КРИТИЧЕСКИЕ ЗНАЧЕНИЯ МНОГОЧЛЕНОВ

ЧАСТЬ 1: АЛГЕБРА

Пусть P — многочлен степени n с комплексными коэффициентами. Тогда его производная P' имеет степень $n-1$ и, соответственно, $n-1$ корней $z_1, \dots, z_{n-1}$. Числа $c_1 = P(z_1), \dots, c_{n-1} = P(z_{n-1})$ называются *критическими значениями* многочлена P. Мы будем изучать задачу восстановления многочлена P по набору его критических значений; точнее, говоря, нас будет интересовать, сколько различных многочленов имеют заданный набор критических значений.

В буквально такой постановке ответ на вопрос тривиален — многочленов существует бесконечно много. Действительно, пусть P — какой-нибудь многочлен и $a, b \in \mathbb{C}, a \neq 0$; рассмотрим тогда многочлен $Q(z) \stackrel{\text{def}}{=} P(az+b)$. Имеем $Q'(z) = aP'(az+b)$, так что корнями производной Q будут числа $w_i = (z_i - b)/a$, $i = 1, \dots, n-1$. Отсюда вытекает, что $Q(w_i) = P(z_i)$, то есть набор критических значений у многочлена Q такой же, как и у многочлена P.

Чтобы справиться с этой трудностью, потребуем впредь, чтобы многочлен P имел вид $P(z) = z^n + a_{n-2}z^{n-2} + \dots + a_1 z + a_0$. Нетрудно видеть, что каждый многочлен можно привести к такому виду заменой переменных типа $z \mapsto az+b$, так что общность не ограничивается. В то же время для всякого многочлена P указанного вида существует лишь конечный набор преобразований $z \mapsto az+b$ — а именно, n штук — сохраняющих этот вид: нетрудно видеть, что для этого необходимо и достаточно, чтобы $b=0$ и $a^n = 1$.

Пример 1. Пусть $n=3$, то есть $P(z) = z^3 + a_1 z + a_0$. Тогда $P'(z) = 3z^2 + a_1$, так что $z_1, z_2 = \pm\sqrt{-a_1/3}$, и $P(z_1), P(z_2) = a_0 \pm \frac{2}{3}a_1\sqrt{-a_1/3}$. Система уравнений $P(z_i) = c_i$, $i = 1, 2$, равносильна системе уравнений $P(z_1) + P(z_2) = c_1 + c_2 \stackrel{\text{def}}{=} C_1$, $P(z_1)P(z_2) = c_1 c_2 \stackrel{\text{def}}{=} C_2$, то есть системе уравнений $2a_0 = C_1$, $a_0^2 + 4a_1^3/27 = C_2$. Очевидно, что система имеет 3 решения при почти любых значениях C_1 и C_2 (точнее, при C_1 и C_2 таких, что $C_2 \neq C_1^2/4$).

Напомним следующее хорошо известное утверждение:

Предложение 1. *Пусть $R(x_1, \dots, x_n)$ — многочлен от n переменных, не изменяющийся при любой перестановке аргументов (симметрический). Тогда существует и единствен такой многочлен $H(p_1, \dots, p_n)$, что $R(x_1, \dots, x_n) \equiv H(e_1(x), \dots, e_n(x))$, где $e_i(x)$ — элементарный симметрический многочлен степени i от переменных $x_1, \dots, x_n$, т.е. сумма всевозможных произведений по i переменных $x_1, \dots, x_n$ (в частности, $e_1(x) = x_1 + \dots + x_n$, $e_n(x) = x_1 \dots x_n$).*

Начало доказательства. Рассмотрим многочлен $A(z) = (z + x_1)\dots(z + x_n) = z^n + e_1(x)z^{n-1} + \dots + e_n(x)$. Поскольку коэффициенты многочлена $e_1(x), \dots, e_n(x)$ однозначно определяют его корни $-x_1, \dots, -x_n$ с точностью до перестановки, всякий симметрический многочлен от $x_1, \dots, x_n$ является однозначно определенной функцией от $e_1(x), \dots, e_n(x)$; обозначим эту функцию H. Почему H — многочлен, мы разберемся позже. $\square$

