Design and Verification of the Sequential Systems Automata Using Temporal Logic Specifications

Ursu A., Gruita G., Zaporojan S.
Technical University of Moldova,
Information Technology Department,
Blvd. Stefan Cel Mare 168, Chisinau, Moldova, Romania
phone: (+373-2) 49-70-18, fax: (+373-2) 24-71-14

Abstract

A design and verification method of sequential systems automata using temporal logic specifications is proposed. The method is based on well-known Z.Manna and P.Wolper temporal logic satisfiability analysis procedure. A new satisfiability analysis algorithm for temporal logic specifications which includes past time as well as future time temporal logic operators is proposed. A case study is carried out which deals with two design examples.

The method is developed to facilitate the design of the finite state automata of the sequential systems and is based on the analysis of the temporal logic specifications which describe the desired input/output behaviour of the systems. The method can be considered in fact a state identification method since it determines the states of the sequential system. Determining the finite state automaton is important not only for the design process. The verification of a sequential system is usually based on the automaton of the designed system. Generating the finite state automaton of the designed system the designer can analyse the properties of this automaton and to determine whether the initial specifications of the system are correct or not. More over the designer usually needs to test an implemented system. To do this the designer may need the automaton of the system. Verifying the initial automaton generated from the functional specifications with the automaton generated from the temporal logic specifications of the input/output behaviour of the implemented system it is possible to determine if the implementation is correct or not. Te method is dedicated:

- to facilitate the design of the sequential systems finite state automata;
- to verify the correctness of the finite state automata implementation;

provided the timing charts are given in both cases and the initial automaton of the system is also known in the verification case. We consider the method as two different methods in two different cases: the design case and the verification case.

The design method consists of the following steps:

1. functional description of the designed sequential system;
2. design of the temporal logic specifications which describe the input/output behaviour of the system;
3. satisfiability analysis of the temporal logic specifications;
4. design of the finite state-graph of the specifications;
5. design of the finite automaton of the specifications;
6. design of the state and output logical functions.

The verification method consists of the following steps:

1. functional description of the verified sequential system as follows from its timing charts;
2. design of the temporal logic specifications which describe the input/output behaviour of the system;
3. satisfiability analysis of the temporal logic specifications;
4. design of the finite state-graph of the specifications;
5. design of the finite automaton of the specifications;
6. analysis of the equivalence relation between the initial automaton of the system and the automaton generated from the temporal logic specifications of the timing charts.

The satisfiability analysis of the specifications (step 3) is based on an algorithm like the Z.Manna and P.Wolper procedure but is developed by authors to include the analysis of the past time intervals formulas.

ED&TC '97 on CD-ROM