Оптимизация оценки для коэффициентов делителей полиномов над целыми числами

Е. А. Поцелуевкая

1. Введение

Как известно, задача разложения на неприводимые множители многочлена с целыми коэффициентами от одной переменной была решена давно. Были созданы алгоритмы, позволяющие находить требуемое разложение за конечное число шагов. Один из таких алгоритмов был получен в 1882 году Кронекером, чьим именем он и называется, хотя за сто лет до Кронекера этот был известен австрийскому астроному Шуберту. Однако помимо известного алгоритма Кронекера, есть другое решение задачи факторизации за конечное число шагов, которое следует из того, что коэффициенты делителя — целые числа и их абсолютная величина ограничена сверху некоторой функцией от коэффициентов делимого. При реализации таких алгоритмов факторизации полиномов, а также алгоритма вычисления наибольшего общего делителя примитивных многочленов с целыми коэффициентами, количество итераций программы напрямую зависит от оценки модулей коэффициентов делителей полинома через коэффициенты самого полинома. Существующие на данный момент оценки недостаточно точны, что приводит к дополнительным затратам времени при расчётах.

В настоящей работе предпринята попытка получения более точной оценки для модулей коэффициентов делителей целочисленных полиномов в целях усовершенствования указанных алгоритмов, направленного на увеличение их быстродействия.

2. Существующие на текущий момент оценки для коэффициентов делителей целочисленных полиномов

Пусть $F(x) \in \mathbb{Z}[x]$ и $F(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, a_n \neq 0$.

Определение 1. Обозначим $L(F) = |a_n| + |a_{n-1}| + \ldots + |a_0|$ и назовём эту величину *длиной полинома* $F(x)$.

Определение 2. *Высотой полинома* $F(x)$ называется величина $H(F) = \max\{|a_n|, \cdots, |a_0|\}$.

Пусть $Q(x), F(x) \in \mathbb{Z}[x]$, при этом $Q(x)$ имеет вид $Q(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ и является делителем полинома $F(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$. Необходимо найти верхнюю оценку для величин L(Q) и H(Q) в зависимости от характеристик полинома $F(x)$.

В дальнейшем помимо оцениваемых значений $L(Q)$ и $H(Q)$ нам понадобятся следующие величины:

Обозначение. Пусть $F = \sum\limits_{k=0}^{n} a_k x^k$. Положим $M(F) = |a_n| \prod\limits_{j=1}^{n} \max\{1, |z_j|\}$.

Обозначение. Пусть $F = \sum\limits_{k=0}^{n} a_k x^k$. Положим $\|F\| = (\sum\limits_{k=0}^{n} |a_k|^2)^{\frac{1}{2}}$.

Определение 3. *Нормой Бомбьери* называется величина $[F]_2 = \sqrt{\sum\limits_{j=0}^{n} (|a_j|^2 / C_n^j)}$.

Существует несколько способов оценки для коэффициентов делителей полиномов, выведенные из известных неравенств Коши и Ландау.

Теорема 1 (Неравенство Коши). *Пусть $n \geqslant 1$, $F(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_n \neq 0$ — полином с комплексными коэффициентами. Тогда любой корень z полинома $F(x)$ удовлетворяет неравенству:*

$$|z| < 1 + \frac{\max\{|a_{n-1}|, \ldots, |a_0|\}}{|a_n|}.$$

Доказательство. Пусть $F(z) = 0$. Если $|z| \leqslant 1$, то утверждение теоремы тривиально.

Предположим, что $|z| > 1$ и положим $H = \max\{|a_{n-1}|, \dots, |a_0|\}$. По предположению $a_n z^n = -a_{n-1}z^{n-1} - \dots - a_0$. Следовательно,

$$|a_n||z|^n \leqslant H(|z|^{n-1} + \dots + 1) < \frac{H|z|^n}{|z| - 1},$$

то есть $|a_n|(|z| - 1) < H$. Теорема доказана.

Воспользуемся неравенством Коши для получения оценки коэффициентов делителя полинома, которая известна как неравенство Ландау.

Пусть $F = \sum\limits_{k=0}^{n} a_k x^k$. Положим $\|F\| = (\sum\limits_{k=0}^{n} |a_k|^2)^{\frac{1}{2}}$ и $M(F) = |a_n| \prod\limits_{j=1}^{n} \max\{1, |z_j|\}$.

Теорема 2 (Неравенство Ландау). *Предположим, что полином $F(x)$ задан формулой $F(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0, a_n \neq 0$. Пусть $z_1, \dots, z_n$ — корни полинома $F(x)$. Тогда $M(F) \leqslant \|F\|$.*

Для доказательства теоремы нам понадобится следующая лемма.

