Алгоритмы компьютерной алгебры

Конспект лекций

2019

Содержание

1. Лекция 1.

Предмет изучения компьютерной алгебры - точные вычисления. Рассматриваются именно алгоритмы точного, а не приближенного вычисления, как в вычислительной математике. Эти алгоритмы лежат в основе математических пакетов MATLAB, Mathematica. Основной объект исследований - числовые системы с точными вычислениями.

1.1. Основные факты из теории многочленов

Определение 1. ***Числовым полем*** *называется множество* $\mathrm{F} \subset \mathbb{C}$, *если:*

1. $0, 1 \in F$,
2. $|\mathrm{F}| \geqslant 2$,
3. $\forall a, b \in F : a \pm b,\ ab \in F;\ b \neq 0, \dfrac{a}{b} \in F$.

Пример 1. *Числовые поля* - $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$

Множество многочленов над полем рациональных чисел обозначается как $\mathbb{Q}[x]$, над целыми $-$ $\mathbb{Z}[x]$, над произвольным числовым полем F $-$ $F[x]$.

Определение 2. *Многочлен* $f(x) \in \mathrm{F}[x]$, *отличный от константы, называют* ***приводимым*** *над полем* F, *если он допускает представление вида* $f(x) = \varphi(x)\psi(x)$, *где* $\varphi(x), \psi(x) \in \mathrm{F}[x]$ *и* $\deg\varphi, \deg\psi < \deg f$, *и* ***неприводимым***, *если он не допускает такого разложения (то есть один из многочленов* φ, ψ *является константой).*

1. $\deg f = 1$. Пусть f допускает разложение: $f(x) = \varphi(x)\psi(x)$.

$$\underset{=0}{\deg\varphi}, \underset{=0}{\deg\psi} < \deg f \Rightarrow \deg f = 0.$$

   Полученное противоречие доказывает неприводимость любого многочлена первой степени.

2. Пусть $\deg f > 1$ и $f(\alpha) = 0, \alpha \in F$.

$$(x - \alpha) \mid f(x) \Rightarrow \exists g(x) : f(x) = (x - \alpha)g(x).$$

$$\deg(x - \alpha) = 1 < \deg f.$$

$$\deg g = \deg f - 1 < \deg f.$$

   Если многочлен f имеет корень в поле F, то f приводим над полем F.

Обратное утверждение. *Если многочлен* $f \in F[x]$ *степени 2 или 3 приводим над полем* F, *то он имеет в этом поле корень.*

Доказательство. Допустим, многочлен приводим, следовательно, $f(x) = \varphi(x)\psi(x)$.

$$\deg\varphi, \deg\psi < \deg f \Rightarrow \deg\varphi = 1 \text{ или } \deg\psi = 1.$$

Допустим, $\varphi(x) = ax + b, a \neq 0 \Rightarrow \alpha = -\dfrac{b}{a}, \alpha \in F.$ $\square$

Пример 2.

1. $f(x) = x^2 - 1 = (x-1)(x+1)$. *Многочлен приводим над полями* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2. $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. *У него нет рациональных корней, следовательно, он неприводим над* $\mathbb{Q}$. *Но* $f(x) = (x - \sqrt{2})(x + \sqrt{2}) \Rightarrow f(x)$ *приводим над* $\mathbb{R}$.
3. $f(x) = x^2 + 1$ *неприводим над* $\mathbb{Q}$ *и* $\mathbb{R}$. *Но* $f(x) = (x - i)(x + i) \Rightarrow f(x)$ *приводим над* $\mathbb{C}$.

Многочлены второй и третьей степени приводимы над полем F тогда и только тогда, когда имеют в этом корень. Для многочленов степени, больше чем 3, данное утверждение не является справедливым.

Пример 3. $f(x) = (x^2 + 1)^2 \in \mathbb{R}[x]$ *не имеет действительных корней, но приводим.*

Определение 3. *Многочлен называется* ***нормированным****, если его старший коэффициент равен единице.*

Теорема 1 (Фундаментальная теорема о многочленах)**.** *Пусть* $f \in \mathrm{F}[x]$, $deg\ f \geqslant 1$. *Тогда* f *допускает разложение* $f(x) = a_0\varphi_1(x)\varphi_2(x)...\varphi_k(x)$, *где* $a_0 \in \mathrm{F}$, $\varphi_i \in \mathrm{F}[x]$ *и любой многочлен* φ_i *- нормированный и неприводимый. При этом данное разложение является единственным с точностью до порядка следования сомножителей.*

