Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____ А. В. Замятин
« 19 » мая 2022 г.

Рабочая программа дисциплины

Математические модели и методы решения задач информационной безопасности-1*BDD-representations of Boolean functions

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2022

Код дисциплины в учебном плане: Б1.В.01.06

СОГЛАСОВАНО:
Руководитель ОП
_____ А.Ю. Матросова

Председатель УМК
_____ С.П. Сущенко

Томск – 2022

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-4 – Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

– ПК-2 – Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИОПК-4.2 Учитывает основные требования информационной безопасности.

ИОПК-4.1 Анализирует задачи прикладной математики и информатики средствами информационных технологий.

2. Задачи освоения дисциплины

– Изучить представления булевых функций на графах, изучить основные алгоритмы манипулирования такими представлениями.

– Научиться применять графовые представления булевых функций для решения практических задач профессиональной деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений. Дисциплина входит в модуль «Специализация».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Третий семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.
-лабораторные: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Различные способы представления булевых функций.

Рассматриваются различные представления булевых функций. Вводится определение Сокращенных Упорядоченных Двоичных Диаграмм Решений (Reduced Ordered Binary Decision Diagram - ROBDD). Формулируется Лемма о каноническом представлении булевой функции в виде ROBDD-графа.

Тема 2. Реализация основных операций над ROBDD-графами.

Рассматриваются основные способы представления ROBDD-графов в памяти и реализация базовых операций.

Тема 3. Примеры использования ROBDD-графов.

Рассматриваются примеры использования ROBDD-графов при решении некоторых практических задач: задача о восьми ферзях, задача верификации комбинационных схем и задача определения эквивалентности двух схем.

Тема 4. Представление систем булевых функций.

Рассматриваются различные графовые способы представления систем булевых функций: совмещенный (многокорневой) BDD-граф (Shared BDD - SBDD) и многотерминальный BDD-граф (MTBDD). Предлагается решение задачи кодирования с помощью MTBDD – графов.

Тема 5. Новые типы декомпозиций и соответствующие типы диаграмм – PPRDDD (FDD), NPRMDD.

Рассматриваются новые типы декомпозиций и соответствующие им типы диаграмм – PPRDDD (FDD), NPRMDD. Также рассматривается спектральная интерпретация различных типов декомпозиций. Диаграммы KDD, PKDD.

Тема 6. BDD с помеченными ребрами.

BDD с помеченными ребрами. Edge valued Binary Decision Diagram (EVBDD). Синтез комбинационных схем из мультиплексоров по ROBDD.

Тема 7. Zero suppressed Decision Diagram (ZDD).

Рассматриваются Zero suppressed Decision Diagram и их практическое применение.

Тема 8. Троичные решающие диаграммы (Ternary Decision Diagram - TDD).

Рассматриваются разные типы TDD и их практическое применение.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, выполнения лабораторных работ и фиксируется в форме контрольной точки не менее одного раза в семестр.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет с оценкой в третьем семестре проводится в письменной форме по билетам. Билет содержит теоретический вопрос и практическую задачу. Продолжительность зачета 1,5 часа.

Примерный перечень теоретических вопросов:

1. Способы представления булевых функций (БФ). Задача выполнимости и задача определения тавтологии БФ.
2. Условный оператор (if-then-else). Представление БФ в виде INF.
3. Определить BDT (binary decision tree) и BDD (binary decision diagram) используя INF представление булевой функции.
4. Дать определение ROBDD, сформулировать правила сокращения и свойства.
5. Доказать лемму о каноническом представлении БФ в виде ROBDD.
6. Каким образом порядок разложения по переменным влияет на ROBDD. Продемонстрировать на примере.