Лемма 1. *Если Q — полином и z — комплексное число, то*

$$\|(x + z)Q(x)\| = \|(\overline{z}x + 1)Q(x)\|. \tag{1}$$

Доказательство. Пусть $Q(x) = \sum\limits_{k=0}^{n} c_k x^k$. Тогда квадрат выражения в левой части равенства (1) равен

$$\sum_{k=0}^{m+1} (c_{k-1} + zc_k)(\overline{c_{k-1}} + \overline{zc_k}) = (1 + |z|^2)\|Q\|^2 + \sum_{k=0}^{m+1} (zc_k\overline{c_{k-1}} + \overline{zc_k}c_{k-1})$$

(полагаем $c_{-1} = c_{m+1} = 0$). Этому же выражению равен и квадрат правой части. Лемма доказана.

Докажем теперь теорему:

Доказательство теоремы 2. Пусть $z_1, \dots, z_k$ — корни полинома $F(x)$, лежащие вне единичного круга. Тогда $M(F) = |a_n||z_1 \cdot \ldots \cdot z_k|$.

Положим $R(x) = a_n \prod\limits_{j=1}^{k} (\bar{z}_j x - 1) \prod\limits_{j=k+1}^{n} (x - z_j) = b_n x^n + \ldots + b_0$, k-кратное применение леммы даёт $\|F\| = \|R\|$. Однако $\|R\|^2 \geqslant |b_n|^2 = (M(F))^2$. Теорема доказана.

Теорема 3. *Пусть* $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0$, $b_m \neq 0$ — *делитель полинома* $F(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0, a_n \neq 0$. *Тогда*

$$|b_m| + |b_{m-1}| + \ldots + |b_0| \leqslant \left| \frac{b_m}{a_n} \right| 2^m \|F\|.$$

Доказательство. Легко проверяется, что $|b_m| + |b_{m-1}| + \ldots + |b_0| \leqslant 2^m M(Q)$, но

$$M(Q) \leqslant \left| \frac{b_m}{a_n} \right| M(F)$$

и из неравенства Ландау следует, что $M(F) \leqslant \|F\|$. Теорема доказана.

Теперь приведём уже известные оценки для величины H(Q). Пусть $z_1, \dots, z_n$ — (в общем случае комплексные) корни полинома $Q(x)$, посчитанные с учётом их кратностей. По известным формулам Виета:

$$\frac{b_{m-j}}{b_m} = (-1)^{m-j} \sum_{i_1 < \ldots < i_j} z_{i_1} \ldots z_{i_j}.$$

Отсюда следуют неравенства: $|b_j| \leqslant C_m^j M(Q)$ и $H(Q) \leqslant C_m^{[m/2]} M(Q)$, где $C_m^j = \frac{m!}{j!(m-j)!}$ — число сочетаний из m по j.

Ещё одна оценка для $|b_j|$ приведена ниже.

Теорема 4. *Пусть* $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$ — *делитель полинома* $F(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, a_n \neq 0$. *Тогда* $|b_j| \leqslant C_{m-1}^j \|F\| + C_{m-1}^{j-1} |a_n|$, $j = 0, \dots, m$.

Доказательство. Пусть $z_1, \dots, z_n$ — (в общем случае комплексные) корни полинома $Q(x)$, посчитанные с учётом их кратностей. По формулам Виета:

$$\frac{b_{m-j}}{b_m} = (-1)^{m-j} \sum_{i_1 < \ldots < i_j} z_{i_1} \ldots z_{i_j}, j = 1, 2, \dots, m.$$

Следовательно, $|b_{m-j}| \leqslant |b_m| \sum\limits_{i_1<\ldots<i_j} \max\{1,|z_{i_1}|\},\ldots,\max\{1,|z_{i_j}|\}$.

Рассмотрим элементарную симметричную функцию $\sigma_{nk} = \sum\limits_{i_1<\ldots<i_k} x_{i_1}\ldots x_{i_k}$. При $x_1 \geqslant 1,\ldots,x_n \geqslant 1$ и $x_1\ldots x_n = M$ для неё выполнено: $\sigma_{nk} = \sum\limits_{i_1<\ldots<i_k} x_{i_1}\ldots x_{i_k} \leqslant C_{n-1}^{k-1} + C_{n-1}^{k}$. В правой части неравенство стоит предполагаемое значение при $x_1 = \ldots = x_{n-1} = 1$ и $x_n = M$. Если же $x_1 \leqslant \ldots \leqslant x_n < M$, то преобразование $x_n \leftarrow x_n x_{n-1}$, $x_{n-1} \leftarrow 1$ увеличивает σ_{nk} на $\sigma_{(n-2)(k-1)}(x_n-1)(x_{n-1}-1)$, являющуюся положительной величиной.