1.2. Многочлены с рациональными коэффициентами

Задача. *Дан многочлен с рациональными коэффициентами. Необходимо найти разложение этого многочлена в произведение многочленов с рациональными коэффициентами.*

Пусть $f \in \mathbb{Q}[x]$. Если мы умножим этот многочлен на подходящее число N (наименьшее общее кратное коэффициентов членов многочлена), то $Nf(x) \in \mathbb{Z}[x]$. Таким образом, приводимость f равносильна приводимости Nf, следовательно, разложение многочлена с рациональными коэффициентами можно свести к разложению многочлена с целыми коэффициентами.

Теорема 2. *Если многочлен* $f \in \mathbb{Z}[x]$ *допускает разложение в произведение многочленов с рациональными коэффициентами, то он допускает разложение в произведение многочленов тех же степеней с целыми коэффициентами.*

1.2.1. Алгоритм Кронекера

Задача. *Дан многочлен* $f \in \mathbb{Z}[x]$, $deg\ f > 1$. *Можно ли подобрать* $u(x), v(x)$, $u, v \in \mathbb{Z}[x]$ *и* $deg\ u$, $deg\ v < deg\ f$?

Предположение 1. *Все возникающие натуральные числа можно факторизовать.*

Предположение 2. *Многочлен формальной степени* n *можно найти с помощью интерполяционного многочлена по* $n+1$ *точке* $x_0, x_1, ..., x_n$ *и значениям многочлена в этих точках* $f(x_0), f(x_1), ..., f(x_n)$.

$$\begin{cases} f(x_0) = u(x_0)v(x_0), \\ f(x_1) = u(x_1)v(x_1), \\ ... \\ f(x_n) = u(x_n)v(x_n). \end{cases}$$

Рассмотрим точки $x_0, x_1, ..., x_n \in \mathbb{Z}$.

$$\forall i \in [0, n] : f(x_i) \in \mathbb{Z} \Rightarrow u(x_i), v(x_i) \in \mathbb{Z},\ deg\ u = m.$$

Пусть все рассматриваемые точки - не корни многочлена f. Тогда $u(x_i) \mid f(x_i)$, $u(x_i)$ может принимать только конечное множество значений, состоящее из делителей $f(x_i)$. Коэффициенты многочлена u восстанавливаются по его значениям. Далее следует непосредственная проверка того, является ли u делителем f. Алгоритм Кронекера используется для сведения от выбора из бесконечного числа вариантов к выбору из конечного числа вариантов.

Теорема 3 (Признак Эйзенштейна)**.** *Пусть многочлен*

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n \in \mathbb{Z}[x],\ n > 1,\ a_0 \neq 0.$$

Если существует простое число p такое, что $p \nmid a_0$, $p \mid a_1$, $p \mid a_2$, ..., $p \mid a_{n-1}$ и $p^2 \nmid a_n$, то f неприводим над $\mathbb{Q}$.

Пример 4. *Многочлен $f(x) = x^n - 2$ не приводим над $\mathbb{Q}$ для $\forall n \geqslant 1$. Таким образом, существуют неприводимые многочлены над $\mathbb{Q}$ любой степени.*

1.2.2. Алгоритм Евклида

Если многочлены $f, g \in F[x]$, $g \neq 0$, то имеет место следующее представление: $f(x) = g(x)h(x) + r(x)$, $h, r \in F[x]$ и $r = 0$ или $r \neq 0$, $deg\ r < deg\ g$. Если считать, что степень нулевого многочлена $r = 0$ равна $-\infty$, то можно рассматривать только вариант $deg\ r < deg\ g$.

Определение 4. *Если многочлены $f, g \in F[x]$, то многочлен $\varphi \in F[x]$ называют* ***наибольшим общим делителем (НОД)*** *f и g, если:*

1. $\varphi(x) \mid f(x)$, $\varphi(x) \mid g(x)$,
2. $\forall \psi \in F[x] : \psi(x) \mid f(x)$, $\psi(x) \mid g(x) \Rightarrow \psi(x) \mid \varphi(x)$.

Можно доказать, что НОД всегда существует и находится с точностью до множителя.

