Программа вступительного экзамена по направлению подготовки

09.06.01 «Информатика и вычислительная техника»

по профилю «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

I. Вопросы по специальной дисциплине

I.1. Общие вопросы по направлению

I.1.1.Раздел 1

1. МЕТОДЫ АНАЛИЗА АЛГОРИТМОВ

1.1. Алгоритмы и их сложность

Представление алгоритмов в машинных командах, на равнодоступной адресной машине (РАМ) и языке высокого уровня. Временная и емкостная сложность алгоритмов для разных представлений. Сложность в среднем и наихудшем. Теоремы о рекуррентных соотношениях для трудоемкости. Примеры алгоритмов и их сложность (полиномиальная, экспоненциальная) для различных представлений.

1.2. Недетерминированные алгоритмы

Функционирование недетерминированного алгоритма. Представление недетерминированных алгоритмов на равнодоступной адресной машине (РАМ) и языке высокого уровня. Машина Тьюринга. Детерминированная (ДМТ) и недетерминированная (НМТ) машины Тьюринга, ее связь с РАМ. Детерминированное моделирование НМТ. Сложность детерминированного и недетерминированного алгоритмов, решающих одну и ту же задачу.

1.3. NP-полные задачи

Классы P и NP языков. Языки и задачи. Задача выполнимости булевых формул, ее NP-полнота. Доказательство NP-полноты некоторой задачи. Примеры NP-полных задач, сведение к ним задачи выполнимости булевых формул.

1.4. Математическое программирование

Теоремы о достижении нижней грани функции (функционала) на множестве (в EN, в метрических пространствах, в гильбертовых пространствах). Выпуклые множества, выпуклые функции, сильно выпуклые функции, их свойства. Правило множителей Лагранжа. Метод проекции градиента. Метод Ньютона. Метод покоординатного спуска. Метод штрафных функций. Метод барьерных функций. Метод динамического программирования. Устойчивость задач оптимизации. Метод стабилизации (регуляризация по Тихонову). Линейное программирование. Симплекс-метод.

2.ИНФОРМАЦИОННЫЙ ПОИСК И СОРТИРОВКА

2.1. Эффективные алгоритмы внутренней сортировки

Минимально возможная трудоемкость в наихудшем. Алгоритм Шелла. Быстрая сортировка Хоара, оценка его сложности в среднем. Вычисление медианы. Пирамидальная сортировка. Сортировка слиянием. Цифровая сортировка. Цифровая сортировка строк.

2.2. Внешняя сортировка

Особенности задачи сортировки информации на файлах. Сбалансированное слияние. Многофазная сортировка, ее анализ. Особенности практической реализации.

2.3. Хеширование

Задача хеширования. Хеш-функция. Формирование хеш-таблицы, поиск, удаление элементов. Хеш-таблица с открытой адресацией, эффективность поиска в среднем. Применение хеш-таблиц в файлах.

3.КОМБИНАТОРНЫЕ АЛГОРИТМЫ И ГРАФЫ

3.1. Структуры для представления графов.

Ориентированные, неориентированные, взвешенные графы. Плоские и планарные графы. Формула Эйлера для плоских графов. Матрица смежности графа. Списки смежных вершин. Массив смежных вершин. Выделение компонент связности.

3.2. Комбинаторный анализ

Основные комбинаторные числа. Оценки и асимптотики комбинаторных чисел. Оценки числа графов различных типов

3.3. Бэктрекинг, ограничения поиска

Бэктрекинг, общий алгоритм. Вычисление гамильтонова цикла в графе. Ограничения поиска. Раскраска графа.

4. ФОРМАЛЬНЫЕ ЯЗЫКИ И МЕТОДЫ ТРАНСЛЯЦИИ

4.1. Формальные грамматики и языки

Порождающие грамматики. Контекстно свободные грамматики. Автоматы с магазинной памятью. Автоматные грамматики и языки. Конечные автоматы и способы их задания.

4.2. Контекстно-свободные языки и анализ сверху-вниз

Дерево порождения. Общий недетерминированный алгоритм анализа сверху-вниз (магазинный автомат). Детерминированный анализ сверху-вниз. Рекурсивный спуск. Преобразование грамматики. LL-анализатор. Использование отношения "first" при построении LL(1)-анализатора.

4.3. Синтаксический анализ снизу-вверх

Общий недетерминированный алгоритм анализа снизу-вверх (магазинный автомат). Грамматики простого предшествования (ПП). Построение отношений ПП. Грамматики операторного предшествования (ОП). Построение отношений ОП.

