РОССИЙСКАЯ АКАДЕМИЯ НАУК

Федеральное государственное бюджетное учреждение науки
Институт системного программирования
Российской академии наук

«УТВЕРЖДАЮ»

Директор ИСП РАН
академик РАН,
д.ф.-м.н., профессор
_____ В.П.Иванников
«___»_____ 2012 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ
«Верификация моделей программ»

для подготовки аспирантов по специальности
05.13.11 - Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Москва 2012

1. Аннотация

Изучается подход к задаче проверки корректности поведения информационных систем – метод верификации моделей программ (model checking). Рассматриваются и обосновываются основные приемы построения моделей информационных систем, включая последовательные и распределенные программы, микроэлектронные схемы, и др., логические средства спецификации их поведения, а также алгоритмы проверки выполнимости спецификаций на заданных моделях программ. Изучаются инструментальные средства верификации моделей для темпоральных логик SMV (Symbolic Model Verifier) и SPIN и их применение для верификации моделей программ и логических схем. При чтении лекций используются компьютерные презентации.

2. Цели и задачи курса

Ознакомление слушателей

- с современными формальными языками описания моделей программ и
- с современными математическими методами и программно-инструментальными средствами верификации описаний информационных систем

Формирование у слушателей целостного представления о математических моделях, методах и средствах проектирования и проверки корректности описаний информационных систем.

3. Место курса в структуре послевузовского профессионального образования (аспирантура)

Курс «Верификация моделей программ» относится к факультативным дисциплинам учебного плана подготовки аспирантов по научной специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Для успешного изучения курса аспиранту необходимо знать общесистемное программное обеспечение, основные средства разработки ПО, уметь работать с персональной ЭВМ.

Получаемые в рамках курса знания могут быть востребованы при подготовке к кандидатскому экзамену по научной специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей», в научно-исследовательской работе и при выполнении диссертации на соискание ученой степени кандидата технических наук.

4. Требования к результатам освоения курса

В результате изучения курса «Верификация моделей программ» аспирант должен:

Знать

- методы построения формальных моделей программ и описаний информационных систем;
- выразительные возможности темпоральных логик, используемых в качестве языков спецификации распределенных программ и описаний информационных систем;
- алгоритмы верификации формальных моделей распределенных программ и описаний информационных систем.

Уметь

- правильно записывать темпоральные спецификации распределенных программ и описаний информационных систем;
- использовать методы и алгоритмы верификации формальных моделей программ.

Владеть

- навыками использования системы верификации моделей программ SMV и SPIN.

5. Содержание и структура курса

В курсе рассматривается математический подход к решению задачи проверки правильности функционирования распределенных программ (систем взаимодействующих процессов, сетевых протоколов, микроэлектронных схем и др.) – верификация моделей программ. Суть этого метода состоит в следующем:

1. проверяемая вычислительная система моделируется размеченной системой переходов с конечным числом состоянием (моделью Крипке);
2. требования правильного функционирования вычислительной системы описываются формулами темпоральной логики;
3. проверка правильного функционирования вычислительной системы сводится к проверке выполнимости заданной темпоральной формулы в заданной модели Крипке.

В курсе рассматриваются методы трансляции программ и описаний микроэлектронных схем в размеченные системы переходов (формальные модели программ). Изучаются основные разновидности темпоральных логик, используемые для описания поведения систем взаимодействующих процессов — темпоральная логика деревьев вычислений (CTL) и логика линейного времени (LTL). Осваивается методика использования указанных логик для построения спецификаций поведения распределенных программ. Формулируется задача проверки выполнимости формул темпоральных логик на конечных размеченных системах переходов и изучаются табличные алгоритмы решения указанной задачи. Поскольку табличные алгоритмы верификации моделей программ неприменимы для проверки правильности программ с большим числом состояний, предлагается символьный метод описания моделей программ при помощи упорядоченных двоичных разрешающих диаграмм (OBDD). Рассматриваются алгоритмы преобразования OBDD, моделирующие алгебраические операции над булевыми функциями. На основании символьного описания моделей программ построены символьные алгоритмы верификации моделей программ, позволяющие проверять правильность поведения программ с большим числом состояний. В заключение курса проводится ознакомление с программно-инструментальными системами верификации программ и логических схем nu-SMV и SPIN. Выполняются работы, посвященные описанию и верификации моделей логических схем при помощи указанных инструментальных средств.

