Оценки коэффициентов полинома, которые делят данный полином в кольце $\mathbf{Z}[\mathbf{x}]$

Задача состоит в том, чтобы определить какое может быть наибольшее значение у коэффициентов полиномов, которые являются делителями данного полинома. Вот пример, в котором у делителя a коэффициенты больше, чем у делимого полинома b:

$a = (x+1)^4; b = (x-1)a; \mathbf{print}(a, b)$

$out:$

$a = x^4 + 4x^3 + 6x^2 + 4x + 1$

$b = x^5 + 3x^4 + 2x^3 - 2x^2 - 3x - 1$

А Б С Т Р А К Т

Мы покажем, что если m – степень полинома делителя, а ||f|| – корень квадратный из суммы квадратов коэффициентов делимого полинома, то можно пользоваться в практических расчетах такой оценкой для коэффициентов полинома делителя:

$$B \leq 2^m ||f||$$

Основны результаты здесь были получены M.Mignotte 70-80 годы. Предварительно надо получить несколько вспомогательных неравенств.

Л Е М М А 1.

Пусть $A_n = \{\alpha \in R : 1 \leq \alpha_1 \leq .. \leq \alpha_n\}$ и $\prod_{i=1}^n \alpha_i = M$, $1 \leq k < n$. Тогда

$$\sum_{i_1<..<i_k} \alpha_{i_1}\alpha_{i_2}..\alpha_{i_k} \leq \binom{n-1}{k-1} M + \binom{n-1}{k}. \qquad (1)$$

Д О К А З А Т Е Л Ь С Т В О.

Для множества $A_n \setminus \{\alpha_{n-1}, \alpha_n\}$ составим сумму $\lambda = \sum_{j_1<..<j_{k-1}} \alpha_{j_1}\alpha_{j_2}..\alpha_{j_{k-1}}$. Заменим в A_n пару (α_{n-1}, α_n) на пару $(1, \alpha_{n-1}\alpha_n)$. В результате замены в сумме, которая стоит слева в (1), изменятся только те слагаемые, в которые входил либо только α_{n-1}, либо только α_n, но не оба вместе. Поэтому эта сумма увеличится на

$$\lambda(\alpha_{i_{n-1}}\alpha_{i_n} + 1 - \alpha_{i_{n-1}} - \alpha_{i_n}) = \lambda(\alpha_{i_{n-1}} - 1)(\alpha_{i_n} - 1). \qquad (2)$$

Будем последовательно заменять в A_n пары (α_{n-i}, α_n) на пары $(1, \alpha_{n-i}\alpha_n)$, $i = 2, 3, .., n-1$. В итоге получим множество $\{1, .., 1, M\}$. Для этого множества $\binom{n-1}{k-1}$ слагаемых ровно M и $\binom{n-1}{k}$ слагаемых равно 1. Из того, что (2) не отрицательные числа, то складывая их, получаем неравенство (1).

□

Обозначение 1.

$$\text{Пусть } \; f = \sum_{i=0}^n a_i x^i \; \text{ обозначим функцию } \; ||f|| = \sqrt{(}\sum_{i=0}^n |a_i|^2) \qquad (3)$$

и назовем ее диагональю (по аналогии с диагональю параллелепипеда).

Л Е М М А 2.

Пусть B и $\bar{B}$ – комплексно сопряженные числа, тогда

$$||(x - B)f|| = ||(x\bar{B} - 1)f||. \qquad (4)$$

Д О К А З А Т Е Л Ь С Т В О.

Воспользуемся тождеством для комплексных a и b: $|a-b|^2 = |a|^2 + |b|^2 - 2\mathbf{re}(a\bar{b})$. Получим, соответственно, для левой и правой части (4):

$$||(x-B)f|| = |Ba_0|^2 + \sum_{i=1}^{n} |a_{i-1} - Ba_i|^2 + |a_n|^2 =$$

$$|B|^2|a_0|^2 + |a_n|^2 + \sum_{i=1}^{n}(|a_{i-1}|^2 - 2\mathbf{re}(\bar{B}\bar{a}_i a_{i-1}) + |\bar{B}|^2|a_i|^2, \qquad (5)$$

$$||(x\bar{B}-1)f|| = |a_0|^2 + \sum_{i=1}^{n} |\bar{B}a_{i-1} - a_i|^2 + |\bar{B}a_n|^2 =$$

$$a_0^2 + |\bar{B}|^2|a_n|^2 + \sum_{i=1}^{n}(|\bar{B}||a_{i-1}|)^2 - 2\mathbf{re}(\bar{B}a_{i-1}\bar{a}_i) + |a_i|^2. \qquad (6)$$

Суммы (5) и (6) состоят из одних и тех же слагаемых.
□
С Л Е Д С Т В И Е 1.

$$\text{Если } f = a_n \prod_{i=1}^{n}(x-\alpha_j) \text{ и } f^* = a_n \prod_{|\alpha_j|\geq 1}(x-\alpha_j) \prod_{|\alpha_j|<1}(\bar{\alpha}_j x - 1), \text{ то } ||f|| = ||f^*||. \qquad (7)$$

