Демьянович Ю. К.

Компьютерная алгебра.

Системы аналитических вычислений.

1999

ВВЕДЕНИЕ

Предлагаемый курс лекций соответствует лекциям, которые автор читает студентам IY-Y курса математико-механического факультета СПбГУ, специализирующимся по кафедре системного программирования. В курсе рассмотрена проблема аналитических преобразованиий на компьютерах и трудности, связанные с реализацией программных систем аналитических вычислений (САВ). Центральной трудностью представляется значительное разрастание промежуточных результатов (чаще всего это разрастание носит экспоненциальный характер), что ведет к огромным затратам ресурсов компьютера. Поэтому основное направление преодоления возникающих трудностей - создание наиболее экономичных алгоритмов обработки аналитических выражений. При решении такой задачи требуются определенные сведения из теории сложности алгоритмов; многие из них приводятся без доказательства. Достаточно подробно излагается быстрое дискретное преобразование Фурье (в том числе и в кольце вычетов), идеи которого широко используются при разработке САВ. Далее рассматриваются представление данных в системах аналитических вычислений, полиномиальное упрощение (базисы Грёбнера и др.), а также алгоритмы неопределенного интегрирования (в том числе методы Эрмита и Горовица). Для удобства читателя в изложении курса автор следовал книгам [1-4], к которым по-видимому следует обращаться для более глубокого изучения предлагаемого материала.

Лекции распадаются на пять параграфов. Первый параграф посвящен быстрому дискретному преобразованию Фурье, во втором параграфе обсуждаются вопросы о взаимоотношении аналитических преобразований и численного счета, о месте компьютерной алгебры и теории сложности вычислений в использовании и создании САВ. Важному вопросу представления данных в САВ посвящен третий параграф. В четвертом и пятом параграфах рассматриваются полиномиальное упрощение (редукция полиномов, базисы Грёбнера и алгоритм Бухбергера) и формальное интегрирование (расширенный алгоритм Эвклида, метод Горовица, отыскание результанта и др.)

Автор надеется, данный курс будет полезен для студентов, аспи-

рантов и всех лиц, заинтересованных в использовании имеющихся или в создании новых систем аналитических вычислений.

§1. Быстрое дискретное преобразование Фурье (БПФ)

1. О понятии многочлена в кольце $\mathcal{K}$

Пусть $\mathcal{K}$ – коммутативное, ассоциативное кольцо с единицей, и пусть буква x – посторонняя для кольца $\mathcal{K}$.

Кратко напомним, как вводится понятие многочлена в кольце $\mathcal{K}$. Рассмотрим выражение ax^m (здесь m – неотрицательное целое число, а $a \in \mathcal{K}$), назовем его одночленом в кольце $\mathcal{K}$ и введем (обычные для комплексных многочленов) действия умножения и приведения одночленов. Степенью этого одночлена называется число m. Далее введем понятие многочлена как формальной суммы одночленов, где порядок безразличен. Канонической формой многочлена называется многочлен с приведенными подобными членами, расположенными по убыванию степеней,

$$P(x) = a_0x^n + \ldots + a_n.$$

Два многочлена называются равными, если их канонические формы совпадают.

Сумму и произведение двух многочленов можно определить совершенно формально, написав для них соответствующие равенства (подробно на этих очевидных вещах останавливаться не будем).

Степенью $deg(P)$ ненулевого многочлена называется старшая степень его одночленов. За степень нулевого многочлена O принимают число $degO = -\infty$.

Высшим (старшим) членом ненулевого многочлена называется первое слагаемое его канонической формы. Считается, что нулевой многочлен не имеет высшего (старшего) члена.

Нетрудно видеть, что буква x фактически играет роль разделителя: ее безболезненно можно убрать, и упомянутые выше действия совершать лишь над коэффициентами, помещая их на места, занумерованные показателем степени убранной буквы x.

Предположим, что кольцо $\mathcal{K}$ – область целостности, т.е. что произведение двух элементов из $\mathcal{K}$ равно нулю только если хотя бы

один из них равен нулю[1].

Теорема 1. *Если $\mathcal{K}$ – область целостности, то кольцо полиномов $\mathcal{K}[x]$ – тоже область целостности.*

Доказательство приводить здесь не будем.

2. Схема Хорнера (и теорема Безу)

Здесь кратко напомним схему Хорнера и теорему Безу.

Определение 1. *Если для полиномов $P(x)$ и $Q(x)$ из $\mathcal{K}[x]$ существует такой полином $H(x) \in \mathcal{K}[x]$, что*

$$P(x) = Q(x)H(x), \tag{2.1}$$

то говорят, что $P(x)$ делится на $Q(x)$ без остатка. Говорят, что $P(x)$ делится на $Q(x)$ с остатком $R(x)$, если существует $H(x)$ такой, что

$$P(x) = Q(x)H(x) + R(x), \quad deg\, R < deg\, Q. \tag{2.2}$$

Нас будет интересовать деление на $Q(x) = x - c$,

$$P(x) = (x - c)H(x) + r, r \in \mathcal{K}. \tag{2.3}$$

Теорема 2. *Если $P(x) = a_0x^n + \ldots + a_n \in \mathcal{K}[x]$ и $c \in \mathcal{K}$, то найдутся полином $H(x) \in \mathcal{K}[x]$ и $r \in \mathcal{K}$ такие, что*

$$P(x) = (x -)H(x) + r. \tag{2.4}$$

Доказательство. Будем искать $H(x)$ в форме $b_0x^{n-1} + \ldots + b_{n-1}$. Сравнение коэффициентов в равенстве

$$a_0x^n + a_1x^{n-1} + \ldots + a_n =$$

$$= (x - c)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + r$$

показывает равносильность его цепочке равенств

$$a_0 = b_0,$$

$$a_1 = b_1 - b_0c,$$

[1]Вспомнить определение кольца. Привести примеры некоммутативного кольца, а также кольца, не являющегося областью целостности.

$$a_2 = b_2 - b_1 c,$$

$$\cdots\cdots\cdots\cdots$$

$$a_{n-1} = b_{n-1} - b_{n-2} c,$$

$$a_n = r - b_{n-1} c,$$

откуда последовательно находим коэффициенты полинома $H(x)$ и остаток r,

$$\begin{aligned} b_0 &= a_0, \\ b_1 &= a_1 + b_0 c, \\ b_2 &= a_2 + b_1 c, \\ &\cdots\cdots\cdots\cdots \\ b_{n-1} &= a_{n-1} + b_{n-2} c, \\ r &= a_n + b_{n-1} c. \end{aligned} \tag{2.5}$$

Теорема доказана. ■

Равенства(2.5) называются схемой Хорнера.

Замечание 1. Для реализации схемы (2.5) требуется n умножений и n сложений.

Теорема 3 (теорема Безу). *Для того, чтобы $P(x) \in \mathcal{K}[x]$ делился на $x - c$ необходимо и достаточно, чтобы $P(c) = 0$.*

Доказательство легко следует из теоремы 2 и определений (2.1) и (2.3). ■

3. Дискретное преобразование Фурье

Рассмотрим теперь дискретное преобразование Фурье; оно по существу является дискретным аналогом непрерывного преобразования Фурье.

В дальнейшем единицу кольца $\mathcal{K}$ обозначаем символом $\mathbf{1}$.

Определение 2. *Элемент ω из кольца $\mathcal{K}$, обладающий свойствами*

$$1). \quad \omega \neq \mathbf{1}, \qquad 2). \quad \omega^n = \mathbf{1}, \tag{3.1}$$

$$3). \sum_{j=0}^{n-1} \omega^{jp} = 0 \qquad\qquad 1 \leq p < n. \tag{3.2}$$

называется примитивным корнем n-ой степени из единицы. Элементы

$$\omega^0, \omega^1, \ldots, \omega^{n-1} \tag{3.3}$$

называются корнями n-ой степени из единицы.

Пример. Если $\mathcal{K}$ – кольцо комплексных чисел, то $\omega = e^{\frac{2\pi i}{n}}$ примитивный корень n-ой степени из $\mathbf{1}$.

Пусть $a = (a_0, a_1, \ldots, a_{n-1})^T$ – n-мерный вектор-столбец с элементами из кольца $\mathcal{K}$.

В дальнейшем для удобства будем буквой n обозначать элемент $n \cdot \mathbf{1}$ из кольца $\mathcal{K}$ $(n \cdot \mathbf{1} = \underbrace{\mathbf{1} + \mathbf{1} + \ldots + \mathbf{1}}_{n})$ и будем считать, что элемент $\frac{1}{n} \stackrel{def}{=} (n \cdot \mathbf{1})^{-1}$ существует и лежит в кольце $\mathcal{K}$.

Рассмотрим квадратную матрицу A с элементами

$$A[i, j] = \omega^{ij}, \qquad i, j = 0, 1, \ldots, n-1. \tag{3.4}$$

Определение 3. *Пусть матрица A определена формулой (3.4). Дискретным преобразованием Фурье вектора a называется вектор* $\widehat{a} = (\widehat{a}_0, \widehat{a}_1, \ldots, \widehat{a}_{n-1})^T$, *получаемый по формуле*

$$\widehat{a} = Aa. \tag{3.5}$$

Операция перехода от вектора a к вектору $\widehat{a}$ *носит название (операции) дискретного преобразования Фурье.*

Обозначим её F, так что

$$\widehat{a} = F(a). \tag{3.6}$$

Лемма 1. *Матрица A обратима и элементы* $B[i, j]$ *обратной матрицы* $B = A^{-1}$ *даются формулой*

$$B[i, j] = \frac{1}{n}\omega^{-ij}. \tag{3.7}$$

Доказательство. Символ Кронекера (в кольце $\mathcal{K}$) обозначим δ_{ij}, т.е. положим

$$\delta_{ij} = \begin{cases} 0, & i \neq j, \\ \mathbf{1}, & i = j \end{cases}.$$

Лемма будет доказана, если установить, что

$$\sum_{k=0}^{n-1} A[i,k]B[k,j] = \delta_{ij}, \tag{3.8}$$

или (ввиду формул (3.4),(3.5)) если установить, что

$$\frac{1}{n}\sum_{k=0}^{n-1} \omega^{ik}\omega^{-kj} = \delta_{ij}. \tag{3.9}$$

При $i = j$ левая часть в (3.9) равна единице,

$$\frac{1}{n}\sum_{k=0}^{n-1} \omega^{0} = \mathbf{1}. \tag{3.10}$$

Пусть $i \neq j$; обозначим $p = i - j$. Тогда левая часть в (3.9) имеет вид

$$W = \frac{1}{n}\sum_{k=0}^{n-1} \omega^{pk}, \qquad 0 < p \leq n-1. \tag{3.11}$$

При $p = 1, 2, \ldots, n-1$ (3.11) обращается в нуль в силу свойства (3.2). Умножим (3.11) на (ненулевой) множитель $\omega^{-p(n-1)}$. Тогда

$$W = \frac{1}{n}\sum_{k=0}^{n-1} \omega^{p(k-(n-1))},$$

так что заменяя индекс суммирования $-k' = k - (n-1)$, найдём

$$W = \frac{1}{n}\sum_{k'=0}^{n-1} \omega^{-pk'} = \frac{1}{n}\sum_{k'=0}^{n-1} \omega^{p'k'},$$

где

$$p' = -p; \quad p' = 1, 2, \ldots, n-1.$$

Итак, ввиду свойства (3.2) при $p \neq 0$ получаем равенство $W = 0$.

Лемма доказана. ∎

Определение 4. *Обратным дискретным преобразованием Фурье вектора* $a = (a_0, a_1, \ldots, a_{n-1})$ *называется вектор* $\check{a} = (\check{a}_0, \check{a}_1, \ldots, \check{a}_{n-1})$, *получаемый применением к нему матрицы* B *с элементами (3.7),*

$$\check{a} = Ba. \tag{3.12}$$

Ввиду леммы 1 соотношение (3.12) может быть записано в форме

$$\check{a} = A^{-1}a. \tag{3.13}$$

Операция обратного дискретного преобразования Фурье обозначается F^{-1}; пишут также

$$\check{a} = F^{-1}a. \tag{3.14}$$

Теорема 4 (Свойства обратного дискретного преобразования Фурье). *Для n-мерного вектора a, $a = (a_0, a_1, \ldots, a_{n-1})$ справедливы формулы*

$$F(\check{a}) = a, \qquad F^{-1}(\widehat{a}) = a, \tag{3.15}$$

а также формулы

$$\widehat{\check{a}} = a, \qquad \check{\widehat{a}} = a. \tag{3.16}$$

Доказательство. Формулы (3.15) могут быть записаны в виде $ABa = a$ и $BAa = a$ соответственно; последние эквивалентны лемме 1. Соотношения (3.16) эквивалентны формулам (3.15).

Теорема доказана. ∎

4. О связи с задачей вычисления многочлена и интерполяцией Лагранжа

Рассмотрим многочлен $P(x)$ с коэффициентами из кольца $\mathcal{K}$,

$$P(x) = \sum_{i=0}^{n-1} a_i x^i. \tag{4.1}$$

Он однозначно представляется списком его коэффициентов

$$a_0, a_1, \ldots, a_{n-1}, \tag{4.2}$$

а также списком

$$b_0, b_1, \ldots, b_{n-1} \tag{4.3}$$

его значений

$$b_i = P(x_j) \tag{4.4}$$

в n различных точках

$$x_0, x_1, \ldots, x_{n-1}. \tag{4.5}$$

Переход от списка (4.2) к списку (4.3) согласно формулам (4.4) представляет собой вычисление многочлена (4.1) в n различных точках (4.5), а переход от списка (4.3) к списку (4.2) сводится к задаче определения коэффициентов многочлена (4.1) по его значениям в n различных точках, т.е. к задаче отыскания $a_i, i = 0, 1, \ldots, n-1$ из уравнений

$$P(x_j) = b_j, \quad j = 0, 1, \ldots, n-1. \tag{4.6}$$

Эта задача, как известно, называется интерполяционной задачей Лагранжа.

Из сказанного ясно, что рассматриваемые задачи взаимно обратны (в первой по списку (4.2) отыскивается список (4.3), а во второй – наоборот, по списку (4.3) отыскивается список (4.2)). Обе задачи определяются совокупностью точек (4.5).

Выберем эту совокупность специальным образом, а именно, положим

$$x_j = \omega^j, \quad j = 0, 1, \ldots, n-1. \tag{4.7}$$

При таком выборе первая задача сводится к дискретному преобразованию Фурье списка(4.2), а вторая – к обратному дискретному преобразованию Фурье списка (4.3). Как будет видно впоследствии, выбор (4.7) значительно упрощает решение обеих задач.

5. Понятие свёртки двух векторов

Определение 5. *Пусть*

$$a = (a_0, a_1, \ldots, a_{k-1})^T, \qquad b = (b_0, b_1, \ldots, b_{k-1})^T. \tag{5.1}$$

Свёрткой $a * b$ называется вектор

$$c = (c_0, c_1, \ldots, c_{2k-2})^T \tag{5.2}$$

так, что [2]

$$c_i = \sum_{j=0}^{k-1} a_j b_{i-j}, \quad i = 0, 1, 2, \ldots, 2k-2, \tag{5.3}$$

[2] Доказать, что при условиях (5.4) запись (5.3) эквивалентна записи

$$c_i = \sum_{j=-\infty}^{+\infty} a_j b_{i-j}, \quad i = 0, 1, 2, \ldots, 2k-2 \tag{5.3′}$$

где считают

$$a_i = b_i = 0 \qquad \text{при} \quad i < 0 \qquad i > k-1. \tag{5.4}$$

Пример. При $k = 3$ для векторов

$$a = a_0, a_1, a_2, \qquad b = b_0, b_1, b_2$$

имеем (здесь $2k - 2 = 4$)

$$c_0 = a_0 b_0,$$

$$c_1 = a_1 b_0 + a_0 b_1,$$

$$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2,$$

$$c_3 = a_2 b_1 + a_1 b_2,$$

$$c_4 = a_2 b_2.$$

Замечание 2. Иногда рассматривают пространство бесконечномерных векторов и векторы (5.1), (5.2) с конечным числом компонент дополняют нулями (в обе стороны), так что (5.1) принимают вид

$$a = (\ldots, 0, 0, a_0, a_1, \ldots, a_{k-1}, 0, 0, \ldots)^T,$$
$$b = (\ldots, 0, 0, b_0, b_1, \ldots, b_{k-1}, 0, 0, \ldots)^T, \tag{5.5}$$

а (5.2) записывается в виде

$$= (\ldots, 0, 0, {}_0, {}_1, \ldots, {}_{2k-2}, 0, 0, \ldots)^T. \tag{5.6}$$

В этом случае нет необходимости доопределять нулями и думать о пределах суммирования при определении свёртки: свёрткой $a \times b$ является вектор c

$$c_j = \sum_j a_j b_{i-j}, \tag{5.8}$$

где суммирование распространяется по всем целым j, а i также пробегает все целые значения (см. также задачу [2]).

Доказать также, что вместо (5.3) - (5.4) можно было бы положить ($i = 0, 1, 2, \ldots, 2k-2$)

$$c_i = \sum_{\max\{0, i-(k-i)\} \le j \le \min\{i, k-1\}} a_j b_{i-j}, \tag{5.3''}$$

В дальнейшем там, где это удобно, мы будем пользоваться применённой здесь нотацией – бесконечными представлениями (5.5), (5.6) (не оговаривая этого специально).

Заметим, что произведением двух многочленов степени $k-1$

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \qquad Q(x) = \sum_{j=0}^{k-1} b_j x^j \tag{5.9}$$

является многочлен степени $2k-2$

$$P(x)Q(x) = \sum_{i=0}^{2k-2} \{ \sum_{j=0}^{i} a_j b_{i-j} \} x^i, \tag{5.10}$$

так что коэффициентами произведения является свёртка (5.8) векторов, предоставляющих коэффициенты многочленов $P(x)$ и $Q(x)$ (здесь мы пользуемся нотацией замечания 2).

6. Применение дискретного пребразования Фурье для вычисления свёртки двух векторов

Пусть два многочлена степени $k-1$ представлены списками своих коэффициентов. Для того,чтобы найти список коэффициентов многочлена, представляющего их произведение, перейдём сначала к спискам их значений в корнях некоторой степени из единицы (с помощью дискретного преобразования Фурье), затем найдём список значений их произведения в этих точках (перемножением соответствующих значений в этих точках), а затем сделаем обратное дискретное преобразование Фурье, найдя тем самым список коэффициентов произведения многочленов. Точное описание этого приёма содержится в теореме 4.

Определение 6. *Покомпонентным произведением $c = a \cdot b$ двух n-мерных векторов a и b,*

$$a = (a_0, \ldots, a_{n-1}), \qquad b = (b_0, \ldots, b_{n-1}) \tag{6.1}$$

называется n-мерный иектор c,

$$c = (c_0, \ldots, c_{n-1}), \tag{6.2}$$

где

$$c_j = a_j b_j, \quad j = 0, 1, \ldots, n-1. \tag{6.3}$$

Покомпонентное произведение a и b обозначается $a \cdot b$.

Теорема 5. *Пусть*

$$a = (a_0, a_1, \ldots, a_{k-1}, 0, \ldots, 0)^T, \tag{6.4}$$

$$b = (b_0, b_1, \ldots, b_{k-1}, 0, \ldots, 0)^T \tag{6.5}$$

– векторы размерности $2k$, пусть $n = 2k$ и

$$\widehat{a} = F(a), \quad \widehat{b} = F(b) \tag{6.6}$$

– их дискретные преобразования Фурье, т.е.

$$\widehat{a} = (\widehat{a}_0, \widehat{a}_1, \ldots, \widehat{a}_{n-1})^T, \tag{6.7}$$

$$\widehat{b} = (\widehat{b}_0, \widehat{b}_1, \ldots, \widehat{b}_{n-1})^T, \tag{6.8}$$

$$\widehat{a}_j = \sum_{i=0}^{n-1} a_i \omega^{ij}, \quad \widehat{b}_j = \sum_{i=0}^{n-1} b_i \omega^{ij}, \tag{6.9}$$

ω – первообразный корень n-ой степени из единицы (в кольце $\mathcal{K}$). Тогда

$$a * b = F^{-1}(\widehat{a} \cdot \widehat{b}). \tag{6.10}$$

Д о к а з а т е л ь с т в о. Ввиду соотношений (6.4),(6.5)

$$\widehat{a}_j = \sum_{i=0}^{k-1} a_i \omega^{ij}, \quad \widehat{b}_j = \sum_{s=0}^{k-1} b_s \omega^{sj}, \tag{6.11}$$

и значит

$$\widehat{a}_j \widehat{b}_j = \sum_{i=0}^{k-1} \sum_{s=0}^{k-1} a_i b_s \omega^{(i+s)j}, \tag{6.12}$$

Введём в рассмотрение свёртку

$$c = a * b, \tag{6.13}$$

По определению свёртки [3]

$$c = (c_p), \qquad c_p = \sum_i a_i b_{p-i}, \tag{6.14}$$

[3]Проверить, что представление (6.14), (6.15) с учётом формул (5.5), (5.6) соответствуют определениям преобразования Фурье и свёртки, данным ранее в пунктах 3 и 5 соответственно.

так, что дискретное пребразование Фурье $\widehat{c}$ вектора c имеет вид

$$\widehat{c} = (\widehat{c}_j), \qquad \widehat{c}_j = \sum_p \sum_i a_i b_{p-i} \omega^{pj}, \tag{6.15}$$

Меняя порядок суммирования в (6.15) и подставляя s вместо $p-i$, найдём ($s = p - i \Leftrightarrow p = s + i$):

$$\widehat{c}_j = \sum_i \sum_s a_i b_s \omega^{(i+s)j}, \tag{6.16}$$

Сравнивая (6.12) и (6.16) находим, что

$$\widehat{a}_j \widehat{b}_j = \widehat{c}_j, \tag{6.17}$$

Так что

$$\widehat{c} = \widehat{a}\widehat{b}. \tag{6.18}$$

Применяя к (6.18) обратное преобразование Фурье и принимая во внимание вторую из формул в (3.15), придём к соотношению (6.10).

Теорема доказана. ∎

Определение 7.*Пусть*

$$a = (a_0, a_1, \ldots, a_{n-1})^T, \quad b = (b_0, b_1, \ldots, b_{n-1})^T. \tag{6.19}$$

– два n-мерных вектора. Положительно обёрнутой свёрткой $a \overset{(+)}{*} b$ векторов a и b называется вектор

$$c = (c_0, c_1, \ldots, c_{n-1})^T$$

такой, что

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} + \sum_{j=i+1}^{n-1} a_j b_{n+i-j}, \quad i = 0, 1, \ldots, n-1. \tag{6.20}$$

Отрицательно обёрнутой свёрткой $a \overset{(-)}{*} b$ векторов a и b называется вектор $d = (d_0, d_1, \ldots, d_{n-1})^T$ такой, что

$$d_i = \sum_{j=0}^{i} a_j b_{i-j} - \sum_{j=i+1}^{n-1} a_j b_{n+i-j}, \quad i = 0, 1, \ldots, n-1. \tag{6.21}$$

Примеры. Пусть $n = 3$ и

$$a = a_0, a_1, a_2, \qquad b = b_0, b_1, b_2.$$

Нетрудно проверить, что положительно обёрнутая свёртка $= {}_0, {}_1, {}_2$ имеет компоненты

$$c_0 = a_0b_0 + a_1b_2 + a_2b_1,$$

$$c_1 = a_0b_1 + a_1b_0 + a_2b_2,$$

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0,$$

а отрицательно обёрнутая свёртка $d = d_0, d_1, d_2$ имеет компоненты

$$d_0 = a_0b_0 - a_1b_2 - a_2b_1,$$

$$d_1 = a_0b_1 + a_1b_0 - a_2b_2,$$

$$d_2 = a_0b_2 + a_1b_1 + a_2b_0.$$

Теорема 6. [4] *Для векторов a и b справедлива формула*

$$a \overset{(+)}{*} b = F^{-1}(\widehat{a}\widehat{b}). \tag{6.22}$$

Теорема 7. [5] *Пусть $\psi^2 = \omega$ и пусть $\tilde{\Psi}$ – операция, переводящая вектор $a = (a_0, a_1, \ldots, a_{n-1})^T$ в вектор*

$$\tilde{\Psi}a = (a_0, \psi a_1, \ldots, \psi^{n-1}a_{n-1})^T. \tag{6.23}$$

Тогда

$$\tilde{\Psi}(a \overset{(-)}{*} b) = F^{-1}(\widehat{\tilde{\psi}a} \cdot \widehat{\tilde{\psi}b}). \tag{6.24}$$

7. Об алгоритме быстрого преобразования Фурье (основная идея)

Дискретное преобразование Фурье (и обратное к нему) определяется как умножение специальной полностью заполненной квадратной матрицы порядка n на n-мерный вектор (см. п. 3). Ясно, что при этом достаточно n^2 умножений и $n(n-1)$ сложений. Считая, что арифметические операции на ЭВМ выполняются за один

[4] Доказательство теоремы 6 провести самостоятельно

[5] Доказательство теоремы 7 провести самостоятельно

шаг и время их выполнения не зависит от операндов, общее время, необходимое для выполнения дискретного преобразования Фурье, имеет порядок $O(n^2)$.