7. Способы хранения ROBDD в памяти. Функции: MK[T,h}(I,l,h) и Build[T,H](t).
8. Способы хранения ROBDD в памяти. Функции: Apply[T,H](op,u1,u2) и Restrict[T,H](u,j,b).
9. Функции: SatCount[T](u), AnySat(u), AllSat(u).
10. Функции: Simplify(d,u). Оценки времени работы основных алгоритмов оперирующих ROBDD.
11. Примеры практических задач решаемых с помощью ROBDD.
12. Представления систем БФ в виде BDD (SBDD, MTBDD).
13. Представление конечных автоматов в виде BDD, характеристические функции и отношения.
14. Троичные диаграммы (Ternary DD) общий случай и вариации.
15. BDD с помеченными ребрами (Attributed Edges BDD). Общий случай (произвольное отображение) и частный случай (с инверсными ребрами). Основные свойства, пример построения.
16. Декомпозиция Шеннона, Давио (позитивная и негативная) их представления в виде INF. Примеры построения деревьев разложения БФ для заданных декомпозиций.
17. Функциональные диаграммы (FDD~PPRMDD) и NPRMDT. Пример построения и правила сокращения.
18. Кронекеровские и псевдо-кронекеровские диаграммы. Примеры построения.

Примеры задач:

1. Задача 1.

Для булевых функций $f_1 = xy \oplus z$; $f_2 = (x \vee y) \to z$ построить диаграмму SBDD(f_1, f_2).

2. Задача 2.

Для булевых функций $f_1 = xy \square z$; $f_2 = (x \vee y) \square z$ построить диаграмму MTBDD(f_1, f_2).

3. Задача 3.

Для булевой функции $f_1 = xy \square z$ построить диаграмму FDD(f_1).

Результаты зачета с оценкой определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Промежуточная аттестация дает 35% (теоретический вопрос – 20%, практическая задача – 15%). Посещаемость – 5%. Лабораторная работа – 35%. Контрольная работа – 25%.

От 70% до 100% - оценка «отлично».

От 40% до 69% - оценка «хорошо».

От 25% до 39% - оценка «удовлетворительно».

До 25% - оценка «неудовлетворительно».

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=566331

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– D. E. Knuth, «The Art of Computer Programming Volume 4, Fascicle 1: Bitwise tricks & techniques; Binary Decision Diagrams» (Addison-Wesley Professional, March 27, 2009) viii+260pp, ISBN 0-321-58050-8. Draft of Fascicle 1b available for download.

– H. R. Andersen «An Introduction to Binary Decision Diagrams», Lecture Notes, 1999, IT University of Copenhagen.

– Ch. Meinel, T. Theobald, «Algorithms and Data Structures in VLSI-Design: OBDD — Foundations and Applications», Springer-Verlag, Berlin, Heidelberg, New York, 1998. Complete textbook available for download.

б) дополнительная литература:

– Representation of Discrete Functions (edited by Tsutomu Sasao, Masahiro Fujita). – Kluwer Academic Publishers. -1996. - 331 p.

– R.Drechsler, D.Sieling, “Binary decision diagram in theory and practice”/ Int J STTT. - 2001. – p. 112-136.

– R.E.Bryant, “Graph-based algorithms for Boolean function manipulation”// IEEE Trans Computer, 35(8). -1986. – p. 677-691.

в) ресурсы сети Интернет:

– https://eecs.ceas.uc.edu/~weaversa/BDD_Visualizer_Tutorial_1.html– Журнал «Эксперт» - http://www.expert.ru

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/

– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

Аудитории для проведения лабораторных занятий, оснащенные компьютерной техникой и доступом к сети Интернет.

Характеристики компьютерных систем:

- Процессор с тактовой частотой 1,6 ГГц или большей;
- ОЗУ объемом 1 ГБ;
- 10 ГБ доступного пространства на жестком диске;
- Жесткий диск с частотой вращения 5400 об/мин;

- Видеоадаптер, соответствующий стандарту DirectX 9 и поддерживающий разрешение экрана 1024 x 768 или выше.

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»).

15. Информация о разработчиках

Останин Сергей Александрович, заведующий кафедрой компьютерной безопасности, канд. техн. наук, доцент.