Программа спецкурса «Теория автоматов и шифров» (3 курс, осень)

Сост. Асс. каф. ИВЭ А. М. Пеленицын

Модуль 1. Введение в теорию автоматов.

1. Понятие о конечном автомате. Простейший пример конечного автомата: модель турникета. Подход к формализации понятия автомата (входные и выходные сигналы, состояния, переходы). Формальное определение.
2. Пример: модель детектора вращения цилиндрического вала. Границы вычислительных возможностей конечных автоматов: автомат-двоичный сумматор, доказательство отсутствия автомата-множителя. Доказательство отсутствия автомата, который выписывает любое наперёд заданное вещественное число.
3. Варианты конечных автоматов. Автоматы-генераторы , проблематика, области применения. Понятие о случайных, псевдослучайных и криптографически стойких псевдослучайных последовательностей, тест следующего бита.
4. Линейный конгруэнтный генератор. Пример ЛКГ с плохими параметрами: RANDU, спектральный анализ на его примере. Полный период. Теорема Халла —Добелла: критерий для ЛКГ с полным периодом.
5. Регистры сдвига. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Пример. Задание регистра сдвига с линейной обратной связью с помощью полинома. Примитивные полиномы в поле $\mathbf{F}_2$ и линейные регистры сдвига с полным периодом. Пример.
6. Системы переходов (автоматы без лент). Понятие клеточного автомата: элементарные состояния, позиции, локальные условия для преобразования каждой клетки, окрестность Мура и окрестность Фон Неймана. Игра «Жизнь» как пример игры с нулевым числом игроков. Краткий очерк истории клеточных автоматов.
7. Основные вопросы в рамках исследования игры «Жизнь». Типы конфигураций в игре «Жизнь» (с примерами): стационарные популяции, осциляторы, планёр как пример мигрирующей популяции, ружьё Госпера как пример неограниченного роста. Райские сады и вопрос обратимости, использование в криптографии (пример с тремя последовательными популяциями). Полнота по Тьюрингу игры «Жизнь»: идея доказательства. Варианты игрового поля для игры «Жизнь»: игра «Жизнь» на торе, на шестиугольниках, увеличение числа элементарных состояний (цветная игра).
8. Элементарные клеточные автоматы. Пример: правило 30. Числовые последовательности, порождаемые элементарными клеточными автоматами, их производящие функции. Классификация клеточных автоматов по Стивену Вольфраму.
9. Конечные автоматы-распознаватели (КАР). Язык КАР. Определение замыкания функций переходов g^*. Определение отношения $\vdash$ и его транзитивного замыкания $\vdash^*$. Представление автомата в виде графа переходов. Примеры: автомат-распознаватель для языка всех слов, содержащих букву a; для языка всех чисел, делящихся на 3. Идея

необходимости формального доказательства совпадения $L = L(A)$.

10. Недетерминированные конечные автоматы-распознаватели (НКАР). Определение языка НКАР. Принцип работы НКАР. Теорема об эквивалентности НКАР и ДКАР, алгоритм детерминизации. Примеры.
11. Варианты автоматов-преобразователей: машины Мили и машины Мура. Доказательство эквивалентности машин Мили и машин Мура. Построение по машине Мура эквивалентной ей машины Мили. Построение по машине Мили эквивалентной ей машины Мура.

Модуль 2. Введение в теорию шифров.

1. Основные направления в математических методах защиты информации. Модель канала передачи данных. Принцип Керкгоффса. Задачи помехоустойчивого и сжимающего кодирования в общей модели канала. Математическая модель симметричного шифра.
2. Алгебраическая структура для определения шифров: конечные кольца (коммутативные, с единицей), основной пример: $\mathbf{Z}_n$.
3. Ассиметричная криптография, модель канала для неё, математическая модель; пример: шифрсистема RSA. Пример шифрования с помощью RSA.
4. Классические шифры. Шифр сдвига и шифр перестановки. Шифр простой замены. Ключевое пространство. Полиалфавитное шифрование: шифр Виженера. Шифр гаммирования, теорема Шеннона.
5. Общий вид шифра гаммирования. Понятие квазигруппы и латинского квадрата, примеры. Таблица Виженера.
6. Поточный шифр. Пример: аффинный шифр, оценка ключевого пространства: понятие группы обратимых элементов кольца. Блочный шифр. Пример: шифр Хилла, оценка ключевого пространства: обратимость матрицы над кольцом, общая линейная группа $GL_n(\mathbf{Z}_m)$.
7. Современные шифры: сети Фейстеля и блочные шифры на их основе, поточный шифр A5.

Литература

Модуль 1

Автоматы-генераторы

1. Shallit. A Second Course in Formal Languages and Automata Theory (2008, CUP, 252 p.)
2. Брауэр В. Введение в теорию конечных автоматов (Радио и связь, 1987, 392 с.)
3. Гилл А. Введение в теорию конечных автоматов (Наука, 1966, 272 с.)

Автоматы-распознаватели

4. Sipser. Introduction To The Theory Of Computation (Thomson, 2nd ed, 2005, 456 p.)
5. Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений (2002, 2-е изд, М: Вильямс, 528 с.)

Системы переходов: клеточные автоматы

6. Астафьев Г.Б., Короновский А.А., Храмов А.Е. Клеточные автоматы: Учебно-методическое пособие. (Саратов: Изд–во ГосУНЦ «Колледж», 2003. 24с.)
7. Ceccherini-Silberstein, Coornaert. Cellular Automata and Groups (Springer, 2010, 440 p.)

Автоматы-гненераторы

8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си (Триумф, 2012, 816 с.)

9. Кнут Д. Искусство программирования, т. 2 «Получисленные алгоритмы» (М: Вильямс, 2011, 832 с.)

Модуль 2

1. Алфёров и др. Основы криптографии (Гелиос, 2002, 480 с.)
2. Salomaa. Computation and automata (CUP, 1985, 281 p.).