Однако, если n – натуральная степень числа 2, то известны алгоритмы, работающие с большей скоростью, так что время их выполнения $O(n \lg n)$. Рассмотрим подобный алгоритм лишь для прямого дискретного преобразования Фурье; алгоритм для обратного ему преобразования аналогичен. Подобные алгоритмы вычисления дискретного преобразования Фурье носят названия алгоритмов быстрого пребразования Фурье (БПФ). Основная идея БПФ состоит в использовании подобия отдельных частичных сумм. Впервые он предложен Рунге и Кенига в 1924 году. Подробное описание алгоритма дано в работе Кули и Тьюки в 1965 году.

В дальнейшем будем считать

$$n = 2^k. \tag{7.1}$$

Нам известно, что вычисление преобразования Фурье $\widehat{a} = A \cdot a$ эквивалентно вычислению многочлена

$$P(x) = \sum_{i=0}^{n-1} a_i x^i \tag{7.2}$$

в точках $\omega^0, \omega^1, \ldots, \omega^{n-1}$ (см. п.4, формулы (4.4), (4.5), (4.7)). Но вычисление многочлена в точке c согласно теореме Безу (см. п. 2) эквивалентно вычислению остатка этого многочленм при делении на $x-c$. Следовательно, вычисление преобразования Фурье $\widehat{a} = A \cdot a$ сводится к вычислению остатков от деления $P(x)$ на биномы

$$x - \omega^j, \qquad j = 0, 1, \ldots, n-1. \tag{7.3}$$

Последовательное деление (7.2) на биномы (7.3) согласно схеме Хорнера (см. (2.5) и замечание 1 в п. 2) даст, очевидно, $O(n^2)$ арифметических действий (или, как говорят, процесс сложности $O(n^2)$).

Для построения более быстрого алгоритма биномы (7.3) перемножают попарно, затем перемножают попарно $n/2$ получившихся многочленов и т.д., пока останутся два полинома $q_1(x)$ и $q_2(x)$ степеней $n/2$ каждый.

Теперь разделим $P(x)$ на $q_1(x)$ и $q_2(x)$ по-очереди; получаемые при этом остатки обозначим $r_1(x)$ и $r_2(x)$ соответственно (степени остатков, очевидно, не более $n/2 - 1$).

Нетрудно видеть, что для каждого корня ω^j, для которого $x-\omega^j$ входит в $q_1(x)$, вычисление остатка $P(x)$ при делении на $x-\omega^j$ эквивалентно вычислению остатка $r_1(x)$ при делении на тот же бином $x-\omega^j$. Рекурсивное применение этого соображения (как видно далее) приводит к значительной экономии.

Заметим также, что при перемножении пар одночленов вида $x-\omega^j$, а также при перемножении пар полученных произведений и т.д. на каждом шаге можно иметь дело лишь с одночленами вида x^j-c при подходящем упорядочивании исходных точек $\omega^0, \omega^1, \ldots, \omega^{n-1}$.

8. Более точное описание алгоритма БПФ

Пусть

$$0, 1, \cdots, n-1 \tag{8.1}$$

– некоторая перестановка элементов $\omega^0, \omega^1, \ldots, \omega^{n-1}$, которая будет указана впоследствии.

Определим многочлены $q_{l,m}$ (степени 2^m) формулой

$$q_{l,m} = \prod_{j=l}^{l+2^m-1} (x - c_j) \tag{8.2}$$

для индексов l и m, удовлетворяющих условиям

$$0 \le m \le k, \quad 0 \le l \le 2^k - 1, \quad l = \sigma \cdot 2^m, \quad \sigma = 0, 1, \ldots \tag{8.3}$$

$$l + 2^m - 1 \le 2^k - 1. \tag{8.4}$$

Тем самым [6]

$$q_{0,k}(x) = (x - c_0)(x - c_1)\ldots(x - c_{n-1}), \tag{8.5}$$

$$q_{l,0}(x) = (x - c_l). \tag{8.6}$$

Ввиду определения (8.2)

$$q_{l,m}(x) = q_{l,m-1}(x) q_{l+2^{m-1},m-1}(x). \tag{8.7}$$

Нетрудно видеть, что [7] существует ровно 2^{k-m} различных многочленов $q_{l,m}$ со вторым индексом, равным числу m. При этом каждый бином $x - c_l$ делит ровно один из этих многочленов.[8]

[6] Проверить формулы (8.4), (8.5), (8.6).

[7] Доказать существование указанного числа многочленов $q_{l,m}$

[8] Доказать последнее утверждение.

Многочлены $q_{l,m}$ удобно изобразить в виде дерева.

Окончательная цель – вычислить остатки от деления многочлена $P(x)$ на биномы $q_{l,0} = x - c_l$. Для этого вычислить остатки от деления $P(x)$ на $q_{l,m}(x)$ для каждого $q_{l,m}$, начиная с $m = k$ и кончая $m = 0$. При $m = k$ приходится делить многочлен $P(x)$ степени $n-1$ на многочлен $q_{0,k}(x)$ степени n (см. формулы (7.2) и (8.5) соответственно). Очевидно, остатком такого деления явится многочлен $r_{0,k} = P(x)$. Далее через $r_{l,m}(x)$ обозначим остаток от деления многочлена $P(x)$ на многочлен $q_{l,m}(x)$ (степени 2^m). Очевидно, степень многочлена $r_{l,m}$ не превосходит $2^m - 1$.

Перепишем представления (8.7) в краткой форме

$$q_{l,m}(x) = q'(x) \cdot q''(x), \tag{8.8}$$

где

$$q'(x) = q_{l,m-1}(x), \tag{8.9}$$

$$q''(x) = q_{l+2^{m-1},m-1}(x). \tag{8.10}$$

Лемма 2. *Остаток от деления $P(x)$ на $q'(x)$ равен остатку от деления $r_{l,m}(x)$ на $q'(x)$, а остаток от деления $P(x)$ на $q''(x)$ равен остатку от деления $r_{l,m}(x)$ на $q''(x)$.*

Доказательство. Очевидно (см. формулу (8.9)), что

$$p(x) = h'(x)q'(x) + r_{l,m-1}(x), \tag{8.11}$$

$$p(x) = \tilde{h}(x)q_{l,m}(x) + r_{l,m}(x), \tag{8.12}$$

откуда $h'(x)q'(x) + r_{l,m-1}(x) = \tilde{h}(x)q_{l,m}(x) + r_{l,m}(x)$.

Ввиду представления (8.8) $q_{l,m}(x)$ делится на $q'(x)$, а значит $r_{l,m-1}(x)$ совпадает с остатком от деления $r_{l,m}(x)$ на $q'(x)$. Первая часть леммы доказана.

Аналогичным образом доказывается вторая её часть; при этом вместо соотношения (8.11) используем соотношение

$$p(x) = h''(x)q''(x) + r_{l+2^{m-1},m-1}(x). \tag{8.13}$$

Лемма доказана. ∎

Следствие. *Остатки от деления $P(x)$ на $q'(x)$ и на $q''(x)$ можно получить делением на q' и q'' многочлена $r_{l,m}$ степени $2^m - 1$, а не исходного многочлена степени $2^k - 1$. Можно ввести*

такое упорядочение чисел $\omega^j, \quad j = 0, 1, \ldots, n-1$, *что каждый многочлен* $q_{l,m}$ *имеет вид*

$$x^{2^m} - \omega^s$$

при некотором неотрицательном целом s.

Доказательство этого факта следует из леммы 2.

Определение 8. *Пусть* j – *целое число,* $0 \le j < 2^k$, *а* $[d_{k-1} \quad d_{k-2} \ldots d_0]$ – *его двоичное представление,*

$$j = \sum_{i=0}^{k-1} d_i 2^i, \quad d_i \in \{0, 1\}.$$

Инверсией числа j *будем называть целое число* $\overline{j}$ *с двоичным представлением* $[d_0 \quad d_1 \ldots d_{k-1}]$,

$$\overline{j} = \sum_{i=0}^{k-1} d_i 2^{k-1-i}.$$

Операцию перехода от j к $\overline{j}$ обозначают rev_k (от английского reverse order),

$$\mathrm{rev}_k : j \to \overline{j},$$

т.е. $\overline{j} = \mathrm{rev}_k(j)$.

Свойство инверсии. *Для* $0 \le j < 2^{k-1}$ *справедлива формула*

$$\mathrm{rev}_k(2j) = \mathrm{rev}_k(j)/2. \tag{8.14}$$

Доказательство. Ввиду условия $0 \le j < 2^{k-1}$ имеем $j = \sum_{i=0}^{k-2} d_i 2^i, \quad d_i \in \{0, 1\}$, и поэтому

$$\mathrm{rev}_k(j) = \sum_{i=0}^{k-2} d_i 2^{k-1-i}. \tag{8.15}$$

$$2^j = \sum_{i=1}^{k-1} d_{i-1} 2^i.$$

Из последнего соотношения найдём (подстановкой $i' = i - 1$)

$$\mathrm{rev}_k(2j) = \sum_{i=1}^{k-1} d_{i-1} 2^{k-1-i} = \sum_{i'=0}^{k-2} d_{i'} 2^{k-2-i'}. \tag{8.16}$$

Теперь из (8.15) и (8.16) вытекает свойство (8.14). ∎

Лемма 3. *Положим*

$$c_j = \omega^{\mathrm{rev}_k(j)}. \tag{8.17}$$

Тогда многочлены (8.2) могут быть представлены в виде

$$q_{l,m} = x^{2^m} \omega^{\mathrm{rev}_k(l/2^m)} \tag{8.18}$$

Доказательство. Воспользуемся индукцией по m. Случай $m = 0$ тривиален, ибо согласно формулам (8.6) и (8.14) $q_{l,0}(x) = x - c_l = x - \omega^{\mathrm{rev}_k(l)} = x^{2^0} - \omega^{\mathrm{rev}_k(l/2^0)}$, что совпадает с (8.18) при $m = 0$.

Для проведения шага индукции возьмём $m > 0$. Согласно предположению индукции

$$q_{l,m-1}(x) = x^{2^{m-1}} - \omega^{\mathrm{rev}_k(l/2^{m-1})}$$

$$q_{l+2^{m-1},m-1}(x) = x^{2^{m-1}} - \omega^{\mathrm{rev}_k(l/2^{m-1}+1)}$$

из формулы (8.7) имеем

$$q_{l,m}(x) = q_{l,m-1}(x) q_{l+2^{m-1},m-1}(x) =$$

$$= (x^{2^{m-1}} - \omega^{\mathrm{rev}_k(l/2^{m-1})})(x^{2^{m-1}} - \omega^{\mathrm{rev}_k(l/2^{m-1}+1)}). \tag{8.19}$$

Заметим, что $l/2^{m-1}$ – чётное число между 0 и 2^{k-1}, ибо в соответствии с (8.3), (8.4)

$$l = \sigma \cdot 2^m, \quad \sigma = 0, 1, \ldots, 2^{k-m} - 1,$$

и потому

$$\omega^{\mathrm{rev}_k(l/2^{m-1}+1)} = \omega^{2^{k-1}+\mathrm{rev}_k(l/2^{m-1})} =$$

$$= -\omega^{\mathrm{rev}_k(l/2^{m-1})}; \tag{8.20}$$

в последнем равенстве использовано очевидное соотношение

$$\omega^{2^{k-1}} = \omega^{n/2} = -1.$$

Из (8.19), (8.20) и (8.14) следуют равенства

$$q_{l,m}(x) = x^{2^{m-1}\cdot 2} - \omega^{2\mathrm{rev}_k(l/2^{m-1})} = x^{2^m \cdot 2} - \omega^{\mathrm{rev}_k(l/2^m)}.$$

Лемма доказана.

Пример. При $n = 8$ имеем $k = 3$. Составим список $c_0, c_1, \ldots, c_7$ следуя правилу (8.17). Для этого найдём $\overline{j} = rev_3(j)$ для $j = 0, 1, 2, 3, 4, 5, 6, 7$. Нетрудно видеть, что

$$\mathrm{rev}_3(0) = \mathrm{rev}_3(000) = 000 = 0,$$

$$\mathrm{rev}_3(1) = \mathrm{rev}_3(001) = 100 = 4,$$

$$\mathrm{rev}_3(2) = \mathrm{rev}_3(010) = 010 = 2,$$

$$\mathrm{rev}_3(3) = \mathrm{rev}_3(011) = 110 = 6$$

и т.д., так что приходим к списку

$$\omega^0, \quad \omega^4, \quad \omega^2, \quad \omega^6, \quad \omega^1, \quad \omega^5, \quad \omega^3, \quad \omega^7.$$

Соответствующие многочлены $q_{l,m}$ имеют вид (8.18). Их удобно изображать в виде дерева.

Для БПФ в этом случае последовательно вычисляются остатки:

при $m = 2$ – остатки $r_{0,2}, r_{4,2}$ от деления $p(x)$ на $x^4 - \omega^0$ и на $x^4 - \omega^4$ (степень 3),

при $m = 1$ остатки $r_{0,1}, r_{2,1}$ от деления $r_{0,2}(x)$ на $x^2 - \omega^0$ и на $x^2 - \omega^4$ (степень 1),

при $m = 1$ остатки $r_{4,1}, r_{6,1}$ от деления $r_{4,2}(x)$ на $x^2 - \omega^2$ и на $x^2 - \omega^6$ (степень 1),

при $m = 0$ остатки $r_{0,0}, r_{1,0}$ от деления $r_{0,1}(x)$ на $x - \omega^0$ и на $x - \omega^4$ (степень 0),

при $m = 0$ остатки $r_{2,0}, r_{3,0}$ от деления $r_{2,1}(x)$ на $x - \omega^2$ и на $x - \omega^6$ (степень 0) и т.д.

Заметим, что ввиду леммы 1 те же остатки получились бы, если бы каждый раз делился бы многочлен $p(x)$, но делить остатки экономнее, ибо их степень меньше (здесь в примере степени остатков 3, 1 и 0, а в общем случае степень $r_{l,m}$ равна $2^m - 1$).

Заметим также, что в этой схеме остаток $r_{l,m}$ (имеющий, как отмечено выше, степень $2 * 2^{m-1} - 1$) приходится делить на бином вида $x^{2^{m-1}} - c$. Оказывается, многочлен степени $2t - 1$ достаточно просто разделить на бином $x^t - c$ (в интересующем нас случае $t = 2^{m-1}$).

Лемма 4. *Если многочлен $Q(x)$ имеет вид*

$$Q(x) = \sum_{j=0}^{2t-1} a_j x^j,$$

то остаток $R(x)$ от его деления можно на бином $x^t - c$ может быть записан в форме

$$R(x) = \sum_{j=0}^{t-1} (a_j + c a_{j+t}) x^j. \tag{8.21}$$

Д о к а з а т е л ь с т в о ; вытекает из легко проверяемого тождества (для проверки достаточно раскрыть скобки)

$$\sum_{j=0}^{2t-1} a_j x^j = (\sum_{j=0}^{t-1} a_{j+t} x^j)(x^t - c) + \sum_{j=0}^{t-1} (a_j + c a_{j+t}) x^j.$$

Лемма доказана. ∎

Следствие. *Вычисление остатка от деления многочлена степени $2t-1$ на многочлен степени t вида $x^t - c$ требует $O(t)$ арифметических действий (t умножений и t сложений).*

Далее здесь дается описание алгоритма на псевдоалгоритмическом языке, который представлется достаточно ясным для понимания; поэтому заниматься его описанием здесь не будем: читатель достаточно подготовлен, чтобы дать это описание самостоятельно.

ОПИСАНИЕ АЛГОРИТМА БПФ НА ПСЕВДОАЛГОРИТМИЧЕСКОМ ЯЗЫКЕ

. Вектор $a = (a_0, a_1, \ldots, a_{n-1})$, $n = 2^k$, k – целое

. Вектор $F(a) = (b_0, b_1, \ldots, b_{n-1})$, где $b_i = \sum_{j=0}^{n-1} a_j \omega^{ij}$, $0 \le i < n$

```
begin
1.    r_0k = Σ_{j=0}^{n-1} a_j x^j;
                    { ; }
                    { }
                    { }
```

2. for m:=k-1 step -1 until 0 do

3. for l:= 0 step 2^{m+1} until n-1 do
begin

4. $r_{l,m+1}(x) := \sum_{j=l}^{l+2^{m+1}-1} a_j x^j$;
{ ; }
{ }
{ }
{a_j-}
{; (.(8.19)}

5. $s := rev_k(l/2^m)$;
{(.(8.18))}

6. $r_{l,m}(x) := \sum_{j=l}^{l+2^m-1}(a_j + \omega^s a_{j+2^m})x^j$;

{(.(8.21))}

7. $r_{l+2^m,m}(x) :=$
$\sum_{j=l}^{l+2^m-1}(a_j + \omega^{s+n/2} a_{j+2^m})x^j$;

end;

8. for l:= 0 step 1 until n-1 do
$b_{rev_k(l)} := r_{l,0}$;

{(.(8.17))}

end

Алгоритм БПФ

Пример. Пусть $n = 2^k, \quad k = 3$ (так что $n = 8$). Развернем алгоритм БПФ в этом случае. При $k = 3 \quad (n = 8)$ он приобретает следующий вид.

1. $r_{0,3} := \sum_{j=0}^{7} a_j x^j$;

2. `for m:=2 step -1 until 0 do`

3. `for l:=0 step` 2^{m+1} `until 7 do`

`begin`

4. $r_{l,m+1}(x) := \sum_{j=0}^{2^{m+1}-1} a_j x^j$;

5. $s := rev_3(l/2^m)$;

6. $r_{l,m}(x) := \sum_{j=0}^{2^m-1}(a_j + \omega^{s+n/2} a_{j+2^m})x^j$;

7. $r_{l+2^m,m}(x) := \sum_{j=0}^{2^m-1}(a_j + \omega^{s+n/2} a_{j+2^m})x^j$;

`end;`

8. `for l:=0 step 1 until 7 do` $b_{rev_3(l)} := r_{l,0}$;

Полное разворачивание алгоритма приводит к следующей последовательности строк (обозначения понятны без пояснений).

1) 1. $r_{0,3} := \sum_{j=0}^{7} a_j x^j$;
2) 2. m:=2;
3) 3. l:=0;
4) 4. дано $r_{0,3} := \sum_{j=0}^{7} a_j x^j$;
5) 5. $s := rev_3(0/2^m) = 0$;
6) 6. $r_{0,2}(x) := \sum_{j=0}^{2^2-1}(a_j + \omega^0 a_{j+2^2})x^j =$
$= (a_0 + \omega^0 a_4) + (a_1 + \omega^0 a_{1+2^2})x +$
$+(a_2 + \omega^0 a_{2+2^2})x^2 + (a_3 + \omega^0 a_{3+2^2})x^3 =$
$= (a_0 + \omega^0 a_4) + (a_1 + \omega^0 a_5)x +$
$+(a_2 + \omega^0 a_6)x^2 + (a_3 + \omega^0 a_7)x^3$;
7) 7. $r_{2^2,2}(x) := \sum_{j=0}^{2^2-1}(a_j + \omega^{0+8/2} a_{j+2^2})x^j =$
$= (a_0 + \omega^4 a_4) + (a_1 + \omega^4 a_5)x +$
$+(a_2 + \omega^4 a_6)x^2 + (a_3 + \omega^4 a_7)x^3$;
8) 3. l:=$2^{m+1} = 2^3 = 8 > 7$ {fail}
9) 2. m:=1;
10) 3. l:=0;
11) 4. дано $r_{0,2} := \sum_{j=0}^{2^2-1} a_j x^j$;
12) 5. $s := rev_3(0/2^1) = 0$;
13) 6. $r_{0,1}(x) := \sum_{j=0}^{2^1-1}(a_j + \omega^0 a_{j+2^1})x^j =$
$= (a_0 + \omega^0 a_2) + (a_1 + \omega^0 a_3)x$;
14) 7. $r_{0+2^1,1}(x) := \sum_{j=0}^{2^1-1}(a_j + \omega^{0+8/2} a_{j+2^1})x^j =$
$= (a_0 + \omega^4 a_2) + (a_1 + \omega^4 a_3)x$;
15) 3. l:=2^2; $(2^2 < 7)$
16) 4. дано $r_{2^2,2} := \sum_{j=0}^{2^2-1} a_j x^j$;
17) 5. $s := rev_3(2^2/2^1) = rev_3(010) = 2$;
18) 6. $r_{2^2,1}(x) := \sum_{j=0}^{2^1-1}(a_j + \omega^2 a_{j+2^1})x^j =$
$= (a_0 + \omega^2 a_2) + (a_1 + \omega^2 a_3)x$;
19) 7. $r_{2^2+2^1,1}(x) := \sum_{j=0}^{2^1-1}(a_j +$
$+\omega^{2+8/2} a_{j+2^1})x^j = (a_0 + \omega^6 a_2) + (a_1 + \omega^6 a_3)x$;
20) 3. l:=$2^2 + 2^2 > 7$ {fail}
21) 2. m:=0;
22) 3. l:=0; (≤ 7)
23) 4. дано $r_{0,1}(x) := \sum_{j=0}^{2^1-1} a_j x^j$;
24) 5. $s := rev_3(0/2^0) = 0$;

25) 6. $r_{0,0}(x) := \sum_{j=0}^{2^0-1}(a_j + \omega^0 a_{j+2^0})x^j =$
$= (a_0 + \omega^0 a_1);$

26) 7. $r_{0+2^0,0}(x) :=$
$\sum_{j=0}^{2^0-1}(a_j + \omega^{0+8/2} a_{j+2^0})x^j =$
$= (a_0 + \omega^4 a_1);$

27) 3. l:=$2^{0+1} = 2;$ (≤ 7)

28) 4. дано $r_{2,0+1}(x) := \sum_{j=0}^{2^1-1} a_j x^j;$

29) 5. $s := rev_3(2/2^0) = 2;$

30) 6. $r_{2,0}(x) := \sum_{j=0}^{2^0-1}(a_j + \omega^0 a_{j+2^0})x^j =$
$= (a_0 + \omega^2 a_1);$

31) 7. $r_{2+2^0,0}(x) :=$
$\sum_{j=0}^{2^0-1}(a_j + \omega^{2+8/2} a_{j+2^0})x^j =$
$= (a_0 + \omega^6 a_1);$

32) 3. l:=$2^2 = 4;$ (≤ 7)

33) 4. дано $r_{4,1}(x) := \sum_{j=0}^{2^1-1} a_j x^j;$

34) 5. $s := rev_3(4/2^0) = rev_3(100) = 001 = 1;$

35) 6. $r_{4,0}(x) := \sum_{j=0}^{2^0-1}(a_j + \omega^1 a_{j+2^0})x^j =$
$= (a_0 + \omega^1 a_1);$

36) 7. $r_{4+2^0,0}(x) :=$
$\sum_{j=0}^{2^0-1}(a_j + \omega^{1+8/2} a_{j+2^0})x^j =$
$= (a_0 + \omega^5 a_1);$

37) 3. l:=6; (≤ 7)

38) 4. дано $r_{6,1}(x) := \sum_{j=0}^{2^1-1} a_j x^j;$

39) 5. $s := rev_3(6/2^0) = rev_3(110) = 011 = 3;$

40) 6. $r_{6,0}(x) := \sum_{j=0}^{2^0-1}(a_j + \omega^3 a_{j+2^0})x^j =$
$= (a_0 + \omega^3 a_1);$

41) 7. $r_{6+2^0,0}(x) :=$
$\sum_{j=0}^{2^0-1}(a_j + \omega^{3+8/2} a_{j+2^0})x^j =$
$= (a_0 + \omega^7 a_1);$

42) 3. l:=8; (> 7) {fail}

Конец цикла по m

43) 8. цикл по l=0,2,...,7 делать$b_{rev_3(l)} := r_{l,0};$

КОНЕЦ РАБОТЫ ПРОГРАММЫ

Замечание 3. Представление алгоритма, данное выше, конечно не является единственным представлением. Нетрудно видеть, что

поскольку проводится лишь работа с коэффициентами многочленов, то присутствие x не обязательно (представление с помощью многочленов служит для наглядности). [9]

Замечание 4. Из записи алгоритма видно, что можно "почти" ограничиться памятью, необходимой для записи исходных данных (вектора коэффициентов исходного многочлена). [10]

Теорема 8. *Алгоритм быстрого преобразования Фурье содержит $O(n \log n)$ арифметических операций.*

Доказательство. Обратимся к алгоритму БПФ

Прежде всего заметим, что вычисление $rev_k(j)$ требует не более k делений на 2. Если рассмотреть вычисление $rev_k(j)$ для всех $j, \quad 0 \le j < n-1, \quad n = 2^k$, то число D делений оценивается выражением $kn = n \log_2 n$, так что

$$D \le n \log_2 n. \tag{8.22}$$

Таблицу $rev_k(j)$ следует получить заранее. В этом случае можно считать, что строки 5 и 8 алгоритма БПФ не содержат арифметических операций.

