**Доп. дисциплины.**

**Магистры весна 2021.**

**Занятие 3**

# АЛГОРИТМЫ МНОГОЧЛЕНОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

25.03.2021

## МНОГОЧЛЕНЫ, КАК ФУНКЦИИ

Пусть $f(\mathrm{x}) \in K[\mathrm{x}]$ многочлен над кольцом K, тогда мы можем задать функцию $f : \mathrm{K} \to \mathrm{K}, \mathrm{a} \to \mathrm{f(a)}, \mathrm{a} \in \mathrm{K}$. Такую функцию называют полиномиальной. Полиномиальных функций больше, чем многочленов.

Например, над кольцом $Z_3$ любой многочлен вида $(x^3 - x)\,\mathrm{g(x)}, \mathrm{g(x)} \in \mathrm{Z}_3[\mathrm{x}]$ задает тождественно нулевую функцию. Таким образом, несколько, а может и бесконечно много разных многочленов могут задавать одну и ту же полиномиальную функцию.

**Определение**. *Элемент a называется корнем многочлена f(x), если f(a)=0.*

**Теорема**. *Многочлен над полем имеет корней, с учетом кратности, не больше, чем степень многочлена.*

Эта теорема имеет важное применение. Если у нас задано значение многочлена в n+1 точке, то мы однозначно можем определить многочлен n-й степени. В самом деле, пусть таким многочленов два f(x) и g(x), тогда их разность h(x) = f(x) – g(x) степени не выше n имеет n+1 корень. Противоречие.

Поэтому есть много аппроксимирующих формул, задающих многочлен по значениям в фиксированных точках. Одна из самых известных **интерполяционная формула Лагранжа**

$$f(\mathrm{x}) = \sum_{i=1}^{n} b_i \frac{(\mathrm{x}-\mathrm{a}_1)(\mathrm{x}-\mathrm{a}_2)\ldots(\mathrm{x}-\mathrm{a}_{i-1})(\mathrm{x}-\mathrm{a}_{i+1})\ldots(\mathrm{x}-\mathrm{a}_n)}{(\mathrm{a}_i-\mathrm{a}_1)(\mathrm{a}_i-\mathrm{a}_2)\ldots(\mathrm{a}_i-\mathrm{a}_{i-1})(\mathrm{a}_i-\mathrm{a}_{i+1})\ldots(\mathrm{a}_i-\mathrm{a}_n)},$$

задающая многочлен f(x) степени n-1 принимающий следующие значения $f(\mathrm{a}_i) = \mathrm{b}_i, i = 1, 2, \ldots, n$.

**Упражнение**. Проверить, что для формулы Лагранжа выполняются равенства $f(\mathrm{a}_i) = \mathrm{b}_i, i = 1, 2, \ldots, n$.

**Пример.** *Над полем GF(3) построить многочлен, который в точках 0, 1, 2 принимает значения 2, 1, 0*

Решим задачу двумя способами.

**Первый способ.** Учитывая, что поле GF(3) очень маленькое, содержит всего 3 элемента, а многочлен строится всего по трем точкам, т.е. является многочленом второй степени, задачу вполне можно решить в лоб. Т.е. рассмотреть многочлен второй степени с неопределенными коэффициентами, подставить в него по очереди значения переменной равные 0, 1, 2 и приравнять полученные формулы заданным значениям 2, 1, 0. В результате получится система трех линейных уравнений от трех переменных над полем GF(2).