4.4. Обратная польская строка, как внутренний язык

Обратная польская строка (ОПС) для арифметических выражений. Интерпретатор ОПС. ОПС для условных и циклических конструкций. ОПС для индексации массивов. Генерация ОПС при синтаксическом анализе сверху-вниз и снизу-вверх.

I.1.2.Раздел **2**

5. ОПЕРАЦИОННЫЕ СИСТЕМЫ

5.1. Ресурсы и процессы

Аппаратные и программные ресурсы. Функции ОС. Эксплуатационные требования к ОС. Понятие процесса. Свойства процесса. Дескриптор процесса. Критический ресурс. Критический участок процесса. Синхронизация процессов с помощью элементарных приемов нижнего уровня. Аппаратные неделимые операции "Блокировка памяти" и "Проверить и установить". Семафоры общие и двоичные. Синхронизация процессов на двоичных семафорах. Задача "Поставщик-потребитель". Синхронизация процессов с помощью приемов верхнего уровня. Монитор на основе таблицы синхронизации.

5.2.Тупики и распределение времени процессора

Тупики. Условия возникновения тупиков. Предупреждение тупиков. Обход тупиков. Обнаружение тупиков. Восстановление после тупиков. Распределение времени процессора. Разделение времени. Квантование времени. Алгоритмы планирования времени в мультипрограммных системах. Планирование по наивысшему приоритету. Круговорот. Очереди с обратной связью.

5.3. Распределение памяти. Виртуальная память

Статическое и динамическое распределение памяти. Методы динамического распределения памяти. Перекрытие программ. Попеременная загрузка заданий. Сегментация программ. Страничная организация памяти. Сегментация программ со страничной организацией памяти. Внешняя и внутренняя фрагментация памяти. Многоуровневая организация виртуальной памяти. Методы организации свободной памяти для сегментов переменной длины. Список свободной памяти, способы его организации. Уплотнение. Стратегии подкачки и вытеснения.

5.4. Управление внешней памятью. Оценка производительности ВС.

Планирование работы с магнитными дисками. Цели и принципы планирования. Стратегии поиска цилиндра. Оптимизация времени отыскания записи. Организация ввода-вывода и файловые системы. Принципы оценки производительности вычислительной системы (цели, исходные данные, направления использования оценок, показатели производительности, методы оценки).

5.5. Многопроцессорные системы

Варианты организации мультипроцессорных ОС. Планирование времени мультипроцессора для независимых и связанных процессов. Коммуникационные средства многомашинных систем. Доменная архитектура многопроцессорных вычислительных систем (ВС). Системные и прикладные разделы ВС. Разделение ВС на классы приложений.

6. КОМПЬЮТЕРНЫЕ СЕТИ

6.1. Эволюция компьютерных сетей.

Ресурсы сети. Концептуальные требования к архитектуре сетей. Классификация сетей. Семиуровневая (эталонная) модель взаимодействия открытых систем Международной организации по стандартизации. Функции уровней. Модель сети интернет. Понятие протокола. Преобразование форматов протокольных блоков данных (принцип

инкапсуляции). Методы коммутации в сетях передачи данных (коммутация каналов, коммутация пакетов). Сравнение методов коммутации.

6.2. Протокол управления физическим и информационным каналом связи

Физический уровень. Методы модуляции непрерывных сигналов. Цифровое кодирование. Канальный уровень. Протокол управления звеном передачи данных HDLC. Фазирование и прозрачность. Понятие окна. Старт-стопный протокол. Нормальные и асинхронные процедуры управления звеном передачи данных. Групповой и селективный режимы повторной передачи последовательности кадров.

6.3. Протокол сетевого уровня.

Методы адресации сетевых объектов. Адресация в IP-сетях. Методы экономии адресного пространства в IP-сетях. Задача маршрутизации. Требования к алгоритмам маршрутизации. Команды протокола пакетной коммутации. Алгоритм маршрутизации АРПА-1. Недостатки алгоритма. Способы борьбы с ложными маршрутами. Алгоритм маршрутизации АРПА-2. Протокол IP. Таблица маршрутизации IP-протокола и ее использование IP-протоколом.