Заранее получим также таблицу степеней

$$\omega^0, \omega^1, \ldots, \omega^{n-1};$$

при этом потребуется число умножений M_1, которое очевидно оценивается сверху числом n,

$$M_1 \le n. \tag{8.23}$$

Далее, среди остальных строк арифметические операции содержат только строки 6 и 7. Подсчитаем лишь число умножений, которые порождаются в алгоритме этими строками (число сложений подсчитывается аналогично). В строках 6 и 7 по 2^m умножений в каждой, так что общее их число 2^{m+1}. Строки 6 и 7 во внутреннем цикле повторяются $n/2^{m+1}$ раз, а внешний цикл повторяет внутренний k раз. Таким образом, число M_2 умножений, порождаемых этими строками, равно $2^{m+1}kn/2^{m+1} = n \log_2 n$, т.е.

$$M_2 = n \log_2 n. \tag{8.24}$$

[9] Записать алгоритм в "упрощённой" форме, исключив из записи многочлены

[10] Записать алгоритм, стремясь сэкономить объём используемой памяти (минимизируя число используе- мых массивов)

Ввиду соотношений (8.22) – (8.24) общее число мультипликативных операций $M = D + M_1 + M_2$ имеет оценку

$$M \leq n(2\log_2 n + 1). \tag{8.25}$$

Число аддитивных операций оценивается аналогично.[11]

Замечание 5. Оценка (8.25) может быть уточнена. [12]

Замечание 6. Логические операции и пересылки обычно делаются быстрее арифметических действий на ЭВМ, однако, большое их число может повлиять на производительность алгоритма. В случае БПФ это влияние несущественно.[13]

Замечание 7. Весьма важным является объём необходимой памяти для реализации алгоритма. Как видно БПФ позволяет ограничиться небольшим увеличением памяти, необходимой для исходных данных. [14]

9. Быстрое преобразование Фурье с использованием битовых операций

В ряде случаев при применении преобразования Фурье нужен точный результат. Если же в качестве кольца $\mathcal{K}$ брать кольцо комплексных чисел, то при использовании вычислений на ЭВМ это может привести к ошибкам округления, связанным со спецификой разрядной сетки. Для точных вычислений удобно использовать конечное поле (например, поле вычетов по модулю m, где m достаточно велико).

В дальнейшем будет показано, что если n и ω – степени числа 2, то можно вычислять свёртки по модулю $\omega^{n/2} + 1$ с помощью преобразования Фурье, покомпонентного умножения и обратного преобразования.

Итак, пусть $\mathcal{K} = \{S, +, \cdot, 0, 1\}$ – коммутативное кольцо,

$$n = 2^k, \quad k \geq 1. \tag{9.1}$$

Лемма 5. *Для всякого* $a \in S$

$$\sum_{i=0}^{2^k-1} a^i = \prod_{i=0}^{k-1} (1 + a^{2^i}). \tag{9.2}$$

[11] Подсчитать число аддитивных операций в алгоритме БПФ.

[12] Уточнить оценку (8.25).

[13] Оценить число логических операций и число пересылок в алгоритме БПФ.

[14] Дать оценку необходимой памяти для алгоритма БПФ.

Д о к а з а т е л ь с т в о. Проведём доказательство индукцией по k. При $k = 1$ (9.2) превращается в очевидное равенство

$$\sum_{i=0}^{2^1-1} a^i = \prod_{i=0}^{0}(1 + a^{2^i}).$$

При $k > 1$ предположим, что утверждение (9.2) Справедливо при замене k на $k - 1$, т.е. при любом $b \in S$

$$\sum_{i=0}^{2^{k-1}-1} b^i = \prod_{i=0}^{k-2}(1 + b^{2^i}) \tag{9.3}$$

и докажем, что справедливо соотношение (9.2). Действительно, для правой части (9.2) имеем

$$\sum_{i=0}^{2^k-1} a^i = a^0 + a^2 + \ldots + a^{2^k-2} + a(a^0 + a^2 + \ldots + a^{2^k-2}),$$

откуда

$$\sum_{i=0}^{2^k-1} a^i = (1 + a) \sum_{i=0}^{2^{k-1}-1} (a^2)^i. \tag{9.4}$$

Заменяя в (9.3) b на a^2 получим

$$\sum_{i=0}^{2^k-1} (a^2)^i = \prod_{j=0}^{k-2}(1 + a^{2^{j+1}}). \tag{9.5}$$

Из (9.4) и (9.5) найдём ($j' = j + 1$)

$$\sum_{i=0}^{2^k-1} a^i = (1 + a) \prod_{j'=1}^{k-1}(1 + a^{2j'}) = \prod_{j'=0}^{k-1}(1 + a^{2^{j'}}). \tag{9.6}$$

Итак, установлено соотношение (9.2).

Лемма доказана. ■

Лемма 6. *Пусть*

$$m = \omega^{n/2} + 1, \tag{9.7}$$

где

$$\omega \in S, \quad \omega \neq 0, \quad n = 2^k. \tag{9.8}$$

Тогда для любого p, $\quad 1 \le p < n$, *справедливо соотношение*

$$\sum_{i=0}^{n-1} \omega^{ip} \equiv 0 \pmod{\mathrm{m}}. \tag{9.9}$$

Д о к а з а т е л ь с т в о. Ввиду формулы (9.2), применённой к $a = \omega^p$, достаточно показать, что

$$1 + \omega^{2^j p} \equiv 0 \pmod{\mathrm{m}} \tag{9.10}$$

при некотором j, $\quad 0 \le j < k$.

Очевидно, что p можно представить в виде

$$p = 2^s p', \tag{9.11}$$

где p' – нечётно, а

$$0 \le s < k. \tag{9.12}$$

Возьмём j так, чтобы

$$s + j = k - 1. \tag{9.13}$$

Тогда благодаря (9.11) и (9.13) получим

$$1 + \omega^{2^j p} = 1 + \omega^{2^{j+s} p'} = 1 + \omega^{2^{k-1} p'}. \tag{9.14}$$

Ввиду (9.7) и (9.8)

$$\omega^{2^{k-1}} = \omega^{n/2} = m - 1,$$

так что из (9.14) найдём

$$1 + \omega^{2^j p} = 1 + (m-1)^{p'}. \tag{9.15}$$

Очевидно, что

$$m - 1 = -1 \pmod{\mathrm{m}} \tag{9.16}$$

и потому из (9.15) (ввиду нечётности $p\prime$) выводим

$$1 + (m-1)^{p'} \equiv 1 + (-1)^{p'} = 0 \pmod{\mathrm{m}}. \tag{9.17}$$

Подставляя (9.17) в (9.15) получим (9.10), откуда найдём (9.9). Лемма доказана. ∎

Теорема 9. *Пусть n и ω – положительные степени числа 2, и $m = \omega^{n/2} + 1$. В кольце R_m вычетов по модулю m элемент n имеет обратный (по модулю m) и ω – примитивный корень n-степени из 1.*

Д о к а з а т е л ь с т в о. Поскольку $n = 2^k$, а m – нечётно, то m и n взаимно просты. Поэтому n имеет обратный элемент в R_m. [15] Далее из (9.16) найдём

$$\omega^n = \omega^{n/2}\omega^{n/2} \equiv (-1)(-1) = 1. \tag{9.18}$$

Докажем, что

$$\omega \not\equiv 1 \pmod{\text{m}}. \tag{9.19}$$

Предполагая противное, получим

$$\omega \equiv 1 \pmod{\text{m}} \Longleftrightarrow \omega - 1 = d(\omega^{m/2} + 1), \tag{9.20}$$

где d – целое. Однако, по условию теоремы $\omega - 1 \neq 0$ и поэтому $d \neq 0$; теперь видно, что в равенстве (9.20) слева стоит число заведомо меньше, чем справа, так что (9.20) невозможно. Соотношение (9.19) установлено.

Используя лемму 6 из (9.9), (9.18) и (9.19) видим, что ω – примитивный корень n-степени из 1 в R_m.

Теорема доказана. ∎

Для определения количества битовых операций в свёртке важно следующее утверждение.

Лемма 7. *Пусть $m = \omega^p + 1$ и $A = \sum_{i=0}^{l-1} a_i \omega^{ip}$, где $0 \leq a_i < \omega^p$ для каждого $i = 0, 1, \ldots, l-1$. Тогда*

$$A \equiv \sum_{i=0}^{l-1} a_i (-1)^i \pmod{\text{m}}. \tag{9.21}$$

Д о к а з а т е л ь с т в о. Составим разность между левой и правой частями соотношения (9.21); имеем

$$A - \sum_{i=0}^{l-1} a_i (-1)^i = \sum_{i=0}^{l-1} a_i ((\omega^p)^i - (-1)^i). \tag{9.22}$$

[15] Обосновать это утверждение, используя теоретико-числовые соображения.

Поскольку при $i > 0$ разность $(\omega^p)^i - (-1)^i$ делится на $(\omega^p - (-1) = \omega^p + 1$, а $m = \omega^p + 1$, то (9.22) делится на m без остатка. Это эквивалентно сравнению (9.21).

Лемма доказана. ∎

Пример (иллюстрация использования леммы 7). Пусть требуется найти вычет числа $A = [101100]$ по модулю $m = 2^2 + 1$. Здесь $n = 3, \quad \omega = 2, \quad p = 2$. Очевидно, в этом случае p – число в двоичном представлении коэффициентов a_i (иногда называемых "блоками"). Итак $a_0 = [00], a_1 = [11], a_2 = [10], A = [10] \cdot (2^2)^2 + [11] \cdot (2^2)^1 + [0] \cdot (2^2)^0$. Согласно (9.21) имеем

$$A \equiv a_0 - a_1 + a_2 = -1 \pmod 5$$

так что вычетом может служить 4,

$$A \equiv [000100] \pmod 5.$$

Теорема 10. *Пусть n и ω – степени числа 2, $m = \omega^{n/2} + 1, \quad a = (a_0, a_1, \ldots, a_{n-1})$ – вектор с целочисленными компонентами, где $0 \le a_i < m, \quad i = 0, 1, \ldots, n-1$. Тогда дискретное преобразование Фурье в R_m для вектора a и обратное к нему можно вычислить за $O(n^2 \log n)$ битовых операций.*

Доказательство. Доказательство этой теоремы аналогично доказательству теоремы 8. Используя алгоритм БПФ ,видим, что дополнительно к подсчётам, проводимым в теореме 8 нужно определить число битовых операций, необходимых при сложении чисел по модулю m и при умножении их на степень числа ω. Согласно лемме 8 (см. следствие) сложение чисел по модулю ω требует $O(n)$ битовых операций, а умножение на степень ω эквивалентно сдвигу разрядов влево с последующим вычислением вычета, что (согласно упомянутому следствию) опять - таки требует $O(n)$ битовых операций. Умножая число арифметических действий $O(n \log n)$ (см. теорему 8) на число битовых операций $O(n)$, приходим к нужному результату.

Теорема доказана. ∎

Следствие. *Пусть для вычисления произведения двух k – разрядных двоичных чисел требуется $O(M(k))$ битовых операций. Пусть a и b – n-мерные векторы с целочисленными компонентами между 0 и ω^n, где n и ω – степени числа 2. Тогда свёртки*

$a * b$, $a \overset{(+)}{*} b$ и $a \overset{(-)}{*} b$ векторов a и b по модулю $m = \omega^n + 1$ можно вычислить с помощью

$$O(n^2 \log n + nM(n)) \tag{9.23}$$

битовых операций.

Доказательство. Доказательство вытекает из определения свёрток и результата теоремы 10. Первое слагаемое в формуле (9.23) представляет собой число битовых операций, необходимых для вычисления прямого и обратного преобразования Фурье, а второе слагаемое – число битовых операций, необходимых для вычисления покомпонентного произведения соответствующих векторов.

Следствие доказано. ∎

Замечание 8. Поскольку произведение двух многочленов сводится к свёртке векторов их коэффициентов, то оценка (9.23) справедлива для числа битовых операций, необходимых для вычисления упомянутого произведения.

Замечание 9. При умножении целых чисел A и B можно применить алгоритм БПФ, если рассматривать целые числа A и B представленными с помощью позиционной системы счисления по основанию ω^p,

$$A = \sum_{i=0}^{l-1} a_i \omega^{ip}, \quad B = \sum_{i=0}^{l-1} b_i \omega^{ip}. \tag{9.24}$$

Действительно, задача отыскания произведения AB фактически состоит в отыскании представления

$$AB = \sum_{i=0}^{2l-2} c_i \omega^{ip},$$

где вектор c представляет собой свёртку векторов a и b, $c = a * b$.

Это приводит к алгоритму Шёнхаге – Штрассека для умножения целых чисел. На подробном описании алгоритма мы не останавливаемся. Можно показать, что для умножения n-разрядных двоичных чисел понадобится

$$o(n \log n \log \log n) \tag{9.25}$$

битовых операций.

Замечание 10. Из оценки (9.25) видно, что в качестве $M(k)$ в следствии из теоремы 10 можно взять

$$M(k) = k \log k \log\log k. \tag{9.26}$$

При больших n в этом случае в оценке (9.23) будет доминировать второе слагаемое, так что оценка (9.23) примет вид

$$O_\omega(n^2 \log n \log\log n) \tag{9.27}$$

(каждый может также определить роль ω в этой оценке [16]).

§2. Об аналитических преобразованиях и об их реализации с помощью ЭВМ

1. Стимулы к развитию систем аналитических вычислений

На первом этапе после появления компьютеров основным являлся "численный счёт". Большой класс физических явлений характеризуется так называемыми полями (скалярными или векторными). Эти понятия определяются как соответствия, в которых точке плоскости или трёхмерного пространства сопоставляются скалярные или векторные величины; иначе говоря, речь идёт о скалярных или векторных функциях, заданных в области плоскости или пространства.

Обычно эти функции неизвестны, их следует определить из того или иного дифференциального уравнения, часто – из уравнений в частных производных с соответствующими начальными и граничными условиями. Количество таких задач огромно, ибо большинство физических характеристик (температура, влажность, электрическая и магнитная напряжённости и др.) представляют собой поля и рассматриваются в различных обстоятельствах (в различных газах, на поверхностях тел различной формы и различного материала и т.п.). Для решения таких задач разработаны методы, позволяющие определить численные значения упомянутых полей на достаточно густой сетке точек с той или иной точностью. Густота сетки существенна для детального описания явления. Методы эти

[16] Проследить роль ω в оценке (9.27).

приводят к большому (иногда – к огромному) количеству арифметических действий. Счёт обычно идёт в системе с плавающей точкой, что влечёт за собой погрешности на каждом шаге вычислений (называемые ошибками округления). Это приводит к накоплению ошибок, которые могут стать причиной неустойчивости счёта вплоть до остановки процесса вычислений из-за выхода за пределы разрядной сетки ЭВМ. Накопление ошибок приводит к потере точности так что результат вычислений может оказаться неприемлемым.

Кроме того, сама идеология ограничивает исследователя при получении результата: вместо поля, интересующего исследователя, получаются лишь значения его в отдельных точках. Поэтому широко разрабатываются методы, позволяющие получать упомянутые поля в виде формулы, представляющей собой некоторое аналитическое выражение. Конечно и в этом случае получается обычно лишь некоторое приближение к искомому полю. Для уточнения аналитического приближения формулы приходится усложнять специально разработанными итерационными процессами, использующими данное дифференциальное уравнение. Разработка аналитических методов – основной стимул для развития систем аналитических вычислений (САВ), позволяющих привлечь компьютер к рутинной работе по выводу подобных формул.

Второй стимул к развитию САВ связан с упомянутыми выше методами численного счёта. Изощрённые численные методы решения сложных задач математической физики требуют предварительного вывода формул для рассматриваемой задачи и программирования этих формул (обычно на одном из языков высокого уровня). И то и другое характеризуется применением определённых правил; алгоритмы для вывода упомянутых формул и написания программ можно считать известными. Тем самым открывается возможность использовать ЭВМ и для этой цели.

2. О некоторых выдающихся аналитических вычислениях в прошлом веке

Знаменитые великие вычисления XIX века содержат большое количество манипуляций с формулами. Одним из наиболее известных является расчёт Лаверье орбиты Нептуна, который был осно-

ван на аналитических вычислениях возмущённой орбиты Урана и который собственно привёл к открытию Нептуна “на кончике пера”. Вторым впечатляющим вычислением с карандашом и бумагой является вывод 40000 аналитических формул, которые были выполнены французским астрономом Делоне для вычисления орбиты Луны и которые потребовали 10 лет работы для получения этих формул и ещё 10 лет для их проверки. Окончательный результат представляет собой формулу, занимающую 128 страниц его книги. Проверка этих аналитических выкладок проведена двумя американскими математиками с использованием ЭВМ в 70-х годах этого столетия; она потребовала около двух суток вычислений, причём в результате проверки была обнаружена всего лишь одна (!) ошибка (заметим, что подготовка соответствующих программ отняла около года).

3. Соотношение аналитических и численных вычислений

Из сказанного в первом пункте ясно, что к недостаткам численного счёта относится следующее:

– неточность получаемого числового результата (ввиду накопления ошибок округления),

- -неустойчивость вычислений в ряде задач из-за накопления упомянутых выше ошибок,

– “сеточный” характер получаемого результата (т.е. возможность определить функцию лишь в узлах некоторой сетки),

– потеря существенной информации в процессе вычислений (получаемые числа не дают полной характеристики использованных формул).

Однако численные расчёты не исключают алгебраических вычислений: написание простейших программ требует вывода и переписывания формул, на которых основан алгоритм, а это можно поручить ЭВМ. Рост мощности компьютеров для описанных в пункте 1 задач численного счёта не решает всех проблем; например, расчёт развития атмосферных процессов с точностью, необходимой для 48-часового прогноза, на наиболее мощных компьютерах (типа CRAY) требует значительно больше 48 часов. Увеличение производительности в 10 раз едва ли поможет, ибо для уточнения прогноза

нужно в 2 раза уменьшить шаг сетки (а значит, в 4 раза увеличить число неизвестных), что потребует 8-кратного увеличения объёма вычислений. Однако, можно надеяться, что комбинация численного счёта с аналитическими вычислениями приведёт к существенному успеху.

Особенности аналитических вычислений на ЭВМ состоят в следующем:

– имеется возможность проводить аналитические (и численные) преобразования без погрешностей,

– в результате не теряется исходная информация о характере исследуемого процесса,

– на этапе аналитических вычислений неустойчивость процесса не проявляется,

– в ряде случаев наблюдается быстрое (экспоненциальное) возрастание результатов промежуточных вычислений,

– ввиду упомянутого разрастания результатов резко повышаются требования к объёму памяти и к быстродействию компьютера,

– резко повышаются требования к предварительному изучению алгоритма: к оценке его быстродействия, необходимой памяти и к эффективному представлению результата,

– имеется возможность производить генерацию программ, использующих найденные формулы.

4. О связи компьютерной алгебры и систем аналитических вычислений

Понятие компьютерной алгебры появилось в связи с разработкой и применением систем аналитических вычислений. Цель компьютерной алгебры в изучении алгоритмов аналитических преобразований с точки зрения эффективной их реализации на ЭВМ. Ввиду указанного в предыдущем пункте разрастания результатов промежуточных вычислений (которое часто имеет катастрофический характер) центральная задача компьютерной алгебры – оценка сложности аналитических выражений и длительности аналитических преобразований. Зачастую это сводится к оценке числа арифметических действий с входящими в аналитическое выражение символами. Поскольку размер символов обычно нетрудно оценить задача сводится именно к оценке числа операций. Заметим,

что часто результаты, связанные с анализом вычислительных алгоритмов, применимы и к компьютерной алгебре (с некоторым смещением акцента: кроме времени вычисления по той или иной формуле следует говорить также об оценке её длины, которая обычно пропорциональна указанному времени).

Наиболее популярными и достаточно мощными системами компьютерной алгебры общего назначения к настоящему времени является:

– MACSYMA (мало доступна),

– REDUCE (наиболее широко распространена),

– muMATH (на микрокомпьютерах),

– SCRATCHPAD (новая система с ограниченным доступом).

Эти и ряд других не названных здесь систем обладают общими свойствами:

– программирование интерактивное,

– данные представляют собой аналитические выражения,

– язык пользователя похож на Паскаль,

– языки реализации близки к языку ЛИСП (или совпадают с ним).

Особенность работы состоит в том, что в отличие от численного счёта здесь пользователь передоверяет ЭВМ много таких функций, которые раньше он выполнял самостоятельно. Тем самым в ещё большей степени, чем при численном счёте, утрачивается контроль за проводимыми преобразованиями. Для того, чтобы в какой-то степени уравновесить этот недостаток, пользователю необходимо более детально, чем в процессе численного счёта, представлять себе работу используемого программного продукта, т.е. хорошо представлять себе результаты применения тех или иных операций и процедур применяемой системы аналитических вычислений, а также знать свойства применяемых алгоритмов (в отношении сложности вычислений и длины промежуточных результатов).

§3. О представлении данных в САВ

1. Введение

Этот параграф, как и предыдущий, представляет собой некоторый обзор имеющихся результатов. При любом таком обзоре нет

возможности отразить отдельные детали рассматриваемой ситуации и дать доказательства приводимых утверждений. Более того, многие утверждения в этих условиях не удаётся даже точно сформулировать.

С другой стороны полезность такого обзора несомненна: он позволяет понять основные трудности и обратиться к их изучению в нужной последовательности.

Здесь мы кратко рассмотрим фундаментальную проблему наиболее эффективного представления данных в максимально универсальной постановке, т.е без технических деталей. Многие из рассматриваемых результатов носят характер рецептов, объяснение или доказательства которых иной раз являются результатами обширных теорий и потому выходят за рамки настоящего курса.

К моменту чтения этого параграфа читателю уже известны результаты изучения быстрого преобразования Фурье (см. предыдущий параграф), и это существенно облегчает понимание последующего материала.

2. Представление целых чисел

Представление целых чисел представляет собой определённую проблему в CAB, поскольку при проведении аналитических преобразований промежуточные результаты требуют значительной памяти, хотя исходные данные невелики.

