Программа спецкурса
«Быстрые вычисления»
2010–2011 уч. г.

проф. Гашков С. Б., к.ф.-м.н. Сергеев И. С.

Тема 1. Аддитивные цепочки.

Возведение в степень и аддитивные цепочки. Линейные аддитивные цепочки. Методы построения аддитивных цепочек: бинарный метод, метод множителей, асимптотически наилучший 2^k-арный метод Брауэра. Построение аддитивных цепочек для чисел вида $2^n - 1$ (метод Брауэра). Векторные аддитивные цепочки. Метод Страуса построения векторных аддитивных цепочек. Лемма Пиппенджера о транспонировании. [БГФЧ, К]

Тема 2. Простейшие арифметические схемы.

Схемы из функциональных элементов и неветвящиеся программы. Сложность и глубина схем. Стандартные схемы сложения и умножения. Минимизация глубины булевых схем для сложения (метод золотого сечения, метод Храпченко, метод Гринчука) и умножения чисел (метод компрессоров). Параллельные префиксные схемы, префиксный сумматор (метод Ладнера-Фишера). [W]

Тема 3. Быстрые алгоритмы умножения. Дискретное преобразование Фурье.

Методы Карацуба и Тоома умножения чисел. Дискретное преобразование Фурье. Теоремы Кули—Тьюки и Гуда—Томаса. Алгоритм быстрого преобразования Фурье (БПФ). БПФ над полем комплексных чисел (метод БПФ с расщепленным основанием и метод ван Бускирка). Быстрое умножение многочленов (методы Шёнхаге и Штрассена). Метод Фюрера умножения чисел. [АХУ, ГЧ, Be, F, W]

Тема 4. Элементарные арифметические операции с числами и многочленами.

Метод последовательных приближений. Алгоритмы приближенного деления и извлечения квадратного корня из чисел и степенных рядов. Метод Штрассена деления многочленов с остатком. Вычисление элементарных аналитических функций степенных рядов и чисел (логарифм, экспонента, тригонометрические функции): метод Брента—Саламина. [Br, BCS]

Тема 5. Алгоритмы, основанные на быстром умножении.

Бинарный алгоритм вычисления НОД многочленов. Лемма Лехмера. Применение принципа «деления пополам»: быстрый расширенный алгоритм вычисления НОД многочленов, быстрые алгоритмы интерполяции и вычисления значений многочлена на наборе точек. Быстрое вычисление факториала (метод Шёнхаге). [АХУ, ГЧ, BCS, GG]

Тема 6. Быстрое умножение матриц.

Билинейные алгоритмы умножения матриц. Метод Штрассена. Метод приближенных разложений. Теорема Бини—Шёнхаге. Пример Шёнхаге, основанный на приближенном билинейном алгоритме умножения матриц размера 3×3. Тау-теорема Шёнхаге. Построение алгоритма умножения $n \times n$ матриц сложности $O(n^{2,55})$. [A, BCS]

Тема 7. Арифметика конечных полей.

Конечные поля. Стандартные и нормальные базисы конечных полей. Умножение в конечном поле. Модулярная композиция многочленов и реализация автоморфизмов Фробениуса в стандартных базисах конечных полей (метод Брента—Кунга). Переходы между нормальными и стандартными представлениями элементов. Инвертирование в конечном поле: метод аддитивных цепочек. [БГФЧ, ГЧ, GG]

Литература

[A] Алексеев В. Б. Сложность умножения матриц. // Кибернетический сборник. Вып. 25. — М.: Мир, 1988. — С. 189–236.

[АХУ] Ахо А., Хопкрофт Дж., Ульман Дж. Проектирование и анализ вычислительных алгоритмов. — М.: Мир, 1979.

[БГФЧ] Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. — М.: КомКнига, 2006.

[ГЧ] Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. — М.: Изд-во МГУ, Дрофа, 2005.

[К] Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. — М.: Вильямс, 2000–2008.

[Be] Bernstein D. J. The tangent FFT // Proc. AAECC. LNCS. — 2007. — V. 4851. — P. 291–300.

[Br] Brent R. Multiple-precision zero-finding methods and the complexity of elementary function evaluation // Analytic computational complexity. — NY.: Academic Press, 1975, 151–176.

[BCS] Bürgisser P., Clausen M., Shokrollahi M. A. Algebraic complexity theory. — Berlin—Heidelberg: Springer-Verlag, 1997.

[F] Fürer M. Faster Integer Multiplication // SIAM J. Comput. — 2009. — Vol. 39(3), P. 979–1005.

[GG] von zur Gathen J., Gerhard J. Modern computer algebra. — Cambridge University Press, 1999, 2003.

[W] Wegener I. The complexity of boolean functions. — Stuttgart: Wiley, 1987.