Определение 5. *Если НОД многочленов $f(x)$ и $g(x)$ - нормированный многочлен, то он обозначается как $(f(x), g(x))$.*

Алгоритм Евклида. Шаг 1.

$$f(x) = g(x)h_1(x) + r_1(x).$$

$$(f(x), g(x)) = (g(x), r_1(x)),\ deg\ r_1 < deg\ g.$$

Алгоритм Евклида. Шаг 2.

$$g(x) = r_1(x)h_2(x) + r_2(x).$$
$$(g(x), r_1(x)) = (r_1(x), r_2(x)),\ deg\ r_2 < deg\ r_1.$$

Если степень многочлена f (делимого) меньше, чем степень многочлена g (делителя), то алгоритм сам поменяет их местами:

$$f(x) = g(x) \cdot 0 + f(x)$$
$$g(x) = f(x)h_1(x) + r_1(x)$$

Поскольку остаток - неотрицательный, то процесс завершится.

Алгоритм Евклида. Заключительные шаги.

$$r_{k-2}(x) = r_{k-1}(x)h_k(x) + r_k(x)$$
$$r_{k-1}(x) = r_k(x)h_{k+1}(x)$$
$$(r_{k-2}(x), r_{k-1}(x)) = (r_{k-1}(x), r_k(x))$$

Строго говоря, $(r_{k-1}(x), r_k(x))$ необязательно равен $r_k(x)$. $r_k(x)$ является лишь одним из НОД.

1.2.3. Каноническое разложение

Определение 6. *Пусть для многочлена $f(x)$ существует разложение:*

$$f(x) = ap_1(x)p_2(x)...p_k(x),$$

где все многочлены p_i - неприводимые и нормированные. Тогда такое разложение называют ***разложением на неприводимые множители*** *или* ***факторизацией многочлена****.*

Определение 7. *Пусть для многочлена $f(x) \in F[x]$ существует разложение:*

$$f(x) = a_0(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_r(x))^{k_r},$$

где все многочлены p_i - неприводимые, нормированные и попарно различные. Тогда такое разложение называют ***каноническим разложением над полем****, а значение k_i -* ***кратностью множителя*** *p_i. Если $k_i = 1$, то множитель p_i называется* ***простым****.*

Задача. *Дан многочлен f. Нужно найти вид $f(x) = a\varphi_1(x)(\varphi_2(x))^2...(\varphi_s(x))^s$, в котором φ_i - произведение всех множителей кратности i.*

Пример 5. *Получить каноническое разложение многочлена*

$$f(x) = (x-1)(x-2)(x^2+x+1)^2(x^2-x+1)^2(x^3-2)^3.$$
$$f(x) = \varphi_1(x)(\varphi_2(x))^2(\varphi_3(x))^3.$$
$$\varphi_1(x) = (x-1)(x-2).$$
$$\varphi_2(x) = (x^2+x+1)(x^2-x+1).$$
$$\varphi_3(x) = x^3-2.$$

2. Лекция 2.

2.1. Каноническое разложение

Рассмотрим каноническое разложение многочлена $f(x)$:

$$f(x) = a_0(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_r(x))^{k_r}$$

Вынесем первый полином $p_1(x)$:

$$f(x) = a_0(p_1(x))^{k_1}(p_2(x))^{k_2}...(p_r(x))^{k_r} = (p_1(x))^{k_1}g(x),\ (g(x), p_1(x)) = 1.$$

$$f'(x) = k_1(p_1(x))^{k_1-1} \cdot (p_1(x))'g(x) + (p_1(x))^{k_1}g'(x) =$$
$$= (p_1(x))^{k_1-1} \cdot (k_1(p_1(x))'g(x) + p_1(x)g'(x)).$$

Докажем, что многочлен $k_1(p_1(x))'g(x) + p_1(x)g'(x)$ не делится на $p_1(x)$. Допустим, что он делится. Так как второе слагаемое $p_1(x)g'(x)$ делится на $p_1(x)$, то должно делиться и первое. Однако $(p_1(x))'$ не делится на $p_1(x)$, так как его степень меньше, чем у $p_1(x)$. Но и $(g(x), p_1(x)) = 1$, следовательно, первое слагаемое не делится на p_1, не делится и вся сумма. Полученное противоречие доказывает, что многочлен $k_1(p_1(x))'g(x) + p_1(x)g'(x)$ не делится на $p_1(x)$.

