorithms: (i) For a fragment of PLTL defined by *bounded response* formulae, a tree-based constraint computation algorithm is given. A salient feature of this algorithm is the use of only Boolean satisfiability checks while computing the constraint. (ii) For the fragment PLTL$_{\Box}$ consisting of formulae in which only $\Box_{\leq y}$ operator contains parameter variables, a search based technique to find the extreme points called *corner points* for the given formula has been defined. The required constraint is defined over these points. For general PLTL, we have proved an inadequacy result for constraint computation and hence used a heuristic.

We have developed a tool called *Time-Budgeting Tool* for the hierarchical time-budgeting methodology. By using the tool, the efficacy of the methodology on case studies involving two automotive features: Adaptive Cruise Control (ACC) and Collision Mitigation (CM) has been demonstrated.

Keywords: *Requirements Engineering, Formal Specifications, Real-time Systems, Temporal Logics, Synthesis Problems, Component Based Design*