6.4. Транспортный протокол

Сети дейтаграммного и виртуального сервиса. Протоколы, ориентированные на соединение (для сетей виртуального сервиса). Протоколы без соединения (для дейтаграммных сетей). Транспортный протокол TCP. Система моделей для исследования индексов быстродействия протоколов и сетевых структур. Задержка мультипакетного сообщения в многозвенном детерминированном тракте передачи данных. Конвейерный эффект.

6.5. Управление потоками. Структура протоколов верхних уровней

Уровни управления потоками. Схемы управления потоками (межузловой, вход-выход, управление доступом в сеть). Блокировки процессов передачи пакетов. Сеансовый уровень. Сетевой метод доступа. Представительный уровень. Варианты преобразования представлений. Фазы работы представительного уровня.

6.6. Локальные вычислительные сети (ЛВС)

Протоколы доступа к разделяемой среде передачи данных локальных сетей. Кольцо с тактированным доступом. Кольцо и шина с маркерным доступом (методы доступа Token Ring и Token Bus). Шина со случайным доступом (метод доступа Ethernet). Коммутируемые ЛВС.

I.1.3. Раздел **3**

7. МОДЕЛИ ДАННЫХ И СУБД

7.1. Технология БД

Функциональная схема системы БД, роли ее участников. Архитектуры систем БД. Два основных класса систем БД – OLTP и OLAP. Многоуровневая система представлений предметной области. Модель данных. Атомарная единица информации. База данных. Схема БД. Конструктивные элементы модели данных. Система управления БД. Язык определения данных. Язык манипулирования данными.

7.2. Структуры

Знак. Тип. Основные способы структуризации данных: абстракция, обобщение, агрегация. Формы представления данных: комплекс, множество, кортеж, домен, атрибут, отношение. Интерпретация данных. Представления информации: таблицы, графы.

7.3. Ограничения целостности

Ограничение целостности. Виды ограничений: внутренние и явные. Верификация ограничений целостности. Типы ограничений: ограничения на значения атрибутов, ограничения на отображения. Отображение. Кардинальное число (КЧ). Минимальное КЧ. Максимальное КЧ. Виды отображений: неограниченное, полностью определенное, функциональное (частичное, полное). Виды бинарных отношений: "многие-ко-многим", "один-ко-многим", "один-к-одному". Ограничения на отображения между атрибутами одного отношения. Ключ. Ограничения на отображения между отношениями.

7.4. Операции

Расширенное состояние БД. Операции над данными, селекция, действие. Виды действий. Способы селекции. Навигационные операции. Спецификационные операции. Процедуры БД.

7.5. ER-модель

Место ER-модели в многоуровневой системе представлений предметной области. Структуры: множество сущностей, множество связей, роль, множество значений, атрибут. Представление интенсионала БД: ER-диаграмма. Представление экстенсионала БД: графы, таблицы. Ограничения целостности: ключ сущности, ключ связи, зависимость существования, зависимость по идентификации. Назначение модели. Модификации ER-модели Чена: расширенная ER-модель, нотация Баркера, нотация IDEF1X.

7.6. Реляционная модель

Структуры: отношение, кортеж, домен, степень отношения, мощность отношения, атрибут. Ограничения целостности: возможный ключ, первичный ключ, суррогатный ключ, внешний ключ, триггер. Навигационные операции, курсоры. Спецификационные операции: РЕЛЯЦИОННАЯ АЛГЕБРА, РЕЛЯЦИОННОЕ ИСЧИСЛЕНИЕ С ПЕРЕМЕННЫМИ-КОРТЕЖАМИ, РЕЛЯЦИОННОЕ ИСЧИСЛЕНИЕ С ПЕРЕМЕННЫМИ НА ДОМЕНАХ, РЕЛЯЦИОННЫЙ ЯЗЫК SQL.

7.7. Теория реляционных БД и классическая методика проектирования реляционных схем БД

Универсальное отношение. Аномалии. Функциональные зависимости. Нормальные формы отношений. Нормальная форма Бойса-Кодда. Аксиомы функциональных зависимостей. Минимальное покрытие множества функциональных зависимостей. Классическая методика проектирования реляционных схем БД.

7.8. Семантическая методика проектирования реляционных схем БД

Функциональное моделирование предметной области. Семантическое моделирование данных с использованием ER-модели. Логическое проектирование данных. Правила трансформации схемы БД из ER-модели в реляционную модель. Физическое проектирование БД.

8. Программная инженерия

8.1. Язык UML. Общая характеристика.