В CAB обычно рассматриваются точные аналитические преобразования (и это имеет глубокий смысл в ряде исследований). Поэтому никакие округления или другие искажения целых чисел недопустимы. Для иллюстрации приведём известный пример (Knuth, Broun) вычисления НОД двух многочленов

$$P(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, \tag{2.1}$$

$$Q(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21, \tag{2.2}$$

В результате деления $3^3 P(x)$ на $Q(x)$ в остатке получится число

$$1259333879550074310093115199218750 0, \tag{2.3}$$

содержащее 35 десятичных цифр (117 бит), откуда следует, что многочлены P и Q взаимно просты. Полученный ответ (“простота”,“непростота”) требует для хранения 1 бит, а число (2.3) можно рассматривать как результат промежуточных вычислений.

Отсюда следует, что необходимо рассматривать целые числа произвольной

величины. Поэтому САВ обычно допускает такую возможность и для представления таких чисел (называемых "bignums") выбирают в качестве основания некоторое число N и представляют числа относительно этого основания (с помощью "цифр" из диапазона от 0 до $N-1$), к которым добавляется знаковый бит. Используются обычно два представления: десятичное и двоичное, так что в качестве N употребительны 10^9 и 2^{30} (или 2^{31}).

Для вычитания и сложения чисел используются обычные алгоритмы поразрядного сложения с переносом из одного разряда в другой, а для результата умножения требуется два слова.

Деление представляет собой значительные трудности, связанные с необходимостью угадывания цифры частного (Knuth предложил достаточно надёжный алгоритм получения этой цифры, который почти всегда даёт правильный или близкий к правильному результат). Что касается времени счёта, то для сложения и вычитания это время пропорционально числу n цифр (будем писать в этом случае $O(n)$), а для умножения это время пропорционально числу n^2 т.е. $O(n^2)$. Согласно предыдущему параграфу использование быстрого дискретного преобразования Фурье (см. §1) позволяет довести это время до

$$O(n \log n \log\log n).$$

Однако следует заметить, что фактически последнее выражение имеет вид

$$20n \log n \log\log n,$$

так что исследования БПФ в этой ситуации эффективно для n порядка нескольких тысяч. В большинстве САВ такой алгоритм не используется.

Для вычисления НОД двух целых чисел требуется время $O(n^3)$; его достаточно просто снизить до $O(n^2)$ и даже до

$$O(n \log^2 n \log\log n),$$

однако алгоритм, связанный с последней оценкой, в САВ чаще всего не используется.

Отсюда следует, что всегда следует стремиться к работе с числами минимальной длины.

Если требуется разложить число N на множители, то ситуация оказывается весьма трудной. Попытка разделить на все простые числа, которые меньше чем $N^{1/2}$, требует $O(N^2 \log^2 N)$ операций, так что если N – целое число из n десятичных цифр, то получаем порядок $O(10^{1/2} n^2)$, растущий экспоненциально в зависимости от длины числа. Имеются более эффективные алгоритмы с меньшей скоростью роста числа операций, а именно со скоростью $O(\exp(n \log n)^{1/2})$. Однако, такая скорость роста всё-таки выше полиномиальной; эти алгоритмы пока не применялись в CAB.

Для "реально встречающихся" чисел можно строить алгоритмы со скоростью $O(10^{n/6})$ (на том, какой размер чисел считать "реально встречающимся" останавливаться не будем).

3. О представлении обыкновенных дробей

Обыкновенные дроби (т.е. дроби вида p/q где p и q – целые числа, $q \neq 0$) представляются в виде пары целых чисел: числителя и знаменателя.

Без специальных указаний пользователя при работе CAB обыкновенные дроби не следует заменять их приближёнными значениями (например, на числа с плавающей точкой, которые также обычно допустимы в CAB); ибо это может привести к непредсказуемым результатам. Например, НОД многочленов

$$x^3 - 8 \qquad \text{и} \qquad 1/3x^2 - 4/3 \tag{3.1}$$

равен $1/3x - 2/3$, в то время как НОД многочленов

$$x^3 - 8 \qquad \text{и} \qquad 0.333333x^2 - 1.33333 \tag{3.2}$$

равен 0.000001 из-за округления [17]

Поскольку все вычисления с обыкновенными дробями требуют вычисления НОД, а это проводит к большим затратам машинного времени, то следует избегать обыкновенных дробей (если возможно). В частности, вместо вычисления НОД многочленов (3.1) можно ограничиться вычислением НОД многочленов

$$x^3 - 8 \qquad \text{и} \qquad x^2 - 4 \tag{3.3}$$

[17] Разобрать предложенную ситуацию детально для ЭВМ с шестиразрядной (десятичной) мантиссой и бесконечным порядком.

последнее не требует применения обыкновенных дробей.

Хотя алгоритмы сложения и умножения дробей достаточно просты, но если предполагать, что исходные дроби представлены в несократимом виде, то при перемножении двух дробей $\frac{a}{b}$ и $\frac{c}{d}$,

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{p}{q} \tag{3.4}$$

вместо вычислений

$$p = ac, \quad q = bd \tag{3.5}$$

с последующим определением НОД (p, q) и сокращением на него дроби p/q, следует воспользоваться очевидным равенством

$$\text{НОД}(p, q) = \text{НОД}(a, d) \cdot \text{НОД}(b, c). \tag{3.6}$$

Таким образом, начиная с вычисления НОД(a, d) и НОД(b, c) и определяя

$$a' = a/\text{НОД}(a, d), \qquad c' = c/\text{НОД}(b, c),$$

$$b' = b/\text{НОД}(b, c), \qquad d' = d/\text{НОД}(a, d), \tag{3.7}$$

приходим к формулам

$$p = a'c', \quad q = b'b', \tag{3.8}$$

где очевидно вычисления проще, чем при вычислении (3.5) с последующим вычислением НОД(p, q) и сокращением на него чисел p и q.

Аналогичным образом для сложения

$$\frac{a}{b} + \frac{c}{d} = \frac{p}{q} \tag{3.9}$$

вместо формул

$$p = ad + bc, \quad q = bd \tag{3.10}$$

с последующим вычислением НОД(p, q) и сокращением на него чисел p и q, более эффективно найти

$$q = bd/\text{НОД}(b, d) \qquad b' = b/\text{НОД}(b, d)$$

$$d' = d/\text{НОД}(b, d), \tag{3.11}$$

$$p = ad' + b'c \tag{3.12}$$

с последующим вычислением НОД(p, q) и сокращением на него чисел p и q, полученных в (3.11), (3.12), ибо здесь получаются значения $p, \quad q$ меньше, чем в (3.10).

4. Представление многочленов

Основные вычисления, которые отличают САВ от других систем, это – работа с многочленами, понимаемыми в обощенном смысле.

Для того, чтобы прояснить ситуацию, приведём примеры. Вычисление

$$(x - y)(x + y) = x^2 - y^2 \tag{4.1}$$

является многочленным (полиномиальным) вычислением, но таким же является и вычисление

$$(\cos a - \sin b)(\cos a + \sin b) = \cos^2 a - \sin^2 b, \tag{4.2}$$

в котором фактически произведено то же вычисление, что и в (4.1) с заменой x на $\cos a$, а y на $\sin b$.

Обычно САВ могут работать с многочленами произвольного числа переменных. Их можно складывать, вычитать, умножать и делить, но наиболее интересной (как ни странно) представляется операция упрощения.

Понятие “упрощение” требует строгого определения и фактически речь идёт о выделении удобного представителя из класса эквивалентных (в том или ином смысле) выражений. Особенностью может являться то, что в различных условиях “удобными” могут оказаться различные представители.

Например, обсуждение вопроса, какой из представителей класса эквивалентных выражений $(x - 1)(x + 1)$ или $x^2 - 1$ более удобен, возможно, не имеет принципиального значения, однако, то же, повидимому, не удаётся сказать относительно выражений

$$(x^{1000} - 1)/(x - 1) \tag{4.3}$$

и

$$x^{999} + x^{998} + \ldots + x + 1, \tag{4.4}$$

второе из которых имеет 1000 слагаемых.

5. Каноническое и нормальное представления

Представление объектов называется каноническим, если две различные записи соответствуют всегда двум различным объектам:

$$o_1 \rightarrow r_1$$

$$o_2 \rightarrow r_2$$

$$o_3 \nearrow r_3 \searrow r_4$$

Определение 1. *Говорят, что соответствие f классов O и R*

$$f : O \rightarrow R \tag{5.1}$$

является O в R, если каждый элемент, принадлежащий R, соответствует только одному элементу из O, и каждому элементу из O соответствует хотя бы один элемент из R.

Тем самым, представлений может быть несколько.

Определение 2. *Представление называется каноническим, если отображение f взаимно однозначно (биективно).*

Более слабым условием (в случае моноида) является нормальность представления. Напомним, что моноид – это множество объектов с одной бинарной (обычно ассоциативной) операцией, для которой (в мультикативной терминологии) имеется единица. Если упомянутая операция называется сложением, то вместо единицы требуется существование нуля.

Определение 3. *Представление моноида называется , если представление его нуля единственно.*

Ясно, что если представление каноническое, то оно и нормальное.

Если представление нормальное, то для определения совпадения двух объектов моноида составляют их разность и смотрят её представление: если это – представление нуля, то считают элементы совпадающими, в противном случае – различными.

Таким образом нужно, чтобы представление было по крайней мере нормальным, а ещё лучше – каноническим.

Кроме того, желательно, чтобы оно было “регулярным” в том или ином смысле, а кроме того “естественным” и “компактным”. Последним двум критериям, по-видимому, не удовлетворит представление целого числа единицами, например, 7=“1111111”.

Существует несколько представлений, удовлетво- ряющих перечисленным критериям, и обычно САВ используют два или три из них.

6. Плотные и разреженные представления

Обычно различают два типа представлений: плотные и разреженные. На наш взгляд больше соответствуют содержанию термины полные и частичные представления.

Традиционно этим понятиям не придают чёткого математического содержания, поскольку они касаются возможных реализаций и носят обычно утилитарный характер. Следуя этой традиции, можно сказать, что представлением какого-либо класса объектов называется представление, ориентированное на экономное (в том или ином смысле) представление выделенного класса объектов. Полным представлением называется представление, не обладающее упомянутым свойством.

Например, сравним следущие два представления многочлена:

1) представление многочлена $a_0 + a_1x + \ldots + a_nx^n$ таблицей его коэффициентов

$$[a_0a_1 \ldots a_n], \tag{6.1}$$

2) представление многочлена списком пар упорядоченных чисел (коэффициент, степень), где пара с нулевым коэффициентом пропускается, так что многочлен $1 + x^{10}$ представляется в виде списка

$$(1, 0), (1, 10). \tag{6.2}$$

Заметим, что здесь следует ввести ещё представление нулевого многочлена (оно должно быть особым).

Если считать, что под каждое число отводится одинаковая память (не зависящая от числа), то первое представление экономнее, если число ненулевых слагаемых больше entier(n/2), иначе экономнее второе представление (здесь, конечно, не учитываются дополнительные технические детали).

Второе представление принято называть разреженным, а первое плотным представлением многочлена. Согласно нашей терминологии и то, и другое представление можно называть (первое – относительно подкласса многочленов, число ненулевых слагаемых в

которых больше половины степени, второе – относительно подкласса многочленов с противоположным соотношением между числом ненулевых слагаемых и степеней). Полным называем то представление, в котором упомянутый подкласс экономных представлений не выделяется.

Замечание 1. Отсюда видно, что понятие "частичное представление" зависит от выделяемого подкласса и потому более естественно понятие "частичного представления относительно подкласса $\mathcal{K}$" (более подробно на этом не останавливаемся).

Полезность понятия иллюстрируется на примере проверки соотношения

$$(x^{1000}+1)(x^{1000}-1) = x^{2000}-1. \tag{6.3}$$

Здесь применение представления 1) привело бы к миллиону умножений слева, а в представлении 2) можно обойтись лишь четырьмя умножениями.

Заметим также, что в слуае многочлена нескольких переменных аналог представления 1) дает 7776 членов, а аналог представления 2) – всего лишь один член в представлении многочлена

$$P(x,y,z,u,v) = x^5y^4z^3u^2v. \tag{6.4}$$

Замечание 2. Количество членов результата для последних трёх операций уже не определяется числом ненулевых членов исходных многочленов; примером служит деление многочленов x^n-1 и $x-1$

$$\frac{x^n-1}{x-1} = x^{n-1}+x^{n-2}+\ldots+1. \tag{6.5}$$

Замечание 3. Относительность "частичного представления" легко прочувствовать на примере (6.5), в качестве представления многочлена (с ненулевыми коэффициентами при всех степенях!)

$$x^{n-1}+x^{n-2}+\ldots+1 \tag{6.6}$$

может быть взят список $((1,n),(-1,0),(1,1),(-1,0))$, соответствующий представлению 2) типа (6.2) делимого и делителя левой части (6.5).

Замечание 4. Известно, что для многочлена

$$p = (1+2x-2x^2+4x^3+4x^4)(1+2x^4-2x^8+4x^{12}-$$

$$-10x^{16} + 28x^{20} - 84x^{24}) \tag{6.7}$$

многочлен p^2 имеет меньше слагаемых чем p, а НОД многочлена p^2 и $(p^2)'$ содержит больше слагаемых, чем каждый из этих многочленов. [18]

Замечание 5. Почти очевидно, что время счёта зависит в значительной степени от предпринятой подстановки; например, время развёртывания выражений

$$(x^{1000} + 1)^2 \tag{6.8}$$

и

$$((t-1)^{1000} + 1)^2 \tag{6.9}$$

отличается в тысячи раз.

7. Наибольший общий делитель (НОД)

Нетривиальность процесса отыскания НОД двух многочленов хорошо иллюстрируется на следующем примере (Brown), где используется алгоритм Евклида. Пусть

$$P(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, \tag{7.1}$$

$$Q(x) = 3x^6 + 5x^4 - 4x^2 - 9x - 21. \tag{7.2}$$

Первый шаг состоит в вычислении

$$P(x) - (\frac{x^2}{3} - \frac{2}{9})Q(x) = -\frac{5}{9}x^4 + \frac{1}{9}^2 - \frac{1}{9}. \tag{7.3}$$

Аналогичным образом сделаем следующие шаги:

$$\frac{-117}{25}x^2 - 9x + \frac{441}{25}, \tag{7.4}$$

$$\frac{233150}{6591}x - \frac{102500}{2197}, \tag{7.5}$$

и окончательно

$$\frac{1288744821}{543589225}. \tag{7.6}$$

Отсюда видно, что в процессе вычислений необходимо часто вычислять НОД двух целых чисел.

[18] Попытаться дать более эффективную оценку для НОД, чем та, которая приведена в таблице 1.

Оказывается можно всегда работать с многочленами с целыми коэффициентами, если домножать $P(x)$ на некоторую степень старшего коэффициента у $Q(x)$ (а именно на степень $deg\ P - deg\ Q + 1$). Тогда мы получим следующую последовательность:

$$-15x^4 + 3x^2 - 9, \tag{7.7}$$

$$15795x^2 + 30375x - 59535, \tag{7.8}$$

$$1254542875143750x - 1654608338437500, \tag{7.9}$$

$$12593338755007431009331151992187500. \tag{7.10}$$

Последовательность многочленов (7.7) - (7.10) называется последовательностью Евклида, длина коэффициентов такой последовательности имеет экспоненциальный рост (относительно степеней исходных многочленов). Однако (Коллинз, Браун) можно выбирать числовые множители перед делением многочленов так, что в соответствующей последовательности (называемой последовательностью субрезультантов) будет наблюдаться лишь линейный рост. Опишем этот приём (без доказательства) более подробно.

Пусть даны два многочлена P_1 и P_2 с целыми коэффициентами, а $P_3, P_4, \ldots$ – соответствующая последовательность для вычисления НОД, $\delta_i = degP_i - degP_i + 1$, A_i – старший коэффициент многочлена P_i. Тогда остаток от деления $A_i^{\delta_{i-1}+1} P_{i-1}$ на P_i всегда является многочленом с целыми коэффициентами; его будем записывать в виде $\beta_{i+1} P_{i+1}$, где β_{i+1} подлежит определению. Алгоритм Евклида соответствует выбору $\beta_{i+1} = 1$. Если взять

$$\beta_3 = (-1)^{\delta_{i+1}}, \tag{7.11}$$

$$\beta_i = -A_{i-2} \psi_i^{\delta_{i-2}}, \tag{7.12}$$

где ψ_i задаются формулами

$$\psi_3 = -1, \quad \psi_i = (-A_{i-2})^{\delta_{i-3}} \psi_{i-1}^{1-\delta_{i-3}},$$

то (по теореме о субрезультантах) все P_i окажутся многочленами с целыми коэффициентами, а длина коэффициентов растёт не более, чем линейным образом.

В нашем примере получаем последовательность

$$P_3 = 15x^4 - 3x^2 + 9, \tag{7.14}$$

$$P_4 = 665x^2 + 125x - 245, \tag{7.15}$$

$$P_5 = 9326x - 12300, \tag{7.16}$$

$$P_6 = 260708, \tag{7.17}$$

которая значительно компактнее, чем (7.7) - (7.10).

8. Многочлены от нескольких переменных

Представление многочленов от нескольких переменных связано с решением более общей проблемы: как выбрать способ упорядочивания членов при рассмотрении коммутирующих операций. Хотя этот вопрос кажется в какой-то степени исскуственным, но решение его необходимо при выборе канонического представления выражения.

Итак, какое из представлений одного и того же выражения $f(x, y, z) = x^2+y+z$ выбрать $x^2+y+z, \quad y+x^2+z, \quad z+xx+y$ или что-нибудь ещё?

Аналогичен вопрос по отношению (к коммутативному) произведению.

Произведение степеней будем называть .

Примеры мономов: $xyz, \quad x^3uv$.

Здесь также по отношению к моному возникает вопрос представления. Например, для монома $\varphi(u, v, x) = x^2uv$ можно выбрать различные представления

$$xxuv, \quad xuvx, \quad uvx^2$$

и т.п. Какое из них предпочтительнее?

Обычно применяют один из следующих способов:

a) лексикографический,

b) степенно-лексикографический,

c) обратный лексикографический.

Известно, что введение в исходном алфавите полного упорядочивания приводит к полному упорядочиванию составленных из него слов. В каждом выражении с коммутативной операцией производится упорядочивание составляющих его слов в соответствии с указанным отношением, и в качестве представителя класса эквивалентных выражений выбирается старшее из них. Так реализуется лексикографический способ (a).

Степенно - лексикографический способ (b) отличается от упомянутого тем, что приоритетным является упорядочение по группам равных степеней (тех или иных переменных), а затем уже производится лексикографическое упорядочение. Так, например, согласно способу (a) выражение $x^2 + xy + xz^3$ принимает вид ($x < y < z$)

$$x^2 + xy + xz^3, \tag{8.1}$$

а согласно способу (b) оно примет вид

$$xz^3 + x^2 + xy. \tag{8.2}$$

Обратный лексикографический способ (c) характеризуется вытеснением переменных максимального веса в конец последовательности. Его проиллюстрируем на примере выражения

$$uzx + xy + yz + x. \tag{8.3}$$

Применение способа (c) к выражению (8.3) даёт представление ($x < y < z < u$)

$$x + xy + yz + xzu, \tag{8.4}$$

в то время как применение (a) приводит к представлению

$$x + xy + xzu + yz, \tag{8.5}$$

и применение (b) к представлению

$$xzu + xy + yz + x. \tag{8.6}$$

Замечание 1. Лексикографическое упорядочение удобно для группировки относительно выделенной переменной (см. (8.5), где в качестве выделенной переменной можно рассматривать x). Форму, где проведена группировка, иногда называют , в отличие от общей записи, которую называют . Итак, из (8.5) легко получить рекурсивную форму

$$x(1 + y + zu) + yz. \tag{8.7}$$

Формы (8.4) - (8.6) – распределённые.

Замечание 2. Рекурсивная форма определяется выделенной переменной, при разных выделениях переменной получаются различные рекурсивные формы. Переход от одной рекурсивной формы к

другой является трудной задачей для САВ, такие переходы следует избегать. Точно также можно сказать о переходе от одного типа упорядочения к другому.

Замечание 3. Выделение переменной (выделенную переменную иногда называют главной) может влиять на полученный результат. Например, если x – выделенная переменная, то при делении $2x - y$ на $x + y$ частное равно 2, а остаток равен $-3y$; если y – выделенная переменная, то частное равно -1, а остаток равен $3x$.

9. Представление рациональных функций

Отношение многочленов представляет собой рациональную функцию. К действиям с рациональными функциями следует, конечно, отнести преобразования вида

$$\frac{1}{\sin x} + \frac{1}{\cos x} = \frac{\cos x + \sin x}{\sin x \cos x} \tag{9.1}$$

ибо это то же, что вычисление

$$\frac{1}{a} + \frac{1}{b} = \frac{a+b}{ab}. \tag{9.2}$$

Если представлением рациональной функции считать отношение многочлена (в числителе) к многочлену (в знаменателе), то получается представление (нуль имеет единственное представление – нуль в числителе).

Однако, трудно получить каноническое представление. Например, можно считать, что формулы

$$\frac{x-1}{x+1}, \qquad \frac{x^2 - 2x + 1}{x^2 - 1} \tag{9.3}$$

представляют один и тот же элемент, но формулы эти различны.

Более очевидным примером двух записей одной функции в R^1 являются формулы

$$\frac{x+1}{x-1}, \qquad \frac{(x+1)(x^2+1)}{(x-1)(x^2+1)}. \tag{9.4}$$

Замечание 1. Иногда вопросы представления перемешивают с достаточно

тонкими вопросами теории функций, как это произошло в примере (9.3). Как известно, функцией называется не просто формула,

по которой следует действовать, чтобы по заданному числу (прообразу) найти значение функции (образ), а однозначное отображение одного числового множества в другое. Иначе говоря, помимо формулы (алгоритма) должна быть задана область определения. Итак, если действовать несколько упрощённо, то под функцией подразумевается

формула (алгоритм) + область определения.

При одной и той же формуле, но при разных областях определения мы имеем разные функции. Правда, часто явно область определения не указывается; в этом случае подразумевается "максимально возможная" в рассматриваемой ситуации область определения, для которой формула имеет смысл.

В частности, если рассматриваются действительные функции действительного переменного, то записывая $f(z) = \sqrt{z}$ и не указывая область определения, (по умолчанию) считают, что областью определения служит множество

$$R^1_+ = [0, +\infty),$$

а в случае исследования функции комплексного переменного $f(z) = \sqrt{z}$ считают, что $\sqrt{z}$ представляет собой главное значение квадратного корня с областью значений – комплексная плоскость (иногда – риманова поверхность).

С этой точки зрения вещественно-значные функции (9.3) вещественного переменного x различны, ибо область определения второй из них у́же области определения первой (вторая определена для всех $x \in R^1$ кроме $x = 1, x = -1$, а первая – для всех $x \in R^1$, кроме $x = -1$).

Замечание 2. Имеются различные обобщения понятия функции, с которыми часто приходится иметь дело (например, в математической физике). Необходимо учитывать эти обобщения при символьных преобразованиях, проводимых САВ. Одним из подобных обобщений является рассмотрение классов функций, отличающихся друг от друга на мнжестве меры нуль. Итак, функциями в этом случае называются упомянутые классы. С этой точки зрения функции (9.3), отличающиеся на множестве меры нуль (в точке $x = 1$ вторую функцию можно определить произвольным образом), лежат в одном классе и значит представляют одну функцию.

Замечание 3. В силу сказанного вещественнозначные функции (9.4) вещественного переменного имеют естественную область определения R^1 и здесь они совпадают (однако на комплексной плоскости в классическом смысле эти функции различны).

С учётом указанных замечаний для перехода к каноническому представлению необходимо ликвидиро- вать неоднозначность представления. В рассматриваемом случае (при рациональных коэффициентах) делают следующее:

1) сокращают на общие делители числитель и знаменатель,

2) переходят к целым коэффициентам,

3) замечают, что в совокупностях целых коэффициентов нет отличных от единицы целых, которые делят числитель и знаменатель,

4) производят тождественное преобразование, при котором старший коэффициент знаменателя становится положительным.

Конечно, можно выбрать и другие правила, но эти правила наиболее употребительны.