Это равенство можно получить в результате применения леммы 2 к каждому сомножителю $(x - \alpha_j)$, у которого $|\alpha_j| < 1$.
Так как свободный член полинома f^* с точностью до знака равен $a_n \prod_{|\alpha_j|\geq 1} \alpha_j$, отсюда следует
С Л Е Д С Т В И Е 2.

$$||f||^2 \geq |a_n|^2 \prod_{|\alpha_j|\geq 1} |\alpha_j|^2. \qquad (8)$$

END
out :

END

Т Е О Р Е М А 1. (Неравенство Ландау-Миньотта)[Mignotte M., An Inequality about Factors of Polynomials. Math.Comp. 28 (1974), 1153-1157.]
Пусть $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i$ – полиномы с целыми коэффициентами и g является делителем f, тогда

$$\forall k (0 < k < m): \ |b_k| \leq \binom{m-1}{k-1}||f|| + \binom{m-1}{k}|a_n|. \qquad (9)$$

Д О К А З А Т Е Л Ь С Т В О.
Пусть $f = a_n \prod_{i=1}^{n}(x-\alpha_j)$, обозначим $M_a = \prod_{j=1}^{n} max(1, |\alpha_j|)$, рассмотрим коэффициенты $a_k = a_n \sum_{i_1<..<i_k} \alpha_{i_1}\alpha_{i_2}..\alpha_{i_k}$ полинома f и применим лемму 1:

$$|a_k| = |a_n| \sum_{i_1<..<i_k} |\alpha_{i_1}||\alpha_{i_2}|..|\alpha_{i_k}| \leq$$

$$|a_n| \sum_{i_1<..<i_k} max(1, |\alpha_{i_1}|)max(1, |\alpha_{i_2}|)..max(1, |\alpha_{i_k}|) \leq |a_n|(\binom{n-1}{k-1}M + \binom{n-1}{k}).$$

Обозначим $M_b = \prod_{j=1}^{m} max(1, |\beta_j|)$, где β_j – корни полинома g.
Аналогично получим

$$|b_k| \le |b_m|(\binom{m-1}{k-1}M_b + \binom{m-1}{k}). \qquad (10)$$

В соответствии с неравенством (8) и принятыми обозначениями для M_a и M_b: $||f||^2 \ge |a_n|^2 M_a^2$ и $||g||^2 \ge |b_m|^2 M_b^2$.

Так как все корни полинома g являются корнями и полинома f, то $M_b \le M_a$.

А так как g делит f, то и $|b_m| \le |a_n|$.

Подставляя эти неравенства в (10), получим утверждение теоремы (9).

□

С Л Е Д С Т В И Е 1.

Пусть f и $g = \sum_{i=0}^m b_i x^i$ – полиномы с целыми коэффициентами и g является делителем f, тогда

$$||g|| \le ||f||\binom{2m}{m}^{1/2} \le 2^m ||f|| (\pi m)^{-1/4} exp(\frac{-36m+1}{12m(12m+1)}) \le 2^m ||f|| \qquad (11)$$

Д О К А З А Т Е Л Ь С Т В О. Так как $|a_n| \le ||f||$, то из (9) следует

$$\forall k(0 < k < m):\ b_k \le \binom{m-1}{k-1}||f|| + \binom{m-1}{k}|a_n| \le ||f||(\binom{m-1}{k-1} + \binom{m-1}{k}) = ||f||\binom{m}{k}.$$

$$||g||^2 = \sum_{i=0}^m |b_i|^2 \le ||f||^2 \sum_{i=0}^m \binom{m}{k}^2 = ||f||^2\binom{2m}{m}.$$

Последнее равенство легко доказать, сравнивая коэффициенты при t^m в левой и правой части равенства $(1+t)^m(1+t)^m = (1+t)^{2m}$ и учитывая симметрию $\binom{m}{k} = \binom{m}{m-k}$.

Для завершения доказательства (11) воспользуемся формулой Симпсона для оценки факториалов:

$$(2\pi m)^{1/2}(m/\mathbf{e})^m e^{1/(12m+1)} \le m! \le (2\pi m)^{1/2}(m/\mathbf{e})^m e^{1/(12m)})$$

□

П О Г Р Е Ш Н О С Т Ь.

Покажем, что множитель при $2^m||f||$ в (11) мало толичается от единицы. И им можно пренебрегать в практических оценках коэффициентов полиномов.

$S = \mathbf{O}_{11,2}; S = (s_{i,j}); m = 2;$

$for(i = 1; i < 12; i = i + 1)\{s_{i,2} = m; s_{i,1} = \mathbf{value}((\pi m)^{-1/4} e^{\ (-36m+1)/(12m(12m+1))}); m = m + 50;\}S^T$

$out:$

$$\begin{pmatrix} 0.561 & 0.278 & 0.236 & 0.214 & 0.199 & 0.188 & 0.18 & 0.173 & 0.168 & 0.163 & 0.159 \\ 2 & 52 & 102 & 152 & 202 & 252 & 302 & 352 & 402 & 452 & 502 \end{pmatrix}$$