

ПРОГРАММА АСПИРАНТСКОГО ЭКЗАМЕНА
по специальности 05.13.11
“Математическое и программное обеспечение вычислительных
машин, комплексов и компьютерных сетей”

1 Математические основы программирования

1. Понятие алгоритма и его уточнения: машины Тьюринга, нормальные алгоритмы Маркова, рекурсивные функции. Эквивалентность данных формальных моделей алгоритмов. Понятие об алгоритмической неразрешимости. Примеры алгоритмически неразрешимых проблем.
2. Понятие сложности алгоритмов. Классы P и NP. Полиномиальная сводимость задач. Теорема Кука об NP-полноте задачи выполнимости булевой формулы. Примеры NP-полных задач, подходы к их решению. Точные и приближенные комбинаторные алгоритмы.
3. Автоматы. Эксперименты с автоматами. Алгебры регулярных выражений. Теорема Клини о регулярных языках.
4. Алгебра логики. Булевы функции, канонические формы задания булевых функций. Понятие полной системы. Критерий полноты Поста. Минимизация булевых функций в классах нормальных форм.
5. Исчисление предикатов первого порядка. Понятие интерпретации. Выполнимость и общезначимость формулы первого порядка. Понятие модели. Теорема о полноте исчисления предикатов первого порядка.
6. Отношения и функции. Отношение эквивалентности и разбиения. Фактор множества. Отношения частичного порядка. Теоретико-множественное и алгебраическое определения решетки, их эквивалентность. Свойства решеток. Булевы решетки. Полные решетки.
7. Формальные языки и способы их описания. Классификация формальных грамматик. Их использование в лексическом и синтаксическом анализе.
8. λ -исчисление, правила редукции, единственность нормальной формы и правила ее достижения, представление рекурсивных функций.
9. Основы комбинаторного анализа. Метод производящих функций, метод включений и исключений. Примеры применения.
10. Коды с исправлением ошибок. Алфавитное кодирование. Алгоритмы сжатия данных: RLE, Хаффмена, LZW, арифметического кодирования. Адаптивные алгоритмы. Теоремы об оптимальности кода Хаффмена. Теоремы о сжатии в методе арифметического кодирования.
11. Основы криптографии. Задачи обеспечения конфиденциальности и целостности информации. Теоретико-информационный и теоретико-сложностный подходы к определению криптографической стойкости. Американский стандарт шифрования DES и российский стандарт шифрования данных ГОСТ 28147-89. Системы шифрования с открытым ключом (RSA). Цифровая подпись. Методы генерации и распределения ключей.

2 Методы хранения данных и доступа к ним. Организация баз данных и знаний

1. Динамические структуры данных: стек, дек, очередь, последовательность, список, дерево, множество. Непрерывные и ссылочные реализации структур данных.
2. Реализации множеств. Хэширование. Совершенные, минимальные хеш-функции. Различные варианты хэш-реализаций множеств. Эффективность процедур поиска, включения и исключения элементов при различных реализациях.
3. Бинарные деревья. Процедуры восходящего, нисходящего, горизонтального обхода бинарного дерева. Деревья поиска. Добавление и удаление элементов в дерево поиска. Сбалансированные бинарные деревья. Алгоритмы балансировки дерева. Теорема о глубине сбалансированного дерева.
4. Красно-черные деревья. Сравнение эффективности поиска со сбалансированным деревом. Процедуры добавления и удаления элементов. Оценки их эффективности. Теорема о глубине красно-черного дерева.
5. В-деревья. Процедуры добавления и удаления элементов. Оценки их эффективности.
6. Контейнеры данных переменного и фиксированного размера. Методы реализации функций динамического выделения памяти.
7. Сортировки обменом, линейной вставкой, выбором, слиянием (Неймана). Сортировка Шелла. Сортировка с помощью дерева (heapsort). Быстрая сортировка. Теоремы об оценке снизу для трудоемкости сортировок. Теоремы о средней трудоемкости быстрой сортировки. Алгоритм сортировки с линейной оценкой трудоемкости.
8. Основные понятия реляционной и объектной моделей данных.
9. Теоретические основы реляционной модели данных (РДМ). Реляционная алгебра, реляционное исчисление. Функциональные зависимости и нормализация отношений.
10. CASE-средства и их использование при проектировании базы данных (БД).
11. Организация и проектирование физического уровня БД. Методы индексирования.
12. Обобщенная архитектура, состав и функции системы управления базой данных (СУБД). Характеристика современных технологий БД. Примеры соответствующих СУБД.
13. Основные принципы управления транзакциями, журнализацией и восстановлением.
14. Язык баз данных SQL. Средства определения и изменения схемы БД, определения ограничений целостности. Контроль доступа. Средства манипулирования данными.
15. Информационно-поисковые системы. Классификация. Методы реализации и ускорения поиска.
16. Методы представления знаний: процедурные представления, логические представления, семантические сети. Интегрированные методы представления знаний. Языки представления знаний. Базы знаний.
17. Экспертные системы (ЭС). Области применения ЭС. Архитектура ЭС. Механизмы вывода, подсистемы объяснения, общения, приобретения знаний ЭС. Жизненный цикл экспертной системы.