10. Представление алгебраических функций

10.1. Простые радикалы

К простым радикалам относят такие радикалы, как например $\sqrt{2}$ или $\sqrt[3]{x^2-1}$, а также радикалы вида

$$\alpha = \sqrt[n]{a}, \qquad \alpha^i; \quad i = 0, 1, \ldots, n-1.$$

А/ Нетрудно видеть, что выражения с радикалами имеют различные представления; например,

$$\frac{1}{\sqrt{2}-1} = \sqrt{2}+1.$$

Отсюда возникает проблема однозначного представления подобных выражений. Ее универсальное решение представляется весьма сложным; действительно, если потребовать, чтобы радикалы были лишь в числителе, то следующий пример оказывается разочаровывающим:

$$\frac{1}{\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}} =$$
$$= (22\sqrt{3}\sqrt{5}\sqrt{7} - 34\sqrt{2}\sqrt{5}\sqrt{7} - 50\sqrt{2}\sqrt{3}\sqrt{7} + 135\sqrt{7} +$$

$$+62\sqrt{2}\sqrt{3}\sqrt{5} - 133\sqrt{5} - 145\sqrt{3} + 185\sqrt{2})/215$$

Другие же варианты универсального решения представляются еще более спорными (на них останавливаться не будем).

В/ Вторая проблема – проблема взаимной зависимости радикалов; она состоит в том, что корни различных степеней могут выражаться один через другой. Простым примером является следующий:

$$\sqrt[4]{-4} \Longrightarrow \alpha^2 = 2\alpha - 2 \Longrightarrow \sqrt[4]{-4} = (\sqrt{-4} + 2)/2,$$

поскольку

$$x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

10.2. Вложенные радикалы

В этом аспекте имеются следующие проблемы.

А/ Проблема эквивалентности рациональных дробей с радикалами те же, что и выше (см. 10.1 А/).

В/ Проблема тождественности выражений для радикалов не решена удовлетворительным образом; сложность проблемы подчеркивается рядом удивительных соотношений:

$$\sqrt{9 + 4\sqrt{2}} = 1 + 2\sqrt{2},$$

$$\sqrt{5 + 2\sqrt{6}} + \sqrt{5 - 2\sqrt{6}} = 2\sqrt{3},$$

$$\sqrt{x + \sqrt{x^2 - 1}} = \sqrt{\frac{x+1}{2}} + \sqrt{\frac{x-1}{2}},$$

$$\sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}} =$$

$$= \sqrt{22 + 2\sqrt{5}} - \sqrt{11 + 2\sqrt{29}} + \sqrt{5},$$

$$\sqrt[3]{\sqrt[5]{32}/5 - \sqrt[5]{27}/5} =$$

$$= \sqrt[5]{1}/25 + \sqrt[5]{3}/25 - \sqrt[5]{9}/25 =$$

$$= \sqrt[5]{1}/25(1 + \sqrt[5]{3} - \sqrt[5]{3^2}),$$

$$\sqrt{(112 + 70\sqrt{2}) + (46 + 34\sqrt{2})\sqrt{5}} =$$

$$= (5 + 4\sqrt{2}) + (3 + \sqrt{2})\sqrt{5}.$$

10.3. Алгебраические функции общего вида

Если α – корень многочлена $p(\alpha)$, то многое зависит от того, является ли многочлен $p(\alpha)$ неприводимым (т.е. неразложимым).

Речь идёт об однозначности (каноничности) представления $\sum_{i=0}^{n} a_i\alpha^i$. Если a_i– рациональные числа, а $n \leq deg\ p$ и $p(\alpha)$ – неприводимый, то упомянутую сумму можно считать каноническим представлением (если $p(\alpha)$ – приводимый, то нет даже нормальности).

В случае, когда появляется несколько корней, то проблема усложняется. Например, если α и β корни многочленов $p(\alpha)$ и $q(\beta)$, то нужно проверить, являются ли они совместно неприводимыми. Нетривиальность вопроса демонстрирует следующий пример.

Пусть α – корень многочлена $p(\alpha) = \alpha^5 - \alpha - 1$, β – корень многочлена $q(\beta) = \beta^5+5\beta^4+10\beta^3+10\beta^2+4\beta-1$, который получен из $p(\alpha)$ подстановкой $\alpha = \beta + 1$. Ясно, что $\beta = \alpha - 1$ – корень $q(\beta)$ и потому $q(\beta) = (\beta - \alpha + 1)(\beta^4 + \beta^3(\alpha + 4) + \beta^2(\alpha^2 + 3\alpha + 6) + \beta(\alpha^3 + 2\alpha^2 + 3\alpha + 4) + \alpha^4 + \alpha^3 + \alpha^{@} + \alpha)$, так что $p(\alpha)$ и $q(\beta)$ в этом примере не являются совместно неприводимыми.

Для проверки того, что система корней α_i полиномов p_i допустима (в смысле однозначности представления полиномами с рациональными коэффициентами) следует разложить p_1 на множители как полином с целыми коэффициентами, затем разложить p_2 как полином с коэффициентами из $\mathcal{K}[\alpha_1]$, затем p_3 – как полином с коэффициентами из $\mathcal{K}[\alpha_1, \alpha_2]$ и т.д. Процесс этот может быть очень трудоёмким, так что в реальных системах он не проводится.

10.4. Примитивные элементы

Всегда в поле нулевой характеристики (в расширении кольца целых чисел) можно вернуться к работе в терминах единственного алгебраического числа – примитивного элемента поля.

Например, если α – корень многочлена

$$\alpha^4 - 10\alpha^2 + 1,$$

т.е. $\alpha = \sqrt{2} + \sqrt{3}$, то $\sqrt{2} = (\alpha^3 - 9\alpha)/2$ и $\sqrt{3} = (11\alpha - \alpha^3)/2$; итак α – примитивный элемент поля $Q[\sqrt{2}, \sqrt{3}]$.

Однако, примитивные элементы могут быть весьма сложными. Например, примитивный элемент, соответствующий корням α и β полинома

$$x^4 + 2x^3 + 5$$

равен корню многочлена

$\gamma^{12} + 18\gamma^{11} + 132\gamma^{10} + 504\gamma^9 + 991\gamma^8 + 372\gamma^7 -$

$-3028\gamma^6 - 6720\gamma^5 + 11435\gamma^4 + 91650\gamma^3 + 185400\gamma^2 + 194400\gamma +$ 164525,

причём выражение α и β через этот корень использует 14-значные десятичные числа. Заметим, что в CAB примитивные элементы не применяются.

11. Представление трансцендентных функций

Трансцендентные функции группируются в несколько классов, каждый из которых имеет свои правила преобразовния (и упрощения).

Наиболее употребительными классами являются

— класс тригонометрических функций,

— класс экспоненциальных функций,

— класс логарифмических функций,

— класс обратных тригонометрических функций.

Приведём некоторые правила преобразований для класса тригонометрических функций:

$$\sin(x+y) \Rightarrow \sin x \cos y + \cos x \sin y, \tag{11.1}$$

$$\sin x \cos y \Rightarrow \frac{1}{2}(\sin(x+y) + \sin(x-y)), \tag{11.2}$$

$$\sin \pi \Rightarrow 0, \tag{11.3}$$

$$\operatorname{tg} x + \operatorname{tg} y \Rightarrow \frac{\sin(x+y)}{\cos x \cos y}. \tag{11.4}$$

Естественно, что трансцендентные функции могут являться аргументами и коэффициентами рациональных функций, рассмотренных выше, а также входить в алгебраические функции.

Преобразования только что упомянутых функций ничем не отличается от рассмотренных в предыдущих пунктах. Однако, применение правил (11.1) – (11.4) может повлечь неожиданные результаты, поэтому обращаться к ним нужно с определённой осторожностью. Например, автоматизированные преобразования, включающие правила (11.1) и (11.2) могут повлечь зацикливание процесса преобразований. Поэтому чаще всего введение в действие тех или иных правил является прерогативой пользователя.

Отметим ещё некоторые трудности, которые могут встретиться, если не учитывать возможности применяемой САВ. Например, если САВ не имеет в виду возможность преобразования

$$2x \Rightarrow x + x, \tag{11.5}$$

(а это относится к большинству САВ, ибо постоянное наблюдение за возможностью (11.5) весьма дорого стоит), то задания правила (11.1) недостаточно, чтобы проводить преобразование

$$\sin 2x \Rightarrow 2 \sin x \cos x; \tag{11.6}$$

легко видеть, что правило (11.1) должно быть дополнено правилом (11.6). Вместо (11.6) часто вводят правило

$$\sin Nx \Rightarrow \sin(N-1)x \cos x + \cos(N-1)x \sin x, \tag{11.7}$$

которое, конечно, включает и правило (11.6).

Правила (11.1) – (11.7), рассмотренные в этом пункте, называют правилами перезаписи. Заметим, что введение нового правила перезаписи может оказаться весьма дорогостоящим, так как может повести к большим преобразованиям аналитических вычислений.

По отношению к тому или иному классу трансцендентных функций можно поставить вопрос о минимальном наборе правил перезаписи, из которого следуют все

возможные правила для этого класса.

Например, рассмотрим класс, полученный объединением классов показательных и логарифмических функций. Для этого класса характерны следующие правила:

$$\log(fg) = \log f + logg, \tag{11.8}$$

$$\exp \log f = \log \exp f = f, \tag{11.9}$$

$$\exp(f + g) = \exp f \cdot \exp g. \tag{11.10}$$

Являются ли они минимальным набором, полным в том смысле, что все мыслимые преобразования в этом классе можно совершить, используя это правила?

Следующее утверждение даёт положительный ответ на этот вопрос.

Теорема 1 (Risch, 1979). *Пусть $\mathcal{K}$ – поле констант и пусть функции $\Theta_1, \ldots, \Theta_n$ являются алгебраическими, экспоненциальными ($\Theta_i = u_i = \exp v_i$) или логарифмическими ($\Theta_i = v_i = \log u_i$) функциями, причём каждая функция Θ_i определена над $\mathcal{K}(x, \Theta_1, \ldots, \Theta_{i-1})$ и пусть подполе констант поля $\mathcal{K}(x, \Theta_1, \ldots, \Theta_n)$ совпадает с $\mathcal{K}$. При этих условиях*

(a) функция $\Theta_i = u_i = \exp v_i$ трансцендентна над $\mathcal{K}(x, \Theta_1, \ldots, \Theta_{i-1})$ тогда и только тогда , когда v_i не может быть представленна в виде

$$c + \sum_{j=1}^{i-1} n_j v_j, \tag{11.11}$$

где c принадлежит $\mathcal{K}$, а n_j – рациональные числа,

(b) функция $\Theta_i = v_i = \log u_i$ трансцендентна над $\mathcal{K}(x, \Theta_1, \ldots, \Theta_{i-1})$ тогда и только тогда, когда никакая степень u_i^n элемента u_i не может быть представлена в виде

$$c \prod_{j=1}^{i-1} u_j^{n_j}, \tag{11.12}$$

где $c \in \mathcal{K}$, а n, n_j – целые числа, $n \neq 0$.

Доказательство приводить не будем.

Теорема 1′ *(переформулировка теоремы 1). Справедливы следующие утверждения:*

(a) Экспоненциальная функция не зависит от экспонент и логарифмов, которые уже введены, тогда и только когда, когда её аргумент не может быть представлен в виде линейной комбинации с рациональными коэффициентами логарифмов и аргументов экспонент введённых ранее; наличие такой линейной комбинации означает, что новая экспонента является произведением степеней введённых ранее экспонент и аргументов логарифмов.

(b) Логарифмическая функция не зависит от экспонент и логарифмов, которые уже введены, тогда и только тогда, когда её аргумент не может быть представлен в виде произведения экспонент с рациональными коэффициентами и аргументов логарифмов, введённых ранее. Наличие такого произведения означает,что новй логарифм – линейная комбинация с рациональными коэффициентами логарифмов и аргументов экспонент, введённых ранее.

12. Представление матриц *12.1. Виды представлений*

Матрица (вообще говоря с элементами, являющимис аналитическими выражениями) имеет вид

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nk} \end{pmatrix}; \tag{12.1}$$

здесь a_{ij} – некоторые аналитические выражения, n, k – натуральные числа.

Представление (12.1) кратко записывается в виде

$$A = (a_{ij})_{\substack{i=1,\dots,n \\ j=1,\dots,k}}. \tag{12.2}$$

Если n и k явно заданные натуральные числа, то запись может быть более конкретной. Например, если $n = 2, k = 3$, то возможна запись

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}. \tag{12.3}$$

Проиллюстрируем на примере выриант записи матрицы (12.3) в том случае, когда элементы заданы явно

$$A = \begin{pmatrix} \sin x & \sin y & \sin(x+y) \\ \cos x & \cos(a+b) & \sin x \end{pmatrix}. \tag{12.4}$$

Желательно, чтобы САВ имела все указанные формулами (12.1) – (12.4) представления. Однако, наиболее употребительны записи, даваемые правыми частями равенств (12.3) –(12.4); такие записи называются явными представлениями матриц. Кроме того, употребляются односимвольные представления матриц, даваемые в упомянутых выше формулах (12.1) – (12.4) левой частью равенств, т.е. в наших примерах – символом A; такие представления называются неявными представлениями.

Заметим, что умножение для матриц, вообще говоря, не коммутативно. Поэтому в рациональных выражениях с участием неявных представлений матриц требуется специальное объявление, в котором указывается перечень некоммутирующих объектов, неявно представляющих матрицы. Иногда удобно ввести специальный

символ для умножения матриц (символ некоммутативного умножения), однако, этот подход удачен в простых случаях, в более сложных случаях упомянутый выше перечень – более эффективное средство.

12.2. Плотные матрицы

Плотными матрицами принято называть матрицы с большим количеством ненулевых элементов (конечно, это нестрогое определение; само понятие носит субъективный характер).

Плотные матирцы представляют в виде прямоугольной таблицы или списка списков, или другими подходящими для используемого языка средствами.

Сложение и умножение двух $n \times n$-матриц требует $O(n^2)$ и $O(n^3)$ операций соответственно. Имеются более быстрые методы (например, для умножения – алгоритм Штрассена), но они эффективны лишь при больших n (например, алгоритм Штрассена сложности $O(n^{\log_2 7})$ даёт 18%-й выигрыш лишь при $n \geq 100$), а потому они пока не применяются в CAB.

Если говорить об обращении матриц, то прежде всего надо отметить, что результат – обычно весьма громоздкое выражение, и поэтому нужно избегать обращения матриц. Положительным моментом в компъютерной алгебре является то, что как правило не возникает проблем чиленной неустойчивости, ибо вычисления проводятся точно.

Проиллюстрируем сложность вычисления обратной матрицы на примере 3×3 матрицы с простыми элементами

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix}. \tag{12.5}$$

Очевидно

$$\det A = a(ek - fh) - b(dk - gh) + c(dh - ge), \tag{12.6}$$

а алгебраические дополнения, необходимые для вычисления элементов первого столбца обратной матрицы суть

$$\begin{pmatrix} ek - fh & \dots \\ -(dk - fg) & \dots \\ dh - ge & \dots \end{pmatrix} \frac{1}{\det A} \tag{12.7}$$

(упомянутые алгебраические дополнения записаны в столбце искомой обратной матрицы, невычисленные элементы отмечены многоточиями).

Определитель общей матрицы четвёртого порядка займёт 3 – 4 строки, а обратная матрица займёт несколько страниц. Конечно в процессе вычислений можно ввести промежуточные обозначения, но это не изменит дело в окончательном результате (если он необходим в развёрнутом виде). Правда, могут встретиться ситуации, когда введение удачных обозначений очень полезно, например, в случае клеточной (блочной) матрицы вида

$$\begin{pmatrix} M & M \\ M & M \end{pmatrix}, \tag{12.8}$$

где M – квадратная матрица. Определитель матрицы (12.8) равен нулю какова бы ни была матрица M.

Другая проблема состоит в том, что при вычислении определителя или обратной матрицы может понадобиться деление, которое в кольце может оказаться невыполнимым, хотя результирующий объект (обратная матрица) корректно определён. Так, например, не удастся воспользоваться методом исключения с делением на 5 или на 2 при вычислении определителя матрицы

$$\begin{pmatrix} 5 & 2 \\ 2 & 5 \end{pmatrix} \tag{12.9}$$

в кольце вычетов по модулю 10, хотя результирующий объект – определитель матрицы (12.9) существует и равен 1.

В тех же случаях, когда деление возможно, вся реализация затруднительна из-за необходимости постоянно вычислять НОД (без этих вычислений промежуточные результаты катастрофически разрастаются).

Барейс [Bareiss,1968] предложил такую модификацию исключения Гаусса, в которой каждое деление в кольце должно давать результат из того же кольца, а не дробь. Этот метод используется часто в компъютерной алгебре, если кольцо – область целостности.

При вычислении определителя применение метода Крамера приводит к $O(n{\cdot}n!)$ операций вместо $O(n^3)$ в алгоритме гауссова исключения, поэтому он относится к весьма неэффективным методикам.

Однако учёт необходмости постоянно вычислять НОД и приводить подобные члены позволяет сделать заключение, что алгоритм гауссова исключения по числу операций в ряде случаев приближается к методу Крамера.

Представляется, что для матриц, элементами которых являются разрежённые многочлены нескольких переменных, этот метод более быстрый, чем метод Гауссова исключения[19].

12.3. Алгоритм Барейса

Барейс предложил целое семейство методов, где все необходимые деления выполняются точно. Это решает проблему отыскания алгоритма, не требующего вычислений с дробями.

Фактически простейший вариант был известен ещё Жордану и основан на обобщениях тождества Сильвестра.

Пусть $a_{i,j}^{(k)}$ – определитель вида

$$a_{i,j}^{(k)} = \begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,k} & a_{1,j} \\ a_{2,1} & a_{2,2} & \dots & a_{2,k} & a_{2,j} \\ \dots & \dots & \dots & \dots & \dots \\ a_{k,1} & a_{k,2} & \dots & a_{k,k} & a_{k,j} \\ a_{i,1} & a_{i,2} & \dots & a_{i,k} & a_{i,j} \end{vmatrix}. \tag{12.10}$$

В частности $a_{n,n}^{(n-1)}$ – определитель матрицы

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Тогда

$$a_{ij}^{(k)} = \frac{1}{a_{k-1\,k-1}^{(k-2)}} \begin{vmatrix} a_{kk}^{(k-1)} & a_{kj}^{(k-1)} \\ a_{ik}^{(k-1)} & a_{ij}^{(k-1)} \end{vmatrix}. \tag{12.11}$$

Поскольку упомянутые определители не содержат дробей, то это означает, что определитель правой части делится на $a_{k-1\,k-1}^{(k-2)}$.

Продемонстрируем этот метод на примере. Рассмотрим матрицу

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

[19]Уточнить формулировку задачи и дать варианты её решения (т.е. описать ситуации, в которых один метод быстрее другого).

После исключения с помощью первой строки (без деления!) получим

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22}a_{11} - a_{12}a_{21} & a_{11}a_{23} - a_{13}a_{21} \\ 0 & a_{32}a_{11} - a_{12}a_{31} & a_{33}a_{11} - a_{13}a_{31} \end{pmatrix}. \tag{12.12}$$

Следующий шаг (без деления!) приводит к матрице

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{21}a_{11} - a_{12}a_{21} & a_{11}a_{23} - a_{13}a_{21} \\ 0 & 0 & (a_{23}a_{11} - a_{13}a_{31})(a_{21}a_{11} - \\ & & a_{12}a_{21}) - (a_{11}a_{23} - \\ & & a_{13}a_{21})(a_{32}a_{11} - a_{12}a_{31}) \end{pmatrix}. \tag{12.13}$$

При раскрытии скобок в последнем элементе этой матрицы, нетрудно заметить, что несодержащее a_{11} слагаемое первого произведения только одно, а именно

$$+a_{13}a_{31}a_{12}a_{21}, \tag{12.14}$$

а несодержащее a_{11} слагаемое второго произведения тоже только одно – оно имеет вид

$$-a_{13}a_{21}a_{12}a_{31}, \tag{12.15}$$

так что при сложении (12.14) и (12.15) уничтожаются, и остаётся выражение, заведомо делящееся на a_{11}. Итак, последний элемент главной диагонали матрицы (12.13) равен

$$a_{33}a_{11}a_{22}a_{11} - a_{33}a_{11}a_{12}a_{21} - a_{13}a_{31}a_{22}a_{11} -$$

$$-(a_{11}a_{23}a_{32}a_{11} - a_{11}a_{23}a_{12}a_{31} - a_{13}a_{21}a_{32}a_{11}).$$

Это наглядно иллюстрирует формулу (12.11) в этом частном случае.

12.4. Разреженные матрицы

Методы запоминания разреженных матриц с символьными элементами аналогичны методам запоминания разреженных векторов (см. п. 6, "Плотные и разреженные представления векторов."). В частности можно использовать списки вида $\{(a_{ij}, i, j)\}$; каждый элемент такого списка содержит три объекта – значение элемента (аналитическое выражение) и два натуральных числа (номер

строки и номер столбца), указывающие положение этого элемента в матрице.

Для вычисления определителя широко применяется рекурсия, получаемая разложением определителя по строке (или столбцу). При большом числе нулевых элементов такие способы дают достаточно компактные выражения. Они применяются также для плотных матриц, т.к. позволяют использовать вычисленные ранее выражения; однако, следуе отметить, что в этом случае вычисленные на предыдущем шаге аналитические выражения требуют достаточно много места в памяти ЭВМ.

Имеется три основных способа решения системы линейных алгебраических уравнений, применяемых в САВ.

Первый из них – формулы Крамера. Этот путь состоит в том, что система уравнений

$$Ax = b, \qquad A \stackrel{def}{=} (a_{ij})_{i,j=1,\ldots,n}, \qquad b = (b)_{i=1,\ldots,n} \tag{12.16}$$

решается по формулам

$$x_j = \frac{\sum\limits_{i=1}^{n} A_{ij} b_i}{\det A}, \qquad j = 1, 2, \ldots, n, \tag{12.17}$$

где A_{ij} – алгебраическое дополнение элемента a_{ij} в матрице A. Основная задача – вычисление A_{ij} и $\det A$ – хорошо реализуется с использованием предыдущих вычислений (однако, экономя таким образом время, мы вынуждены расходовать много места для хранения промежуточных результатов).

Второй путь – использование гауссова исключения с переупорядочиванием (строк и/или столбцов). В этом случае выбирают исключаемые строки (столбцы) в соответствии с числом ненулевых элементов. Однако в процессе исключения число ненулевых элементов обрабатываемой матрицы нарастает и их количество сохраняется прежним, а именно $O(n^3)$.

Третий путь – итерационные методы, обычно применяемые для числовых матриц. Схема их применения в случае, когда элементы – аналитические выражения, та же: эквивалентными преобразовани-

ями (умножением на неособенные матрицы и представлением матрицы в виде суммы двух матриц) уранения (12.16) приводят к виду

$$x = Bx + b' \tag{12.18}$$

и применяют итерационный процесс

$$x_{n+1} = Bx_n + b', n = 0, 1, \ldots, \tag{12.19}$$

начиная с некоторого аналитического выражения x_0. При удачном выборе упомянутых эквивалентных преобразований и начального приближения x_0 несколько шагов процесса (12.19) позволят заменить начальное приближение x_0 на аналитическое выражение x_{n+1}, достаточно близкое к решению системы (12.19).

Решение вопроса о сходимости процесса (12.19) представляет довольно сложную задачу, ибо сходимость требуется проверять для всех значений рассматриваемых параметров, фигурирующих в аналитических выражениях a_{ij}. Общий критерий сходимости, как обычно, состоит в том, что

$$\|B\| \leq q < 1,$$

q – некоторое положительное число, а в качестве нормы допускается любая операторная норма в рассматриваемом (конечномерном!) пространстве.