Далее, $|b_j| \leqslant C_{m-1}^{j} M(Q) + C_{m-1}^{j-1}|b_m| \leqslant C_{m-1}^{j} M(F) + C_{m-1}^{j-1}|a_n|$, поскольку $M(Q) \leqslant M(F)$ и $|b_m| \leqslant |a_n|$.

Пользуясь неравенством Ландау, получаем: $|b_j| \leqslant C_{m-1}^{j}\|F\| + C_{m-1}^{j-1}|a_n|$. Теорема доказана.

Одна из лучших известных оценок на $H(Q)$ использует норму Бомбьери $[F]_2 = \sqrt{\sum\limits_{j=0}^{n}(|a_j|^2/C_n^j)}$ и выглядит следующим образом:

$$H(Q) \leqslant l_n[F]_2, \text{ где } l_n = \frac{3^{3/4}3^{n/2}}{2(\pi n)^{1/2}}.$$

3. Оптимизация существующих оценок

Сформулируем и докажем теорему, позволяющую наилучшим образом оценить высоту делителя через высоту делимого в случае, когда степень делителя на единицу меньше степени делимого.

Теорема 5. *Пусть $Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0$ — делитель полинома $F(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, a_n \neq 0$. Тогда $H(Q) \leqslant]\frac{n}{2}[(F)$.*

Равенство в этой оценке достигается, как следует из леммы ниже.

Лемма 2. *Для любого натурального n существует полином $F(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, a_n \neq 0$, с делителем $Q(x) = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0, b_m \neq 0$, такой что $H(Q) =]\frac{n}{2}[H(F)$.*

Доказательство.

1) Пусть n нечётно, то есть $n = 2k-1$. В этом случае рассмотрим в качестве $F(x)$ полином вида $x^{2k-1}+x^{2k-2}+\ldots+x^k-x^{k-1}-\ldots-x-1$ и $Q(x) = x^{2k-2}+2x^{2k-3}+3x^{2k-4}+\ldots+kx^{k-1}+(k-1)x^{k-2}+\ldots+2x+1$. Проверим, что $Q(x)$ — делитель $F(x)$:

$$(x^{2k-2} + 2x^{2k-3} + 3x^{2k-4} + \ldots + kx^{k-1} + (k-1)x^{k-2} + \ldots$$
$$\ldots + 2x + 1)(x-1) = x^{2k-1} + 2x^{2k-2} + 3x^{2k-3} + \ldots + kx^k +$$
$$+(k-1)x^{k-1}+\ldots+2x^2+x-x^{2k-2}-2x^{2k-3}-3x^{2k-4}-\ldots-kx^{k-1}-$$
$$-(k-1)x^{k-2}-\ldots-2x-1=x^{2k-1}+x^{2k-2}+\ldots+x^k-x^{k-1}-\ldots-x-1.$$

Тогда $H(F) = \max\{|1|,\ldots,|1|,|-1|,\ldots,|-1|\} = 1$ и $H(Q) = \max\{|1|,|2|,|3|,\ldots,|k|,\ldots,|3|,|2|,|1|\} = k =]\frac{n}{2}[H(F)$.

2) Пусть теперь n чётно: $n = 2k$. Аналогичным образом возьмём $F(x) = x^{2k}+x^{2k-2}+x^{2k-3}+\ldots+x^k-x^{k-1}-\ldots-x-1$ и $Q(x) = x^{2k-1}+x^{2k-2}+2x^{2k-3}+3x^{2k-4}+\ldots+kx^{k-1}+(k-1)x^{k-2}+\ldots+2x+1$. Проверим, что $Q(x)$ — делитель $F(x)$:

$$(x^{2k-1} + x^{2k-2} + 2x^{2k-3} + 3x^{2k-4} + \ldots + kx^{k-1} +$$
$$+ (k-1)x^{k-2} + \ldots + 2x + 1)(x-1) = x^{2k} + x^{2k-1} + 2x^{2k-2} + \ldots$$
$$\ldots + kx^k + (k-1)x^{k-1} + \ldots + 2x^2 + x - x^{2k-1} - x^{2k-2} -$$
$$- 2x^{2k-3} - \ldots - kx^{k-1} - (k-1)x^{k-2} - \ldots - 2x - 1 =$$
$$= x^{2k} + x^{2k-2} + \ldots + x^k - x^{k-1} - \ldots - x - 1.$$

Тогда $H(F) = \max\{|1|,|0|,|1|,\ldots,|1|,|-1|,\ldots,|-1|\} = 1$ и $H(Q) = \max\{|1|,|1|,|2|,|3|,\ldots,|k|,\ldots,|3|,|2|,|1|\} = k =]\frac{n}{2}[H(F)$.

