Transferring model-checking, satisfiability, and validity, problems of LTL to problems of Buchi automata

Lecture Scribe: Mark Lemay

4/9/2015

State explosion

Recall,

- The regular set \( \{a, b\}^* \) is defined by the regular expression \((a + b)^*\). The set \( \{a, b\}^* \) has countable cardinality.

- \( 2^{AP} \) defined in handout 23 page 20, as the set of all possible assignments to a set of propositions.
  - For Example, if \( AP \) has the a single proposition \( p \), \( AP = \{p\} \) then the cardinality of \( 2^{AP} \) is \( |2^{AP}| = 2 \), since there are only 2 assignments that can be assigned to \( p \).

- Consider the regular expression \( (2^{AP})^* \) it grows exponentially.

- Now consider \( (2^{AP})^\omega \), it has cardinality \( 2^{\aleph_0} \) and is uncountable. For the purposes of this course we can limit ourselves to countable subsets.

Example

Consider the model

For the path \( \pi \triangleq (s_1 s_2 s_3)^\omega \) the trace would be \( \text{trace}(\pi) \triangleq ((tt, ff), (tt, tt), (ff, tt))^\omega \) where the ordered pair of truth and false values stand for \( p \) and \( q \) respectively.
Problems

See also Hanwen Wu's scribe notes.

There are several common problems we want to solve in our logic systems.

⋄ Model checking (MC) given a model $M$, and a wff $\varphi$, decide if $M \models \varphi$?

⋄ Satisfiability (SAT) given a wff $\varphi$, decide if there exists a model $M$ such that $M \models \varphi$?

⋄ Validity (VAL) given a wff $\varphi$, is it the case that for all models $M$ that $M \models \varphi$?

Complexity classes

<table>
<thead>
<tr>
<th>Logic</th>
<th>Model checking</th>
<th>Satisfiability</th>
<th>Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTL</td>
<td>PSPACE-complete</td>
<td>PSPACE-complete</td>
<td>PSPACE-complete</td>
</tr>
<tr>
<td>CTL</td>
<td>PSPACE-complete</td>
<td>EXPTIME-complete</td>
<td>EXPTIME-complete</td>
</tr>
<tr>
<td>CTL*</td>
<td>PSPACE-complete</td>
<td>2-EXPTIME-complete</td>
<td>2-EXPTIME-complete</td>
</tr>
<tr>
<td>PL (Propositional Logic)</td>
<td>Linear time</td>
<td>NP-complete</td>
<td>co-NP-complete</td>
</tr>
<tr>
<td>FOL (First Order Logic)</td>
<td>Undecidable</td>
<td>Undecidable</td>
<td>Undecidable(semi-decidable)</td>
</tr>
</tbody>
</table>

Note that

⋄ Model checking in Propositional Logic is very efficient, by assigning the truth values of the model to the leaves of the parse tree and evaluating it up.

⋄ The Satisfiability of Propositional Logic was the first problem to be shown NP-complete.

⋄ The Validity of First Order Logic is semi-decidable (recursively enumerable), because we can enumerate over all proofs of finite length.

Probabilistic Computation Tree Logic (PCTL)

Consider the non probabilistic model $M$ over the propositional atom $p$

We can answer some simple questions about it.

⋄ $M, s_1 \models_{\text{LTL}} Fp$? NO!

⋄ $M \models_{\text{CTL}} AFp$? NO!

⋄ $M \models_{\text{CTL}} EFp$? YES!

Now consider a probabilistic version of that model, $M'$

More on LTL, CTL, and CTL*
○ $\mathcal{M}' \models_{FCTL} \mathcal{F}_{\geq 1/2} p$, because

- $\mathcal{M}', s_1^\omega \not\models \mathcal{F} p$. The path that stays on $s_1$ forever will not satisfy $\mathcal{F} p$. It is the only such path.
- For every other path, $\mathcal{M}', s_1^n s_2^n \models \mathcal{F} p$, for every $n \geq 1$
- The probability of the path starting with $s_1 s_1$ is $1/2$

* $s_1 s_1 s_1$ is $1/4$
* $s_1^n$ is less than $1/4$

By the same reasoning, for every probability $\rho$ such that $0 \leq \rho < 1$

$\mathcal{M}' \models \mathcal{F}_{\geq \rho} p$

It is possible to say $\rho \leq 1$ with a more complicated argument from measure theory.

Unsurprisingly,

$\mathcal{M}' \not\models \mathcal{F}_{< \rho} p$

First Order LTL

We can extend LTL with first order connectives

$\varphi ::= P(x_1, \ldots, x_n) \mid \bot \mid \neg \varphi \mid \varphi_1 \land \varphi_2 \mid \exists x \varphi \mid X \varphi \mid \varphi_1 U \varphi_2$

Derived Temporal Connectives

Adapted from Davie Proserpio’s scribe notes.

We can define additional convenient connectives from existing connectives

$$X^k \varphi \triangleq \underbrace{XX \ldots X}_{k} \varphi$$

Means “$\varphi$ holds after exactly $k$ steps”

$$F^{\leq k} \varphi \triangleq \varphi \lor X \varphi \lor \ldots \lor X^k \varphi$$

Means “$\varphi$ will hold within at most $k$ steps”

$$G^{\leq k} \varphi \triangleq \neg F^{\leq k} \neg \varphi$$

Means “$\varphi$ holds now and will hold during the next $k$ steps”

Let’s see an example for $k = 3$ using the last WFF $G^{\leq k} \varphi$:

$$G^{\leq 3} \varphi \triangleq \neg F^{\leq 3} \neg \varphi$$

$$= \neg (\neg \varphi \lor X \neg \varphi \lor XX \neg \varphi \lor XXX \neg \varphi)$$

$$= \neg (\neg \varphi \lor \neg X \varphi \lor \neg XX \varphi \lor \neg XXX \varphi)$$

$$= \varphi \land XX \varphi \land XXX \varphi$$

“$\varphi$ holds now and will hold during the next 3 steps”
Past Temporal Connectives

Adapted from Davie Proserpio’s scribe notes.

All the temporal connectives so far may be called future connectives. These are the ones considered in the book. But, for some applications, we need to consider past connectives which are useful for specifying properties of past behavior rather than future behavior.

Let’s define them:

- $F \phi$ “eventually $\phi$”
  - $F^{-1} \phi$ “once $\phi$”

- $G \phi$ “henceforth $\phi$”
  - $G^{-1} \phi$ “so far $\phi$”

- $\phi U \psi$ “$\phi$ until $\psi$”
  - $\phi U^{-1} \psi$ “$\phi$ since $\psi$”

- $X \phi$ “next $\phi$”
  - $X^{-1} \phi$ “before $\phi$”

Just as we have the equivalence:

$$G \phi \equiv \neg F \neg \phi$$

we also have the equivalence:

$$G^{-1} \phi \equiv \neg F^{-1} \neg \phi$$

Here is a counter-intuitive fact:

Past temporal connectives do not increase the expressive power of LTL, i.e, every WFF of LTL with past connective can be written equivalently without them.

On the other hand, past temporal connectives do increase the expressive power of CTL and CTL*.

Other issues which are mentioned but not studied extensively in the book are:

- Adequate set of temporal connectives in LTL [LCS,p 186]
  - E.g.: \{X, U\}, \{X, R\} and \{X, W\} are all adequate.

- Adequate set of temporal connectives in CTL [LCS,p 216]