13. Представление рядов *13.1. Ряды Тейлора*

Для получения рядов Тейлора так же, как это делается в анализе можно использовать формулу Тейлора (с вычислением производной средствами САВ) или использовать итерационный процесс. Например, разложение

$$y = \sqrt{1 + \alpha}, \tag{13.1}$$

α – малое число, $|\alpha| < 1$, можно получить решая итерациями уравнение

$$y^2 = 1 + \alpha. \tag{13.2}$$

В частности, можно представить y в виде

$$y = a_0 + a_1\alpha + a_2\alpha^2 + \ldots, \tag{13.3}$$

подставить (13.3) в (13.2) и, приравнивая коэффициенты при одинаковых степенях, и получить соответствующий алгоритм.

Естественно, подобные разложения в САВ заканчиваются конечным числом членов, так что фактически приходится работать с многочленами от α. Отличие состоит в том, что необходимо предусмотреть алгоритмы "отбрасывания высших степеней". Например, при обработке произведения

$$\sum_{i=0}^{10} a_i \alpha^i \cdot \sum_{i=0}^{10} b_i \alpha^i$$

естественно сохранить лишь степени не выше 10 (хотя получаются также степени $11, \ldots, 20$).

Можно ввести специальные алгоритмы вычисления коэффициентов результирующего разложения. Пусть, например, имеются разложения

$$A = \sum_i a_i \alpha^i, \qquad B = \sum_i b_i \alpha^i.$$

Требуется найти разложения для C

$$C = \sum_i c_i \alpha^i,$$

где C получено из A и B одной из операций $\pm, */$. Нетрудно получить формулы

$$C = A \pm B \qquad c_i = a_i \pm b_i$$

$$C = A \cdot B \qquad c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

$$C = A/B \qquad c_i = \frac{a_i - \sum\limits_{j=0}^{i-1} c_j b_{i-j}}{b_0}$$

Последнее равенство написано лишь для случая $b_0 \neq 0$, в других случаях формула другая.

Метод (восходящий к Норману) состоит в том, что коэффициент c_i вычисляется лишь в момент обращения к нему. Это значительно экономит память. Если запоминать уже проведённые вычисления $c_0, \ldots, c_{i-1}$, то вычисление c_i потребует лишь $O(i^2)$ операций (в случае деления). Заметим, что если такое запоминание не делать, то число операций будет расти по показательному закону.

13.2. Ряды Фурье

Речь идёт о рядах вида

$$f = a_0 + \sum_{j=1}^{\infty} a_j \cos jt + b_j \sin jt,$$

которые появляются во многих вопросах.

Обычно ограничиваются конечным числом слагаемых, причём основная проблема состоит в усечении, ибо нет очевидного способа определять порядок слагаемых.

Здесь возможно несколько вариантов, главными из которых являются

a/ усечение "по частоте", т.е. отбрасывание членов с $j > n$, n – заданное число,

b/ усечение "по амплитуде": если известно, что $|a_j|$ и $|b_j|$ убывают по определённому закону до нуля, то по заданному $\varepsilon > 0$ находят $n = n(\varepsilon)$ так, что при $j > n(\varepsilon)$ $|a_j| < \varepsilon$, $|b_j| < \varepsilon$.

Указанное n является границей усечения.

Замечание 1. Случай b/ проще случая a/, т.к. при действиях с рядами Фурье в этом случае можно поступать аналогично рядам Тейлора. В случае a/ трудность в том,что $\cos j_1 t \cdot \cos j_2 t \neq \cos(j_1 + j_2)t$ и

потому исчезает ясность для решения вопроса об усечении. Однако логично перейти к экспоненциальному представлению (правда, это громоздко) или действовать по каким-либо специальным правилам, диктуемым сущностью задачи.

§4. Полиномиальное упрощение

1. Постановка задачи

Основная задача, которая будет здесь рассмотрена – решение систем полиномиальных уравнений. Под полиномами здесь подразумеваются многочлены от многих переменных.

Каждая рассматриваемая система обычно может быть преобразована к более простой системе некоторыми "элементарными" преобразованиями. Вопрос состоит в выборе цепочки таких преобразований и в эквивалентности систем, полученных в этой цепочке.

Иначе говоря, вопрос в том, каким конечным списком соотношений мы должны пользоваться, и какие исходные элементы следует взять.

Как известно, идеалом в полугруппе называется множество, замкнутое относительно операции "умножения", причём "умножение"на любой его элемент приводит к элементу этого множества. Семейством образующих идеала называется множество элементов, умножением на которые элементов полугруппы можно получить все элементы идеала.

В случае кольца многочленов получаем следующие определения.

Определение 1. *Идеалом, порождённым семейством образующих называется множество линейных комбинаций этих образующих с полиномиальнами коэффициентами.*

Определение 2. *Полиномы f и g называют эквивалентными относительно идеала I, если $f - g \in I$.*

2. Редукция полиномов

Рассмотрим полиномы от переменных $x_1, \ldots, x_n$, коэффициенты которых принадлежат некоторому полю $\mathcal{K}$. Введём на множестве мономов некоторый порядок, обозначаемый символом $<$ и удовлетворяющий следующим условиям:

(a) если a, b, c – мономы, то из соотношения $a < b$ следует $ac < bc$,

(b) если a, b – мономы и $b \neq 1$, то $a < ab$.

Три упорядочения – лексикографический, степенно-лексикографический, и обратный лексикографический (как легко проверить) удовлетворяют этим условиям.

Любой полином (отличный от нулевого) можно представить в порядке убывания своих мономов

$$\sum_{i=1}^{n} a_i X_i, \qquad a_1 \neq 0,$$

где $X_i > X_{i+1}, \quad i = 1, \ldots, n$. При такой записи X_1 называется старшим мономом, а $a_1 X_1$ – старшим членом монома.

Пусть $\mathbf{g}$ — система образующих полиномиального идеала.

Определение 3. *Говорят, что полином f редуцирован относительно $\mathbf{g}$, если старший моном полинома f не делится на старшие члены полиномов из $\mathbf{g}$.*

Эквивалентным определением является следующее.

Определение 3′. *Говорят, что полином f редуцирован относительно* $\mathbf{g}$ *тогда и только тогда, когда старший моном никакой из комбинаций $f - hg_0$, где $g_0 \in \mathbf{g}$, а h – произвольный полином не меньше старшего монома полинома f.*

Замечание 1. Таким образом, утверждение "полином f редуцирован относительно $\mathbf{g}$"эквивалентно тому, что "степень"полинома f не может быть понижена вычитанием из него произведения hg_0, где $g_0 \in \mathbf{g}$, а h – произвольный полином.

Если полином f нередуцирован относительно $\mathbf{g}$, то из него можно вычесть hg_0, $g_0 \in \mathbf{g}$, h – некоторый полином, так, что в результате получится полином $f_1 = f - hg_0$, старший член которого меньше старшего монома полинома f.

Переход от f к f_1 называется редукцией f относительно $\mathbf{g}$.

Поскольку hg_i принадлежит идеалу, порождённому множеством $\mathbf{g}$, то, очевидно, f и f_1 эквивалентны относительно упомянутого идеала.

Отметим, что может быть несколько вариантов редукции (несколько редукций), приводящих к различным результатам. Например, пусть

$$\mathbf{g} = \{g_1 = x - 1, \quad g_2 = y - 2\}, \qquad f = xy.$$

Здесь имеется две редукции f относительно $\mathbf{g}$:

1) редукция с помощью g_1 даёт

$$f - yg_1 = +y,$$

2) Редукция с помощью g_2 позволяет получить

$$f - xg_2 = +2x.$$

Последовательные редукции образуют цепочку редукций для f относительно $\mathbf{g}$ (как видно из предыдущего примера такая цепочка, вообще говоря, неединственна), которая в конце концов приводит к редуцированному полиному. Очевидно, для каждого нередуцированного полинома существует конечная цепочка редукций, сводящая его к редуцированному полиному.

До сих пор речь шла о старшем мономе полинома f и о возможности построения полинома $f_1 = f - hg_0$, $g_0 \in \mathbf{g}$, так чтобы моном

из f_1 был меньше старшего монома из f. Если f редуцирован, то упомянутого полинома f_1 не существует (согласно определению), т.е. нельзя "исключить"из f старший моном с помощью $\mathbf{g}$. Однако, в этом случае иногда можно построить полином

$$\bar{f}_1 = f - \bar{h}\bar{g}_0, \qquad \bar{g}_0 \in \mathbf{g},$$

такой, что в $math\bar{s}trut f_1$ "исключены"некоторые другие мономы полинома f.

Например, если x и y подчинены порядку $y < x$, а $\mathbf{g} = \{g_0 = y - 1\}$, то полином

$$f = x + y^2 + y$$

редуцирован относительно $\mathbf{g}$ (его старший моном – x). Однако, из него можно исключить мономы y^2 и y. Действительно, умножая $y_0 = y - 1$ на y и вычитая из f, получим $\bar{f}_1 = f - yg_0 = x + 2y$, и умножая $g_0 = y-1$ на 2 и вычитая из $\bar{f}_1$, найдём $\bar{f}_2 = \bar{f}_1 - 2g_0 = x-2$. В результате получаются полиномы $\bar{f}_1$ и $\bar{f}_2$ с "меньшей линейной комбинацией".

Определение 4. *Полином f называется вполне редуцированным относительно* $\mathbf{g}$*, если ни один моном полинома f не делится ни на один старший моном элементов множества* $\mathbf{g}$*.*

3. Базисы Грёбнера

Предыдущие рассуждения наводят на мысль о том, что системой образующих идеала могут служить различные наборы элементов. Иначе говоря, можно поставить вопрос об изменении системы образующих $\mathbf{g}$ (называемой так же базисом) идеала I и о выборе системы образующих наилучшим (в некотором смысле) образом.

Определение 5. *Система образующих (или базис)* $\mathbf{g}$ *идеала I называется стандартным базисом или базисом Грёбнера, если в результате любой редукции элемента f идеала I к редуцированному полиному относительно* $\mathbf{g}$ *всегда получается нуль.*

Эквивалентным является следующее

Определение 5′. *Базисом Грёбнера (стандартным базисом) называется такое множество* $\mathbf{g}$ *образующих рассматриваемого идеала I, что любой полином f обладает единственной редуцированной относительно* $\mathbf{g}$ *формой.*

В этом случае говорят также, что редукция относительно $\mathbf{g}$ обладает свойсвом Чёрча-Россера.

В качестве примера рассмотрим идеал I, порождённый тремя полиномами

$$g_1 = x^3yz - xz^2, \tag{3.1}$$

$$g_2 = xy^2z - xyz, \tag{3.2}$$

$$g_3 = x^2y^2 - z. \tag{3.3}$$

Заметим, что в рассматриваемой ситуации (т.е. когда речь идёр о кольце полиномов) множество, на котором обращаются в нуль все полиномы идеала определяется порождающими полиномами. В данном случе все три полинома (3.1) – (3.3) обращаются в нуль, если

$$x = y = z = 0, \tag{3.4}$$

однако, не ясно, есть ли другие решения системы

$$\begin{cases} g_1 = 0, \\ g_2 = 0, \\ g_3 = 0. \end{cases} \tag{3.5}$$

Стандартный базис этого идеала (относительно лексикографического упорядочения $x > y > z$) образуют полиномы g_2, g_3, g_4, g_5, g_6, из которых g_2 и g_3 заданы формулами (3.2), (3.3), а g_4, g_5, g_6 определяются равенствами

$$g_4 = x^2yz - z^2, \tag{3.6}$$

$$g_5 = yz^2 - z^2, \tag{3.7}$$

$$g_6 = x^2z - z^3. \tag{3.8}$$

Мы не будем здесь доказывать стандартность этого базиса, однако отметим, что число элементов стандартного базиса может быть больше числа элементов исходного.

Ввиду представлений

$$g_2 = xyz(y - 1), \tag{3.9}$$

$$g_3 = x^2y^2 - z, \tag{3.10}$$

$$g_4 = z(x^2y - z), \tag{3.11}$$

$$g_5 = z^2(y-1), \tag{3.12}$$

$$g_6 = z^2(x^2 - z) \tag{3.13}$$

ясно, что $g_1 = xz(x^2y - z) = zg_4$. С другой стороны, одновременное обращение в нуль полиномов стандартного базиса

$$g_2 = 0, \qquad g_3 = 0, \qquad g_4 = 0, \qquad g_5 = 0, \qquad g_6 = 0 \tag{3.14}$$

возможно либо в случае $z = 0$ и тогда должно быть $xy = 0$, либо в случае $z \neq 0$, и тогда $y = 1, \quad x^2 - z = 0$. Итак, множество $\mathcal{N}$ нулей системы (3.14) имеет вид

$$\mathcal{N} = \{(x, y, z) | (xy = 0 \bigwedge z = 0) \bigvee (x^2 - z = 0 \bigwedge y = 1), \tag{3.15}$$

т.е. это множество состоит из двух прямых $x = 0, \quad y = 0$ плоскости (x, y) и параболы $z = x^2$ в плоскости $y = 1$, парллельной координатной плоскости (x, z).

Сформулируем несколько утверждений не приводя их доказательства.

Теорема 1. *Любой идеал обладает стандартным базисом.*

Определение 6. *Редуцированным базисом называется базис, каждый полином которого редуцирован относительно всех остальных.*

Пример. Базисы $\{x - 1, (x - 1)^2\}$ и $\{x - 1\}$ отличаются тем, что первый из них не редуцирован: после редукции первый из них превращается во второй.

Теорема 2. *Два идеала равны тогда и только тогда, когда они имеют один и тот же редуцированный стандартный базис.*

Замечание 1. Эта теорема даёт каноническое представление идеалов.

Теорема 3. *Система полиномиальных уравнений несовместна тогда и только тогда, когда соответствующий стандартный базис содержит константу.*

4. Решение системы полиномиальных уравнений

В том случае, когда интересно знать, конечно ли число решений системы полиномиальных уравнений, полезно следующее утверждение.

Теорема 4. *Если каждая переменная появляется изолированно в одном из старших членов стандартного базиса, то система*

полиномиальных уравнений в комплексной плоскости C *имеет не более конечного числа решений (т.е. если имеет решения, то их конечное число, однако может не иметь ни одного решения).*

Рассмотрим набросок доказательства. Можно определить все решения следующим способом. Пусть имеющиеся переменные $x_1, x_2, \ldots, x_n$ упорядочены:

$$x_1 > x_2 > \ldots > x_n.$$

По условию переменная x_n появляется в старшем члене одного из базисных многочленов. Поскольку остальные x_j – старше, они не могут содержаться в этом базисном многочлене, значит в нём могут содержаться лишь x_n в различных степенях и числовые коэффициенты.

Если степень рассматриваемого многолена k, то в результате получим не более чем k различных корней в C.

Теперь отыщем тот многочлен стандартного базиса, в котором появляется изолировано x_{n-1} в его старшем члене. Остальные члены могут содержать разве лишь x_{n-1} и x_n. Подставляя сюда упомянутые выше значения x_n, при каждом x_n найдём не более k_1 корней x_{n-1} рассматриваемого многочлена, где k_1 его степень по переменной x_{n-1}. Итак, общее число допустимых значений пары (x_{n-1}, x_n) не более $k_1 k$. Продолжая таким образом далее, придём к завершению доказательства теоремы 4.

Замечание 2. Нетрудно построить примеры, показывающие, что невозможно полностью отбросить предположение об изолированности. Действительно, если $x > y$ и идеал порождён полиномами

$$\{(y-1)x + (y-1), y^2 - 1\}, \tag{4.1}$$

образующими стандартный базис (проверка этого здесь не проводится), то условия теоремы 4 не выполнены, поскольку x не появляется изолированно.

Множество $\mathcal{N}$ решений системы

$$\begin{cases} (y-1)x + y - 1 = 0 \\ y^2 - 1 = 0 \end{cases} \tag{4.2}$$

состоит из множеств $\{y = 1, x$– произвольно$\}$ и $\{y = -1, x = -1\}$. Итак, здесь $\mathcal{N}$ – бесконечно.

Замечание 3. Условия теоремы 4 гарантируют нульмерность множества $\mathcal{N}$ $(\dim \mathcal{N} = 0)$. В общем случае определение размерности множества $\mathcal{N}$ – непростая задача. В последнее время достигнут значительный прогресс в этом отношении.

5. Алгоритм Бухбергера (для нахождения стандартного базиса)

Пусть x – вектор с вещественными или комплексными компонентами, $x = (x_1, \ldots, x_n)$, а α – вектор с целочисленными неотрицательными компонентами $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\alpha_i \geq 0$. Удобным оказывается обозначение

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Если $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ и $x_i < y_i$, $i = 1, 2, \ldots, n$, то пишут $x < y$, а если $x_i \leq y_i$, то принято писать $x \leq y$. Для векторов $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$ удобно ввести операцию максимума: $\max\{\alpha, \beta\}$ – это вектор, i-я компонента которого равна $\max\{\alpha_i, \beta_i\}$.

Рассмотрим неотрицательные целочисленные векторы α и β и соответствующие степени x^α и x^β с числовыми коэффициентами a и b соответственно. Наименьшим общим кратным (НОК) мономов ax^α и bx^β называется моном, определяемый равенством

$$(ax^\alpha, bx^\beta) \stackrel{def}{=} abx^{\max\{\alpha,\beta\}}. \tag{5.1}$$

Определение 7. *Пусть f и g – два ненулевых полинома со старшими членами $\widetilde{f}$ и $\widetilde{g}$, а $h = (\widetilde{f}, \widetilde{g})$. Тогда S-полиномом для f и g называется выражение*

$$S(f,g) \stackrel{def}{=} \frac{h}{\widetilde{f}} f - \frac{h}{\widetilde{g}} g. \tag{5.2}$$

Свойства S-полинома

1) S-полином – линейная комбинация мономов f и g с полиномиальными коэффициентами (ибо $\frac{h}{\widetilde{f}}$ и $\frac{h}{\widetilde{g}}$ – мономы), S лежит в любом идеале, в число порождающих элементов которого входят f и g.

2) Старшие члены полиномов $\frac{h}{\widetilde{f}}f$ и $\frac{h}{\widetilde{g}}g$ равны (они равны старшему члену полинома h) и потому в (5.2) они сокращаются.

3) Справедливы очевидные соотношения

$$S(f,f)=0, \qquad S(f,g)=-S(g,f). \tag{5.3}$$

Теорема 5. *Базис* $\mathbf{g}$ *является стандартным тогда и только тогда, когда для любой пары полиномов* f *и* g *из множества* $\mathbf{g}$ *их S-полином* $S(f,g)$ *редуцируется к нулю относительно* $\mathbf{g}$.

Эта теорема не только позволяет проверить, является ли базис стандартным, но даёт путь к построению стандартного базиса. Действительно, если при проверке оказывается, что для некоторой пары полиномов f,g стандартного базиса $S(f,g)\neq 0$, то полином $S(f,g)$ присоединяют к $\mathbf{g}$. Это приводит к увеличению числа S-полиномов, равенство нулю которых нужно проверять. Продолжение этой процедуры приведёт к дальнейшему расширению множества $\mathbf{g}$.

Проиллюстрируем процесс построения стандартного базиса на примере, считая, что $x>y>z$ и

$$\mathbf{g}=\{g_1,g_2,g_3\}, \tag{5.4}$$

где

$$g_1=x^3yz-xz^2, \tag{5.5}$$

$$g_2=xy^2z-xyz, \tag{5.6}$$

$$g_3=x^2y^2-z. \tag{5.7}$$

Обозначая волной старшие члены полиномов имеем

$$\widetilde{g_2}=xy^2z, \qquad \widetilde{g_3}=x^2y^2 \tag{5.8}$$

и потому

$$h_{23}\overset{def}{=}\mathrm{HOK}(\widetilde{g_2},\widetilde{g_3})=x^2y^2z, \tag{5.9}$$

а значит согласно формуле

$$S(g_2,g_3)=\frac{h_{23}}{\widetilde{g_2}}g_2-\frac{h_23}{\widetilde{g_3}}g_3=xg_2-zg_3,$$

итак

$$S(g_2, g_3) = x(xy^2z - xyz) - z(x^2y^2 - z) = -x^2yz + z^2. \qquad (5.10)$$

Очевидно, этот отличный от нулевого полином редуцирован относительно $\mathbf{g}$, и поэтому базис $\mathbf{g}$ нестандартный. Присоединим его к $\mathbf{g}$ в качестве четвёртого полинома

$$g_4 = -x^2yz + z^2. \qquad (5.11)$$

Теперь $\mathbf{g}$ содержит четыре полинома (5.5) – (5.7), (5.11). Для упрощения ситуации заметим, что $g_1 = xg_4$, так что идеал не изменится, если g_1 удалить из $\mathbf{g}$. Итак, пусть в $\mathbf{g}$ лишь следующие три полинома

$$g_2 = xy^2z - xyz, \qquad (5.11)$$

$$g_3 = x^2y^2 - z. \qquad (5.12)$$

$$g_4 = -x^2yz + z^2. \qquad (5.13)$$

Нам остаётся рассмотреть теперь лишь два S-полинома, а именно $S(g_2, g_4)$ и $S(g_3, g_4)$ (S-полином $S(g_2, g_4)$ рассмотрен ранее, см. формулу (5.10), и в новом составе множества $\mathbf{g}$, $\mathbf{g} = \{g_2, g_3, g_4\}$, этот полином редуцируется к нулю).

Поскольку

$$\widetilde{g_2} = xy^2z, \quad \widetilde{g_4} = -x^2y^2z, \quad h_{24} = -x^2y^2z,$$

$$\frac{h_{24}}{\widetilde{g_2}} = -x, \frac{h_{24}}{\widetilde{g_4}} = y,$$

то

$$S(g_2, g_4) = \frac{h_{24}}{\widetilde{g_2}} g_2 - \frac{h_{24}}{\widetilde{g_4}} g_4 =$$

$$= -x(xy^2z - xuz) - y(-x^2yz + z^2) =$$

$$= -x^2y^2z + x^2yz + x^2y^2z - yz^2 = x^2yz - yz^2.$$

Полученный полином упрощается добавлением g_4, а именно

$$S(g_2, g_4) + g_4 = z^2 - yz^2. \qquad (5.14)$$

Присоединяя (5.14) с обратным знаком к множеству $\mathbf{g}$, имеем

$$\mathbf{g} = \{g_2, g_3, g_4, g_5\}, \qquad (5.15)$$

где g_2, g_3, g_4 даются формулами (5.11) – (5.13), а g_5 – формулой

$$g_5 = z^2 y - z^2. \tag{5.16}$$

Теперь следует рассмотреть S-полиномы

$$S(g_3, g_4), \quad S(g_2, g_5), \quad S(g_3, g_5), \quad S(g_4, g_5). \tag{5.17}$$

Имеем

$$\widetilde{g_3} = x^2 y^2, \quad \widetilde{g_4} = -x^2 yz,$$
$$h_{34} = -x^2 y^2 z, \quad \frac{h_{34}}{\widetilde{g_3}} = -z, \quad \frac{h_{34}}{\widetilde{g_4}} = y,$$

так что

$$S(g_3, g_4) = -z(x^2 y^2 - z) - y(-x^2 yz + z^2) = z^2 - yz^2, \tag{5.18}$$

и этот полином редуцируется к нуля (добавлением g_5):

$$S(g_3, g_4) + g_5 = 0. \tag{5.19}$$

Далее

$$\widetilde{g_2} = xy^2 z, \quad \widetilde{g_5} = yz^2, \quad h_{25} = xy^2 z^2,$$
$$\frac{h_{25}}{\widetilde{g_2}} = z, \quad \frac{h_{25}}{\widetilde{g_5}} = xy,$$
$$S(g_2, g_5) = zg_2 - xyg_5 = z(xy^2 z - xyz) -$$
$$-xy(z^2 y - z^2) = -xyz^2 + xuz^2 = 0.$$

Теперь находим $S(g_4, g_5)$:

$$\widetilde{g_4} = -x^y z, \quad \widetilde{g_5} = yz^2, \quad h_{45} = -x^2 yz^2,$$
$$d\frac{h_{45}}{\widetilde{g_4}} = z, \quad \frac{h_{45}}{\widetilde{g_5}} = -x^2,$$
$$S(g_4, g_5) = zg_4 + x^2 g_5 =$$
$$= z(-x^2 yz + z^2) + x^2(z^2 y - z^2) = z^3 - x^2 z^2. \tag{5.21}$$

Этот полином отличен от нуля и его следует добавить в $\mathbf{g}$; его будем обозначать g_6.