Лемма доказана.

Перейдём к доказательству теоремы

Доказательство теоремы 5. В условиях теоремы полином $F(x)$ имеет вид:

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 =$$
$$= (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0)(cx + d) =$$
$$= cb_{n-1}x^n + (cb_{n-2} + db_{n-1})x^{n-1} + \ldots + (cb_0 + db_1)x + b_0 d$$

При $d = 0$ очевидно, что утверждение верно. Будем считать, что $d \neq 0$ и $c > 0$, в противном случае выносим минус за скобки. Обозначим $a = H(F)$. Тогда:

$$\begin{cases} |db_0| \leqslant a \\ |cb_0 + db_1| \leqslant a \\ |cb_1 + db_2| \leqslant a \\ \cdots \\ |cb_{n-2} + db_{n-1}| \leqslant a \\ |cb_{n-1}| \leqslant a \end{cases}.$$

Из этих неравенств вытекает:

$$\begin{cases} -\frac{a}{d} \leqslant b_0 \leqslant \frac{a}{d} & \text{при } d > 0 \\ \frac{a}{d} \leqslant b_0 \leqslant -\frac{a}{d} & \text{при } d < 0 \end{cases};$$

$$\begin{cases} -\frac{a}{d} - \frac{c}{d}b_0 \leqslant b_1 \leqslant \frac{a}{d} - \frac{c}{d}b_0 & \text{при } d > 0 \\ \frac{a}{d} - \frac{c}{d}b_0 \leqslant b_1 \leqslant -\frac{a}{d} - \frac{c}{d}b_0 & \text{при } d < 0 \end{cases};$$

$$\begin{cases} -\frac{a}{d} - \frac{c}{d}\frac{a}{d} \leqslant b_1 \leqslant \frac{a}{d} + \frac{c}{d}\frac{a}{d} & \text{при } d > 0 \\ \frac{a}{d} - \frac{c}{d}\frac{a}{d} \leqslant b_1 \leqslant -\frac{a}{d} + \frac{c}{d}\frac{a}{d} & \text{при } d < 0 \end{cases};$$

$$\begin{cases} -\frac{a}{d} - \frac{c}{d}b_1 \leqslant b_2 \leqslant \frac{a}{d} - \frac{c}{d}b_1 & \text{при } d > 0 \\ \frac{a}{d} - \frac{c}{d}b_1 \leqslant b_2 \leqslant -\frac{a}{d} - \frac{c}{d}b_1 & \text{при } d < 0 \end{cases};$$

$$\begin{cases} -\frac{a}{d} + \frac{c}{d}(-\frac{a}{d} - \frac{c}{d}\frac{a}{d}) \leqslant b_2 \leqslant \frac{a}{d} + \frac{c}{d}(\frac{a}{d} + \frac{c}{d}\frac{a}{d}) & \text{при } d > 0 \\ \frac{a}{d} - \frac{c}{d}(\frac{a}{d} - \frac{c}{d}\frac{a}{d}) \leqslant b_2 \leqslant -\frac{a}{d} - \frac{c}{d}(-\frac{a}{d} + \frac{c}{d}\frac{a}{d}) & \text{при } d < 0 \end{cases};$$

$$\begin{cases} |b_2| \leqslant \frac{a}{d}(1 + \frac{c}{d} + \frac{c^2}{d^2}) & \text{при } d > 0 \\ |b_2| \leqslant -\frac{a}{d}(1 + \frac{c}{d} - \frac{c^2}{d^2}) & \text{при } d < 0 \end{cases}.$$

Продолжая таким образом выражать каждый следующий коэффициент через предыдущий, получим следующую оценку для коэффициентов $Q(x)$:

$$|b_k| \leqslant \frac{a}{|d|}(1 + \frac{c}{|d|} + \frac{c^2}{|d|^2} + \cdots + \frac{c^k}{|d|^k}), k = 0, \cdots, n-1.$$

С другой стороны, аналогичным образом получается ограничение на коэффициенты, если начинать их оценивать не со свободного члена b_0, а со старшего коэффициента b_{n-1}.

