Formal Verification of Safety Critical Software with SPIN: Model Checking Applied to Railway Interlocking Systems

Fabio Tosi  
fabio.tosi@ticino.com  
Department of Informatics, University of Fribourg  
Boulevard de Pérolles 90, CH-1700 FRIBOURG

Linear temporal logic (LTL) has become a very basic tool for specifying properties of reactive and concurrent systems. For finite-state systems, it is possible to use techniques based on Büchi automata – along with LTL – to verify if a given system meets its specifications, that is, if specified properties hold or do not. There are two types of properties that can be expressed using LTL: \textit{safety} and \textit{liveness} properties. Together, such properties can be used to characterize the principal functionalities of the investigated system.

The intimate relationship between Büchi automata and propositional LTL (PLTL) has made both tools fundamental components of the model checking approach to formal verification of the above mentioned systems. Because of its proven effectiveness and ease of use, such an approach has become a viable alternative to simulation and testing in industry, it seeks to automatically verify if a given system satisfies its specifications, and it is based on the translation of both the abstract system’s model and the properties, expressed as PLTL formulae, into their equivalent Büchi automata.

Concretely, the method consists in expressing the desired properties using PLTL operators – in PLTL one can encode formulae about the future of paths – and checking if the (abstract) model of the investigated system satisfies such properties. The used technique is to develop the negated version of the property that should hold in the model, translate it into an automaton representing the bad behaviours, build the automaton representing the model, construct the intersection of the two automata and do an emptiness check of the obtained intersection. If the latter is empty, that is, the model and the negated property do not have any common behaviour, then the model is correct with respect to the property.

The goal of the project has been the development of an application that can model, simulate and verify the behaviour of real railway interlocking systems (RISs). Since the created models describe real, safe-critical RISs, it is necessary to formally verify their properties: the above described method has been used to achieve the goal. The results obtained from RISs of different sizes (i.e., of different complexity), show that PROMELA, along with SPIN – which acts as an efficient simulation and verification tool for the (PROMELA) generated models –, can be employed as a mean to achieve the application’s requested goal, but only on condition that the hardware on which the verification processes run are equipped with a (very) huge amount of main memory. The existence of the so called \textit{states space explosion problem}, by increasing models’ complexity, is simply confirmed.

**Supervisor:** Professor Ulrich, Ultes-Nitsche  
**Assistant:** Thierry, Nicola