

COMP424/524-06A Topics in Software Engineering

Part I – Model Checking Algorithms
17. Symbolic Model Checking

Robi Malik

THE UNIVERSITY OF
WAIKATO DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

Calculating State Sets

- State sets of an automaton can be represented as an OBDD!

$\neg \wedge \vee \Rightarrow \Leftrightarrow$

- Propositional connectives can be evaluated using OBDD algorithms.
- What about temporal connectives?

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 4

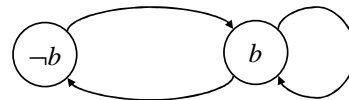
Why Symbolic?

Symbolic Model Checking

Any model checking method that represents state sets *symbolically* as opposed to *explicitly* enumerating states, usually using OBDDs.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 2

Example



$$T = (\neg b \wedge b') \vee (b \wedge \neg b') \vee (b \wedge b')$$

$$= (\neg b \wedge b') \vee b$$

Calculating EX

$$\mathbf{EX} \neg b = \exists b' (T \wedge \neg b')$$

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 5

Model Checking Task

Given:

- Kripke-Structure K
- CTL Formula φ

Task:

- Identify the *set of states* of K where φ is true.

p
 $\neg\varphi \quad \varphi \wedge \psi \quad \dots$
 $\mathbf{AX} \varphi \quad \mathbf{EX} \varphi$
 $\mathbf{AG} \varphi \quad \mathbf{EG} \varphi$
 $\mathbf{AF} p \quad \mathbf{EF} \varphi$
 $\mathbf{A}(\varphi \mathbf{U} \psi)$
 $\mathbf{E}(\varphi \mathbf{U} \psi)$

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 3

Boolean Quantification

$$\exists x f = f|_{x \leftarrow 0} \vee f|_{x \leftarrow 1}$$

$$\forall x f = f|_{x \leftarrow 0} \wedge f|_{x \leftarrow 1}$$

$f|_{x \leftarrow v} =$ The formula obtained from f when x is evaluated as v .

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 6

The General Case

$\mathbf{EX} \phi = \exists V' (T \wedge \phi')$

$\mathbf{AX} \phi = \forall V' (T \Rightarrow \phi')$

Boolean
quantification over
all primed variables.

Replace every
Boolean variable x
in ϕ by its primed
version x' .

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 7

Evaluating $\mathbf{E}(\phi \mathbf{U} \psi)$

$\mathbf{E}(\phi \mathbf{U} \psi) = \text{lfp } \lambda X. (\psi \vee (\phi \wedge \mathbf{EX} X))$

```

OBDD evalEU(OBDD  $\phi$ , OBDD  $\psi$ ) {
  OBDD x = OBDD_FALSE;
  do {
    OBDD prevx = x;
    x =  $\psi \vee (\phi \wedge \text{evalEX}(x))$ ;
  } while (prevx != x)
  return x;
}

```

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 10

Symbolic Model Checking for $\mathbf{EF} \phi$

1. Build OBDD T for transition relation;
2. Build OBDD X_0 for ϕ ;
3. $i := 0$;
4. **do**
5. $i := i + 1$;
6. $X_i := X_{i-1} \vee \exists V' (T \wedge X'_i)$;
7. **while** $X_i \neq X_{i-1}$;
8. **return** X_i ;

$\mathbf{EX} X_i$

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 8

Symbolic Model Checking Procedure

```

OBDD eval(Formula  $f$ )
{
  case
   $f$  is an atomic proposition: return  $f$ ;
   $f = \neg\phi$ : return  $\neg\text{eval}(\phi)$ ;
   $f = \phi \vee \psi$ : return  $\text{eval}(\phi) \vee \text{eval}(\psi)$ ;
   $f = \mathbf{EX} \phi$ : return  $\exists V' (T \wedge \phi')$ ;
   $f = \mathbf{EG} \phi$ : return  $\text{evalEG}(\phi)$ ;
   $f = \mathbf{E}(\phi \mathbf{U} \psi)$ : return  $\text{evalEU}(\phi, \psi)$ ;
  esac
}

```

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 11

Using Fixed Point Characterisation

$\mathbf{EF} \phi = \text{lfp } \lambda X. (\phi \vee \mathbf{EX} X)$

```

OBDD evalEF(OBDD  $\phi$ ) {
  OBDD x = OBDD_FALSE;
  do {
    OBDD prevx = x;
    x =  $\phi \vee \text{evalEX}(x)$ ;
  } while (prevx != x)
  return x;
}

```

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 9

Other Temporal Operators ...

The missing temporal connectives

$\mathbf{AX} \mathbf{EF} \mathbf{AG} \mathbf{AF} \mathbf{A}(_ \mathbf{U} _)$

can be expressed using the others:

$\mathbf{AX} \phi \equiv \neg \mathbf{EX} \neg \phi$
 $\mathbf{EF} \phi \equiv \mathbf{E}(\text{true} \mathbf{U} \phi)$
 $\mathbf{AG} \phi \equiv \neg \mathbf{EF} \neg \phi$
 $\mathbf{AF} \phi \equiv \neg \mathbf{EG} \neg \phi$
 $\mathbf{A}(\phi \mathbf{U} \psi) \equiv \neg (\mathbf{E}(\neg \psi \mathbf{U} \neg \phi \wedge \neg \psi) \vee \mathbf{EG} \neg \psi)$

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-17 Slide 12