Instead of manipulating to show that one does not exist
the aim is to construct a counterexample to the specified property

• the property to check \( P_{10}(s) \)
• there exists a loop \( s \) with \( D(s) \)
  
Consider the above formulas together with a description of
(\( \text{Prop} \)') the behavior \( \rho \) to the \( g \) in the state transitions
(i) \( \text{Init}(s) \) that enables to line for all initial states
• transition system described by \( \text{Propositional formula} \)
  
(b) states are assigned to the state variables (a vector) \( s \)
  
Circuits on which \( \text{Propositional formula} \) used to feed are often transition systems

---

Experiments comparing the runtime of different approaches

• \( \text{Runs} \) symbolic Boolean evaluation
• \( \text{Runs} \) bounded model checking
• Two methods:
  
 1. model checking methods that use SAT solvers instead of BDDs
  
2. search for counterexamples to detect properties of interest

Search for bugs in a memory system of Alpha, Inc.

Please, Chapter 7

---

3 December 2001

Sanh Vinhlin, Subject:

Model Checking Using SAT Solvers

EUC-98 Postgraduate Course in Digital Systems Seminar
Merge buffer


defined as an example: \[ [x, y] \] \[=\] \[\{ \{x, y\} \} =\]

Note: A register file \( M \) is not even a type of \( M \)

the required level of abstraction is zero, and no specific

high level of abstraction for STF

now applied to verification of the correctness of gamess which is a

not previously combined with SAT solvers always with BDDs

merge abstract verification and symbolic execution

Symbolic trajectory evaluation (STE)
Methodology Proposal

1. Begin analyzing a new system with BNC
2. Use a small bound to make the inspection quicker
3. Determine false counterexamples by modifying the transactions
4. Check longer and longer runs with the limited strategy
5. Observe the failure trace to check for other similar failures
6. After a bug has been found and fixed, ensure removal by STBE
7. When BNC starts to take too long (or if, use STBE in parallel
8. When nothing is found anymore, try SWP or move on

& X is not equivalent to Y equivalently deeper exploration
a version SAT-based of STBE implemented in PICT

SAT-based symbolic trajectory evaluation

Bounded Model Checking

Followed by backtracking
A simple strategy: limited strategies consisting of 1-satification
Cartesian product sessions for modes using subroutines
State variables for the verification maintained less than with SWP
Powers not available for Alpha = experiments on a 32-bit PC

SAT-based model checking with BDDs

Symbolic model checking with BDDs

Many bugs were found
Verification takes several hours
The memory bricked too large to handle: some bugs were fixed
SWP ported to 64-bit Alpha with 8 GB main memory
Proofs one evaluation of several BDD-based tools, SWP being the only