$$-\frac{a}{c} \leqslant b_{n-1} \leqslant \frac{a}{c};$$

$$-\frac{a}{c}-\frac{d}{c}b_{n-1}\leqslant b_{n-2}\leqslant \frac{a}{c}-\frac{d}{c}b_{n-1};$$

$$\begin{cases} -\frac{a}{c}-\frac{d}{c}\frac{a}{c}\leqslant b_{n-2}\leqslant \frac{a}{c}+\frac{d}{c}\frac{a}{c} & \text{при } d>0 \\ -\frac{a}{c}+\frac{d}{c}\frac{a}{c}\leqslant b_{n-2}\leqslant \frac{a}{c}-\frac{d}{c}\frac{a}{c} & \text{при } d<0 \end{cases};$$

$$-\frac{a}{c}-\frac{d}{c}b_{n-2}\leqslant b_{n-3}\leqslant \frac{a}{c}-\frac{d}{c}b_{n-2};$$

$$\begin{cases} -\frac{a}{c}+\frac{d}{c}(-\frac{a}{c}-\frac{d}{c}\frac{a}{c})\leqslant b_{n-3}\leqslant \frac{a}{c}+\frac{d}{c}(\frac{a}{c}+\frac{d}{c}\frac{a}{c}) & \text{при } d>0 \\ -\frac{a}{c}-\frac{d}{c}(-\frac{a}{c}+\frac{d}{c}\frac{a}{c})\leqslant b_{n-3}\leqslant \frac{a}{c}-\frac{d}{c}(\frac{a}{c}-\frac{d}{c}\frac{a}{c}) & \text{при } d<0 \end{cases};$$

$$\begin{cases} |b_{n-3}|\leqslant \frac{a}{c}(1+\frac{d}{c}+\frac{d^2}{c^2}) & \text{при } d>0 \\ |b_{n-3}|\leqslant \frac{a}{c}(1-\frac{d}{c}+\frac{d^2}{c^2}) & \text{при } d<0 \end{cases}.$$

Итак, вывели следующую оценку:

$$|b_{n-m-1}|\leqslant \frac{a}{c}(1+\frac{|d|}{c}+\frac{|d|^2}{c^2}+\cdots+\frac{|d|^m}{c^m}), m=0,\cdots,n-1$$

Сделав замену $k=n-m-1$, получим оценку для коэффициентов $Q(x)$:

$$\begin{cases} |b_k|\leqslant \frac{a}{|d|}(1+\frac{c}{|d|}+\frac{c^2}{|d|^2}+\cdots+\frac{c^k}{|d|^k}) \\ |b_k|\leqslant \frac{a}{c}(1+\frac{|d|}{c}+\frac{|d|^2}{c^2}+\cdots+\frac{|d|^{n-k-1}}{c^{n-k-1}}) \end{cases}, \text{при } k=0,\cdots,n-1.$$

То есть $|b_k|\leqslant \min\{\frac{a}{|d|}(1+\frac{c}{|d|}+\frac{c^2}{|d|^2}+\cdots+\frac{c^k}{|d|^k}), \frac{a}{c}(1+\frac{|d|}{c}+\frac{|d|^2}{c^2}+\cdots+\frac{|d|^{n-k-1}}{c^{n-k-1}})\}$.

Сделаем замену $x=\frac{c}{|d|}$. Так как $c>0$, то и $x>0$.

Рассмотрим функцию

$$y(x)=\min\{\frac{a}{|d|}(1+x+x^2+\cdots+x^k), \frac{a}{c}(1+\frac{1}{x}+\frac{1}{x^2}+\cdots+\frac{1}{x^{n-k-1}})\}$$

и найдём, при каких аргументах она принимает наибольшее значение.

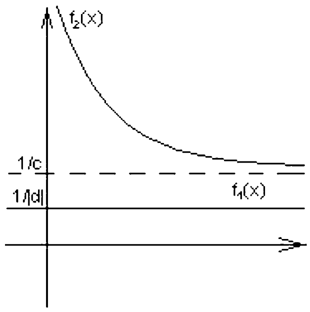
Обозначим:

$$f_1(x)=\frac{1}{|d|}(1+x+x^2+\cdots+x^k);$$

$$f_2(x)=\frac{1}{c}(1+\frac{1}{x}+\frac{1}{x^2}+\cdots+\frac{1}{x^{n-k-1}}).$$

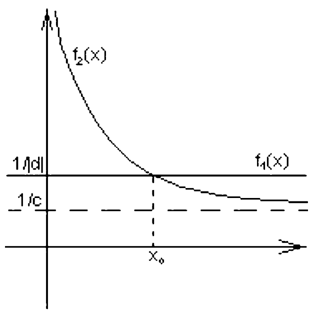
Возможны следующие случаи:

1) $k = 0, |d| \geqslant c$. Тогда $f_1(x) \equiv \frac{1}{|d|}, f_2(x) = \frac{1}{c}(1 + \frac{1}{x} + \frac{1}{x^2} + \cdots + \frac{1}{x^{n-1}})$ и для любого $x > 0$ $f_1(x) < f_2(x)$.



