S. B. Gashkov, The complexity of monotone calculations of polynomials, *Vestnik Moskov. Univ. Ser. 1. Mat. Mekh.*, 1987, Number 5, 7–13

МАТЕМАТИКА

УДК 519

С. Б. Гашков

О СЛОЖНОСТИ МОНОТОННЫХ ВЫЧИСЛЕНИЙ МНОГОЧЛЕНОВ

В 1983 г. О. М. Касим-заде [1] построил многочлен степени n от n переменных с аддитивной монотонной сложностью $O(2^{n/2})$, усилив один из результатов К. П. Шнорра, указавшего в [2] многочлен степени n^2 от $4n^2$ переменных с аддитивной монотонной сложностью

$$C_{2n}^{n}-1=O\left(2^{2n}/\sqrt{n}\right).$$

Близкие к этому результаты получил в 1984 г. С. Е. Кузнецов [3].

В настоящей работе обобщаются методы [1, 2]. Отметим, что это обобщение не удается применить к оценке монотонной сложности булевых функций. Другим методом А. Е. Андреев [4] получил почти экспоненциальную оценку монотонной сложности булевых функций.

Будем рассматривать многочлены, вычисляемые схемами в базисе $\{x+y,\ xy\}\cup\mathbf{R}_+$. Для любого такого многочлена $f(x_1, \ldots, x_n)$ обозначим $L_+(f)$ — наименьшее число сложений, а $L_\times(f)$ — наименьшее число умножений, требуемые для его вычисления.

Пусть $\mathbf{R}_+[x_1, \ldots, x_n]$ — полукольцо монотонных многочленов с операциями $+$, $\cdot$, $\mathbf{P}(\mathbf{N}^n)$ — полукольцо подмножеств множества $\mathbf{N}^n$ (где $\mathbf{N}=\{0, 1, 2, \ldots\}$) с операциями $\cup$ и $\times$ (где $A\times B=\{a+b: a\in A,\ b\in B\}$), $\mathbf{R}_+[x_1, \ldots, x_n]\xrightarrow{\mathrm{mon}}\mathbf{P}(\mathbf{N}^n)$ — гомоморфизм полуколец, такой, что $\alpha\in\operatorname{mon} f\Leftrightarrow\alpha=(\alpha_1, \ldots, \alpha_n)\in\mathbf{N}^n\ \&\ a_\alpha x_1^{\alpha_1}\ldots x_n^{\alpha_n}$ — одночлен многочлена $f(x_1, \ldots, x_n)$.

Подмножество H полугруппы $(G, +)$ назовем k-редким, если оно не содержит подмножеств вида $A\times B=\{a+b: a\in A,\ b\in B\}$, где $A=\{a_1, \ldots, a_k\}\subset G$, $B=\{b_1, \ldots, b_k\}\subset G$. Если $(G, +)$ — группа, то это определение эквивалентно следующему: для различных элементов $g_1, \ldots, g_k\in G$ мощность пересечения $\bigcap_{i=1}^{k} g_iH$, где $g_iH=\{g_i\}\times H$, меньше k.

Обозначим $\alpha(k)$ последовательность, определяемую равенствами $\alpha(2)=2$, $\alpha(3)=3$, $\alpha(4)=5$, $\alpha(k)=2^{k-2}$ при $k>4$. Всюду далее $f(n)\geqslant O(g(n))$ означает неравенство по порядку.

Теорема 1. *Пусть $k>1$ и $\operatorname{mon} f$ — k-редкое подмножество $(\mathbf{N}^n, +)$, тогда справедливы неравенства*

(i) $L_+(f)\geqslant\dfrac{|\operatorname{mon} f|}{(k-1)^3}-1$;

(ii) $L_\times(f)+n\geqslant O(|\operatorname{mon} f|^{1/2}k^{-3/2})$, *а если* $|\operatorname{mon} f|k^{-3}\geqslant O(\alpha(k)^2)$, *то*

$$L_\times(f)+n\geqslant O(k^{-3/2})\,|\operatorname{mon} f|^{\frac{\alpha(k)}{2\alpha(k)-1}};$$

(iii) *если* $k=2$ *и* $|\operatorname{mon} f|n^{-3/2}\to\infty$, *то* $L_\times(f)\geqslant 2|\operatorname{mon} f|^{2/3}$.