5.1 Содержание разделов курса

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Методы формальной верификации схем	Основные методы верификации аппаратуры и программного обеспечения – тестирование, имитационное моделирование, дедуктивный анализ, верификация моделей. Преимущества метода верификации моделей. Алгоритмические и комбинаторные трудности применения метода верификации моделей.	Т

2	Построение формальных моделей программ	Моделирование схем. Системы переходов. Представление систем переходов формулами логики предикатов первого порядка. Синхронные и асинхронные схемы. Формальные языки спецификации моделей. Построение модели автомата (протокола, управляющего алгоритма) на языках описания моделей программ (SMV, Promela).	Т
3	Способы представления булевых функций и формальных моделей программ	Двоичные разрешающие диаграммы (BDD). Алгоритм редукции BDD к каноническому виду (ROBDD). Выполнение операций над ROBDD: унарные и бинарные Булевы операции, операция ITE (мультплексорная функция от трех переменных), квантификация, проверка выполнимости, подсчет числа единиц. Эффективная машинная реализация ROBDD на основе хэш-таблиц. Общие представления о сложности в классе ROBDD (зависимость сложности от порядка переменных, сложность умножения целых чисел). Реализация алгоритмов работы с ROBDD на примере одного из распространенных пакетов (CUDD, ABCD, и др.). Конъюнктивные нормальные формы (CNF). Задачи выполнимости КНФ. Сведение задачи выполнимости булевой формулы (или схемы) к задаче выполнимости КНФ. Алгоритм DPLL. Эвристические методы повышения производительности на примере существующего SAT-солвера (Chaff, BerkMin, MiniSat, etc.) Схемные SAT-солверы (решение задачи выполнимости схемы без сведения к КНФ).	Т
4	Темпоральные логики	Темпоральная логика деревьев вычислений CTL. Синтаксис и семантика CTL. Примеры спецификаций моделей в терминах формул CTL. Темпоральная логика линейного времени PLTL. Синтаксис и семантика PLTL. Свойства живости и безопасности. Ограничения справедливости. Задача верификации моделей (model-checking).	Т
5	Табличный алгоритм верификации моделей для CTL	Обоснование корректности и сложности табличного алгоритма верификации моделей. Проблема “комбинаторного взрыва”.	Т
6	Символьная верификация моделей для CTL	Представления неподвижной точки. Алгоритм символьной верификации моделей. Особенности реализации алгоритма: учет ограничений справедливости, расщепленные отношения переходов, рекомбинация	Т

		произведений.	
7	Верификация схем с использованием логики линейного времени PLTL	Табличная верификация моделей для PLTL. Обобщенные автоматы Бюхи, трансляция формул LTL в автоматы. Сведение задачи проверки выполнимости формул PLTL к проблеме пустоты для автоматов Бюхи. Алгоритм двойного поиска в глубину с возвратом (DDFS) для проверки пустоты автомата Бюхи.	Т
8	Повышение эффективности алгоритмов верификации моделей	Редукция частичных порядков. Композиционные доказательства правильности. Абстракции. Учет симметрии. Ограниченная верификация моделей программ. Интерполяционная теорема Крейга для исчисления высказываний. Построение интерполянта на основе доказательства невыполнимости КНФ. Интерполяционный алгоритм МакМиллана.	Т
9	Инструментальное средство SMV (Symbolic Model Verifier)	Устройство SMV. Язык описания моделей и задания спецификаций в системе SMV. Примеры применения системы SMV на практике. Верификации простых моделей с использованием системы SMV: описание моделей, формальное задание спецификаций, проверка выполнимости спецификаций.	Т
10	Инструментальное средство SPIN	Язык описания систем взаимодействующих процессов Promela. Примеры описаний распределенных систем. Примеры применения системы SPIN на практике. Верификации простых моделей с использованием системы SPIN: описание моделей, формальное задание спецификаций, проверка выполнимости спецификаций.	Т

5.2 Структура курса

Общая трудоемкость курса составляет 2 зачетные единицы (72 часа).

Вид работы	Трудоемкость, часов
	1 курс
Общая трудоемкость	**72**
Аудиторная работа:	**32**
Лекции (Л)	32
Практические занятия (ПЗ)	-
Лабораторные работы (ЛР)	-
Самостоятельная работа:	**40**
Самостоятельное изучение разделов	-
Самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, выполнение практических заданий)	40
Вид итогового контроля (зачет, экзамен)	**Кандидатский экзамен**

Трудоемкость отдельных разделов курса.