Пусть неизвестный нам многочлен имеет вид $a_2 * X^2 + a_1 * X + a_0$. Тогда система имеет вид

$$\begin{cases} a_2 * 0^2 + a_1 * 0 + a_0 = 2 \\ a_2 * 1^2 + a_1 * 1 + a_0 = 1 \\ a_2 * 2^2 + a_1 * 2 + a_0 = 0 \end{cases} \Rightarrow \begin{cases} a_0 = 2 \\ a_2 + a_1 + a_0 = 1 \\ a_2 + a_1 * 2 + a_0 = 0 \end{cases} \Rightarrow \begin{cases} a_0 = 2 \\ a_2 + a_1 = 2 \\ a_2 + a_1 * 2 = 1 \end{cases} \Rightarrow \begin{cases} a_0 = 2 \\ a_1 = 2 \\ a_2 = 0 \end{cases}$$

Таким образом, многочлен имеет вид 2*X + 2, т.е. имеет даже не вторую, а первую степень.

**Второй способ.** Это более универсальный способ, использующий известную интерполяционную формулу Лагранжа.

Пусть в различных точках $a_1, a_2, \ldots, a_n$ многочлен принимает значения $b_1, b_2, \ldots, b_n$ соответственно. Тогда, по известной формуле Лагранжа, он имеет степень не выше $n - 1$ и может быть явно записан в следующем виде:

$$f(X) = \sum_{i=1}^{n} b_i * \frac{(X - a_1)(X - a_2)\ldots(X - a_{i-1})(X - a_{i+1})\ldots(X - a_n)}{(a_i - a_1)(a_i - a_2)\ldots(a_i - a_{i-1})(a_i - a_{i+1})\ldots(a_i - a_n)}$$

В нашем случае $n = 3$, и мы получаем сумму трех слагаемых

$$f(X) = 2 * \frac{(X-1)(X-2)}{(0-1)(0-2)} + 1 * \frac{(X-0)(X-2)}{(1-0)(1-2)} + 0 * \frac{(X-0)(X-1)}{(2-0)(2-1)} =$$

$$(X-1)(X-2) - (X-0)(X-2) = X^2 + 2 - X^2 + 2 * X = 2 * X + 2$$

Как и следовало ожидать, многочлен получился тот же самый.

## МНОГОЧЛЕНЫ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

**Определение**. *Пусть K – кольцо, тогда* $K[x_1, x_2 \ldots, x_n]$*, где n – натуральное число, называется кольцом многочленов от n коммутирующих переменных.*

**Определение**. Покоординатный порядок. *Пусть* $x(a) = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ *и* $x(b) = x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$ *- два монома. Скажем, что* $x(a) \le x(b)$*, если* $a_1 \le b_1, a_2 \le b_2, \ldots, a_n \le b_n$.

Это частичный порядок, поскольку мономы $x_1^2 x_2^3, x_1^3 x_2^2$ не сравнимы.

Определим **лексикографический порядок**, словарный, который принят в словарях и при подсчетах медалей на олимпиадах. Когда одна золотая медаль больше любого числа серебряных и бронзовых.

**Определение**. Лексикографический порядок. *Пусть* $x(\mathrm{a}) = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ *и* $x(\mathrm{b}) = x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$ *- два монома. Скажем, что* $x(\mathrm{a}) < \mathrm{x}(\mathrm{b})$, *если* $a_1 = b_1, a_2 = b_2, \ldots, a_{i-1} = b_{i-1}, a_i < b_i$.

Другими словами, символы у нас имеют такой словарный порядок $x_1 > x_2 > \ldots > x_n$, т.е. $x_1$ - это “золото”, $x_2$ - серебро и т.д.

Лексикографический порядок является линейным, любые два монома сравнимы. Но у него есть недостаток. Между любыми двумя мономами можно вставить бесконечно много промежуточных мономов, которые больше одного и меньше другого.

**Упражнение.** Даны мономы от двух переменных, вставьте бесконечно много мономов y между ними $x_1^2 x_2^3 < y < x_1^3 x_2^2$.

**Определение.** Градуированный лексикографический порядок. *Вначале мы мономы сравниваем по полной степени. У кого полная степень больше – тот больше. А уже мономы одинаковой полной степени сравниваем лексикографически.*

**Упражнение.** Мономов данной полной степени конечное число, а значит и меньших данного монома, в лексикографическом порядке тоже конечное число.