Замечание. Подмножество H группы $(G, +)$ назовем полуразностным, если для любых элементов $a, b, c, d \in H$ $0 \neq a-b=c-d \Rightarrow$ $\Rightarrow \begin{cases} a=c \\ b=d \end{cases}$.

В абелевой группе любое полуразностное множество является 2-редким, поэтому из теоремы можно вывести результат О. М. Касимзаде [1].

Согласно Шнорру [2], подмножество $M \subset \mathbf{N}^n$ называется разделенным, если $r+u=s+t \Rightarrow r=s \vee r=t$ для любых элементов $r, s, t \in M$, $u \in \mathbf{N}^n$. Разделенное множество является полуразностным и, следовательно, 2-редким, поэтому из теоремы вытекают все результаты пункта 4 [2]. Один из них можно даже несколько обобщить. А именно, если f состоит из одночленов вида $\prod_{i \in I,\ j \in J} x_{i,j}$, где $\varnothing \neq I$, $J \subseteq \{1, 2, \ldots, n\}$, и если мощности подмножеств I, J не обязательно одинаковы, то множество $\operatorname{mon} f$ не является, вообще говоря, разделенным, но является 2-редким.

Докажем теорему 1. Используемые далее определения можно найти в [5, 6]. От схем в базисе $\{x+y, xy\} \cup \mathbf{R}_+$ перейдем к схемам в базисе

$$\{0\} \cup \{u \vee v,\ u \times v\} \cup \{\{a_i\} \in \mathbf{P}(\mathbf{N}^n) : a_i = (\overbrace{0, \ldots, 0}^{i}, 1, 0, \ldots, 0)\}.$$

Лемма 1. *Справедливы неравенства*

$$L_+(f) \geqslant L_\vee(\operatorname{mon} f), \quad L_\times(f) \geqslant L_\times(\operatorname{mon} f).$$

Для каждого элемента e схемы рассмотрим подсхему, состоящую из элемента e и всех его предков. Элемент полукольца $\mathbf{P}(\mathbf{N}^n)$, вычисляемый этой подсхемой, обозначим $\varphi(e)$. Мощность $\varphi(e)$ назовем весом e. Везде далее предполагаем, что множество $\operatorname{mon} f$ — k-редкое. Рассмотрев цепь, соединяющую элемент e с выходом схемы, и применив индукцию, получим, что для некоторого $A \subset \mathbf{N}^n$ справедливо включение $\varphi(e) \times A \subseteq \operatorname{mon} f$. Отсюда следует

Лемма 2. *Хотя бы один предок любого элемента умножения имеет вес меньше k.*

Пусть e — произвольный элемент умножения и e_1, e_2 — его предки. Можно считать, что $|\varphi(e_2)| < k$. Заменим e на одновходовый элемент e', осуществляющий умножение входа на $\varphi(e_2) \in \mathbf{P}(\mathbf{N}^n)$. Выход элемента e_1 подадим на вход элемента e'. Ребро, соединяющее выход элемента e_2 с входом элемента e, уничтожим. Все остальные элементы и ребра оставим без изменения, в том числе и ребра, выходившие из e (теперь они выходят из e'). Далее $\varphi(e_2)$ обозначим через $\psi(e')$. Повторив эту операцию несколько раз, получим схему, состоящую только из элементов дизъюнкции, 1-входовых элементов и констант, вычисляющую множество $\operatorname{mon} f$ и имеющую не большую сложность, чем исходная схема. Действуя аналогично, заменим каждый элемент e веса, меньшего k, на константу, реализующую $\varphi(e)$.

Пусть Ц — произвольная цепь, соединяющая выход элемента e с выходом схемы, и $e_1', \ldots, e_m'$ — все 1-входовые элементы в Ц. Обозначим произведение $\psi(e_1') \times \ldots \times \psi(e_m')$ через $\Psi(\text{Ц})$. Если $m=0$, то положим $\Psi(\text{Ц}) = \{0\}$. Дизъюнкцию всех таких произведений, взятую по всем цепям, выходящим из e, обозначим $\Psi(e)$.