История развития методов объектно-ориентированного анализа и проектирования. Основные задачи языка UML. Прямое и обратное проектирование.

8.2. Основные элементы языка UML.

Элементы языка UML. Механизмы расширения UML. Диаграммы UML.

8.3. Общая характеристика порождающих типовых приемов проектирования.

Контекст применения порождающих типовых приемов проектирования. Краткая характеристика порождающих типовых приемов проектирования. Подробный разбор одного из порождающих приемов проектирования (на выбор). Анализ порождающих типовых приемов проектирования.

8.4. Общая характеристика структурных приемов проектирования.

Контекст применения структурных типовых приемов проектирования. Краткая характеристика структурных типовых приемов проектирования. Подробный разбор одного из структурных приемов проектирования (на выбор). Анализ структурных типовых приемов проектирования.

8.5. Общая характеристика поведенческих типовых приемов проектирования.

Контекст применения поведенческих типовых приемов проектирования. Краткая характеристика поведенческих типовых приемов проектирования. Подробный разбор одного из поведенческих приемов проектирования (на выбор). Анализ поведенческих типовых приемов проектирования.

8.6. Концепция архитектурных слоев. Основные архитектурные слои. Типовые подходы к реализации бизнес-логики.

Понятие архитектурного слоя. Концепция слоев: достоинства и недостатки. Эволюция подхода, основанного на применении слоев. Основная модель приложения. Краткая характеристика пакетов основной модели. Типовые приемы организации бизнес-логики.

8.7. Типовые архитектуры Web-приложений.

Стандартные способы реализации Web-приложений. Особенности реализации стратегии MVC в Web. Типовые приемы реализации контролеров. Типовые приемы реализации видов.

8.8. Эволюция процессов разработки ПО.

Последовательная модель процесса разработки ПО. Эволюционная модель процесса разработки ПО. Достоинства и недостатки этих подходов. Краткая характеристика современных процессов разработки ПО.

8.9. Основные идеи Унифицированного процесса разработки ПО.

Понятие варианта использования (ВИ). Роль вариантов использования в Унифицированном процессе (УП) разработки ПО. Понятие архитектуры. Роль архитектуры в УП. Понятие итерации и инкремента. Управление рисками.

8.10. Обобщенная итерация в рамках Унифицированного процесса разработки.

Понятие обобщенной итерации в рамках Унифицированного процесса разработки ПО. Краткая характеристика основных исполнителей и потоков работ в рамках обобщенной итерации. Специализация обобщенной итерации в контексте одной из фаз Унифицированного процесса (на выбор).

I.1.4.Литература

Раздел 1

1. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Т. 1. Синтаксический анализ. М.: Мир, 1978.
2. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979.
3. Вирт Н. Алгоритмы и структуры данных. – М.: ДМК Пресс, 2010. – 272 с.
4. Вирт Н. Построение компиляторов. – М.: ДМК Пресс, 2010. – 192 с.
5. Гудман С., Хидетмиеми С. Введение в разработку и анализ алгоритмов. – М.: Мир, 1981. – 368 с.
6. Дейкстра Э. Дисциплина программирования. – М.: Мир, 1978. – 275 с.
7. Ершов А.П. Теоретическое программирование. – М.: Наука, 1977.
8. Кнут Д. Искусство программирования для ЭВМ. Т. 3. Сортировка и поиск. – М.: Мир, 1978.
9. Кормен Т., Ч. Лейзерсон, Р. Ривест. Алгоритмы: построение и анализ. – М.: МЦНМО, 2001. – 958 с.
10. Костюк Ю.Л. Основы программирования. Разработка и анализ алгоритмов. – Томск: Изд-во Том. ун-та, 2006. – 244 с.
11. Кристофидес Н. Теория графов. Алгоритмический подход. – М.: Мир, 1978.
12. Рейнгольд Э., Нивергельд Ю., Део Н. Комбинаторные алгоритмы. Теория и практика.– М.: Мир, 1980. – 476 с.

