A Model Checker for Linear Time Temporal Logic

Michael Fisher
The TEMPLE Group, Department of Computer Science, University of Manchester, UK

Keywords: Temporal logic; Program verification; Model checking

Abstract. This report describes the design and implementation of a model checker for linear time temporal logic. The model checker uses a depth-first search algorithm that attempts to find a minimal satisfying model and uses as little space as possible during the checking procedure. The depth-first nature of the algorithm enables the model checker to be used where space is at a premium.

1. Introduction

Temporal logic has been widely used for the specification and verification of reactive systems. It has been successfully used to describe verifiable properties of state-machines derived from practical applications [CES83, BCD84, GoB88]. In this report we consider the verification of temporal properties of such state-machines through model-checking [CES83] (also known as satisfiability checking). Using this approach, a finite state-machine, often derived from some practical system, is checked to see if it satisfies various properties represented by temporal formulae. The satisfaction of these properties by the state-machine generally implies that the original system satisfies such properties.

In this report we consider a model checking algorithm for linear time temporal logic. We will begin by describing the type of logic and the definitions of satisfiability and model checking used here.

---

1 This work was supported both by Alvey under grant PRJ/SE/054 (SERC grant GR/D/57942) and by ESPRIT under Basic Research Action 3096 (SPEC).
Correspondence and offprint requests to: M. Fisher, The TEMPLE Group, Department of Computer Science, University of Manchester, Oxford Road, Manchester M13 9PL, UK.
2. Temporal Logic and Model Checking

Temporal logic is a derivative of modal and tense logics that has been developed for use in the description of reactive computer systems [Pnu77]. Propositional temporal logic can be seen as classical propositional logic extended with various modalities. Commonly, these are $\Diamond$, $\Box$ and $\circ$. The intuitive meaning of these connectives is as follows: $\Diamond \varphi$ is true if $\varphi$ is true sometime in the future; $\Box \varphi$ is true if $\varphi$ is true always in the future; and $\circ \varphi$ is true if $\varphi$ is true at the next moment in time.

Obviously, the model of time used will affect the meaning of such connectives. For example, if we consider time to be a dense ordering of "moments", then we cannot use the $\circ$ operator as there is no distinct "next moment". If we think of the future as being a branching structure, then the meaning of $\Diamond$ must be clarified so that we know whether $\Diamond \varphi$ means that $\varphi$ must be true on some path in the future, or on all paths in the future. Thus there is a great variety of such logics, including dense logics [BKP86], branching logics [Emil82] and past-time logics [LPZ85], many of which can be placed in a single framework [Fis89].

In this report we will only consider a model of time that is linear and discrete, and allows statements about the present and future. The model structure for such a logic can be given as

$$\mathcal{M} = (S, \mathcal{N}, \pi)$$

where $S$ is a set of states, $\mathcal{N}$ is an infix binary relation on states, and $\pi$ is a mapping from states to sets of atomic propositions. Thus, given a set of basic propositions $PROP$, and a state $s$, $\pi(s)$ is the set of propositions (a subset of $PROP$) that are true in state $s$. The relation $\mathcal{N}$ is the "next-time" relation. It is constrained to define a linear sequence of states such that any given state is only related by $\mathcal{N}$ to at most one "next" state.

We give an interpretation for a temporal statement in a model $\mathcal{M}$, and at a particular state $s$. For example, the semantics of the $\circ$ operator is simply

$$\langle \mathcal{M}, s \rangle \models \circ \varphi \quad \text{iff} \quad \forall t \in S. \text{ if } s \mathcal{N} t \text{ then } \langle \mathcal{M}, t \rangle \models \varphi$$

The particular temporal language we use in this report consists of the connectives of standard propositional logic together with the unary operators $\circ$ and $\Diamond$, and the binary operators $\setminus$ and $\cdot$. The informal semantics of these operators are as follows: both $\circ \varphi$ and $\Diamond \varphi$ mean that $\varphi$ must occur in the next state, the difference being that if there is no next state, $\circ \varphi$ is true, while $\Diamond \varphi$ is false; $\varphi \setminus \psi$ means that $\varphi$ must be true up to a point in the future where $\psi$ occurs, or always in the future if $\psi$ never occurs; $\varphi \cdot \psi$ is similar $\varphi \setminus \psi$, the only difference being that with the $\cdot$ operator, $\psi$ must occur sometime in the future. The semantics of these operators is given below. (Note that the relation $\mathcal{R}$ is the transitive closure of $\mathcal{N}$.)