**Определение**. *Если f - многочлен от нескольких переменных, то его моном H(f) - максимальный среди остальных его мономов относительно градуированного лексикографического порядка – называется старшим членом.*

**Утверждение-упражнение**. *Пусть f и g два многочлена, H(f) и H(g) – их старшие члены. Тогда старший член их произведения – произведение старших членов сомножителей, т.е. H(fg) = H(f)H(g).*

**Определение.** *Многочлен, называется симметричным, если он не изменяется при любой перестановке переменных.*

Примеры симметричных многочленов от n переменных.

**Определение.** Элементарные симметрические многочлены. *Положим*

$$s_1 = \sum_{i=1}^{n} x_i \ , \ s_2 = \sum_{i=1}^{n-1} x_i x_{i+1}, \ldots, \ s_n = x_1 x_2 \ldots x_n .$$

**Определение.** *Многочлен от нескольких переменных называется формой, если все его мономы имеют одну и ту же полную степень.*

Элементарные симметрические многочлены – это формы 1, 2, …, n-й степени.

**Теорема.** Основная теорема о симметрических многочленах**.** *Любой симметрический* $\mathrm{f}(\mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_n)$ *многочлен можно представить, как многочлен*

$g(s_1, s_2 ..., s_n)$ *от элементарных симметрических многочленов. При этом если у многочлена f полная степень равна m, то у многочлена g вес равен m.*

**Алгоритм нахождения многочлена** $g(s_1, s_2 ..., s_n)$

Это метод неопределенных коэффициентов. Он подсказан примененным нами способом доказательства основной теоремы о симметрических многочленах.

1. Вначале находим старший член $x(a) = x_1^{a_1} x_2^{a_2} ... x_n^{a_n}$ и находим первый слагаемый многочлена $g(s_1, s_2 ..., s_n)$, а именно, $y(a) = s_1^{a_1 - a_2} s_2^{a_2 - a_3} ... s_{n-1}^{a_{n-1} - a_n} s_n^{a_n}$.

2. Находим следующий монотонный моном $x(b) = x_1^{b_1} x_2^{b_2} ... x_n^{b_n}$, такой, что $b_1 + b_2 + ... + b_n = m$ и при этом между x(a) и x(b) нет других монотонных мономов. Он дает нам второй слагаемый многочлена g, а именно $y(b) = s_1^{b_1 - b_2} s_2^{b_2 - b_3} ... s_{n-1}^{b_{n-1} - b_n} s_n^{b_n}$ Потом находим моном x(c) и связанное с ним произведение y(c) и т.д.

3. Составляем сумму $g = \alpha y(a) + \beta y(b) + \gamma y(c) + ....$ с неопределёнными коэффициентами $\alpha, \beta, \gamma, ...$ Чтобы найти их решаем линейную систему. Если у нас получилось k слагаемых, то систему из k уравнений от k неизвестных.

4. Составляем систему. Переменным $x_1, x_2, ..., x_n$ придаем k различных наборов значений, обычно из 0 и 1. Подставляем выбранный набор в элементарные симметрические многочлены и вычисляем $y(a), y(b), y(c), ...$ Потом вычисляем значение многочлена f. Составляем 1-е уравнение $f = \alpha y(a) + \beta y(b) + \gamma y(c) + ....$ и аналогично k-1 оставшееся.

5. Решаем получившуюся систему, находим числа $\alpha, \beta, \gamma, ...$ и нужный нам многочлен $g = \alpha y(a) + \beta y(b) + \gamma y(c) + ....$

Система линейных алгебраических уравнений, это самое лучшее, о чем только можно мечтать в вычислительной математике. Это идеал (в духовном смысле), к которому стремятся все математические теории.

Алгоритм интуитивно понятный. Ниже будут примеры. А пока пример важного симметрического многочлена.