Раздел 2

1. Бертсекас Д., Галлагер Р. Сети передачи данных: Пер. с англ. М.: Мир, 1989. 544 с.
2. Богуславский Л.Б. Управление потоками данных в сетях ЭВМ. М.: Энергоатомиздат, 1984, 168 с.
3. Блэк Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы. М.: Мир, 1990, 506 с.
4. Бутрименко А.В. Разработка и эксплуатация сетей ЭВМ. М.: Финансы и статистика, 1981, 256 с.
5. Дейтел Г. Введение в операционные системы: В 2-х т. Пер. с англ. М.: Мир, 1987, Т.1 - 359 с., т.2 – 398 с.
6. Дэвис Д., Барбер Д., Прайс У., Соломонидес С. Вычислительные сети и сетевые протоколы. М.: Мир, 1982, 562 с.
7. Кейслер С. Проектирование операционных систем для малых ЭВМ. М.: Мир, 1986, 680 с.
8. Мизин И.А., Богатырев В.А., Кулешов А.П.Сети коммутации пакетов. М.: Радио и связь, 1986, 408 с.
9. Протоколы информационно-вычислительных сетей: Справочник / С.А.Аничкин, С.А.Белов, А.В.Бернштейн и др./ Под ред. И.А.Мизина, А.П.Кулешова. М.: Радио и связь, 1990, 504 с.
10. Стандарты по локальным вычислительным сетям: Справочник / В.К.Щербо, В.М.Киричев, С.И.Самойленко./ Под ред. С.И.Самойленко. М.: Радио и связь, 1990, 304 с.
11. Танненбаум Э. Компьютерные сети. – СПб.: Питер, 2002. – 848 с.

12. Танненбаум Э. Современные операционные системы. – СПб.: Питер, 2002. – 1040 с.
13. Цикритзис Д., Бернстайн Ф. Операционные системы. М.: Мир, 1974, 336 с.
14. Шварц М. Сети ЭВМ. Анализ и проектирование. Пер. с англ./ Под ред. В.А. Жожикашвили. М.: Радио и связь, 1981, 336 с.

Раздел 3

1. Дейт К. Введение в системы баз данных. 7-е издание: Пер. с англ. – М.: Вильямс, 2001. – 1072 с.
2. Чен П. Модель «сущность – связь» - шаг к единому представлению о данных // СУБД. – 1995. – № 3. – С. 137-158.
3. Коннолли Т., Бегг., Страчан А. Базы данных: проектирование, реализация и сопровождение. Теория и практика: Пер. с англ. – М.: Вильямс, 2000. – 1120 с.
4. Джексон Г. Проектирование реляционных баз данных для использования с микроЭВМ: Пер. с англ. – М.: Мир, 1991. – 252 с.
5. Калянов Г.Н. CASE: структурный системный анализ (автоматизация и применение). – М.: Лори, 1996. – 242 с.
6. Кренке Д. Теория и практика построения баз данных: Пер. с англ. – СПб.: Питер, 2003. – 800 с.
7. Хансен Г., Хансен Д. Базы данных: разработка и управление: Пер. с англ. – М.: БИНОМ, 1999. – 699 с.
8. Гарсиа-Молина Г., Ульман Д., Уидом Д. Системы баз данных. Полный курс: Пер. с англ. – М.: Вильямс, 2003. – 1088 с.
9. Ульман Д., Уидом Д. Введение в системы баз данных: Пер. с англ. – М.: Лори, 2000. – 319 с.
10. Ульман Д. Основы систем баз данных: Пер. с англ. – М.: Финансы и статистика, 1983. – 334 с.
11. Грабер М. SQL: Пер. с англ. – М.: Лори, 2000. – 371 с.
12. Энсор Д, Стивенсон Й. Oracle8: рекомендации разработчикам. – К.: Изд. Группа BHV, 1998. – 128 с.
13. Колетски П., Дорси П. Oracle Designer. Настольная книга пользователя: Пер. с англ. – М.:, Лори, 1999. – 592 с.
14. Бэлсон Д. и др. Внутренний мир Oracle8. Проектирование и настройка. – К.: Изд-во «ДиаСофт», 2000. – 800 с.
15. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж., Приемы объектно-ориентированного проектирования. Паттерны проектирования. – СПб.: Изд-во «Питер», 2007. – 368 с.
16. Г. Буч, Д. Рамбо, А. Джекобсон. UML. Руководство пользователя . - М. : ДМК Пресс, 2000. – 432 с.
17. Крэг Ларман. Применение UML и шаблонов проектирования. (2-е издание) . – М.: Вильямс, 2002. – 624 с.
18. М.Фаулер, К.Скотт - UML. Основы - СПБ: Символ-Плюс, 2002. - 192 с.
19. М. Фаулер. Архитектура корпоративных программных приложений. – М.: Изд-во «Вильямс», 2004. – 544 с.
20. Якобсон А., Буч Г., Рамбо Дж. Унифицированный процесс разработки программного обеспечения. – СПб.: Питер, 2002. – 496.
21. Пер Кролл, Филипп Крачтен. Rational Unified Process - это легко. Руководство по RUP для практиков. – М.: Изд-во «КУДИЦ-ОБРАЗ», 2004. – 432 с.
22. Кендалл Скотт. Унифицированный процесс. Основные концепции. – М.: Изд-во «Вильямс», 2002. – 160 с.