Множество элементов схемы назовем сечением, если любая цепь от констант к выходу схемы проходит хотя бы через один из элементов этого множества.

По индукции доказывается

Лемма 3. *Пусть $\mathfrak{S}$ — произвольное сечение. Тогда справедливо равенство* $\operatorname{mon} f=\bigvee\limits_{e\in\mathfrak{S}}\varphi(e)\times\Psi(e)$.

Можно считать, что в схеме есть хотя бы один элемент $\vee$. В каждой цепи, проходящей от констант к выходу схемы, выберем элемент $\vee$, не имеющий в этой цепи среди предков ни одного элемента дизъюнкции. Множество всех выбранных элементов образует сечение, которое обозначим $\mathfrak{B}=\{b_1, \ldots, b_m\}$. Множество элементов, лежащих в этих цепях непосредственно перед элементами из $\mathfrak{B}$ и не имеющих позади элементов $\vee$, тоже будет сечением; обозначим его $\mathfrak{C}=\{c_1, \ldots, c_t\}$.

Превратим элементы $\mathfrak{C}$ в константы, реализующие $\varphi(c_i)$, $i=1, \ldots, t$. Матрицу смежности вершин двудольного графа с долями $\mathfrak{B}$ и $\mathfrak{C}$ обозначим (β_{ij}). Из леммы 3 следует

Лемма 4: $\operatorname{mon} f=\bigvee\limits_{j}\varphi(b_j)\times\Psi(b_j)=\bigvee\limits_{\beta_{ij}=1}\varphi(c_i)\times\Psi(b_j)$.

Заметим, что $|\Psi(b_j)|<k$ для любого j, так как в противном случае $\varphi(b_j)\times\Psi(b_j)\subset\operatorname{mon} f$, что противоречит k-редкости $\operatorname{mon} f$.

Лемма 5. *Если $A_1\times\ldots\times A_p$ — k-редкое множество и $|A_i|<k$ при всех i, то $|A_1\times\ldots\times A_p|\leqslant(k-1)^3$.*

Действительно, пусть s таково, что $|A_1\times\ldots\times A_{s-1}|<k$, $|A_1\times\ldots\times A_s|\geqslant k$. Тогда $|A_{s+1}\times\ldots\times A_p|<k$ (иначе $A_1\times\ldots\times A_p$ не будет k-редким), и поэтому $|A_1\times\ldots\times A_p|\leqslant|A_1\times\ldots\times A_{s-1}|\times|A_s|\times|A_{s+1}+\ldots\times A_p|\leqslant(k-1)^3$.

Из лемм 4, 5 вытекает, что $\sum\limits_{i,j}\beta_{ij}\geqslant(k-1)^{-3}|\operatorname{mon} f|$. Остается повторить рассуждения, дающие оценку числа 2-входовых элементов схемы через число ее входов и констант (см., например, [5, с. 50]), и заметить, что $L_\vee(\operatorname{mon} f)\geqslant\sum\limits_{i,j}\beta_{ij}-1$. Неравенство (i) доказано.

Вернемся к рассмотрению исходной схемы, построенной из элементов $\vee$, 1-входовых элементов и констант $\{0\}$, $\{a_i\}$, $i=1, \ldots, n$. На каждой цепи, проходящей через любой элемент c_i, выберем его ближайшего 1-входового потомка (если такового нет, то выберем элемент $\vee$, являющийся концом цепи и одновременно выходом схемы). Множество выбранных элементов обозначим $\mathfrak{D}=\{d_1, \ldots, d_l\}$. На каждой цепи, проходящей через любой элемент c_i, выберем его ближайшего 1-входового предка или константу. Множество выбранных элементов обозначим $\mathfrak{V}=\{v_1, \ldots, v_q\}$; $\mathfrak{D}$, $\mathfrak{V}$ являются сечениями схемы. Превратим все элементы $\mathfrak{V}$ в константы.