**Определение**. *Пусть* $f(x) = x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ *- приведенный многочлен,* $x_1, x_2, ..., x_n$ *- его корни. Дискриминантом многочлена f называется многочлен*

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

Очевидно, что это симметрический многочлен. Значит по основной теореме о симметрических многочленах он выражается через элементарные симметрические, а те в свою очередь, по теореме Виета, являются, с точностью до знака, коэффициентами многочлена f. Таким образом, не находя корней многочлена f мы можем найти дискриминант. Главное его свойство в том, что он равен нулю только тогда, когда у многочлена есть кратные корни.

Это замечательное достижение. Не находя корни, которые часто невозможно найти точно, а приближенных значений недостаточно, мы можем точно сказать, причем без особых усилий – есть кратные корни или нет.

Однако найти дискриминант не такая простая задача.

**Пример**. Пусть $f(\mathrm{x}) = \mathrm{x}^3 + px + q$ упрощенный многочлен 3-й степени. Поэтому элементарные симметрические многочлены от его корней имеют значения $\begin{cases} 0 = (-1)^1 s_1 \\ p = (-1)^2 s_2 \\ q = (-1)^3 s_3 \end{cases}$ (см. теорему Виета). Найдем его дискриминант.

**Решение**. По определению $D(\mathrm{f}) = (\mathrm{x}_1 - \mathrm{x}_2)^2 (\mathrm{x}_1 - \mathrm{x}_3)^2 (\mathrm{x}_2 - \mathrm{x}_3)^2$. Если раскрыть скобки, то у нас получится 27 слагаемых, работать и даже выписать их достаточно хлопотно. Поэтому делать этого не будем, а сразу применим алгоритм нахождение многочлена $\mathrm{g}(\mathrm{s}_1, \mathrm{s}_2 ..., \mathrm{s}_n)$.

Старший член многочлена D(f), как легко видеть – это $\mathrm{x}_1^4 \mathrm{x}_2^2$. Вектор степеней (**Определение.** *Набор показателей степеней переменных*), соответствующий ему, имеет вид (4,2,0). Ноль, поскольку третья переменная отсутствует.

Теперь нам нужно перечислить монотонные вектора, с суммой координат равной 6, меньших, в лексикографическом порядке, вектора (4,2,0). Это не сложно

(4,2,0) > (4,1,1) > (3,3,0) > (3,2,1) > (2,2,2).

Получилось 5 мономов, значит система будет из 4 уравнений от 4 неизвестных. Первый коэффициент известен – он равен 1.

Строим мономы $s_1^{a_1 - a_2} s_2^{a_2 - a_3} ... s_{n-1}^{a_{n-1} - a_n} s_n^{a_n}$ в нашем случае $s_1^{a_1 - a_2} s_2^{a_2 - a_3} s_3^{a_3}$.

Получаем сумму

$$D(f) = s_1^{4-2} s_2^{2-0} s_3^0 + \alpha s_1^{4-1} s_2^{1-1} s_3^1 + \beta s_1^{3-3} s_2^{3-0} s_3^0 + \delta s_1^{3-2} s_2^{2-1} s_3^1 + \gamma s_1^{2-2} s_2^{2-2} s_3^2 .$$

Теперь, когда ясно, как она получилась, упростим ее

$$D(f) = s_1^2 s_2^2 + \alpha s_1^3 s_3 + \beta s_2^3 + \delta s_1 s_2 s_3 + \gamma s_3^2$$

Поскольку нам придется вычислять значения элементарных симметрических многочленов, вспомним их вид для трех переменных:

$$\begin{cases} s_1 = x_1 + x_2 + x_3 \\ s_2 = x_1 x_2 + x_1 x_3 + x_2 x_3 \\ s_3 = x_1 x_2 x_3 \end{cases}$$

И сам дискриминант $D(\mathrm{f}) = (\mathrm{x}_1 - \mathrm{x}_2)^2 (\mathrm{x}_1 - \mathrm{x}_3)^2 (\mathrm{x}_2 - \mathrm{x}_3)^2$.