3 Языки и системы программирования

1. Языки программирования. Процедурные и объектно-ориентированные языки программирования.
2. Процедурные языки программирования. Основные управляющие конструкции, структура программы. Работа с данными: переменные и константы, типы данных (булевский, целочисленные, плавающие, символьные, типы диапазона и перечисления, указатели), структуры данных (массивы и записи). Процедуры (функции): вызов процедур, передача параметров (по ссылке, по значению, по результату), локализация переменных, побочные эффекты. Обработка исключительных ситуаций. Библиотеки процедур и их использование.
3. Объектно-ориентированный подход в программировании. Объекты, их информационная структура, отношения между объектами. Инкапсуляция, сокрытие информации. Абстрактные типы данных. Их преимущества. Классы и представители. Полиморфизм.
4. Объектно-ориентированный подход в программировании. Наследование. Переопределение информационных и/или поведенческих структур при наследовании. Цели использования наследования. Средства обработки объектов (контейнеры и итераторы).
5. Формальные грамматики. LR(1) разбор для арифметического выражения. Рекурсивный алгоритм построения дерева разбора арифметического выражения. Компилятор модельного языка программирования: проектирование системы команд стекового процессора, реализация операторов перехода в программе, организация вызовов подпрограмм и функций, передача параметров в функции.
6. Основы построения трансляторов. Структура оптимизирующего транслятора. Промежуточные представления программы: последовательность символов, последовательность лексем, синтаксическое дерево, абстрактное синтаксическое дерево.
7. Оптимизация программ при их компиляции. Оптимизация базовых блоков, выделение общих подвыражений, разворачивание циклов, переупорядочивание инструкций. Анализ графов потока управления и потока данных.

4 Операционные системы

1. Операционные системы (ОС). Определения операционных систем реального времени (ОСРВ). Определения основных объектов ОС. Программа, процессор, процесс. Основные составляющие процесса, состояния процесса. Стек, виртуальная память, механизмы трансляции адреса.
2. Ресурсы, приоритеты. Виды ресурсов: аппаратные, программные, активные, пассивные, локальные, разделяемые, постоянные, временные, не критичные, критичные.
3. Параллельные процессы. Многозадачные ОС. Типы взаимодействия процессов: сотрудничающие и конкурирующие процессы, взаимное исключение процессов. Проблемы, возникающие при синхронизации процессов и идеи их разрешения. Связывание. Статическое и динамическое связывание. Особенности реализации для ОСРВ.
4. Определение потока исполнения (thread). Сравнение с процессами: создание, планирование, управление. Состояния процесса, потока исполнения и механизмы перехода из одного состояния в другое.
5. Типы архитектур операционных систем. Монолитная и модульная архитектура. Общее строение ОС. Роли отдельных компонент: планировщика, диспетчера.

6. Механизмы взаимодействия процессов: разделяемая память, семафоры, сигналы, события, критические секции, очереди сообщений. Примитивные операции. Особенности реализации для систем с виртуальной памятью. Особенности реализации для ОСРВ.
7. Планирование задач в ОС. Приоритеты. Схемы назначения приоритетов. Инверсия приоритетов и методы борьбы с ней. Стратегии планирования задач. Типичные схемы планирования в UNIX системах и ОСРВ. Контекст задачи и его переключение. Роль и задачи диспетчера. Прерывания. Процессы обработки прерывания и вызова подпрограмм. Время реакции на прерывание.
8. Файловые системы. Принципы организации хранения файлов на диске. Логическая структура диска. Базовые функции файловой системы. Принципы организации древовидной файловой системы. Организация файловых систем FAT, ext, NTFS. Процедуры поиска всех блоков файла, поиска свободного места, создания и удаления файла.