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Вне-ауд. работа СР
			Л	ПЗ	ЛР	
1	Методы формальной верификации схем	4	2	-	-	2
2	Построение формальных моделей программ	4	2	-	-	2
3	Способы представления булевых функций и формальных моделей программ	14	6	-	-	8
4	Темпоральные логики	6	2	-	-	4
5	Табличный алгоритм верификации моделей для CTL	8	4			4
6	Символьная верификация моделей для CTL	8	4			4
7	Верификация схем с использованием логики линейного времени PLTL	8	4			4
8	Повышение эффективности алгоритмов верификации моделей	8	4			4
9	Инструментальное средство SMV (Symbolic Model Verifier)	6	2			4
10	Инструментальное средство SPIN	6	2			4
	Итого:	72	32	-	-	40

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы аспирантов

Форма контроля знаний:
- кандидатский экзамен по специальности.

Контрольно-измерительные материалы

На кандидатском экзамене аспирант должен продемонстрировать знания в объеме основной программы кандидатского экзамена по специальности 05.13.11 «Математическое обеспечение вычислительных машин, комплексов и компьютерных сетей», а также дополнительной программы, в которую, в зависимости от выбранной аспирантом специализации, могут входить вопросы, рассматриваемые в данном курсе.

Перечень контрольных вопросов для дополнительной программы:

1. Понятие функциональной верификации информационных систем. Основные методы верификации аппаратуры и программного обеспечения – тестирование, имитационное моделирование, дедуктивный анализ, верификация моделей.
2. Моделирование схем. Системы переходов. Представление систем переходов формулами логики предикатов первого порядка. Формальные языки спецификации моделей.
3. Темпоральная логика деревьев вычислений CTL. Синтаксис и семантика CTL. Ограничения справедливости.

4. Задача верификации моделей. Табличный алгоритм верификации моделей для CTL. Обоснование корректности и сложности алгоритма.
5. Применение символьных методов описания моделей схем. Упорядоченные двоичные разрешающие диаграммы (OBDD). Алгоритмы редукции и выполнения операций над OBDD.
6. Конъюнктивные нормальные формы (CNF). Задачи выполнимости КНФ. Сведение задачи выполнимости булевой формулы (или схемы) к задаче выполнимости КНФ. Алгоритм DPLL.
7. Символьная верификация моделей для CTL. Представления неподвижной точки. Алгоритм символьной верификации моделей.
8. Учет ограничений справедливости. Повышение эффективности символьной верификации: расщепленные отношения переходов, рекомбинация произведений.
9. Темпоральная логика линейного времени PLTL. Синтаксис и семантика PLTL. Табличная верификация моделей для PLTL.
10. Автоматы Бюхи. Сведение задачи проверки выполнимости формул PLTL к проверке пустоты автоматов Бюхи. Алгоритм DDFS.
11. Редукция частичных порядков. Композиционные доказательства правильности. Абстракции. Учет симметрии.
12. Ограниченная верификация моделей программ. Интерполяционная теорема Крейга для исчисления высказываний. Построение интерполянта на основе доказательства невыполнимости КНФ. Интерполяционный алгоритм МакМиллана.

7. Список литературы

1. Э.М. Кларк, О. Грамберг, Д. Пелед. «Верификация моделей программ». Москва, 2002, изд-во МЦНМО, 415 с.
2. M. R. A. Huth, M.D. Ryan. Logic in Computer Science: Modelling and Reasoning about Systems. Cambridge University Press, 2002, 387 p.
3. Ю.Г. Карпов. Model checking: верификации параллельных и распределенных программных систем. Изд-во БХВ-Петербург, 2010, 552 с.
4. NuSMV: a new symbolic model checker. http://nusmv.fbk.eu/.
5. Karl S. Brace, Richard L. Rudell and Randal E. Bryant. Efficient Implementation of a BDD Package. In Proceedings of the 27th ACM/IEEE Design Automation Conference (DAC 1990), pages 40–45. IEEE Computer Society Press, 1990.
6. CUDD: CU Decision Diagram Package. http://vlsi.colorado.edu/~fabio/CUDD/.
7. Daniel Kroening, Ofer Strichman. Decision Procedures. Springer, 2008, 304 p.
8. Kenneth L. McMillan, Interpolation and SAT-Based Model Checking. Proceedings of CAV 2003, p. 1-13.

8. Материально-техническое обеспечение курса

Для получения необходимой информации и самостоятельной работы аспирантов используются web-ресурсы Интернет и локальная библиотека электронных материалов.
В компьютерных классах ИСП РАН (ауд. 109) аспиранты могут самостоятельно ознакомиться с программным обеспечением, используемым для верификации моделей программ.

Программу составил д.ф.–м.н. Захаров В.А.

Программа принята на заседании Ученого Совета ИСП РАН
протокол № 2012-5 от 23 мая 2012 г.