Нам нужно выбрать 4 набора значений для 3-х переменных x. Они могут быть любыми, но для быстроты вычислений лучше брать маленькие числа

Выбирать наборы нужно аккуратно. Некоторые, например, (1,0,0) в нашем случае будут бесполезными. Мы получим 0 = 0. Это правда, и даже истина, но новой информации нет.

Первый набор (1,1,0). Тогда мы получаем $D(\mathrm{f}) = 0, s_1 = 2, s_2 = 1, s_3 = 0$.

Первое уравнение

$$0 = 2^2 \cdot 1^2 + \alpha 2^3 \cdot 0 + \beta 1^3 + \delta 2 \cdot 1 \cdot 0 + \gamma 0^2 = 4 + \beta \Rightarrow \beta = -4 .$$

Второй набор (1,1,1). Получаем $D(\mathrm{f}) = 0, s_1 = 3, s_2 = 3, s_3 = 1$

Второе уравнение

$$0 = 3^2 3^2 + \alpha 3^3 \cdot 1 - 4 \cdot 3^3 + \delta 3 \cdot 3 \cdot 1 + \gamma 1^2 \Rightarrow 27\alpha + 9\delta + \gamma = 27$$

Третий набор (1,1, 2). Получаем $D(\mathrm{f}) = 0, s_1 = 4, s_2 = 5, s_3 = 2$

Третье уравнение

$$0 = 4^2 5^2 + \alpha 4^3 2 - 4 \cdot 5^3 + \delta 4 \cdot 5 \cdot 2 + \gamma 2^2 = 400 + \alpha 128 - 500 + 40\delta + 4\gamma = 0$$
$$\Rightarrow \alpha 128 + 40\delta + 4\gamma = 100$$

Четвертый набор (1,2,3). Получим $D(\mathrm{f}) = 4, s_1 = 6, s_2 = 11, s_3 = 6$

Четвертое уравнение

$$4 = 6^2 11^2 + \alpha 6^3 6 \ - 4 \cdot 11^3 + \delta 6 \cdot 11 \cdot 6 + \gamma 6^2$$
$$\Rightarrow 1296\alpha + 396\delta + 36\gamma = 972$$

Получаем систему

$$\begin{cases} 27\alpha + 9\delta + \gamma = 27 \\ 128\alpha + 40\delta + 4\gamma = 100 \\ 1296\alpha + 396\delta + 36\gamma = 972 \end{cases}$$

Решим систему средствами языка Julia https://julialang.org/ - текущая версия 1.4.1

Матрицу, назовем ее M, задается по столбцам

M = [ [27,128,1296] [9,40,396] [1,4,36]]

и столбец свободных членов d = [27,100,972]

искомое решение M^(-1)*d

Вот, что получается

```
julia> M = [ [27,128,1296] [9,40,396] [1,4,36]]
3?3 Array{Int64,2}:
   27    9    1
  128   40    4
```

```
 1296  396  36

julia> d = [27,100,972]
3-element Array{Int64,1}:
   27
  100
  972


julia> M^(-1)*d
3-element Array{Float64,1}
  -4.000000000000025
  18.000000000000156
 -27.00000000000034
```

По смыслу решения должны быть целыми числами, такая добавка из-за формата чисел Float64.

Итак, решение $D(f) = s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 + 18s_1 s_2 s_3 - 27s_3^2$

**Упражнение.** Вычислить дискриминанты многочленов $f(\mathrm{x}) = \mathrm{x}^3 + px + q$ и $f(\mathrm{x}) = \mathrm{x}^3 + ax^2 + bx + c$.

## ЛИТЕРАТУРА


1. Курош А.Г. Лекции по общей алгебре, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. - URL: https://e.lanbook.com/reader/book/104951
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/126718/
3. Фаддеев Д.К. Лекции по алгебре, 7-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/126709/