I.2. Вопросы по профилю подготовки

Математические модели вычислительных систем и компьютерных сетей

Архитектура вычислительных систем. Параллелизм компьютерных вычислений. Одно- и многопроцессорные архитектуры. Подходы к организации многопроцессорных вычислительных систем. Доменная архитектура. Архитектурные приемы реализации микропроцессоров. Коммуникационные среды для объединения компонент вычислительной системы. Шинные интерфейсы. Архитектура иерархической памяти. Организация кэш-памяти.

Модели организации сетевых архитектур. Стандарты, сервисы, уровневые протоколы, стеки протоколов, вычислительные, программные и информационные ресурсы телекоммуникационных технологий; модели и методы программирования и обработки данных в сетевых окружениях; именование телекоммуникационных объектов; сокетная парадигма программирования в компьютерных сетях.

Проблемы организации эффективного функционирования компьютерных сетей. Исследование и оценка характеристик функционирования компьютерных сетей; инструменты исследования операционных характеристик и индексов производительности компьютерных сетей; технология проектирования протокольных систем, платформы для построения распределенных кооперированных систем; программное обеспечение компьютерных сетей.

Средства моделирования вычислительных систем и сетевых структур. Сети и системы массового обслуживания применительно к анализу функционирования компонент вычислительных систем, компьютерных сетей и обеспечения качества сервисов. Индексы быстродействия вычислительных систем и компьютерных сетей. Области применимости систем массового обслуживания с дискретным и непрерывным временем, с конечным и неограниченным накопителем. Формализация подсистем вычислителя и сетевых структур детерминированными и стохастическими конвейерами. Система моделей комплексного исследования вычислительных систем и компьютерных сетей.

Модели многоуровневой памяти вычислительных систем. Модели влияния ассоциативности кэш-памяти на вероятность попадания в кэш. Урновая модель кэша. Модель кэша с идеальным вытеснением. Модель кэша для вытесняющей стратегии с ошибками. Динамические свойства идеального кэша. Модели влияния глубины неблокируемости кэша на быстродействие подсистемы памяти. Модель влияния частоты изменений данных на операционные характеристики подсистемы памяти. Оптимизация архитектуры подсистемы памяти. Модель разделяемой памяти блокирующего типа многопроцессорной вычислительной системы**.**

Замкнутые и открытые модели звена передачи данных. Структура линейного протокола. Замкнутые модели нормальных и асинхронных управляющих конвейерных процедур для режимов групповой и селективной повторной передачи. Оптимизация протокольных параметров (длина кадра, размер окна).

Теория информации и кодирование

Коды, информация, энтропия Канал связи и сообщение. Информация дискретного сообщения. Энтропия. Свойства информации и энтропии. Кодирование равномерным кодом. Избыточность. Кодирование Хаффмана. Оптимальность кодирования. Влияние корреляции частей сообщения на избыточность. Эвристические методы кодирования сообщений со

сжатием без потерь информации.

Кодирование. Избыточное кодирование. Кодирование с проверкой четности. Кодовое расстояние по Хеммингу. Граница Хемминга. Обнаруживающая и исправляющая способность кода. Линейные коды, кодирование и декодирование, синдром. Свойства линейных кодов. Вычисление минимального кодового расстояния по порождающей матрице. Код Хемминга. Расширенный код Хемминга. Полиномиальная арифметика в поле чисел (0,1). Неприводимые полиномы. Циклические коды, кодирование и декодирование, синдром. Построение матрицы линейного кода по порождающему полиному. Циклический код Хемминга. Свойства циклических кодов.

Математические основы защиты информации и информационной безопасности

Основные понятия и протоколы. Предмет криптографии. Терминология в криптографии. Принципы обеспечения конфиденциальности в информационных системах. Протоколы секретного шифрования симметричным ключом. Простейшие ранние алгоритмы секретного шифрования. Методы вскрытия: метод грубой силы, частотный анализ, «встреча посередине». Влияние длины ключа на надежность метода. Проблема распространения ключей. Шифрование открытым ключом. Проблема достоверности открытого ключа. Протоколы электронной подписи.