5 Архитектуры современных вычислительных систем

1. Внутренняя организация процессоров. Выделение независимо работающих устройств: IU, FPU, MMU, BU. CISC и RISC процессоры. Повышение производительности процессоров за счет конвейеризации. Условия оптимального функционирования конвейера. Суперконвейерные и суперскалярные процессоры. Методы уменьшения негативного влияния инструкций перехода на производительность процессора. Исполнение инструкций не по порядку.
2. Повышение производительности процессоров за счет введения кэш памяти. Кэши: единый, Гарвардский, с прямой записью, с обратной записью. Организация кэш-памяти. Алгоритмы замены данных в кэш памяти. Специальные кэши. Согласование кэшей в мультипроцессорных системах с общей памятью. Методы уменьшения времени реакции на прерывание.
3. Архитектуры системных шин. Синхронные и асинхронные шины. Мультиплексирование шины. Отображение ресурсов на память и пространство ввода-вывода. Мосты между шинами. Архитектуры шин PCI, VME, CompactPCI.
4. Виды многопроцессорных архитектур. Системы с общей и распределенной памятью. Поддержка многозадачности и многопроцессорности специальными инструкциями процессора. Организация данных во внешней памяти. Механизмы преобразования данных при обменах между компьютерами по коммуникационному каналу.

6 Программирование параллельных ЭВМ

1. Синхронизация и взаимодействие потоков исполнения. Объекты типа mutex. Примитивные операции. Виды mutex. Особенности реализации для ОСРВ.
2. Синхронизация и взаимодействие потоков исполнения. Объекты типа condvar. Примитивные операции. Виды condvar. Особенности реализации для ОСРВ.
3. Программирование систем с распределенной памятью. Message Passing Interface (MPI). Общая структура MPI-программы. Сообщения и их виды. Группы и коммутаторы. Парный обмен сообщениями. Операции ввода-вывода в MPI программах. Примеры.
4. Коллективный обмен сообщениями. Учет архитектуры параллельной ЭВМ. Ограничение коллективного обмена на подмножество процессов. Время в MPI программах.
5. Пересылка структур данных. Создание нового MPI типа данных. Упаковка/распаковка разнородных данных. Пересылка структур данных в однородных параллельных ЭВМ. Пересылки строк и столбцов матриц.

7 Сети передачи данных

1. Понятие о сетях с коммутацией каналов и пакетов. Достоинства и недостатки каждого из подходов. Базовые топологии локальных сетей: линия, кольцо, звезда. Структурные элементы локальных и глобальных сетей. Повторитель, разветвитель, мост, шлюз.
2. Логика функционирования сетей Ethernet, Infiniband, IEEE 802.11 (WIFI), IEEE 802.15 (Bluetooth), IEEE 802.16 (WiMAX). Адресация. Дисциплина передачи данных.
3. Иерархия сетевых протоколов в модели TCP/IP (Internet) IP адресация. Классы адресов. Широковещательные и другие специальные адреса. Маска подсети. Протоколы ARP, RARP, ICMP, назначение, принципы работы.
4. Протокол IP, назначение, принципы работы. Функции IP протокола, фрагментация и сборка. Уничтожение пакетов. Маршрутизация.
5. Протокол UDP, назначение, принципы работы. Адресация транспортного уровня. Контроль правильности передачи. Протокол TCP, назначение, принципы работы. Обеспечение надежности передачи. Сегментация данных при отправлении и сборка при получении. Процедуры установления и разрыва соединения. Механизм подтверждений. Таймеры.
6. Протокол и система DNS, назначение, принципы работы. Структура доменных имен. Классификация DNS серверов. Формат запроса и ответа. Ресурсная запись. Итеративная, рекурсивная и смешанная процедуры. Поддержка распределенной базы данных DNS.
7. Протокол FTP, назначение, принципы работы. Вид запроса и отклика. Процесс передачи файлов. Классификация кодов откликов.
8. Протокол HTTP, назначение, принципы работы. Формат запроса и отклика. Процесс передачи файлов. Структура и назначение строк-заголовков (header-lines). Виды соединений. Отличие HTTP/1.0 и HTTP/1.1. Классификация кодов откликов.
9. Socket-интерфейс. Основные функции и их назначение. Последовательность действий программы – клиента и программы – сервера.

8 Программная инженерия

1. Понятие жизненного цикла программного обеспечения (ПО). Процессы жизненного цикла ПО: основные, вспомогательные и организационные. Понятия модели и стадии жизненного цикла ПО. Каскадная и итерационная модели жизненного цикла. Методы <быстрой> разработки ПО (Agile Software Development).
2. Понятие технологии создания ПО и ее состав (технологические процессы, технологические операции, рабочие продукты, роли, руководства, инструментальные средства). Унифицированный процесс разработки ПО (Unified Software Development Process). Экстремальное программирование.
3. Метрики ПО. Оценка сложности и размера ПО. Стандартные метрики, применяемые для оценки размера ПО (количество строк кода и функциональных точек (function points)). Методы оценки трудоемкости создания ПО (статистические модели, экспертные оценки, оценки по аналогии).
4. Показатели качества ПО. Методы обеспечения качества ПО (отладка, тестирование, верификация и аттестация ПО). Методы, принципы, стратегии и этапы тестирования ПО (функциональное и нагрузочное тестирование, тестирование интерфейсов, модульное, интеграционное и регрессионное тестирование).