Значит, $y(x) = af_1(x) = \frac{a}{|d|}$ и $|b_k| \leqslant \frac{a}{|d|} \leqslant a \leqslant]\frac{n}{2}[a$, так как $d \geqslant 1$ и $n \geqslant 2$.

2) $k = 0, |d| < c$. Тогда $f_1(x) \equiv \frac{1}{|d|}, f_2(x) = \frac{1}{c}(1 + \frac{1}{x} + \frac{1}{x^2} + \cdots + \frac{1}{x^{n-1}})$.

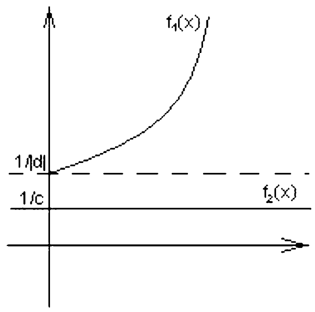


Как видно из рисунка, на промежутке $(0, x_0]$ $f_1(x) \leqslant f_2(x)$, а на (x_0, ∞) $f_2(x) < f_1(x)$. Значит,

$$y(x) = \begin{cases} \frac{a}{|d|} & \text{при } 0 < x \leqslant x_0 \\ \frac{a}{c}(1 + \frac{1}{x} + \frac{1}{x^2} + \cdots + \frac{1}{x^{n-1}}) & \text{при } x > x_0 \end{cases}.$$

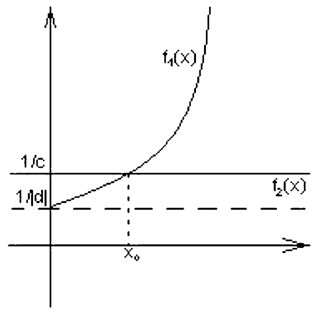
Итак, $|b_k| \leqslant \frac{a}{|d|} \leqslant a \leqslant]\frac{n}{2}[a$, так как $d \geqslant 1$ и $n \geqslant 2$.

3) $k = n-1, |d| \leqslant c$. Тогда $f_1(x) = \frac{1}{|d|}(1+x+x^2+\cdots+x^{n-1}), f_2(x) \equiv \frac{1}{c}$ и для любого $x > 0$ $f_2(x) < f_1(x)$.



Значит, $y(x) = af_2(x) = \frac{a}{c}$ и $|b_k| \leqslant \frac{a}{c} \leqslant a \leqslant]\frac{n}{2}[a$, так как $c \geqslant 1$ и $n \geqslant 2$.

4) $k{=}n{-}1, |d| > c$. Тогда $f_1(x) = \frac{1}{|d|}(1{+}x{+}x^2{+}\cdots{+}x^{n-1}), f_2(x) \equiv \frac{1}{c}$.

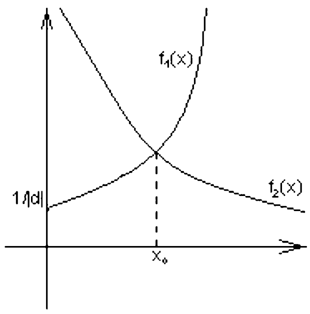


Как видно из рисунка, на промежутке $(0, x_0]$ $f_1(x) \leqslant f_2(x)$, а на (x_0, ∞) $f_2(x) < f_1(x)$. Значит,

$$y(x) = \begin{cases} \frac{a}{|d|}(1 + x + x^2 + \cdots + x^{n-1}) & \text{при } 0 < x \leqslant x_0 \\ \frac{a}{c} & \text{при } x > x_0 \end{cases}.$$

Итак, $|b_k| \leqslant \frac{a}{c} \leqslant a \leqslant]\frac{n}{2}[a$, так как $c \geqslant 1$ и $n \geqslant 2$.

