ИТМО
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Верификация автоматных программ

Г. А. Корнеев
А. А. Шалыто

Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Виды верификации

- Динамическая
  - Тестирование
- Статическая
  - Доказательная
  - **Верификация на модели**

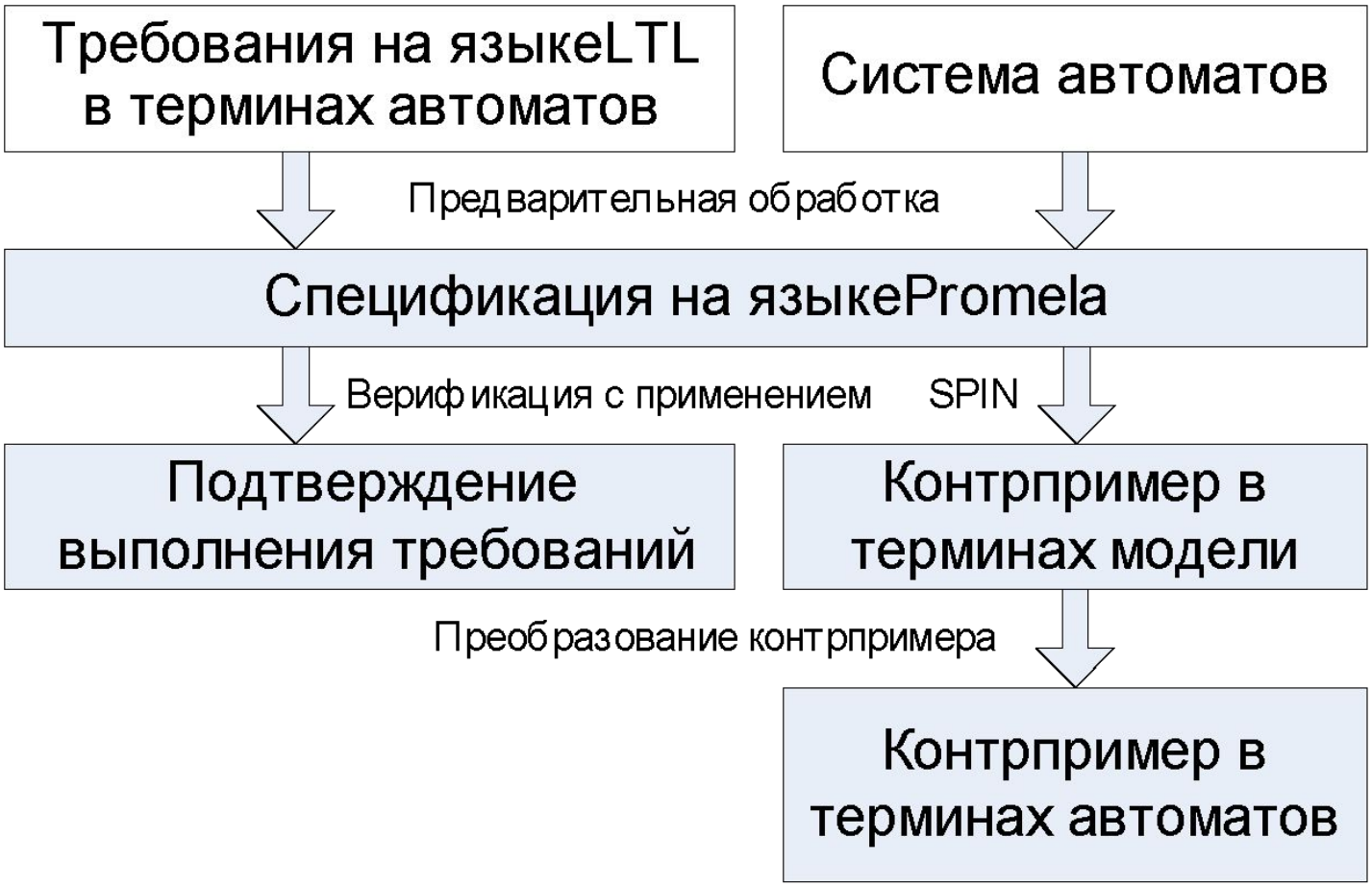
Верификация модели программы

- Построение модели Крипке
  - Соответствие модели программе
- Построение формальных требований
  - Формулировка требований в терминах модели Крипке
- Формальная верификация
  - Большая размерность пространства состояний
- Отображение контрпримеров
  - Преобразования контрпримеров в термины исходной программы

Верификация автоматной модели программы

- Формальное построение модели Крипке
  - Возможность автоматизации
- Формулировка требований
  - В терминах автоматов
- Формальная верификация
  - Рассмотрение управляющих состояний
- Формальное восстановление контрпримеров
  - В терминах исходной модели