Методы симметричного шифрования. Простые блочные методы шифрования. Кодирование и декодирование текста подстановочным и перестановочным кодом. Надежность симметричных методов шифрования. Требования к устойчивости метода. Операция XOR и кодирование одноразовым блокнотом. Кодирование и декодирование текста комбинированным кодом, образованным из подстановочного, перестановочного кодов, а также сдвига и операции XOR. Алгоритм шифрования DES.

Потоковые шифры. Понятие потокового шифра. Использование истинно случайных последовательностей для кодирования и декодирования текста. Линейные конгруэнтные генераторы. Сдвиговый регистр с линейной обратной связью. Алгоритм генерации случайного потока символов RS4 с переменной длиной ключа.

Шифрование открытым ключом и электронное подписывание. Проблема распространения ключей, метод Диффи-Хелмана. Метод RSA. Проблема генерации простых чисел. Методы разложения чисел на множители. Генерация длинных простых чисел с помощью малой теоремы Ферма. Вычисление НОД для длинных чисел. Генерация длинных ключей для метода RSA. Комбинированное применение метода RSA и симметричного алгоритма шифрования для шифрования открытым ключом. Однонаправленные функции, их вычисление. Комбинированное применение метода RSA и однонаправленной функции для электронного подписывания. Возможные уязвимости метода RSA и способы их устранения.

Теория вероятностей и математическая статистика

Вероятностные меры. Алгебры и сигма-алгебры. Конечные и бесконечные измеримые пространства. Примеры наиболее важных для теории вероятностей измеримых пространств R^1, R^n. Вероятностное пространство. Аксиоматика Колмогорова. Измеримые функции. Определение интеграла Лебега. Пространства L^1 и L^2 и их характеристики.

Случайные величины и распределения в R^n. Определение и основные свойства функции распределения и характеристической функции случайных величин. Математическое ожидание и условное математическое ожидание. Закон больших чисел. Центральная предельная теорема. Теорема Берри-Эссеена. Вероятности больших уклонений.

Элементы математической статистики. Теорема Рао—Блекуэлла—Колмогорова. Использование для построения наилучшей несмещенной оценки. Несмещенность. Несмещенные оценки с минимальной дисперсией. Неравенство Рао—Крамера. Метод максимального правдоподобия. Асимптотические свойства оценок максимального правдоподобия. Простая гипотеза. Критерий для проверки простых гипотез. Ошибки 1-го и 2-го родов. Мощность критерия. Лемма Неймана— Пирсона.

Случайные процессы

Определение. Случайный процесс. Непрерывность и дифференцируемость траекторий. Теорема Колмогорова о существовании непрерывной модификации. Процессы с независимыми приращениями. Пуассоновский процесс. Стационарный в широком и узком смысле процесс.

Некоторые виды зависимости. Мартингалы, субмартингалы, тождество Вальда. Теоремы Дуба о разложении и остановке. Цепи Маркова, свойства эргодичности. Процессы рождения и гибели. Марковские процессы. Уравнения Колмогорова.

Стохастическое исчисление и диффузионные процессы. Стохастический интеграл. Формула Ито. Существование и единственность решений стохастических дифференциальных уравнений.

Финансовая математика

Введение. Дисконтирование в дискретном и непрерывном времени. Рыночная норма капитализация. Форварды, фьючерсы, свопы. Теория CAPM. CML-кривая, рыночный портфель, бэта актива.

Ценообразование. Теория арбитража в одношаговой модели. Эквивалентная мартингальная мера. Интервал справедливых цен. CRR-модель. Модель Блэка-Шоулса. Греки

Измерение риска. VaR. Способы расчета. Экономический капитал. Когерентные меры риска. Expected shortfall. RAROC. Инвариантность по распределению.

Оптимальное управление и дискретная оптимизация

Оптимальное управление. Постановка задач оптимального управления, их классификация. Принцип максимума Понтрягина. Краевая задача принципа максимума. Линейная задача быстродействия, ее свойства (существование решения, число переключений). Принцип максимума и вариационное исчисление. Теорема Куна-Такера.

