Maturation

- 1960s, 1970s: axiomatic verification of ADTs
- 1981: Clarke and Emerson, Queille and Sifakis independently introduce model checking *
- mid 1980s: Bryant, McMillan solve the “state explosion” problem by cleverly applying binary decision diagrams to model checking
- 1980s, 1990s: model checking widely used in software verification, e.g. train scheduling, air-traffic collision avoidance, etc.

Overview of Model Checking

- Express the synchronization essentials of code as a state transition diagram (the “model”)
- Express the desired properties in (propositional, branching-time) temporal logic (the “specification”)
- Feed both of these to an efficient program (the “model checker”), which automatically verifies whether the former satisfies the latter by exhaustively searching all the states of the diagram
- The result is yes, no, or timed out, and if no, why

Model Checking Visualized

- Diagram illustrating temporal logic formulas in model checking.
Examples

- Two-process mutual exclusion problem:
  - Each of two processes can be in one of three states: N (non-critical), T (trying), and C (critical)
  - Is mutual exclusion guaranteed: EF (C1 ^ C2) is false?
  - Is non-starvation guaranteed: T1 => AF(C1) is true?
- Alternating Bit Protocol:
  - Is it correct?

Research Method

- Real-world motivation:
  - Checking programs is difficult; existing methods are tedious
- Research problem:
  - Check properties of a simple concurrent program
- Method:
  - Extend/improve existing theory
- Result:
  - New logic and algorithm; breakthrough
- Impact:
  - Seminal work in model checking
  - Proved formal methods to be applicable to large programs

Assessment

- Problem type:
- Research model:
  - Apply theory (temporal logic) in a novel way
- Hypothesis:
  - (1) proof construction can be replaced by fast automatic check
  - (2) the technique can be applied to other problems as well
- Validation:
  - Rigorous analysis; theory
  - Simple examples and EMC implementation
  - Industrial acceptance of the method

Pro Forma Abstract

- Studies of the original logic system (CTL) for model checking proved to be deficient in expressing “fairness” of execution. Authors introduce an improved version of logic which captures fairness, thereby eliminating the possibility of infinite states. By considering only fair execution sequences, authors demonstrate the correctness of the alternating bit communication protocol.
- Note that this paper reports an improved version of the algorithm, an operational implementation of the EMC system, and a new counterexample facility.
Trivia

• What is EMC?
  – $E = MC^2$
  – Extended Model Checker
  – NASDAQ:EMC (EMC Corporation)
  – Edmund M. Clarke’s SCS user id