Для любого неупорядоченного набора $x_1, \dots, x_k$ можно рассмотреть многочлен $Q(x) = (x + x_1)\dots(x + x_k) = x^k + e_1(x_1, \dots, x_k)x^{k-1} + \dots + e_k(x_1, \dots, x_k)$. Поскольку коэффициенты уравнения определяют набор (неупорядоченный) его корней, задать такой набор $x_1, \dots, x_k$ это то же самое, что задать *упорядоченный* набор чисел $e_i(x_1, \dots, x_k)$, $i = 1, \dots, k$. В рассматриваемой задаче нам известны $n-1$ чисел $c_1, \dots, c_{n-1}$, так что вместо них можно рассматривать $C_i = e_i(c_1, \dots, c_{n-1})$, $i = 1, \dots, n-1$. Эти величины зависят от корней $z_1, \dots, z_{n-1}$) многочлена P' симметрично и, согласно предложению 1, являются многочленами от коэффициентов P' — то есть многочленами от $a_0, \dots, a_{n-2}$. Иными словами, задача сводится к системе полиномиальных уравнений на $a_0, \dots, a_{n-2}$. Поэтому будет полезно разобраться, сколько решений может иметь такая система.

Пример 2. Пусть $n = 4$, т.е. $P(z) = z^4 + a_2 z^2 + a_1 z + a_0$. Тогда $P'(z) = 4z^3 + 2a_2 z + a_1$ имеет 3 корня z_1, z_2, z_3. Вычисления показывают, что $e_1(P(z_1), P(z_2), P(z_3)) = 3a_0 - a_2^2/2$, $e_2(P(z_1), P(z_2), P(z_3)) = 3a_0^2 - a_0 a_2^2 + 9a_1^2 a_2/16 + a_2^4/16$, $e_3(P(z_1), P(z_2), P(z_3)) = a_0^3 - a_0^2 a_2^2/2 + 9a_0 a_1^2 a_2/16 + a_0 a_2^4/16 - a_1^2 a_2^3/64 - 27a_1^4/256$.

Уравнение $e_1 = C_1$ однозначно определяет a_0 как функцию от a_2: $a_0 = (C_1 + a_2^2/2)/3$. Подставляя это выражение в уравнение $e_2 = C_2$, получаем равенство $a_1^2 = R(C_1, C_2, a_2)/a_2$, где многочлен R имеет степень 4 относительно a_2. Уравнение $e_3 = C_3$ теперь принимает вид $(C_1 + a_2^2/2)^3/27 - a_2^2(C_1 + a_2^2/2)^2/18 + 3R(C_1, C_2, a_2)(C_1 + a_2^2/2)/16 + a_2^4(C_1 + a_2^2/2)/64 - a_2^2 R(C_1, C_2, a_2)/64 - 27R(C_1, C_2, a_2)^2/a_2^2 = C_3$; после удаления знаменателя получаем уравнение степени 8 на a_2. Таким образом, при почти любых значениях C_1, C_2, C_3 имеется 8 значений a_2, каждому из которых соответствует 2 значения a_1 и 1 значение a_0. Таким образом, система уравнений имеет 16 решений.

Слова “почти любых” означают, что для любого набора C_1, C_2, C_3 и любого (сколь угодно малого) числа $\varepsilon > 0$ найдутся числа C_1', C_2', C_3', для которых утверждение верно и такие, что $|C_1 - C_1'|, |C_2 - C_2'|, |C_3 - C_3'| < \varepsilon$.

Подсчет количества решений в общем случае опирается на следующий фундаментальный результат:

Теорема 1 (Безу)**.** *Пусть $A_1(x_1, \dots, x_k), \dots, A_k(x_1, \dots, x_k)$ — однородные многочлены степеней $d_1, \dots, d_k$, не имеющие общих нулей, кроме $x_1 = \dots = x_k = 0$. Тогда при почти любых $p_1, \dots, p_k$ система уравнений $A_i(x) = p_i$, $i = 1, \dots, k$, имеет $d_1 \dots d_k$ решений*

Пример 3. Система уравнений $x_1^{d_1} = p_1, \dots, x_k^{d_k} = p_k$ имеет $d_1 \dots d_k$ решений, если среди чисел $p_1, \dots, p_k$ нет нулей.

Пример 4. При $d_1 = \dots = d_k = 1$ перед нами система k линейных уравнений с k неизвестными. Если система $A_1(x) = \dots = A_k(x) = 0$ имеет только нулевое решение, она невырождена, и при произвольных $p_1, \dots, p_k$ количество решений системы $A_i(x) = p_i$, $i = 1, \dots, k$, равно 1.