Таким образом, если неприводимый многочлен $p(x)$ входит в каноническое разложение $f(x)$ в степени k, то этот многочлен входит в каноническое разложение $f'(x)$ в степени $k-1$.

$$f'(x) = na_0(p_1(x))^{k_1-1}(p_2(x))^{k_2-1} \ ... \ (p_r(x))^{k_r-1}\,(p_{r+1}(x))^{k_{r+1}}(p_{r+2}(x))^{k_{r+2}} \ ...$$
эти многочлены есть, но неинтересны

$$(f(x), f'(x)) = (p_1(x))^{k_1-1}(p_2(x))^{k_2-1} \ ... \ (p_r(x))^{k_r-1}.$$

Будем предполагать, что старший коэффициент равен 1.

$$f(x) = \varphi_1(x) \cdot (\varphi_2(x))^2 \cdot ... \cdot \varphi_k(x)^k.$$

$$(f(x), f'(x)) = \varphi_2(x) \cdot (\varphi_3(x))^2 \cdot ... \cdot \varphi_k(x)^{k-1}.$$

$$u_1(x) = f(x).$$
$$u_2(x) = (f(x), f'(x)) = (u_1(x), u_1'(x)).$$
$$u_3(x) = (u_3(x), u_3'(x)) = \varphi_3(x) \cdot (\varphi_4(x))^2 \cdot ... \cdot \varphi_k(x)^{k-2}.$$
$$u_4(x) = (u_4(x), u_4'(x)) = \varphi_4(x) \cdot (\varphi_5(x))^2 \cdot ... \cdot \varphi_k(x)^{k-3}.$$
$$...$$
$$u_{k-1}(x) = (u_{k-2}(x), u_{k-2}'(x)) = \varphi_k(x).$$
$$u_k(x) = (u_{k-1}(x), u_{k-1}'(x)) = 1.$$

$$v_1(x) = \frac{u_1(x)}{u_2(x)} = \varphi_1(x) \cdot \varphi_2(x) \cdot ... \cdot \varphi_k(x).$$

$$v_2(x) = \frac{u_2(x)}{u_3(x)} = \varphi_2(x) \cdot ... \cdot \varphi_k(x).$$

$$...$$

$$v_{k-1}(x) = \frac{u_{k-1}(x)}{u_k(x)} = \varphi_k(x).$$

$$\varphi_1(x) = \frac{v_1(x)}{v_2(x)},\ \varphi_2(x) = \frac{v_2(x)}{v_3(x)},\ ...$$

2.2. Уравнения третьей степени

2.2.1. Уравнения с комплексными коэффициентами

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0, a_i \in \mathbb{C}, a_0 \neq 0.$$

Шаг 1. Разделим обе части уравнения на a_0.

$$x^3 + ax^2 + bx + c = 0.$$

Шаг 2. Введем замену $x = y - \frac{a}{3}$.

$$(y - \frac{a}{3})^3 + a(y - \frac{a}{3})^2 + b(y - \frac{a}{3}) + c = 0.$$

$y^3 - \cancel{ay^2} + ... + \cancel{ay^2} + ... = 0$ (других квадратов нет).

Получено уравнение вида $x^3 + px + q = 0,\ p, q \in \mathbb{C}$. Рассмотрим простейшее уравнение третьей степени $x^3 = 1$:

$$x^3 = 1 \Rightarrow x = cos\frac{2\pi k}{3} + i\ sin\frac{2\pi k}{3}, k = 0, 1, 2.$$

- $k = 0 \Rightarrow x = cos(0) + i \cdot sin(0) = 1 + 0 = 1.$
- $k = 1 \Rightarrow x = cos(\frac{2\pi}{3}) + i \cdot sin(\frac{2\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \omega.$
- $k = 2 \Rightarrow x = cos(\frac{4\pi}{3}) + i \cdot sin(\frac{4\pi}{3}) = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \omega^2.$

Рассмотрим общий случай: $x^3 = a,\ a \in \mathbb{C},\ a \neq 0$, если есть корень x_0, то:

$$x_0 = x_0 \cdot 1,\ x_1 = x_0\omega,\ x_2 = x_0\omega^2.$$

Теперь переменную x рассмотрим как сумму переменных u и v: $x = u + v$.

$$(u + v)^3 + p(u + v) + q = 0.$$

$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u + v) + q = 0.$$

$$(u^3+v^3+q)+(u+v)(3uv+p)=0.$$

Потребуем, чтобы $u^3+v^3+q=0$ и $3uv+p=0$.

$$\begin{cases} u^3+v^3+q=0, \\ 3uv+p=0. \end{cases} \Rightarrow \qquad \begin{cases} u^3+v^3=-q, \\ uv=-\dfrac{p}{3}. \end{cases}$$

Выполним (неэквивалентный!) переход к u^3v^3.

$$\begin{cases} u^3+v^3=-q, \\ u^3v^3=-\dfrac{p^3}{27}. \end{cases}$$

Так как переход к кубу неэквивалентен, то появятся лишние решения, поэтому нужно будет вернуться к уравнению: $uv=-\dfrac{p}{3}$.