5) $k \neq 0, n{-}1$. Тогда на промежутке $(0, \infty)$ функция $f_1(x)$ монотонно возрастает, а функция $f_2(x)$ монотонно убывает. Значит, на этом промежутке графики функций имеют единственную точку пересечения:



Как видно из рисунка, на промежутке $(0, x_0]$ $f_1(x) \leqslant f_2(x)$, а на (x_0, ∞) $f_2(x) < f_1(x)$. Значит,

$$y(x) = \begin{cases} \frac{a}{|d|}(1 + x + x^2 + \cdots + x^k) & \text{при } 0 < x \leqslant x_0 \\ \frac{a}{c}(1 + \frac{1}{x} + \frac{1}{x^2} + \cdots + \frac{1}{x^{n-k-1}}) & \text{при } x > x_0 \end{cases}$$

и в точке x_0 функция $y(x)$ достигает максимального значения. Следовательно, $|b_k| \leqslant y(x_0)$.

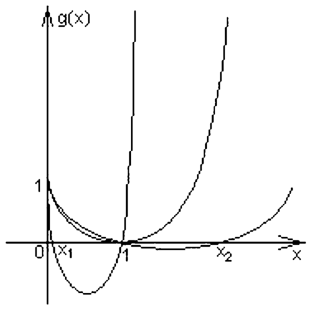
Для того чтобы оценить $y(x_0)$ найдём, какие значения может принимать x_0. В этой точке $f_1(x) = f_2(x)$, то есть $\frac{c}{|d|}(1 + x + x^2 + \cdots + x^k) = 1 + \frac{1}{x} + \cdots + \frac{1}{x^{n-k-1}}$.

Вспомним, что $x = \frac{c}{|d|}$, тогда получим уравнение: $x^{n-k}(1 + x + \cdots + x^k) = 1 + x + \cdots + x^{n-1-k}$.

Домножив обе части равенства на $x - 1$, получим: $x^{n-k}(x^{k+1} - 1) = x^{n-k} - 1$. Итак, необходимо оценить корни уравнения $x^{n+1} - 2x^{n-k} + 1 = 0$.

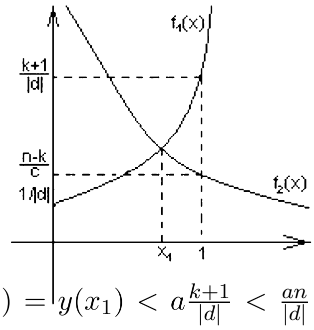
Рассмотрим функцию $g(x) = x^{n+1} - 2x^{n-k} + 1$, её производная $g'(x) = (n + 1)x^{n-k-1}(x^{k+1} - \frac{2(n-k)}{n+1})$.

$g'(x) < 0$ при $0 < x < \sqrt[k+1]{\frac{2(n-k)}{n+1}}$ и $g'(x) > 0$ при $x > \sqrt[k+1]{\frac{2(n-k)}{n+1}}$. На промежутке $(0, \sqrt[k+1]{\frac{2(n-k)}{n+1}})$ функция $g(x)$ убывает, а на $(\sqrt[k+1]{\frac{2(n-k)}{n+1}}, \infty)$ возрастает. Заметим, что $g(0) = 1$ и $g(1) = 0$. Значит, возможны следующие 3 случая расположения графика $g(x)$ относительно оси абсцисс:



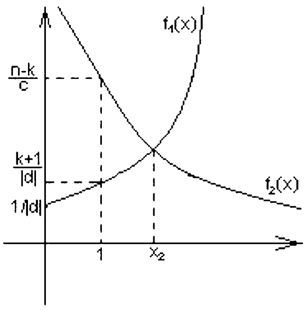
а) Касание в точке $x = 1$, то есть $x_0 = 1 = \sqrt[k+1]{\frac{2(n-k)}{n+1}}$. Отсюда $n = 2k+1$ и $k = \frac{n-1}{2}$.
Тогда $c = |d|$ и $|b_k| \leqslant a\min\{\frac{k+1}{|d|}, \frac{n-k}{c}\} \leqslant a(k+1) = a]\frac{n}{2}[$.

б) Пересечение в точках $0 < x_1 < 1$ и 1. Отсюда $k > \frac{n-1}{2}$ и $1 \leqslant c < |d|$. Тогда графики функций $f_1(x)$ и $f_2(x)$ расположены следующим образом:



Итак, $|b_k| \leqslant y(x_0) = y(x_1) < a\frac{k+1}{|d|} < \frac{an}{|d|} \leqslant \frac{an}{2} \leqslant a]\frac{n}{2}[$, так как $1 \leqslant c < |d|$ и $n \geqslant 2$.

