Solution notes

Specification and Verification II 2005 – Paper 7 Question 7 (MJCG)

(a) What is model checking? [4 marks]

Model checking is an algorithmic method of checking that properties, stated in a property language (usually some kind of temporal logic), hold of a model of a design.

(b) Distinguish between explicit state and symbolic model checking. [4 marks]

Explicit state model checking uses algorithms that explicitly represent the state space of the model being checked in a data structure or peripheral device (e.g. disk). Symbolic model checking encodes the set of states by a symbolic formula (usually in boolean algebra) that is represented in a data structure such as a Binary Decision Diagram (BDD).

(c) Describe briefly the state explosion problem in formal verification. [4 marks]

The number of state of a model is 2^n, where n is the number of boolean variables. It thus grows exponentially. If n is too large this set "explodes" – i.e. is too big to represent.

(d) How might theorem proving help with the state explosion problem. [4 marks]

Theorem proving can help with the state explosion problem by avoiding having to actually compute a represention (explicit or symbolic) of the set of states. Instead, formal descriptions of the state space are manipulated deductively to extablish that properties hold.

(e) How might abstraction help with the state explosion problem. [4 marks]

Abstraction is a method to reduce the size of the state space by creating a simplified model. When creating abstractions one must be careful to ensure that properties checked in the abstracted model do not give false positives or negatives for the real model.

Context

This question is about verification methodology and relates to the last part of the course, which concentrates on model checking.

Marking Scheme

For each of the parts I'll give 4 marks only if the candidate completely understands the question and clearly knows the answer. This will involve some judgement by the assessor (assumed to be me). I'll give 3 marks if I feel the candidate has a good grasp, but maybe writes a minimal or slightly off-center answer. To get 2 marks the candidate will need to demonstate fair knowledge, though this may be incomplete; for 1 mark there should be something correct, but the answer is mostly off target. I regard 2 and higher as a "pass".