Математические методы верификации схем и программ

mk.cs.msu.ru → Лекционные курсы
→ Математические методы верификации схем и программ

Блок 11

Автоматный алгоритм model checking для LTL: общая схема

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2022/2023, осенний семестр

С.п. (и, в частности, модель Крипке) очень похожа по устройству и поведению на автомат, и отличий от автомата имеет не очень много:

1. В с.п. нет чтения входных символов, но вместо этого есть выполнение действий
   - Модель Крипке — это с.п., в которой действия несущественны
2. В с.п. нет выходных символов, но вместо этого есть происхождение событий
3. В с.п. интерес представляют **бесконечные пути**, тогда как в «привычных» автоматах — конечные

Если системы переходов воспринимать как автоматы, то трассы можно расценивать как бесконечные слова, а свойства трасс — как языки, которые могут распознавать такие автоматы

На этих соображениях основывается автоматный алгоритм верификации моделей Крипке относительно LTL

Общая схема автоматного алгоритма

Дано: модель Крипке M и ltl-формула φ

Желаемый результат: «да», если верно соотношение $M \models \varphi$, и «нет» иначе

Общая схема алгоритма:

1. По модели M строится автомат A_M, распознающий $\mathrm{Tr}(M)$
2. По ltl-формуле φ строится автомат $A_{\neg\varphi}$, распознающий $\mathrm{Tr}(\neg\varphi)$
3. Строится пересечение $A_\cap$ автоматов A_M и $A_{\neg\varphi}$: автомат, распознающий $\mathrm{Tr}(M) \cap \mathrm{Tr}(\neg\varphi)$
4. Проверяется пустота автомата $A_\cap$: $\mathrm{Tr}(M) \cap \mathrm{Tr}(\neg\varphi) \stackrel{?}{=} \emptyset$
5. Выдаётся ответ: «да» $\Leftrightarrow$ автомат $A_\cap$ пуст

Согласно схеме автоматного алгоритма, чтобы научиться проверять выполнимость ItI-формулы на модели Крипке, потребуется:

- Ввести разновидность автоматов, способных распознавать языки, состоящие из бесконечных слов
- Научиться строить автоматы, распознающие
  - множество трасс произвольной модели Крипке
  - свойство, задаваемое произвольной ItI-формулой
  - пересечение языков двух произвольных автоматов
- Научиться проверять пустоту произвольного автомата