в) Пересечение в точках $x_2 > 1$ и 1. Отсюда $k < \frac{n-1}{2}$ и $1 \leqslant |d| < c$. Тогда графики функций $f_1(x)$ и $f_2(x)$ расположены следующим образом:



Итак, $|b_k| \leqslant y(x_0) = y(x_2) < a\frac{n-k}{c} < \frac{an}{c} \leqslant \frac{an}{2} \leqslant a]\frac{n}{2}[$, так как $1 \leqslant |d| < c$ и $n \geqslant 2$.

Итак, рассмотрены все возможные случаи и доказано, что $|b_k| \leqslant]\frac{n}{2}[a, k = 0, \cdots, n-1$. Теорема доказана.

Следствие 1. *Пусть* $Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0$ — *делитель полинома* $F(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, a_n \neq 0$ *и* $F(x) = Q(x)H(x)$. *Тогда* $L(Q) \leqslant]\frac{n}{2}[nH(F)$.

Доказанные выше утверждения позволяют улучшить известные оценки для величин $H(Q)$ и $L(Q)$, как видно из примеров ниже.

Пример 1. Рассмотрим полином $F(x) = x^3 + x^2 - x - 1$ с делителем $Q(x) = x^2 + 2x + 1$. В этом случае $L(Q) = 4$ и $H(Q) = 2$. Для них получим следующие оценки:

1) $L(Q) \leqslant 8$ согласно Теореме 4 раздела 2. $L(Q) \leqslant 6$ согласно Следствию 1 данного раздела.
2) $H(Q) < 2,947$ согласно последнему неравенству раздела 2. $H(Q) \leqslant 2$ согласно Теореме 1 данного раздела.

Пример 2. Рассмотрим полином $F(x) = x^8+x^6+x^5+x^4-x^3-x^2-x-1$ с делителем $Q(x) = x^7 + x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1$. В этом случае $L(Q) = 17$ и $H(Q) = 4$. Для них получим следующие оценки:

1) $L(Q) < 363$ согласно Теореме 4 раздела 2. $L(Q) \leqslant 32$ согласно Следствию 1 данного раздела.
2) $H(Q) < 22,22$ согласно последнему неравенству раздела 2. $H(Q) \leqslant 4$ согласно Теореме 1 данного раздела.

4. Дальнейшее уточнение оценки для $H(Q)$

Утверждение 1. *Пусть* $Q(x) = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0$ — *делитель полинома* $F(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, a_n \neq 0$ *и* $F(x) = Q(x)H(x)$. *Оценку для величины* $H(Q)$ *невозможно улучшить до значения* $H(Q) \leqslant]\frac{n}{2}[H(F)$ *для произвольной степени делителя* $Q(x)$.

Доказательство. Контрпримером служит многочлен $F(x) = x^8 + x^7 + x^6 - x^2 - x - 1$ с делителем $Q(x) = -x^5 - 3x^4 - 5x^3 - 5x^2 - 3x - 1$, для которых $\frac{H(Q)}{H(F)} = 5 >]\frac{n}{2}[H(F) = 4$. Утверждение доказано.

5. Заключение

1) Исследования, приведённые в работе, позволили доказать, что для любого натурального n если $Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0$ — делитель полинома $F(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, a_n \neq 0$, то $H(Q) \leqslant]\frac{n}{2}[(F)$.
2) Равенство в данной оценке достигается, что подтверждается примерами.
3) Оценку для величины $H(Q)$ невозможно улучшить до значения $H(Q) \leqslant]\frac{n}{2}[H(F)$ для произвольной степени делителя $Q(x)$.
4) Пусть $Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0$ — делитель полинома $F(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, a_n \neq 0$ и $F(x) = Q(x)H(x)$. Тогда $L(Q) \leqslant]\frac{n}{2}[nH(F)$.

Автор выражает благодарность А. Е. Панкратьеву за научное руководство.

Список литературы

[1] Панкратьев Е. В. Элементы компьютерной алгебры / Конспекты спецкурса.

[2] Панкратьев Е. В. Компьютерная алгебра. Факторизация многочленов. М.: Изд-во МГУ, 1988.

[3] Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. М.–СПб–Киев: Изд. дом «Вильямс», 2003.

[4] Mignotte M. Mathematics for computer algebra. New York: Springer-Verlag, Inc., 1992.

[5] Panaitopol Laurentiu, Stefanescu Doru. Inequalities on polynomial heights // Journal of Inequalities in Pure and Applied Mathematics. Vol. 1. Iss. 1. Art. 7. 2001.