Дизъюнктивные нормальные формы Проблема минимизации булевых функций. Дизъюнктивные нормальные формы (ДНФ). Постановка задачи в геометрической форме. Локальные алгоритмы построения ДНФ. Построение ДНФ ?Т (сумма тупиковых) с помощью локального алгоритма**.**

Дискретная оптимизация. Целочисленное линейное программирование (метод Гомори, свойства унимодулярности матрицы ограничений). Метод ветвей и границ (на примере задач целочисленного или булева линейного программирования). Временная сложность решения задач дискретной оптимизации. Основные классы сложности (P, NP, NPC). NP-трудные задачи (задача о рюкзаке, задача коммивояжера).

Современные платформы информационных систем

Понятие платформы информационной системы. Архитектурные шаблоны и архитектурные стили.

Основные архитектурные типы платформ: потоки данных; слои, компонентная

архитектура; вызов и возврат, событийное управление; данные и объектная организация; архитектура с разделяемыми данными (репозиторий); интерпретатор (виртуальная машина).

Основные архитектурные шаблоны: модель предметной области. Сценарий транзакции. Модуль таблицы. Диспетчер

Архитектурные стили распределенных приложений: клиент/сервер; хост-терминал; широкополосный вызов; пакетный режим.

Шаблоны интеграции информационных систем: топология («точка-точка», «звезда», «общая шина»); первичная ориентация (данные, функции объекты, понятийная модель); технология обмена информацией (файлы, база данных, вызов процедур, сообщения).

Выбор типа платформы. Применение архитектурных шаблонов и шаблонов интеграции. Стандартизация в области архитектуры программных систем. Коммерческие платформы. Примеры реализации архитектурных стилей, подходов и шаблонов в коммерческих платформах.

Программа сформирована на основе федеральных государственных образовательных стандартов высшего образования по программам специалитета и магистратуры.

Литература по доп. источникам

Колмогоров А.Н., Фомин С.В. Элементы теории функции и функционального анализа. М.: Наука, 1976.
Феллер В. Введение в теорию вероятностей и ее приложения. Т.1. М.: Мир, 1984.
Феллер В. Введение в теорию вероятностей и ее приложения. Т.2. М.: Мир 1984.
Боровков А.А. Математическая статистика. Новосибирск: Наука, 1997.
Вентцель А.Д. Курс теории случайных процессов. М.: Наука, 1975.
Ширяев А.Н. Вероятность.
Боровков А.А. Теория вероятностей. М.: Эдиториал УРСС, 1999.
Яблонский С.В. Введение в дискретную математику. М.: Высш. школа, 2001.
Кудрявцев В.В, Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.
Мальцев А. И. Алгоритмы и вычислимые функции. М.: Наука, 1986.
Оре О. Теория графов. М.: Наука, 1980.
Нигматуллин Р. Г. Сложность булевых функций. М.: Наука, 1991.
Математические вопросы кибернетики. 1988—2001. Вып. 1—10. М.: Наука.
Гермейер Ю.Б. Введение в теорию исследования операций. М.: Наука, 1969.
Сухарев А.Г., Тимохов А.В., Федоров В.В. Курс методов оптимизации. М.: Наука, 1986.
Васильев Ф.П. Методы оптимизации. М.: Факториал, 2002.
Карманов В.Г. Математическое программирование. М.: Наука, 2000.
Понтрягин Л. Избранные научные труды. Т. 2. М.: Наука, 1988.
Тихомиров В.М., Фомин С.В., Алексеев В.М. Оптимальное управление. М.: Наука, 1979.
Краснощеков П.С., Петров А.А. Принципы построения моделей. М.: Фазис, 2002.
Подиновский В.В., Ногин В.Д. Парето-оптимальные решения многокритериальных задач. М.: Наука, 1981.
Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. М.: Наука, 198 .
Сэведж Дж. Э. Сложность вычислений. М.: Факториал, 1998.
Булинский А.В., Ширяев А.Н. Теория случайных процессов. М.: Физматлит, 2005, 408 с.

Халл Дж. К. Опционы, фьючерсы и другие производные финансовые инструменты/ пер. с англ. 6-е изд. М.: Вильямс, 2008, 1024 с.
Фелльмер Г., Шид А. Введение в стохастические финансы. Дискретное время/ пер. с англ. Ю. Мишуры, Г. Шевченко, В. Аркина. М.: МЦНМО, 2008, 496 с.
Shreve S. Stochastic calculus for finance. Volume I: The binomial Asset pricing model. Volume II: Continuous-time models. New York: Springer-Verlag, 2004.