Верификация с применением SPIN



Построение описания автомата на языке Promela

- Переменная состояния
  - Инициализируется начальным состоянием
- Автоматная процедура
  - Switch по номеру текущего состояния
  - Недетерминированный переход в следующее состояние

Обработка событий

- Описание потока событий в терминах темпоральной логики
- Извлечение события из очереди при переходе

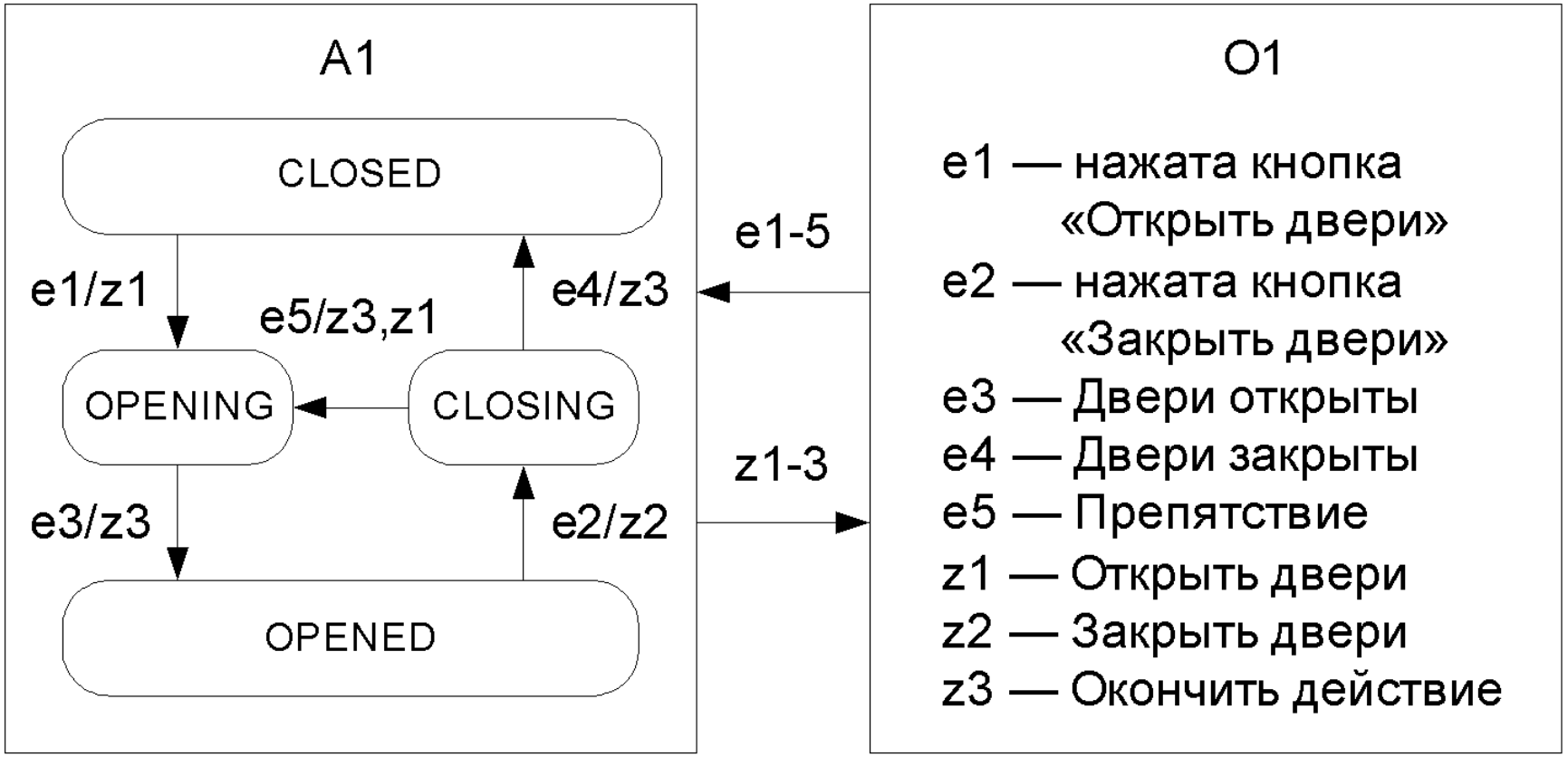
Спецификация системы взаимодействующих автоматов

- Переменная состояния для каждого автомата
- Автоматная процедура для каждого автомата
  - Изменяет переменную состояния своего автомата
  - Читает переменные состояния других автоматов

Состояния объектов управления

- Объекты управления не имеют состояния
- Объекты управления имеют состояния
  - Описание изменения состояния в терминах темпоральной логики