5. Визуальное моделирование ПО. Определение архитектуры ПО. Унифицированный язык моделирования UML. Состав языка (элементы, связи и диаграммы). Структурные модели (диаграммы классов, компонентов и размещения). Модели поведения (диаграммы вариантов использования, взаимодействия, состояний и деятельности). Механизмы расширения UML (стереотипы, примечания и ограничения).
6. Анализ и проектирование ПО. Структурное проектирование ПО. Моделирование потоков данных. Моделирование данных. Модель “сущность-связь”. Объектно-ориентированный анализ и проектирование ПО. Принципы построения объектной модели (абстракция, инкапсуляция, модульность, иерархия). Составляющие объектной модели (объект, класс, атрибут, операция, интерфейс, компонент, связи) и их свойства. Архитектурный анализ. Анализ вариантов использования.
7. Тестирование. Методы “черного” и “белого” ящиков. Критерии полноты тестового покрытия. Тестирование на основе моделей. Тестирование на основе конечно-автоматной модели. Унифицированная архитектура тестовой системы. Компоненты тестовой системы: тестовые драйверы, оракулы, фильтры, сценарии, скрипты, тестовые варианты, тестовые наборы, тестовые планы. Управления требованиями и проектирование тестов.

Список литературы

- [1] Яблонский С.В. Введение в дискретную математику. М.: Наука, 2001.
- [2] Ахо, Сети Р., Ульман Дж. Компиляторы: принципы, техника реализации и инструменты. М., 2001.
- [3] Валединский В.Д., Пронкин Ю.Н. Вычислительные системы и программирование. Системы хранения данных. М.: Изд-во ЦПИ при механико-математическом ф-те МГУ им. М.В.Ломоносова, 2006.
- [4] Валединский В.Д., Пронкин Ю.Н. Вычислительные системы и программирование. Организация вычислительных систем. М.: Изд-во ЦПИ при механико-математическом ф-те МГУ им. М.В.Ломоносова, 2006.
- [5] Кнут Д. Искусство программирования. Т. 1 - 3. М., СПб., Киев: ИД "Вильямс", 2000.
- [6] Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы, построение и анализ. М.: МЦНМО, 2000.
- [7] Когаловский М.Р. Энциклопедия технологий баз данных. М.: Финансы и статистика, 2002.
- [8] Кумсков М.И. Базы данных и процессы их создания. Введение. М.: Изд-во ЦПИ при механико-математическом ф-те МГУ им. М.В.Ломоносова, 2004, 136 с.
- [9] Туманов В. Е. Основы проектирования реляционных баз данных. М.: Изд-во Бином, 2007, 420 с.
- [10] Дейтел Г. Введение в операционные системы. М.: Мир, 1987.
- [11] Богачев К.Ю. Операционные системы реального времени. М.: Изд-во ЦПИ при механико-математическом ф-те МГУ им. М.В.Ломоносова, 2001.
- [12] Назаров С. В., Широков А. И. Современные операционные системы. М.: Изд-во Бином, 2011.
- [13] Воеводин В. В., Воеводин Вл. В. Параллельные вычисления. - СПб: БХВ-Петербург, 2002.
- [14] Богачев К.Ю. Основы параллельного программирования. М.: Изд-во Бином, 2003.

- [15] Галатенко В. А. Основы информационной безопасности. М.: Изд-во Бином, 2008.
- [16] Фороузан Б. А. Криптография и безопасность сетей. М.: Изд-во Бином, 2010.
- [17] Сеницын С. В., Налютин Н. Ю. Верификация программного обеспечения. М.: Изд-во Бином, 2008.
- [18] Семенов Ю. А. Алгоритмы телекоммуникационных сетей. ч. 1. Алгоритмы и протоколы каналов и сетей передачи данных. М.: Изд-во Бином, 2007, 637 с.
- [19] Семенов Ю. А. Алгоритмы телекоммуникационных сетей. ч. 2. Протоколы и алгоритмы маршрутизации в internet. М.: Изд-во Бином, 200, 829 с.
- [20] Кулямин В. В. Технологии программирования. Компонентный подход. М.: ИНТУИТ-Бином, 2007.
- [21] Брауде Э. Дж. Технология разработки программного обеспечения. СПб: Питер, 2004. - 656 с. ISBN 5-94723-663-X, 0-47132-208-3.
- [22] Ларман К. Применение UML и шаблонов проектирования. М.: Изд. дом Вильямс, 2002.
- [23] Лисков Б., Гатег Дж. Использование абстракций и спецификаций при разработке программ. М.: Мир, 1989.
- [24] Соммервилл И. Инженерия программного обеспечения: 6-е изд. М.: Изд. дом Вильямс, 2002.