Итак, теперь $\mathbf{g}$ состоит из полиномов

$$g_2 = xy^2 z - xyz, \tag{5.22}$$

$$g_3 = x^2y^2 - z. \tag{5.23}$$

$$g_4 = -x^2yz + z^2, \tag{5.24}$$

$$g_5 = z^2y - z^2, \tag{5.25}$$

$$g_6 = -x^2z^2 + z^3. \tag{5.26}$$

Нетрудно проверить, что S-полиномы

$$S(g_3, g_5), \quad S(g_2, g_6), \quad S(g_3, g_6), \quad S(g_4, g_6), \quad S(g_5, g_6)$$

редуцируется в $\mathbf{g}$ к нулю. Таким образом базис (5.22) – (5.26) является стандартным базисом рассматриваемого идеала.

Замечание 4. Этот пример показывает, что отыскание стандартного базиса может быть весьма трудоёмким делом и полезны были бы те или иные методы оптимизации. Можно исключить некоторые S-полиномы из рассмотрения, используя следующий факт (критерий Бухбергера): если $S(f, h)$ и $S(g, h)$ редуцируется к нулю в $\mathbf{g}$, и старший моном полинома h делит наибольшее общее кратное НОК$(\widetilde{f}, \widetilde{g})$ старших мономов $\widetilde{f}, \widetilde{g}$ полиномов f и g, то $S(f, g)$ редуцируется к нулю (т.е. его можно не рассматривать).

Остаётся вопрос о наиболее рациональном порядке рассмотрения S-полиномов для полиномов множества $\mathbf{g}$ и о сложности таких вычислений. Показано, что сложность вычисления стандартного базиса (объём памяти) растёт экспоненциально с ростом числа переменных.

В случае двух переменных показано, что если все данные имеют степени ограниченные числом d, то степени элементов стандартного базиса ограничены числом $2d - 1$ при использовании степенно-логарифмического порядка, а число элементов стандартного базиса не превосходит $k + 1$, где k – минимум стпеней старших мономов всех данных (в примере k=4).

Замечание 5. Алгоритм Бухбергера в случае одной переменной и двух полиномов эквивалентен отысканию НОД этих полиномов. Любой S-полином это потином наивысшей степени минус второй полином с некоторым множителем, исключающий наивысшую степень. Расширение базиса с помощью этого S-полинома позволяет отбросить полином старшей степени.

Для случая нескольких переменных и линейных полиномов алгоритм Бухбергера соответствует исключению Гаусса, поскольку

$S(f_1, f_2)$ – линейная комбинация (с постоянными коэффициентами) полиномов f_1 и f_2, исключающая старшую переменную (здесь следует считать $S(f_1, f_2) = 0$, если f_1 и f_2 не содержит одну и ту же старшую переменную). Полином f_2 редуцируется к нулю относительно f_1 и $S(f_1, f_2)$ и потому он исключается (может быть отброшен). Так исключается переменная из всех уравнений; затем продолжать вычисления со следущей переменной. В конце концов приходим к треугольной матрице.

§5. Формальное интегрирование

1. Постановка задачи

Под формальным интегрированием далее подразумевается вычисление неопределённого интеграла.

В современном курсе математического анализа и в связанных с ним областях математики и техники главное место занимают различные виды определённого интеграла: одномерный, двумерный и трёхмерный интегралы (а в некоторых случаях n-мерные интегралы при $n \geq 4$), интегралы по контуру и по поверхностям; сюда же примыкают различные несобственные интегралы: от неограниченных функций, по неограниченным областям, сингулярные интегралы и т.п. В простейшем случае результаты интегрирования представляют собой

число, однако часто подынтегратьная функция зависит от параметров, так что результат представляет собой функцию этих параметров: последние в дальнейшем подбирают из тех или иных соображений. Эти интегралы являются концом целой цепочки определений, в каждом звене которой определяются интегралы на основании предыдущего определения, а для вычисления результата приходится научиться вычислять интегралы во всех звеньях упомянутой цепочки. В начале каждой такой цепочки лежит определённый интеграл по отрезку вещественной оси; вычисление этого интеграла производится по формуле Ньютона

$$\int\_a^b f(x)\,dx = F(b) - F(a), \tag{1.1}$$

где F – первообразная функция для подынтегральной функции f. Выбор первообразной здесь безразличен, ибо как известно все они

отличаются на константу, поскольку (по определению) выполнено соотношение

$$F' = f. \tag{1.2}$$

Семейство таких первообразных называют неопределённым интегрлом, и пишут

$$\int f(x)\,dx = F(x) + C, \tag{1.3}$$

где C – произвольная постоянная.

Итак определённый интеграл (1.1) получается из первообразной $F(x)$ вычислением разности

$$F(b) - F(a)$$

, называемой "двойной подстановкой"для $F(x)$ в точках a и b, и обозначаемой

$$F|_a^b = F(b) - F(a). \tag{1.4}$$

Почему столь большую роль отводят интегралам? Это связано с отысканием (быть может приближённым) обратных операторов ряда задач (дифференциальных уравнений с соответствующими краевыми условиями). Нетрудно видеть, что задача интегрирования является обратной к задаче дифференцирования (см. формулы (1.2), (1.3)). На практике же известно, что процесс интегрирования весьма сложен (вообще, опыт показывает, что обратная операция сложнее исходной: вычитание сложнее сложения, деление сложнее умножения, извлечение корня сложнее возведения в натуральную степень и т.д.).

Действительно, дифференцирование подчиняется довольно простм и легко алгоритмизуемым правилам; например, для двух функций F и $\mathbf{g}$ одной переменной имеем

$$(F \pm \mathbf{g})' = F' \pm \mathbf{g}', \tag{1.5}$$

$$(F\mathbf{g})' = F'\mathbf{g} + F\mathbf{g}', \tag{1.6}$$

$$\left(\frac{F}{\mathbf{g}}\right)' = \frac{F'\mathbf{g} - F\mathbf{g}'}{\mathbf{g}^2}, \tag{1.7}$$

$$(F(\mathbf{g}(t)))' = F'(\mathbf{g}(t)) \cdot \mathbf{g}'(t). \tag{1.8}$$

Эти правила фактически позволяют продифференцировать любую заданную функцию. Эти правила дополняются таблицей производных от элементарных функций. Благодаря прозрачности алгоритма дифференцирования нетрудно включить операцию дифференцирования в САВ.

Главная проблема при дифференцировании – своевременное упрощение промежуточных результатов, ибо иначе может произойти быстрый рост необходимой для вычислений памяти. В частности, дифференцирование выражения $2*x^2+1$ без упрощений принимает вид $0 + x^2 + 2 * 2 * x^{2-1} * 1 + 0$.

В противоположность этому для интегрирования более или менее общих правил не сущесвует, кроме разве лишь равенства

$$\int (\lambda f + \mu g)\, dx = \lambda \int f\, dx + \mu \int g\, dx, \tag{1.9}$$

где λ и μ – числовые константы. Остальные правила носят индивидуальный и скорее искуственный характер, и чаще всего приходится просто исходить из определения интеграла (т.е. из формул (1.2), (1.3)). Используя это, составляют таблицу интегралов, фактически представляющую собой равенства из таблицы производных, переписанные в обратном порядке. Однако, из-за отсутствия правил, аналогичных правилам (1.6) – (1.8) вычисление интеграла от произведения, частного или суперпозиции двух функций, интегралы от которых имеются в упомянутой таблице, может оказаться существенной проблемой.

Вообще здесь возникает вопрос о принципиальной возможности представления интеграла в том классе функций, которому принадлежит подынтегральная функция, и часто ответ на этот вопрос отрицателен.

В частности, доказано, что неопределённые интегралы от функций e^{-x^2}, $\frac{\sin x}{x}$ не могут быть выражены с помощью четырёх арифметических действий и суперпозиции функций, к которым причисляют

$$x^a, \quad a^x, \quad \sin x, \quad \cos x, \quad \ln x, \quad \mathrm{abs}|x|$$

, а также обратные тригонометрические функции. Интегралы от них называют "неберущимися"в виде конечной комбинации элементарных функций.

Таким образом, часто встречающиеся функции, выражаемые интегралами

$$\int e^{-x^2}\,dx, \qquad \int \frac{\sin x}{x}\,dx$$

изучают отдельно и называют "специальными функциями". Конечно, эти интегралы можно представить в виде бесконечных комбинаций элементарных функций (например, в виде сходящихся степенных рядов), так что изучение их не представляется чем-то трансцендентным: имеется большое число книг и справочников, в которых даны все необходимые сведения об этих и о ряде других функций такого рода.

Однако, дело этим невозможно исчерпать, ибо на практике постоянно встречаются новые неберущиеся интегралы. Каждый может легко придумать почти наверняка неберущийся интеграл, создав суперпозицию двух элементарных функций, что-нибудь вроде $\sin(x^2)$, или $\mathrm{arctg} e^x/x$ (можно быть почти уверенным, что интегралы от них не выражаются в виде конечной комбинации элементарных функций).

Алгоритмически трудность состоит в том, что априори неизвестно, какую комбинацию методов нужно применить, чтобы найти данный интеграл, мы также не знаем можно ли это сделать в принципе, располагая данным набором "элементарных"функций. Однако, к настоящему моменту в значительной степени эти трудности преодолены и существует развитая теория алгоритмического интегрирования. В связи с развитием этой теории следует упомянуть прежде всего Мозеса и Бухбергера.

Определение 1. *Для двух данных классов функций A и B задача интегрирования состоит в том, чтобы найти алгоритм, который для любого элемента $a \in A$ либо выдаёт элемент $b \in B$ такой, что $b' = a$, либо доказывает, что в B не существует такого элемента, для которого верно указанное равенство.*

Если, например, $A = \mathrm{Q}(x)$, $B = \mathrm{Q}(x)$ – множество рациональных дробей, то при $a = \frac{1}{x^2}$ ответом алгоритма должна быть функция $b - \frac{1}{x}$, а для $a = \frac{1}{x}$ ответом должно быть: нужной функции в множестве B не существует.

Конечно не для любых двух классов A и B проблема интегрирования разрешима (впрочем, об этом говорилось и выше в этом

пункте); в частности она не разрешима в классах

$$A = B = \ \mathrm{Q}(i, \pi, \exp, \log, \mathrm{abs})$$

. Заметим, что более разочаровывающим утверждением является тот факт, что в $\mathrm{Q}(i, \pi, \exp, \log, \mathrm{abs})$ неразрешима и проблема тождества (т.е. вообще говоря, невозможно определить является ли полученная константа нулём). В дальнейшем не будем акцентировать внимания на разрешимости этой проблемы: будем считать, что этот класс функций является эффективным, т.е. что проблема тождества в нём разрешима.

2. Прямой метод интегрирования рациональных дробей

Если рациональная дробь $P(x)/Q(x)$ – правильная, т.е. $\deg P < \deg Q$, то для её инрегрирования используется разложение на простейшие дроби

$$\frac{P(x)}{Q(x)} = \sum_{i=1}^{n} \sum_{j=1}^{n_i} \frac{b_{ij}}{(x - a_i)^j}, \tag{2.1}$$

где $_i$ – корень многочлена $Q(x)$ кратности n_i, т.е.

$$Q(x) = \prod_{i=1}^{n} (x - a_i)_i^n, \tag{2.2}$$

а b_{ij} – числа.

Известно, что представление (2.1) существует и единственно.

После интегрирования тождества (2.1) получим

$$\int \frac{P}{Q} = \sum_{i=1}^{n} b_{i1} \log |x - a_i| - \sum_{i=1}^{n} \sum_{j=2}^{n_i} \frac{b_{ij}}{(j-1)(x - a_i)^{j-1}}. \tag{2.3}$$

Итак, результат лежит в поле $C(x, \log)$.

Отметим недостатки процесса разложения (2.3):

1) разложение на множители многочлена $Q(x)$ не всегда удаётся сделать без алгебраических расширений исходного поля, что весьма нежелательно,

2) разложение на множители полинома $Q(x)$ высокой степени – дорогостоящая операция,

3) достаточно сложно найти предтавление в виде суммы простейших дробей.

Заметим, что некоторые интегралы от рациональных дробей легко находятся без использования представления (2.1). Например, очевидно

$$\int \frac{8x^7+2x+1}{x^8+x^2+x}\,dx = \ln|x^8+x^2+x| + C,$$

$$\int \frac{5x^4+60x^3+255x^2+450x+274}{x^5+15x^4+85x^3+225x^2+274x+120}\,dx =$$
$$= \log(x+1)(x+2)(x+3)(x+4)(x+5) + C,$$

$$\int \frac{5x^4+1}{(x^5+x+1)^2}\,dx = -\frac{1}{x^5+x+1},$$

$$\int \frac{5x^4+1}{x^5+x+1}\,dx = \log(x^5+x+1).$$

Приведённые примеры показывают, что даже в тех случаях, когда знаменатель не разлагается над полем Q, иногда возможно провести интегрирование.

Отсюда вытекает задача: найти алгоритм интегрирования рациональных функций, который работает только с теми алгебраическими величинами, которые необходимы для отыскания интеграла.

3. Разложение на свободные от квадратов множители

Пусть $P(x)$ – многочлен из кольца $\mathrm{R}[x]$, где R – область целостности нулевой характеристики (например, колцо целых чисел Z), где $P(x)$ имеет вид

$$P(x) = \prod_{i=1}^{n} (x-a_i)_i^n, \tag{3.1}$$

где n_i – натуральные числа, a_i – корни многочлена, являющиеся алгебраическими величинами над кольцом R.

Произведение первых степеней сомножителей $(x-a_i)$ кратности j обозначим $P_{(j)}(x)$, так что

$$P_{(j)}(x) = \prod_{\substack{i \\ i\in\{1,\dots,n\}, \\ n_i=j}} (x-a_i), \qquad j = 1,2,\dots,\max_{i=1,\dots,n} n_i. \tag{3.2}$$

Очевидно

$$P(x) = \prod_{j=1}^{\max\limits_{i=1,\ldots,n} n_i} P_{(j)}^{j}(x). \tag{3.3}$$

Покажем, что получение многочленов $P_{(j)}(x)$ (а тем самым и разложения (3.3)) не требует выхода из кольца R (т.е. при построении многочленов $P_{(j)}$ не требуется использовать алгебраические величины над кольцом R, в том числе не требуются и корни a_i многочлена P(x)).

Из формулы (3.1) ясно, что производная многочлена $P(x)$ имеет вид

$$P'(x) = \sum_{i=1}^{n} \left[n_i (x - a_i)^{n_i - 1} \prod_{\substack{j=1 \\ i \neq j}}^{n} (x - a_j)_j^n \right]. \tag{3.4}$$

Каждое слагемое в (3.4) делится на произведение

$$\prod_{j=1}^{n} (x - a_j)^{n_j - 1}, \tag{3.5}$$

а на степень $(x - a_j)^{n_j}$ делятся все слагаемые кроме одного, $j = 1, \ldots, n$. Отсюда ясно, что (3.5) представляет НОД(P, P'),

$$R \overset{def}{=} \text{НОД}(P, P') = \prod_{j=1}^{n} (x - a_j)^{n_j - 1}. \tag{3.6}$$

Из (3.1) и (3.6) следует, что

$$Q \overset{def}{=} P/\text{НОД}(P, P') = \prod_{j=1}^{n} (x - a_j). \tag{3.7}$$

Далее, найдём

$$\text{НОД}(Q, \text{НОД}(P, P')) = \prod_{\substack{j \in \{1,\ldots,n\} \\ n_j > 1}} (x - a_j). \tag{3.8}$$

Из (3.7) и (3.8) получим

$$P_{(1)}(x) = Q/\text{НОД}(Q, \text{НОД}(P, P')) = \prod_{\substack{j \in \{1,\ldots,n\} \\ n_j = 1}} (x - a_j). \tag{3.9}$$

Равенство (3.9) показывает, что произведение некратных сомножителей можно получить не выходя из кольца $\mathrm{R}[x]$, ибо его левая часть получается лишь операциями дифференцирования многочлена из $\mathrm{R}[x]$, отыскания НОД двух многочленов из $\mathrm{R}[x]$ и деления многочленов из $\mathrm{R}[x]$.

Заметим также, что в процессе вычислений получено произведение $R(x)$ кратных сомножителей многочлена $P(x)$ в степенях на единицу меньших, чем в многочлене $P(x)$ (см. формулу (3.6)). Если теперь в предыдущих рассуждениях заменить $P(x)$ на $R(x)$, то аналогично (3.9) мы найдем произведение $P_{(2)}(x)$ сомножителей (в первых степенях) многочлена $P(x)$ с кратностью два, причём опять-таки это произведение будет получено без выхода из кольца $\mathrm{R}[x]$.

Аналогичным образом получаются все произведения $P_{(j)}(x), \quad j = 1, 2, \ldots, \max\limits_{i=1,\ldots,n} n_j$, без выхода из кольца $\mathrm{R}[x]$, что и требовалось.

Итак, не выходя из кольца $\mathrm{R}[x]$, можно получить представление многочлена $P(x)$ в виде (3.3), где у каждого многочлена $P_{(j)}(x)$ нет кратных сомножителей.

Представление (3.3) называется разложением многочлена $P(x)$ на свободные от квадратов множители.

Ассимптотически сложность разложения многочлена $P(x)$ на свободные от квадратов множители имеют тот же порядок,что и сложность вычисления НОД (правда алгоритм, предложенный выше, придётся модифицировать).

4. Расширенный алгоритм Евклида

Евклидов алгоритм вычисления НОД двух целых чисел q и r имеет вид

```
1) begin
2)   if abs(q) < abs(r) then
3)     begin
4)       t:=q;
5)       q:=r;
6)       r:=t;
7)     end; { перестановка q и r }
8)   until r ≠ 0 do
9)     begin
```

```
10)       t:=residual(q/r)
                { вычисление остатка }
11)       q:=r;
12)       r:=t;
13)     end;
14)  exit (q); { выход:  q}
15) end.
```

Нетрудно видеть, что фактически тот же алгоритм справедлив для вычисления НОД многочленов q и r, если операцию abs взятия абсолютной величины заменить операцией deg вычисления степени многочлена.

С другой стороны, рассматриваемый алгоритм позволяет определить представление НОД в виде линейной комбинации исходных данных. Для этого применим этот алгоритм с использованием скобок [...] для обозначения пары значений, и с использованием Q и R для представления текущих значений q и r в терминах начальных данных. Получится так называемый "Расширенный алгоритм Евклида".

```
1) begin
2)   if abs(q) < abs(r) then
3)     begin
4)       t:=q;
5)       q:=r;
6)       r:=t;
7)       Q:=[0,1];
8)       R:=[1,0];
9)     end
10)   else
11)     begin
12)       Q:=[1,0];
13)       R:=[0,1];
14)     end;
15)   until r ≠ 0 do
16)     begin
17)       t:=residual(q/r)
                { вычисление остатка }
18)       T:=Q-quotient(q/r)R;
```

```
19)       q:=r;
20)       r:=t;
21)       Q:=R;
22)       R:=T;
23)     end;
24)  exit (q,Q);
       { выход: в  q имеется НОД(q,r)}
       { в  Q содержится пара [a,b]  }
       { такая, что НОД= aq+br   }
25) end.
```

Задание 1. Для более глубокого усвоения алгоритма предлагается его применить для случая $q = 12, \quad r = 10$.

Первое значение, вырабатываемое этим алгоритмом – НОД исходных чисел $q = 12$ и $r = 10$, а второе значение – пара чисел $[a, b]$ такая, что

$$\text{НОД}(q, r) = aq + br. \qquad (*)$$

Соотношение (*) называют тождеством Безу.

Задание 2. Применить расширенный алгоритм Евклида к многочленам

$$q = 2x^2 + 4x + 2 \qquad \text{и} \qquad r = x^2 - 1 :$$

Последовательно получим:

$$\langle 2x^2 + 4x + 2 = (x^2 - 1) \cdot 2 + 4x + 4 \rangle$$

При проверке тождества Безу имеем

$$\text{НОД}(q, r) = aq + br \qquad (4.1)$$

$$4x + 4 \stackrel{?}{=} 1 \cdot (2x^2 + 4x + 2) + (-2)(x^2 - 1)$$

Замечание. Если q и r – многочлены с целыми коэффициентами, то НОД(q, r) – многочлен сцелыми коэффициентами, однако, промежуточные вычисления могут иметь нецелые коэффициенты (см. R и T на предпоследнем этапе вычислений).

5. Интерполирование методом Эрмита

Этот метод позволяет определять рациональную часть интеграла рациональной функции без использования дополнительных величин (т.е. без выхода из поля, где лежат коэффициенты интегрируемой функции).

Пусть рассматривается интегрирование правиль- ной рациональной дроби $P(x)/Q(x)$, причём многочлен $Q(x)$ представлен разложением на свободные от квадратов множители вида

$$Q(x)\prod_{i=1}^{n} Q_{(i)}^{i}(x), \tag{5.1}$$

где многочлены $Q_{(i)}(x)$ взаимно просты и представляют собой произведения первых степеней всех биномов вида $x-a_j$, где a_j – корни Q(x) кратности i (см. пункт 3 этого параграфа). Можно показать, что в этом случае справедливо представление

$$\frac{P(x)}{Q(x)} = \sum_{i=1}^{n} \frac{P_i(x)}{Q_{(i)}^{i}(x)}, \tag{5.2}$$

которое называется разложением на простейшие, ибо знаменатели дробей в сумме взаимно просты.

Итак, дело сводится к интегрированию дробей вида $P_i/Q_{(i)}^{i}$. Используем тождество Безу по отношению к (взаимно простым!) многочленам $Q_{(i)}$ и $Q'_{(i)}$,

$$aQ_{(i)} + bQ'_{(i)} = 1. \tag{5.3}$$

Тогда можно написать

$$\int \frac{P_i(x)}{[Q_{(i)}(x)]^i}\,dx = \int \frac{P_i(x)[aQ_{(i)} + bQ'_{(i)}]}{Q_{(i)}^{i}}\,dx =$$

$$= \int \frac{aP_i}{Q_{(i)}^{i-1}}\,dx + \int \frac{bP_iQ(i)'}{Q_{(i)}^{i}}\,dx. \tag{5.4}$$

Используя интегрирование по частям в последнем интеграле, найдём (при $i \neq 1$)

$$\int \frac{bP_iQ'_{(i)}}{Q_{(i)}^{i}}\,dx = \int \frac{bP_i}{-i+1}\,Q_{(i)}^{-i+1} =$$

$$= \frac{1}{-i+1}\left\{ bP_iQ_{(i)}^{-i+1} - \int \frac{bP_i)'}{Q_{(i)}^{i-1}}\,dx \right\}. \qquad (5.5)$$

Из (5.4) и (5.5) видно, что удалось понизить на единицу степень с которой входит функция $Q_{(i)}$ в знаменатель подынтегральной функции. Можно продолжать таким образом дальше, пока степень $Q_{(i)}$ в знаменателе окажется равной единице; нетрудно установить, что оставшийся интеграл будет равен сумме логарифмов.

6. Метод Горовица

Метод Эрмита имеет довольно сложный алгоритм (в него включены алгоритмы разложения на свободные от квадратов множители, разложение на простейшие дроби, тождество Безу) и потому его сложно запрограммировать. Поэтому рассмотрим метод Горовица.

Задача прежняя: представить $\int P/Q\,dx$ в виде

$$\int P/Q\,dx = P_1/Q_1 + \int P_2/Q_2\,dx, \qquad (6.1)$$

где оставшися интеграл представляется в виде суммы логарифмов.

Из предыдущего пункта следует, что многочлен Q_1 имеет те же множители, что и Q, но с показателями, уменьшенными на единицу, что многочлен Q_2 не имеет кратных сомножителей и что его сомножители – все сомножители полинома Q.

