Abstract

The present thesis is about the formal verification of temporal properties of infinite-state reactive systems. We propose a tableau proof system for the model-checking of properties expressed in the full branching time temporal logic CTL* over an assertion language $\mathcal{L}$. The proof system applies to an arbitrary CTL* formula. There is no need to transform formulas into some canonical form.

The basic proof object in our method is a *proof structure* (a.k.a. tableau). There are two types of proof structures (LTL and ELL), each corresponding to a sublogic of CTL*. Accordingly, there are two dual sets of proof rules. Some of these rules require the validity of an assertion from $\mathcal{L}$ to be proven as part of their application. Each type of proof structure has its own *success criterion,* which ensures that eventuality subformulas of the original formula are satisfied as appropriate. Only successful tableaux qualify as legal *proofs* of a property.

Each success criterion is formulated as a temporal property of some specific form. The latter has to be satisfied by a certain transition system associated with a given tableau and the reactive system to be verified. A run of this *associated transition system,* called a *trail* of the proof structure, combines a run of the system with a path in the proof structure. We introduce one additional proof rule for each success criterion. These rules employ a well-foundedness argument to establish that a proof structure of the respective type is successful. A proof of a CTL* property of a given system is then a finite collection of LTL and ELL proof structures the success of which has been established using the respective rules. As the success rules also exclusively rely on reasoning in $\mathcal{L}$ our method reduces all temporal reasoning to proving the validity of formulas from $\mathcal{L}$. Therefore, no theorem proving in the temporal logic itself is required. We call our method *deductive local model checking*, as it generalises both local model checking techniques for finite-state systems as well as proof systems for LTL and CTL that have been described in the literature.

We show that our proof system for model checking is sound and complete relative to validity of formulas from the assertion language $\mathcal{L}$. The major part of the proof relies on a game-theoretic argument. As a first and quite independent step we introduce the notion of a CTL* game, an infinite two-player game, where one player ($\exists$) tries to show that a property holds of the system, while the other player ($\forall$) tries to refute it. We give a characterisation of the satisfaction of a CTL* property in terms of the existence of a winning strategy for Player $\exists$. In a second step, we analyse the internal structure of paths and trails in proof structures and link it up with the game-theoretic ideas developed in the previous step. In particular, to each trail of a LTL (ELL) proof structure corresponds a $\forall$-strategy ($\exists$-strategy) of a LTL (ELL) game. We show that a successful proof structure for a given LTL or ELL formula and system exists precisely if Player $\exists$ has a winning strategy for the corresponding game. In doing so, we compare our notion of success with admissibility, an alternative notion of success proposed in the literature. The results for LTL and ELL are then lifted to full CTL*. As a final step we show that the success rules are sound and relatively complete.

We then study different types of fairness and extend our success rules to account for them. Finally, the application of the proof system is illustrated on a non-trivial example.