Управление дверьми лифта



Фрагмент описания на языке Promela

```
int stateA1 = CLOSED;

inline A1() {
    do
        ::stateA1 == CLOSING ->
            if
                ::stateA1 = CLOSED;
                  event = e4;
                ::stateA1 = OPENING;
                  event = e5;
            fi;
        ...
    od;
}
```

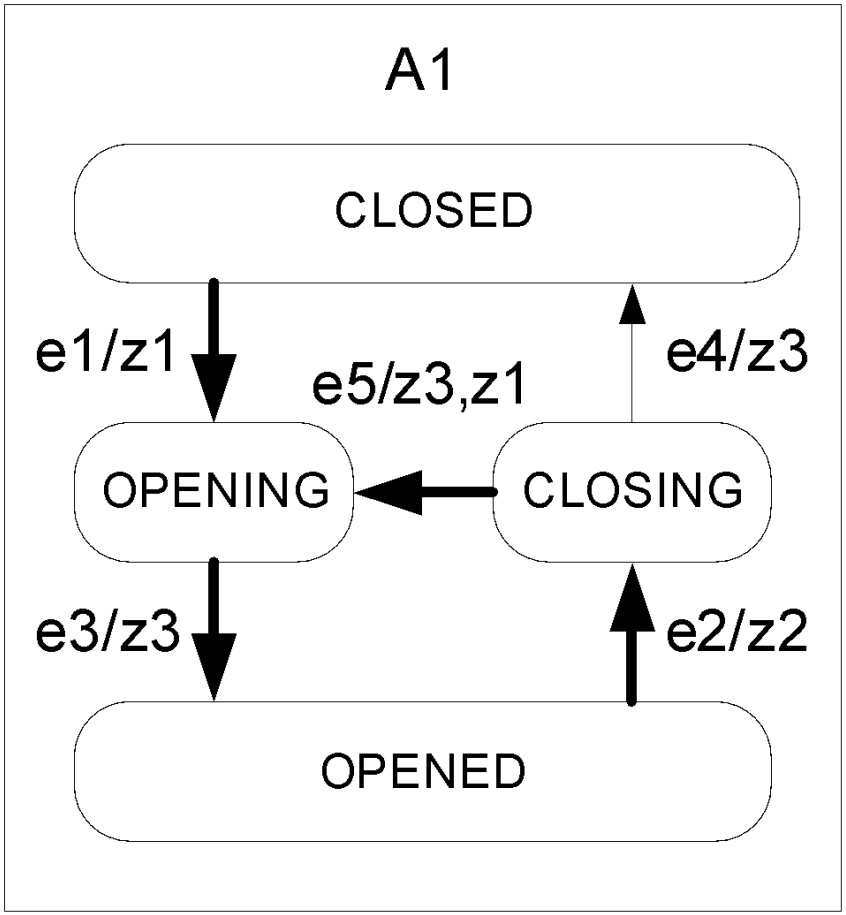
Верифицируемые утверждения

1. Двери открываются бесконечное число раз
   - LTL: **G F** Opened
   - Promela: `- [] <> Opened`
2. Двери закрываются бесконечное число раз
   - LTL: **G F** Closed
   - Promela: `- [] <> Closed`

