Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Методы верификации конечных автоматов, взаимодействующих по акторной модели

Чебатуркин Александр Александрович

Научный руководитель: Мазин Максим Александрович

23 июня 2010 г.

Цели

- Разработать методы верификации многопоточных программных систем, основанных на акторно-автоматной модели.
- Реализовать программное обеспечение для автоматического формирования модели Крипке по исходному коду.

Задачи

- Исследовать свойства акторно-автоматной модели.
- Разработать алгоритм моделирования состояния и поведения актора-автомата.
- Разработать алгоритм композиционного моделирования компонент системы с целью уменьшения размера модели.
- Обосновать корректность алгоритмов.
- Программно реализовать алгоритмы в среде *MPS*.

Метод проверки на модели

- Спецификация свойств – совокупность формул темпоральной логики
- Модель системы представляется в виде модели Крипке
- Проверка модели системы на соответствие спецификации во всех возможных ситуациях

Акторная модель

- Нет общих изменяемых данных
- Взаимодействие асинхронное
- Интерфейс посылаемых и принимаемых сообщений строго задан
- Обработка каждого сообщения атомарна

Ограничения исходной модели

- Поведение конечно-автоматное
- Размер очереди сообщений ограничен

Состояние модели Крипке

- Состояние модели Крипке для исходного автомата
- Состояние очереди – конечная последовательность сообщений

Суть метода

- Разбить модель
- Верифицировать по частям
- Доказать эквивалентность верификации в целом и по частям

Разбиение модели

- Внутренняя компонента – моделируется внутреннее состояние и поведение акторов, состоящих в компоненте;
- Внешняя компонента – моделируется только интерфейс посылаемых/принимаемых сообщений компоненты.

Разбиение модели

- Внутренняя компонента – моделируется внутреннее состояние и поведение акторов, состоящих в компоненте;
- Внешняя компонента – моделируется только интерфейс посылаемых/принимаемых сообщений компоненты.

Проекция состояний моделей Крипке

- *C*, *C'* – модели Крипке акторно-автоматной системы
- $s_{C'} \uparrow s_C$ – проекция состояний моделей Крипке, если
  - $I_{C'} \subseteq I_C$,
  - внутренние состояния автоматов у общих акторов одинаковы,
  - $s_{C'}.q_{C'} \uparrow s_C.q_C$

Отношение слабого моделирования

- $C' = \langle S_{C'}, L_{C'}, T_{C'}, s_{C'0} \rangle$, $C = \langle S_C, L_C, T_C, s_{C0} \rangle$
- $I_{C'} \subseteq I_C$

- $H \subseteq S_C \times S_{C'}$ – отношение слабого моделирования, если

  $\forall s_C \in S_C, s_{C'} \in S_{C'} \qquad H(s_C, s_{C'})$
  - $s_{C'} \uparrow s_C$,
  - $\forall s_{C_1}, l \in L_C : (s_C, l, s_{C_1}) \in T_C$, то $\exists s_{C_1'}$, такое что:
    - если $l \notin L_{C'}$, то $s_{C_1'} = s_{C'}$;
    - если $l \in L_{C'}$, то $(s_{C'}, l, s_{C_1'}) \in T_{C'}$;
    - $H(s_{C_1}, s_{C_1'})$

Теорема о слабом моделировании

- Для любых двух компонент *C’* и *X* заданной модели, *C’* слабо моделирует *C = C’ || X.*

Теорема о сохранении свойств

- Если $C' \leq C$, то для любого свойства безопасности $\phi \in LTL$, из $C' \models \phi$ следует $C \models \phi$

Программная реализация

- Предложенные алгоритмы реализованы и внедрены в мультиязыковую среду MPS.
- В качестве системы, реализующей метод проверки на модели, был выбран внешний инструмент NuSMV.

Результаты

- Предложены методы верификации акторно-автоматной системы.
- Формально обоснована корректность предложенных методов.
- Разработана программная реализация.

Спасибо за внимание!