Значения u^3 и v^3 можно рассматривать в качестве корней следующего квадратного уравнения:

$$z^2+qz-\frac{p^3}{27}=0.$$

$$z=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}.$$

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}\ \textbf{(Формула Кардано)}.$$

$$u^3v^3=-\frac{p^3}{27}.$$

$$uv=-\frac{p}{3}\ \text{или}\ -\frac{p}{3}\omega\ \text{или}\ -\frac{p}{3}\omega^2.$$

Пусть найдены $u_0, v_0 \Rightarrow u_0v_0=-\dfrac{p}{3}$.

$$u_1=u_0\omega, v_1=v_0\omega^2$$

$$u_2=u_0\omega^2, v_2=v_0\omega$$

$$x_1=u_0+v_0$$

$$x_2=\omega u_0+\omega^2 v_0$$

$$x_3=\omega^2 u_0+\omega v_0$$

$$x_2=-\frac{u_0+v_0}{2}+i\sqrt{3}\ \frac{u_0-v_0}{2}$$

$$x_3=-\frac{u_0+v_0}{2}-i\sqrt{3}\ \frac{u_0-v_0}{2}$$

2.2.2. Уравнения с рациональными коэффициентами

Определение 8. *Рассмотрим следующее уравнение:*

$$x^3 + px + q = 0,\ p, q \in \mathbb{R},\ p \neq 0.$$

Дискриминантом *такого уравнения называют выражение D:*

$$D = -108(\frac{q^2}{4} + \frac{p^3}{27}) = -27q^2 - 4p^3.$$

Определение 9. *Рассмотрим следующее уравнение:*

$$x^n + a_1 x^{n-1} + ... + a_n = 0,$$

у которого есть корни $x_1, x_2, ..., x_n$. ***Дискриминантом*** *такого уравнения называют выражение D:*

$$D = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2.$$

$D > 0$.

$$\frac{q^2}{4} + \frac{p^3}{27} < 0 \Rightarrow p < 0, uv = -\frac{p}{3} > 0.$$

$$x = \sqrt[3]{A + Bi} + \sqrt[3]{A - Bi}.$$

$$|A + Bi| = |A - Bi|.$$

$$u = R \cdot (cos(\varphi) + i \cdot sin(\varphi)).$$

$$v = R \cdot (cos(\psi) + i \cdot sin(\psi)).$$

$$R = \sqrt[6]{A^2 + B^2}.$$

$$uv = R^2 \cdot (cos(\varphi + \psi) + i \cdot sin(\varphi + \psi)).$$

$$\varphi = -\psi \Rightarrow u + v = 2R \cdot cos(\varphi).$$

$$u - v = 2i \cdot sin(\varphi).$$

$$x_1 = u + v \in \mathbb{R}.$$

$$x_{2,3} = -\frac{u + v}{2} \pm i\sqrt{3} \cdot \frac{2i \cdot sin(\varphi)}{2} \in \mathbb{R}.$$

$D < 0$.

$$x = \sqrt[3]{A + B} + \sqrt[3]{A - B}.$$

$$B \neq 0 \Rightarrow A + B \neq A - B \Rightarrow \sqrt[3]{A + B} \neq \sqrt[3]{A - B}.$$

$$u = \sqrt[3]{A + B} \in \mathbb{R}.$$

$$x_1 = u + v \in \mathbb{R}.$$

$$x_{2,3} = -\frac{u + v}{2} \pm \frac{i\sqrt{3}}{2}(u - v) \in \mathbb{C}.$$

$D = 0$.

$$x = \sqrt[3]{A} + \sqrt[3]{A}.$$

u - вещественный кубический корень из A, $uv = -\dfrac{p}{3} \Rightarrow v \in \mathbb{R}$, но v - тоже вещественный кубический корень из A, следовательно, $u = v$.

$$\begin{cases} x_1 = u + v = 2u, \\ x_{2,3} = -\dfrac{u+v}{2} \pm \dfrac{i\sqrt{3}}{2}(u - v) = -u. \end{cases}$$