Lecture notes:
Verification with Small and Short Worlds (S\textsuperscript{2}W)

Presenter: Jaesung Park

Feb 28, 2017

1 Overview

1. Problem statement
   (a) System model for large arrays and data structures
   (b) Safety property to verify

2. Methodology of S\textsuperscript{2}W
   (a) Induction, if we are lucky
   (b) Small World, restricting the search space
   (c) Short World, bounding the number of steps

3. Evaluation
   (a) Table Look-ahead Buffer (TLB) of Bochs x86 emulator
   (b) Set-associative cache and Content Adressable Memory (CAM)
   (c) Shadow paging
2 Problem Statement

2.1 System Model

\[ S = (I, O, \mathcal{V}, Init, A) \] : system model

\( I \) : a finite set of input variables
\( O \) : a finite set of output variables
\( \mathcal{V} \) : a finite set of variables
\( Init \) : a finite set of initial values
\( A \) : a finite set of actions

\[ I = \{ addr \} \]
\[ O = \{ out \} \]
\[ \mathcal{V} = \{ \text{mem, cache} \} \]
\( Init = (\text{mem}_0, \text{cache}_0) \)
\( A \) : updating cache and return the value in mem

2.2 Problem Definition

The goal is to verify \( G\Phi \), the temporal safety property we are interested in.

\( G \) : the temporal operator “always”
\( \Phi \) : the temporal operator “always”

In the example,

\[ \Phi_2 = \forall x. (addr = x) \rightarrow ((\text{cache}.addr = addr \land \text{cache}.addr \neq 0) \rightarrow \text{cache}.data = \text{mem}[addr]) \].
3 Methodology of S\textsuperscript{2}W

3.1 Induction

Using one-step induction,

\[ \text{Init}(V) \rightarrow \Phi(V) \]
\[ \Phi(V) \land R(V, V') \rightarrow \Phi(V') . \]

If both checks pass, the verification is complete. Otherwise, S\textsuperscript{2}W continues.

In the example, induction fails when

\[ \text{mem}[i] := a, \quad \text{mem}[j] := b, \quad \text{cache.addr} := i, \quad \text{cache.data} := z, \]

and read(i) is given.

3.2 Small World

Instantiate the free variables in \( \Phi \) with symbols. It defines a dependence set (\( U \)).

In the example,

\[ \Phi_2 = \forall x. (\text{addr} = x) \rightarrow ((\text{cache.addr} = \text{addr} \land \text{cache.addr} \neq 0) \rightarrow \text{cache.data} = \text{mem[addr]}) . \]

In the form of \( \forall x. \Phi(x) \), replacing \( x \) with a fixed symbolic value \( a \), we verify \( \Phi(a) \), and \( U = \{ \text{mem}[a], \text{cache} \} \).

In result, the search space is restricted.

This way, the state space is reduced from \( 2^{3}4 \) states to the following 16 states:

\[
\{ \text{cache.addr} = a, \text{cache.addr} \neq a, \text{cache.addr} = 0, \text{cache.addr} \neq 0 \}
\times \{ \text{cache.data} = 0, \text{cache.data} = 1 \} \times \{ \text{mem}[a] = 0, \text{mem}[a] = 1 \} .
\]
### 3.3 Short World

Diameter $D$ of the abstract model, the smallest integer where for every reachable states, there is a sequence of inputs of length $\leq D$.

Find the upper bound of $D$ denoted by $k$, then run Bounded Model Checking (BMC) with the maximum number of steps $k$.

In result, the search space is restricted.

In the example, at most 2 steps are used to reach all reachable states.

### 4 Evaluation

#### 4.1 Bochs’ TLB

Safety property to verify:

"Does TLB indicate the correct a physical address with respect to a virtual address, if TLB has the entry?"

1. **Induction**: fails.
2. **Small World**: looking only at a specific location of memory and page entry.
3. **Short World**: bounded by 9 steps.

BMC took 25 45 minutes in $S^2W$. 

---

*Diagram showing TLB and Page Table interaction.*
4.2 Content Addressable Memory

Safety property to verify:

“Do the CAM and memory have the same data for all keys present in CAM?”

1. **Induction**: fails.

2. **Small World**: looking only at $\text{mem}[a]$, $\text{map}[a]$ and $\text{cam}[\text{map}[a]]$.

3. **Short World**: bounded by 5 steps.

BMC took 5 15 seconds in $S^3W$. 
4.3 Shadow Paging

Safety property to verify:
(1) "Is the address under fixed limit, if page size extension bit is on?"
(2) "Is the address under fixed limit, if page size extension bit is off?"

1. **Induction**: (1) success, (2) fails.
2. **Small World**: (2) looking only at sPDT[ai] and SPT[aj].
3. **Short World**: (2) bounded by 4 steps.

BMC took < 1 minute in $S^2W$ for verifying (2).