Формальные методы в программной инженерии

Спецификация и верификация программ

- предикатное программирование
- система Why3
- автоматное программирование
- система моделирования Event-B

Шелехов Владимир Иванович,
зав. лаб. Системного программирования ИСИ, к.т.н.,
Институт Систем Информатики, Новосибирск,
Новосибирский Государственный Университет,
vshel@iis.nsk.su, р.т. (383) 330-27-21, ИСИ СО РАН, к.269

Три индустрии

Systems engineering Системная инженерия

Системотехника

Software engineering Программная инженерия

Технология программирования

Requirements engineering Инженерия требований

Определение требований

Hardware engineering

Технология построения интегральных схем

Моделе-ориентированная технология model-based

Материалы к лекциям и инструменты

Классификация программ:

http://persons.iis.nsk.su/files/persons/pages/prog.pdf

Язык P и его формальная семантика:

http://persons.iis.nsk.su/files/persons/pages/semZont1.pdf

Язык предикатного программирования P

https://persons.iis.nsk.su/files/persons/pages/plang14.pdf

Система верификации Why3: http://why3.lri.fr/

Event-B и платформа Rodin: http://www.event-b.org/

Видеолекции по курсу Формальные методы:

http://wasp.iis.nsk.su/

Форум с ликбезами по формальным методам и инженерии требований:

http://forum.oberoncore.ru/viewforum.php?f=140

Содержание лекций по ФМ

Формальные методы всегда надо рассматривать в контексте технологии программирования

Фундаментальные понятия программной инженерии: программа, спецификация, требования, корректность программы, формальная семантика, дедуктивная верификация, …

Программная инженерия в проекции на формальные методы

Классификация программ. Классы программ-функций и программ-процессов.

Предикатное программирование – технология для класса программ-функций.

Программа – это вычислимый предикат.

Приложения с повышенными требованиями к надежности и безопасности

Автоматное программирование - для класса программ-процессов.

Программа – автомат в виде гиперграфа.

Предикатное программирование

Язык вычислимых предикатов P_0 – минимальное полное ядро

Формальная операционная семантика языка P_0

$$P_0 \rightarrow P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P$$

Язык предикатного программирования **P**

Гиперфункции

Технология доказательного построения предикатной программы

Оптимизирующие трансформации предикатной программы

Дедуктивная верификация. Системы автоматического доказательства **PVS и Why3**

Автоматное программирование

Класс реактивных систем (программ-процессов)

Понятие автоматной программы

Язык автоматных программ

Язык спецификации (функциональных) требований

Технология автоматного программирования

Примеры

Верификация автоматных программ

Трансформация автоматных программ

Система верификации Why3

Назначение: дедуктивная верификация

Язык спецификаций **why3** и язык программирования **WhyML**

Нет собственного инструмента доказательства.

Драйверы на внешние инструменты автоматического доказательства терем: **Alt-Ergo, CVC3, CVC4, Gappa, Simplify, Vampire, Yices, Z3 и др.;**

Выход на системы интерактивного доказательства: Coq, PVS, Isabelle/HOL.

Команды доказательства (трансформации)

Стандартная библиотека теорий для поддержки доказательства.

http://why3.lri.fr/ - сайт **Why3**

Event-B и платформа Rodin

Назначение: спецификация и верификация моделей в системной и программной инженерии

Применение: автоматизация в метро, ж.-д. транспорте

Язык спецификаций **Event-B**: статическая и динамическая части, язык теории множеств.

Метод уточнений.

Платформа **Rodin**: генерация формул корректности инвариантов, система автоматического и интерактивного доказательства, набор инструментов доказательства, SMT-решатели, аниматор

Построена на базе среды **Eclipse**

Более 50 расширений с помощью плагинов

http://www.event-b.org/ - сайт **Why3 Event-B.org**

Индивидуальные задания

1. **Задание** на формальную спецификацию и дедуктивную верификацию в системе **Why3** для простой задачи.
2. **Задание** на построение спецификации модели на языке **Event-B** и верификацию свойств модели на платформе **Rodin**

Дифзачет

бонусы и штрафы