Напомним, что многочлен $A(x_1, \dots, x_k)$ называется однородным степени d, если все его одночлены имеют суммарную степень d или, что эквивалентно, он удовлетворяет тождеству $A(\lambda x_1, \dots, \lambda x_k) = \lambda^d A(x_1, \dots, x_k)$ (для любого комплексного λ). Многочлен A называется *квазиоднородным степени d с весами $q_1, \dots, q_k$* (у переменной x_i вес q_i), если он удовлетворяет тождеству $A(\lambda^{q_1} x_1, \dots, \lambda^{q_k} x_k) = \lambda^d A(x_1, \dots, x_k)$, $\forall \lambda \in \mathbb{C}$.

Следствие (теоремы Безу)**.** *Система уравнений $A_1(x_1, \dots, x_k) = p_1, \dots, A_k(x_1, \dots, x_k) = p_k$, где $A_1, \dots, A_k$ — квазиоднородные уравнения степеней $d_1, \dots, d_k$ с весами $q_1, \dots, q_k$ (веса одни и те же для всех уравнений) имеет $d_1 \dots d_k / q_1 \dots q_k$ решений при почти любых $p_1, \dots, p_k$.*

Доказательство следствия. Заменим переменные: $x_1 = y_1^{q_1}, \dots, x_k = y_1^{q_k}$. Полученная система уравнений на переменные $y_1, \dots, y_k$ удовлетворяет теореме Безу и имеет $d_1 \dots d_k$ решений. Поскольку реально в уравнения переменная y_1 входит только в степенях, кратных q_1, переменная y_2 — только в степенях, кратных q_2, и т.д., решения разбиваются на группы по $q_1 \dots q_k$ штук, где значения y_i отличаются друг от друга умножением на корни соответствующих степеней из единицы (при почти любых $p_1, \dots, p_k$ решения отличны от 0, так что в группе действительно $q_1 \dots q_k$ элементов). Решениям, вошедшим в одну и ту же группу, соответствуют одинаковые значения $x_1, \dots, x_k$, откуда количество решений исходной системы равно $d_1 \dots d_k / q_1 \dots q_k$. □

Саму теорему Безу мы доказывать не будем.

Теперь можно получить ответ в исходной задаче. Нетрудно заметить, что если мы умножим z на комплексное число λ, а каждый коэффициент a_k многочлена P на λ^{n-k}, то величина $P(z)$ умножится на λ^n. Отсюда вытекает, что $e_i(P(z_1), \dots, P(z_{n-1}))$ как многочлен от $a_0, \dots, a_{n-2}$ — квазиоднородный степени ni, причем вес переменной a_k равен $q_k = n - k$. Система уравнений $e_1 = 0, \dots, e_{n-1} = 0$ означает, что $P(z_1) = \dots = P(z_{n-1}) = 0$ — все корни производной P' являются также корнями многочлена P, причем большей кратности. Отсюда вытекает, что многочлен P делится на P': $P = (pz + q)P'$. Дифференцируя это равенство, получим $P' = pP' + (pz + q)P''$, то есть $P' = \frac{1}{1-p}(pz + q)P''$. Проделав эту операцию $(n-1)$ раз, получим равенство $P^{(n-1)} = \alpha(pz + q)$ при некотором $\alpha \in \mathbb{C}$, откуда $P(z) = \beta(pz + q)^n$ при некотором $\beta \in \mathbb{C}$. Если у такого многочлена коэффициент при z^{n-1} отсутствует, а старший коэффициент равен 1, то $q = 0$, а $\beta = 1/p^n$. Тем самым $P(z) = z^n$, то есть $a_0 = \dots = a_{n-2} = 0$ — условие теоремы Безу выполнено.

Таким образом, количество решений системы уравнений $e_1 = C_1, \dots, e_n = C_n$ при почти любых $C_1, \dots, C_n$ — то есть количество многочленов вида $z^n + a_{n-2} z^{n-2} + \dots + a_0$ с критическими значениями $c_1, \dots, c_n$, заданными почти произвольным образом — равно $n \cdot (2n) \cdot \dots \cdot ((n-1)n)/(2 \cdot 3 \cdot \dots \cdot n) = n^{n-1}(n-1)!/n! = n^{n-2}$. В частности, как мы уже знаем, при $n = 3$ и $n = 4$ получается, соответственно, $3^1 = 3$ и $4^2 = 16$.