Лемма 6. *Для некоторой булевой матрицы (μ_{ij})*

$$\operatorname{mon} f=\bigvee_{\mu_{ij}=1}\varphi(v_i)\times\Psi(d_j)\times\psi(d_j).$$

Для доказательства используем лемму 3. Пусть Ц — произвольная цепь, выходящая из v_i. Она проходит через некоторый элемент c_j, причем ее участок от v_i до c_j состоит только из дизъюнкций. Найдем в Ц ближайший после c_j элемент из $\mathfrak{D}$, например, d_r. Так как между v_i и d_r нет 1-входовых элементов, то $\Psi(\text{Ц})\subset\Psi(d_r)\times\psi(d_r)$, поэтому $\Psi(v_i)=\bigvee\limits_{l}\Psi(d_{r_l})\times\psi(d_{r_l})$ для некоторых индексов r_l. Без ограничения общности можно считать, что ни одно из $\varphi(v_i)$ не является дизъюнкцией каких-либо $\varphi(v_j)$, $j\neq i$, и аналогичное утверждение верно для $\Psi(d_i)\times\psi(d_i)$ (иначе можно было бы уменьшить размеры матрицы (μ_{ij})). Индукцией по k доказывается

Лемма 7. *При $k>3$ среди любых 2^{k-1} ненулевых k-мерных булевых векторов найдется вектор, равный дизъюнкции каких-то других из этих векторов.*

Лемма 8. *Матрица (μ_{ij}) является $\alpha(k)$-редкой, т. е. не содержит $\alpha(k)\times\alpha(k)$ подматриц, заполненных единицами.*

Действительно, если допустить противное, то для некоторых I, J $|I|=|J|=\alpha(k)$, справедливо, согласно лемме 6, включение

$$(\bigvee_{i\in I}\varphi(v_i))\times(\bigvee_{j\in J}\Psi(d_j)\times\psi(d_j))\subset \operatorname{mon} f,$$

из которого с помощью леммы 7 следует противоречие. Так как $\Psi(d_j)\times\psi(d_j)\subset\Psi(b_i)$ при некотором i, то в силу лемм 5, 6 $\sum\limits_{i,j}\mu_{ij}\geqslant$ $\geqslant(k-1)^{-3}|\operatorname{mon} f|$. Применяя рассуждения, приведенные на с. 62–64 в [7], можно показать, что

$$(\alpha(k)-1)^{1/\alpha(k)}\left(\frac{q+l}{2}\right)^{2-\frac{1}{\alpha(k)}}+(\alpha(k)-1)^{\frac{q+l}{2}}\geqslant\sum_{i,j}\mu_{ij}.$$

Так как $L_\times(f)+n+2\geqslant q+l$, то отсюда следуют неравенства (ii), (iii). Теорема доказана.

Замечания. Для любого многочлена f справедливо неравенство $L_+(f)\leqslant|\operatorname{mon} f|-1$. Поэтому если $\operatorname{mon} f$ — k-редкое множество, то $L_+(f)=O_k(|\operatorname{mon} f|)$, а если $k=2$, то $L_+(f)=|\operatorname{mon} f|-1$. Для любого $k\geqslant$ $\geqslant 2$ существует k-редкое множество $A\subset\mathbf{Z}^n{}_{\mathrm{m}}$, такое, что если $\operatorname{mon} f=A$, то $L_\times(f)\leqslant O_k(|A|^{\frac{k+1}{2k}})$ при $k>3$, $L_\times(f)\leqslant O(|A|^{3/5})$ при $k=3$, $L_\times(f)\leqslant$ $\leqslant 3|A|^{2/3}$ при $k=2$, причем $|A|\geqslant O_{m,k}(m^{\frac{nk}{5k+5}})$ при $n\to\infty$ и фиксированных m, k.

Если верна гипотеза [7, с. 65] о существовании k-редких булевских $n\times n$ матриц с $O_k(n^{2-\frac{1}{k}})$ единицами, то $L_\times(f)\leqslant O_k(|A|^{\frac{k}{2k-1}})$ при любом $k\geqslant 2$. Возможно, что оценка теоремы для $L_\times(f)$ верна и при $\alpha(k)=k$, $k=2, 3, \ldots$.