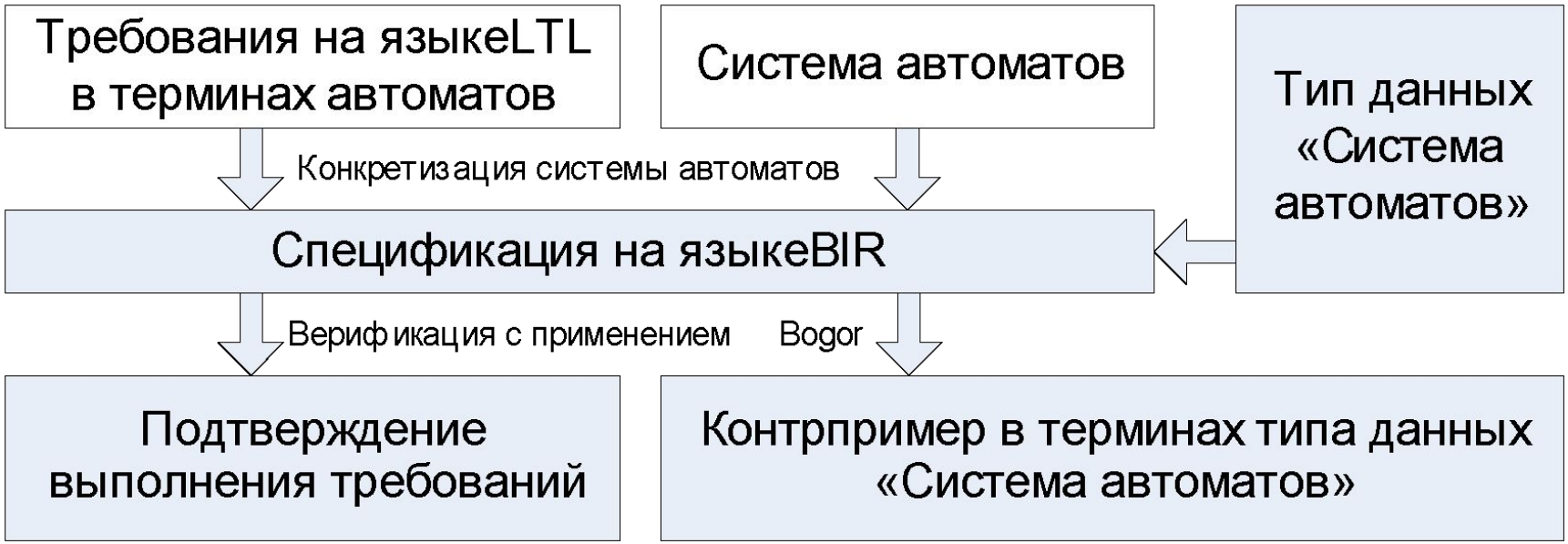
Верификация утверждений

- Утверждение 1 выполняется
- Утверждение 2 не выполняется:

  A1 [stateA1 = CLOSED]
  A1 [stateA1 = OPENING]
  A1 [stateA1 = OPENED]
  A1 [stateA1 = CLOSING]
  A1 [stateA1 = OPENED]



Верификация с применением Bogor



Применяемые методы

- Симуляция
- Двойной поиск в глубину
- Увеличение «масштаба» переходов

ИТМО ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Структура описания автоматов

- Абстрактный тип данных «Автомат»
  - Выбор следующего перехода
  - «Откат» на состояние назад
  - Восстановление ошибочного пути
- Система автоматов
  - Взаимодействия через номера состояний
  - Взаимодействие по вложенности

ИТМО ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Практическое использование

- Ручная верификация
  - Верификация проектов, опубликованных на сайте http://is.ifmo.ru
- Автоматизированная верификация
  - Основана на существующих верификаторах

Повышение качество программного обеспечения

- Верификация управляющих программ в NASA
  - Stateflow
  - SPIN
- Верификация проектов, опубликованных на сайте http://is.ifmo.ru
  - UniMod
  - SPIN или Bogor

ИТМО ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Выводы

- Простота верификации автоматных программ
- Возможность автоматизации верификации
- Практическая применимость

Направление дальнейших исследований

- Разработка примера верификации системы со сложным поведением
- Проведение экспериментальных исследований
- Разработка предложений и рекомендаций по использованию результатов НИР

Публикации по теме (1)

1. *Вельдер С.Э., Шалыто А.А.* О верификации простых автоматных программ на основе метода «Model Checking» //Информационно-управляющие системы. 2007. №3.
2. *Корнеев Г.А., Парфенов В.Г., Шалыто А.А.* Верификации автоматных программ //Тезисы докладов Международной научной конференции, посвященной памяти профессора А.М. Богомолова «Компьютерные науки и технологии». Саратов: Саратовский государственный университет. 2007.
3. *Корнеев Г.А., Шалыто А.А.* Верификация управляющих программ со сложным поведением, построенных на основе автоматного подхода /Материалы международной научно-технической конференции «Многопроцессорные вычислительные и управляющие системы» (МВУС`2007). Таганрог: НИИМВС. Т.1.
4. *Гуров В.С., Шалыто А.А., Яминов Б.Р.* Технология верификации автоматных моделей программ без их трансляции во входной язык верификатора / Материалы международной научно-технической конференции «Многопроцессорные вычислительные и управляющие системы» (МВУС`2007). Таганрог: НИИМВС. Т.1.

Публикации по теме (2)

1. Васильева К.А., Кузьмин Е.В. Верификация автоматных программ с и спользованием LTL //Моделирование и анализ информационных систем. Ярославль: ЯрГУ. Т. 14. 2007, №1.
2. Кузьмин Е.В., Соколов В.А. О дисциплине специализации «Верификация проргамм» /Доклады II научно-методической конференции Ярославского гос. университета. Ярославль: ЯрГУ, 2007.
3. Кузьмин Е.В., Соколов В.А. О некоторых подходах к верификации автоматных программ /Сборник докладов семинара GoIT. М.: Институт системного программирования.
4. Виноградов Р.А., Кузьмин Е.В., Соколов В.А. Свидетельство об официальной регистрации программы для ЭВМ «Система моделирования и анализа автоматных программ» № 2007611856

Дополнительная информация

- Раздел «Генетические алгоритмы» сайта кафедры «Технологии программирования» СПбГУ ИТМО по автоматному программированию http://is.ifmo.ru/genalg/

Спасибо за внимание