Из пункта 3 следует, что $Q_1 = \text{НОД}(Q, Q')$, и что $Q_2 = Q/\text{НОД}(Q, Q\prime)$. Тогда из определения первообразной имеем

$$\frac{P}{Q} = \left(\frac{P_1}{Q_1}\right)' + P_2/Q_2 = \frac{P_1'}{Q_1} - \frac{P_1Q_1'}{Q_1^2} + \frac{P_2}{Q_2} =$$

$$= \frac{P_1'Q_2 - P_1Q_1'Q_1^{-1}Q_2 + P_2Q_1}{Q}. \qquad (6.2)$$

Очевидно многочлен $Q_1'Q_2$ делится на Q_1 без остатка (ясно что отношение $Q_1\prime/Q_1$ может быть представлено в виде суммы дробей, в знаменателях которой содержатся лишь первые степени биномов $x-a_i$, где a_i – корень многочлена Q, а Q_2 – произведение всех таких биномов). Обозначая результат деления через S, из (6.2) приходим к соотношению

$$P_1'Q_2 - P_1S + P_2Q_1 = P. \qquad (6.3)$$

Здесь неизвестными следует считать P_1 и P_2. Заметим, что степени многочленов P_1 и P_2 меньше степеней m и n многочленов Q_1 и Q_2 соответственно, так что

$$P_1 = \sum_{i=0}^{m-1} a_i x^i, \qquad P_2 = \sum_{i=0}^{n-1} b_i x^i.$$

Соотношение (6.3) записывается в виде системы $m+n$ уравнений с $m+n$ неизвестными, которая имеет единственное решение. Таким образом задача представления (6.1) решена.

7. Обработка логарифмической части

Вычисление второго слагаемого правой части (6.1) состоит в разложении Q_2 на множители, что после интегрирования приводит в конечном счёте к логарифмическим слагаемым. Основная проблема в том, чтобы найти интеграл без использования каких-либо алгебраических чисел, кроме тех, которые необходимы для записывания результата. Вместо P_2/O_2 будем дальше писать P/Q.

Предположим, что

$$\int \frac{P}{Q}\,dx = \sum_{i=1}^{n} c_i \log v_i, \tag{7.1}$$

где в правой части используется наименьшее алгебраическое расширение, c_i – константы, v_i – рациональные функции. $v_i = P_i/Q_i$.

Поскольку $\log P_i/Q_i = \log P_i - \log Q_i$, то можно считать, что v_i – многочлены. Посколку каждый многочлен можно представить разложением на свободные от квадратов множители, то можно считать, что v_i – взаимно просты (пока что упомянутое выше минимальное расширение сохраняется). Кроме того, будем считать, что все c_i различны (одинаковые можно объединить).

Дифференцированием (7.1) найдём

$$\frac{P}{Q} = \sum_{i=1}^{n} c_i \frac{v_i'}{v_i}. \tag{7.2}$$

Ввиду сказанного (v_i свободны от квадратов, взаимно просты и никакой элемент суммы не может быть упрощён) ясно, что сокращений в (7.2) нет. Отсюда v_i совпадают с делителями многочлена

Q,

$$Q = \prod_{i=1}^{n} v_i. \tag{7.3}$$

Введём обозначение

$$u_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} v_j. \tag{7.4}$$

Очевидно, что

$$Q' = \sum_{i=1}^{n} v_i' u_i. \tag{7.5}$$

Из (7.2) получим

$$P = \sum_{i=1}^{n} c_i v_i' u_i. \tag{7.6}$$

Далее

$$v_k = \text{НОД}(Q, v_k) = \text{НОД}(P - \sum_{i=1}^{n} c_i v_i' u_i, v_k).$$

Поскольку в правой части последнего равенства все слагаемые u_i делятся на v_k кроме случая $i = k$, то

$$v_k = \text{НОД}(P - c_k v_k' u_k, v_k) =$$

$$= \text{НОД}(P - c_k \sum_{i=1}^{n} v_i' u_i, v_k) = \text{НОД}(P - c_k Q', v_k). \tag{7.8}$$

Если $l \neq k$, то

$$\text{НОД}(P - c_k Q', v_l) =$$

$$= \text{НОД}(\sum_{i=1}^{n} c_i v_i^p rime u_i - c_k \sum v_i' u_l, v_l) =$$

$$= \text{НОД}(c_l v_l' u_l - c_k v_l' u_l, v_l) = 1. \tag{7.9}$$

Равенство (7.9) верно потому, что v_l не имеет множителей общих с произведением остальных многочленов v_i).

Ввиду этих результатов имеем

$$\text{НОД}(P - c_k Q', Q) = \text{НОД}(P - c_k Q', \prod_{i=1}^{n} v_i) =$$

$$= \prod_{i=1}^{n} \text{НОД}(P - c_k Q', v_i) = \text{НОД}(P - c_k Q', v_k) = v_k. \qquad (7.10)$$

Здесь при выислении НОД использована взаимная простота многочленов v_i.

Итак, зная числа c_k можно с сохранением исходного расширения вычислить v_k. Сами же c_k это те значения y, для которых

$$\text{НОД}(P - yQ', Q) \neq 1.$$

Эти значения могут быть получены с помощью результатов, обсуждаемых в следующем пункте.

8. Результант двух многочленов

Пусть f и g – многочлены одной переменной с коэффициентами в кольце R,

$$f = \sum_{i=0}^{n} a_i x^i, \qquad g = \sum_{i=0}^{m} b_i x^i. \qquad (8.1)$$

Определение 1. *Матрицей Сильвестра многочленов f и g называется квадратная матрица S размера $m+n$ вида*

$$S = \begin{pmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & \dots & \dots & a_1 & a_0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & a_n & a_{n-1} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & b_m & b_{m-1} & \dots & b_1 & b_0 \end{pmatrix}, \qquad (8.2)$$

где первые m строк образованы сдвигом совокупности коэффициентов многочлена f, а следующие n строк образованы сдвигом коэффициентов второго многочлена g. Определитель матрицы S называется результантом многочленов f и g; он обозначается $\text{Res}(f, g)$,

$$\text{Res}(f, g) = \det S. \qquad (8.3)$$

Пример Напишем результант для многочленов

$$\begin{aligned} &f = a_3 x^3 + a_2 x^2 + a_1 x + a_0, \\ &b_x^2 + b_1 x + b_0, \end{aligned} \qquad (8.4)$$

В нашем случае $n = 3, \quad m = 2$, и поэтому первые две строки имеют вид

$$\begin{matrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0, \end{matrix}$$

а следующие три строки таковы

$$\begin{matrix} b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0. \end{matrix}$$

Итак, в данном случае результантом $R(f, g)$ многочленов (8.4) служит определитель

$$R(f,g) = \det \begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{pmatrix}.$$

Способы вычисления определителей обсуждались ранее (см. §3, пункты 12.2,12.3). Можно использовать алгоритм Евклида как вариант, или применить алгоритм Барейса.

Роль субрезультанта определяется следующим утверждением.

Теорема 1. $\mathrm{Res}(f, g) = 0$ *тогда и только тогда , когда многочлены* f *и* g *имеют общий сомножитель.*

Теорема 2. *Пусть* α_j *– корни многочлена* $f = \sum_{i=0}^{n} a_i x^i, \quad j = 1, 2, \ldots, n$, *а* β_s *– корни многочлена* $g = \sum_{i=0}^{n} b_i x^i, \quad s = 1, 2, \ldots, m$. *Тогда справедливы равенства*

$$\mathrm{Res}(f,g) = a_n^m \prod_{j=1}^{n} g(\alpha_j),$$

$$\mathrm{Res}(f,g) = (-1)^{mn} b_m^n \prod_{s=1}^{m} f(\beta_s),$$

$$\mathrm{Res}(f,g) = a_n^m b_m^n \prod_{j=1}^{n} \prod_{s=1}^{m} (\alpha_j - \beta_s).$$

Определение 2. *Дискриминантом многочлена*

$$f = \sum_{i=0}^{n} a_i x^i \tag{8.5}$$

называется выражение

$$\mathrm{Disc}(f) \stackrel{def}{=} a_n^{2n-2} \prod_{i=1}^{n} \prod_{j=1}^{n} (\alpha_i - \alpha_j), \tag{8.6}$$

где $\alpha_1, \ldots, \alpha_n$ *– корни многочлена (8.5).*

9. Интегрирование сложных функциональных образований

Понятие сложности в данном контексте весьма относительно. Здесь имеются в виду случаи, когда неопределённый интеграл не берётся в элементарных функциях. Как известно, к таким интегралам относятся

$$\int e^{-x^2}\, dx, \qquad \int \frac{\sin x}{x}\, dx \tag{9.1}$$

и т.д.

Конечно, возникает вопрос, какие функции называть элементарными. Перечень функций, обычно причисляемых к элементрными дан в нвчале этого параграфа. Возможно, кто-то скажет, что сейчас хорошо изучены и другие функции, например, функции (9.1), что служит основанием для того, чтобы причислить их к элементарным.

Обычно следуют, однако, определению, предложенному Лиувиллем.

Определение 1. *Пусть* K *– функциональное поле. Функция* Θ *называется элементарной образующей над* K*, если*

(a) функция Θ *алгебраична над* K*, т.е.* Θ *удовлетворяет полиномиальному уравнению с коэффициентами из поля* K*,*

(b) функция Θ *является экспонентной над* K*, так что в* K *существует элемент* η*, для которого*

$$\Theta' = \eta' \Theta \tag{9.2}$$

(c) функция Θ *является логарифмом над* K*, т.е. существует элемент* η*, для которого*

$$\Theta' = eta'/\eta. \tag{9.3}$$

Заметим, что формулы (9.2) и (9.3) являются алгебраической записью соотношений $\Theta = \exp \eta$ и $\Theta = \log \eta$ соответственно.

Определение 2. *Пусть K – функциональное поле. Расширение $K(\Theta_1, \ldots, \Theta_n)$поля K называется полем элементарных функций над K, если каждая функция Θ_i является элементарной образующей над K.*

Функции, принадлежащие некоторому полю элементарных функций над K, называются элементарными.

Обычно в качестве K рассматривают поле $\mathrm{C}(x)$ рациональных функций.

Примеры. Тригонометрические и обратные тригонометрические функции элементарны над полем $\mathrm{C}(x)$. Например, $\sin x = \frac{1}{2i}(e^{ix} + e^{-ix}) = \frac{1}{2i}(\Theta + \frac{1}{\Theta})$, где Θ – экспонента от ix. Далее

$$\mathrm{arctg}x = \log\left(\frac{x+i}{x-i}\right).$$

Класс элементарных над K функций обозначается $K(elem)$.

Ранее было показано, что каждая рациональная функция обладает элементарным интегралом, причём он имеет вид суммы рациональной функции (для её вычисления не нужны никакие алгебраические расширения) и логарифмов с постоянными коэффициентами.

Оказывается, имеет место значительно более общее утверждение.

Теорема (Принцип Лиувилля). *Пусть f – функция из некоторого функционального поля K. Если f обладает элементарным над K интегралом, то этот интеграл имеет следующий вид*

$$\int f\,dx = v_0 + \sum_{i=1}^{n} c_i \log v_i, \tag{9.4}$$

где v_0 – из поля K, а v_i – из его расширения $\widehat{K}$, полученного добавлением конечного числа алгебраических над K констант; далее c_i – константы из поля $\widehat{K}$.

Итак, если f интегрируема в элементарных функциях над K, то она необходимо имеет вид

$$f = v_0' + \sum_{i=1}^{n} c_i \frac{v_i'}{v_i}. \tag{9.5}$$

10. Заключительные замечания

На этом заканчивается краткое изложение теории отыскания неопределённого интеграла, ориентированный на применение САВ. Максимальность рассматриваемых полей и простота аналитических преобразований являются основными характеристиками рассмотренных алгоритмов.

Л И Т Е Р А Т У Р А

1. Д.К.Фаддеев. Лекции по алгебре. М., Наука. 1984. 416 с.

2. А.Ахо, Дж.Хопкрофт, Дж.Ульман. Построение и анализ вычислительных алгоритмов. М., Мир, 1979. 512 с.

3. Дж.Дэвенпорт, И.Сирэ, Э.Турнье. Компьютерная алгебра. М., Мир, 1991. 352 с.

4. Б.Бухбергер и др. Компьютерная алгебра: символьные и алгебраические вычисления. М., Мир, 1986. 392 с.

ДОПОЛНЕНИЕ

В данном курсе лекций повсюду предполагается, что читатель знаком с основами теории чисел, основами теории групп, теории колец и полей; тем не менее для удобства читателя далее приводятся некоторые сведения из этих теорий.

1. Кое-что из теории чисел

Наибольшее целое число, на которое делятся заданные целые числа $a, b, c, \ldots, l$ называется их *наибольшим общим делителем (кратко – НОД)* и обозначается $(a, b, c, \ldots, l)$.

Если $(a, b, c, \ldots, l) = 1$, то числа $a, b, c, \ldots, l$ называются *взаимно простыми.*

Количество чисел ряда $0, 1, 2, \ldots, a-1$, взаимно простых с числом a, называется *функцией Эйлера;* она обозначается $\phi(a)$.

Зафиксируем натуральное число m. Два целых числа a и b называются *сравнимыми по модулю* m, если остатки от их деления на m одинаковы; при этом пишут

$$a \equiv b \mod m. \tag{1.1}$$

.

Если для чисел a и b соотношение (1.1) не выполнено, то эти числа называются *несравнимыми по модулю* m.

Сравнимые по модулю m числа образуют множество, называемое *классом вычетов по модулю* m. Для данного числа m все целые числа распадаются на m классов вычетов.

Любое число из данного класса называется *представителем этого класса.*

Сравнения можно перемножать и складывать.

Если натуральное число d делит число m без остатка, то из соотношения (1.1) следует соотношение

$$a \equiv b \mod d. \tag{1.2}$$

.

Далее приведены хорошо известные теоремы (доказательсва см. в [1]).

Теорема 1. *Для фиксированного положительного числа m все целые числа распадаются на m различных классов чисел, сравнимых по модулю m между собой (эта система классов называется полной системой вычетов по модулю m).*

Говорят, что *m чисел образуют полную систему вычетов по модулю m*, если среди них есть представители всех классов полной системы вычетов по модулю m.

Теорема 2. *Любые m чисел, несравнимые между собой по модулю m, образуют полную систему вычетов.*

Теорема 3. *Если $(a, m) = 1$ и x пробегает полную систему вычетов, а b – любое фиксированное целое, то выражение $ax + b$ пробегает полную систему вычетов по модулю m.*

Теорема 4. *Если $(a, m) = 1$, то уравнение*

$$ax \equiv b \qquad mod\, m \tag{1.3}$$

однозначно разрешимо в классе всех вычетов при любом целом b (т.е. целочисленные решения этого уравнения существуют, и любые два его решения сравнимы друг с другом по модулю m).

Следствие. *Если $(a, m) = 1$, то элемент a обратим в классе всех вычетов по модулю m (т.е. существуют целочисленные решения уравнения (1.3), и любые два его решения сравнимы друг с другом по модулю m).*

2. Полугруппа, моноид, группа (определения, примеры)

Полугруппой называется множество элементов, в котором задана ассоциативная бинарная операция.

Моноидом называется полугруппа с единицей; иначе говоря, моноидом называется множество M, на котором задана ассоциативная бинарная операция, обычно именуемая умножением, и в котором существует такой элемент e, называемый единицей, что

$$ex = xe = x, \quad \text{при любом} \quad x \in M.$$

В любом моноиде существует ровно одна единица.

Если в моноиде бинарная операция коммутативна, то ее обычно называют *сложением*, а единицу называют *нулем*.

Группой называется множество элементов с ассоциативной бинарной операцией, гарантирующей единицу и обратные элементы.

Абелевой группой называется группа, бинарная операция которой обладает свойством коммутативности.

Примеры.

1) Множество всех отображений произвольного множества в себя является моноидом относительно операции суперпозиции отображений.

2) Всякая группа является моноидом.

3) Примеры групп: группы Галуа, гомологические группы, группы симметрий.

4) Множество целых чисел является абелевой группой по сложению.

3. Кольца, поля (определения, примеры)

Кольцом называется множество $\mathcal{K}$ с двумя определенными в нем операциями – сложением и умножением, обладающими свойствами: относительно операции сложения это множество является абелевой группой, а операция умножения связана с операцией сложения законами дистрибутивности, т.е. для любых $a, b, c \in \mathcal{K}$ верны соотношения

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca. \tag{3.1}$$

Умножение, определенное в кольце, не обязано быть ни ассоциативным, ни коммутативным.

Ассоциативным кольцом называется кольцо с ассоциативным умножением, а если умножение к тому же еще и коммутативно, то кольцо называется *коммутативным*.

В коммутативном кольце второе из равенств (3.1) является следствием первого.

Кольцом Ли называется кольцо, в котором для любого $a \in \mathcal{K}$ выполнено условие

$$a^2 = 0, \tag{3.2}$$

и для любых $a, b, c \in \mathcal{K}$ верно соотношение

$$a(bc) + b(ac) + c(ab) = 0. \tag{3.3}$$

Тождество (3.3) называется *тождеством Якоби.*

Примеры.

1) Все целые числа, все рациональные числа, все действительные числа, все комплексные числа образуют коммутативные кольца.

2) Множество всех многочленов (например, с действительными коэффициентами) с обычными сложением и умножением образует коммутативное кольцо.

3) Множество всех квадратных матриц n-го порядка по отношению к обычным сложению и умножению образует ассоциативное (но некоммутативное) кольцо.

4) Множество всех векторов трехмерного пространства с обычным сложением и векторным умножением образует кольцо Ли.

Аддитивной группой кольца называется абелева группа, которая получится, если в кольце рассмотреть только операцию сложения.

Нулевой элемент этой группы называется *нулем кольца*.

Если для элементов a, b кольца $\mathcal{K}$ верно равенство

$$ab = 0,$$

где $a \neq 0, \quad b \neq 0$, то a и b называются делителями нуля (a – левый делитель нуля, b – правый делитель нуля). Если в кольце $\mathcal{K}$ нет делителей нуля, то $\mathcal{K}$ называется *кольцом без делителей нуля*.

Коммутативное кольцо без делителей нуля называется *областью целостности*.

Дальнейшие примеры.

5) Все кольца, перечисленные в примере 1), являются областями целостности.

6) Все функции, определенные и непрерывные на отрезке $[-1, +1]$ относительно обычных операций сложения и умножения образуют коммутативное кольцо с делителями нуля; в частности, делителями нуля являются следующие функции:

$$f_1(x) = \begin{cases} 0 & \text{при} \quad -1 \leq x \leq 0 \\ x & \text{при} \quad 0 \leq x \leq 1 \end{cases},$$

$$f_2(x) = \begin{cases} x & \text{при} \quad -1 \leq x \leq 0 \\ 0 & \text{при} \quad 0 \leq x \leq 1 \end{cases},$$

поскольку ни одна из них не равна нулю нашего кольца, а их произведение

равно этому нулю.

Если $a, b_1, b_2 \in \mathcal{K}$, причем a отлично от нуля и не является левым делителем нуля, то из равенства $ab_1 = ab_2$ следует $b_1 = b_2$, т.е. на отличный от нуля элемент, не являющийся левым делителем нуля, можно сокращать слева. Аналогично на отличный от нуля элемент, не являющийся правым делителем нуля, можно сокращать справа.

Заметим, однако, что на элемент являющийся делителем нуля, вообще говоря, сокращать нельзя.

Пример.

7) В кольце всех квадратных матриц 2-го порядка для матриц

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix}, \qquad B_2 = \begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}$$

справедливо равенство

$$AB_1 = AB_2,$$

хотя $B_1 \neq B_2$. Здесь матрица A является левым делителем нуля.

Элемент e кольца $\mathcal{K}$ называется *единицей этого кольца*, если для любого элемента $a \in \mathcal{K}$ верны равенства

$$ae = ea = a.$$

Единицы в кольце может не быть.

Если в кольце $\mathcal{K}$ единица есть, то $\mathcal{K}$ называется *кольцом с единицей*.

Примеры.

8) Кольцо всех целых чисел – это кольцо с единицей.

9) Кольцо всех четных чисел – кольцо без единицы.

В кольце с единицей e для взятого элемента $a \neq 0$ этого кольца может существовать элемент b такой, что

$$ab = ba = e.$$

Тогда b называют *обратным* к a и пишут

$$b = a^{-1}.$$

Заметим, что обратного элемента может не быть.

Элементы кольца с единицей, для которых обратный элемент существует, называются *делителями единицы.*

Пример.

10) В кольце всех квадратных матриц n-го порядка единицей является единичная матрица, а ее делителями являются все невырожденные матрицы.

Подкольцо $\mathcal{I}$ кольца $\mathcal{K}$ называется *левым идеалом* кольца $\mathcal{K}$, если оно вместе с каждым элементом a содержит все элементы вида ra, где r – любой элемент кольца $\mathcal{K}$.

Аналогично, подкольцо $\mathcal{J}$ кольца $\mathcal{K}$ называется *правым идеалом* кольца $\mathcal{K}$, если оно вместе с каждым элементом a содержит все элементы вида ar, где r – любой элемент кольца $\mathcal{K}$.

Элемент ноль в любом кольце является двусторонним идеалом. Если других идеалов в кольце нет, то оно называется *простым кольцом.*

Полем называется коммутативно-ассоциативное кольцо с единицей, множество ненулевых элементов которого образует группу относительно умножения.

Примеры полей.

1) $\mathcal{Q}$ – поле рациональных чисел,

2) $\mathcal{R}$ – поле вещественных чисел,

3) $\mathcal{C}$ – поле комплексных чисел,

4) $\mathcal{Q}^*$ – поле конечных расширений поля $\mathcal{Q}$ (поле алгебраических чисел).

С О Д Е Р Ж А Н И Е

Введение 3

§1. Быстрое дискретное преобразование Фурье (БПФ) . . . . .
1. О понятии многочлена в кольце $\mathcal{K}$ . . . . .
2. Схема Хорнера (и теорема Безу) . . . . .
3. Дискретное преобразование Фурье . . . . .
4. О связи с задачей вычисления многочлена и интерполяцией Лагранжа . . . . .
5. Понятие свёртки двух векторов . . . . .
6. Применение дискретного пребразования . . . . .
Фурье для вычисления свёртки двух векторов . . . . .
7. Об алгоритме быстрого преобразования . . . . .
Фурье (основная идея) . . . . .
8. Более точное описание алгоритма БПФ . . . . .
9. Быстрое преобразование Фурье . . . . .
с использованием битовых операций . . . . .

§2. Об аналитических преобразованиях . . . . .
1. Стимулы к развитию систем аналитических вычислений . . . . .
2. О некоторых выдающихся аналитических вычислениях в прошлом веке . . . . .
3. Соотношение аналитических и численных вычислений . . . . .
4. О связи компьютерной алгебры и систем аналитических вычислений . . . . .

§3. О представлении данных в CAB
1. Введение
2. Представление целых чисел
3. О представлении обыкновенных дробей
4. Представление многочленов
5. Каноническое и нормальное представления
6. Плотные и разреженные представления
7. Наибольший общий делитель (НОД)
8. Многочлены от нескольких переменных
9. Представление рациональных функций
10. Представление алгебраических функций
10.1. Простые радикалы
10.2. Вложенные радикалы
10.3. Алгебраические функции общего вида
10.4. Примитивные элементы
11. Представление трансцендентных функций
12. Представление матриц
12.1. Виды представлений
12.2. Плотные матрицы
12.3. Алгоритм Барейса
12.4. Разреженные матрицы
13. Представление рядов
13.1. Ряды Тейлора
13.2. Ряды Фурье

§4. Полиномиальное упрощение
1. Постановка задачи
2. Редукция полиномов
3. Базисы Грёбнера
4. Решение системы полиномиальных уравнений
5. Алгоритм Бухбергера (для нахождения стандартного базиса)

§5. Формальное интегрирование
1. Постановка задачи
2. Прямой метод интегрирования

рациональных дробей . . . . . .
3. Разложение на свободные от квадратов
множители . . . . . .
4. Расширенный алгоритм Евклида . . . . . .
5. Интерполирование методом Эрмита . . . . . .
6. Метод Горовица . . . . . .
7. Обработка логарифмической части . . . . . .
8. Результант двух многочленов . . . . . .
9. Интегрирование сложных функциональных
выражений . . . . . .
10. Заключительные замечания . . . . . .

Литература . . . . . .

Дополнение . . . . . .