Пусть k-редкое множество $\operatorname{mon} f$ таково, что мощность любого его подмножества вида $A_1\times\ldots\times A_p$, где $|A_i|<k$, $i=1, \ldots, p$, не превосходит β; $\beta<(k-1)^3$. Тогда оценки теоремы можно усилить до следующих:

$$L_+(f)\geqslant\frac{|\operatorname{mon} f|}{\beta}-1,\quad L_\times(f)+n+2\geqslant 2\left(\frac{|\operatorname{mon} f|}{\beta}\right)^{1/2},$$

$$L_\times(f)+n\geqslant O(|\operatorname{mon} f|/\beta)^{\frac{\alpha(k)}{2\alpha(k)-1}},\ \text{если}\ \frac{|\operatorname{mon} f|}{\beta}\geqslant O(\alpha(k)^2).$$

Если множество $\operatorname{mon} f$ не содержит подмножеств вида $A\times B$, где $|A|=$ $=2$, $|B|=k$, то в качестве β можно взять $(k-1)^2$. Приведем еще пример. Пусть $f(X)$ — перманент $n\times n$ матрицы $X=(x_{ij})$. Тогда $\operatorname{mon} f$ является $\left[\frac{n}{2}\right]!+1$-редким множеством и в качестве β можно взять $\left[\frac{n}{2}\right]!\left]\frac{n}{2}\right[!$ (это утверждение не следует из предыдущего замечания, однако несложно доказывается). Применяя выписанные ранее неравен-

ства, получаем следующую оценку сложности монотонного вычисления перманента $n\times n$ матрицы X:

$$L_+(f(X))\geqslant O(2^n n^{-1/2}).$$

Все же перманент не слишком удобен для применения этой теоремы.

Известно [8—10], что многочлены с алгебраическими независимыми над полем $\mathbf{Q}$ коэффициентами имеют высокую сложность вычисления даже в базисе $\{x\pm y,\ xy,\ x/y\}\cup\mathbf{R}$. Там же построены примеры имеющих высокую сложность многочленов от одной переменной с алгебраическими над полем $\mathbf{Q}$ и даже с рациональными коэффициентами. Но к многочленам с коэффициентами 0 и 1 методы работ [8—10] пока не удалось применить. С помощью полученной теоремы можно строить многочлены от любого числа переменных с любыми положительными коэффициентами, которые имеют высокую сложность в монотонном базисе. Для этого нужны эффективные примеры «мощных» k-редких множеств.

Если сопоставить k-редкому подмножеству H группы $(G, +)$ булевскую $|G|\times|G|$ матрицу $M=(m_{g,h})$, такую, что $m_{g,h}=1\Leftrightarrow g+h\in H$, то она будет k-редкой.

Из [7, с. 62—64] следует, что $|H|\leqslant O(|G|^{1-\frac{1}{k}}+k)$.

По аналогии с упоминавшейся гипотезой из [7] можно выдвинуть более сильную гипотезу о возможности эффективного построения в полугруппе $(\mathbf{N}^n, +)$ k-редкого подмножества мощности $O(m^{n(1-1/k)}+k)$, лежащего в $\mathbf{Z}_m^n$; $\mathbf{Z}_m=\{0, 1, \ldots, m-1\}$.

Теорема 2. (i) *В группе* $(\mathbf{Z}_p^n, +)$, *где* p — *простое,* $p>2$, *можно указать 2-редкое подмножество мощности* $p^{[n/2]}$.

(ii) *В группе* $(\mathbf{Z}_{p^2+p+1}, +)$, *где* p — *простое, можно указать 2-редкое подмножество мощности* $p+1$.

(iii) *В группе* $(GF(q)^3, +)$, *где* $GF(q)$ — *поле Галуа порядка* q, *не кратного 2, сфера* $\{(x, y, z)\in GF(q)^3: x^2+y^2+z^2=\rho\}$, *где* $(-\rho)$ *является квадратичным невычетом в* $GF(q)$, *представляет собой 3-редкое подмножество мощности* q^2-q.

(iv) *В полугруппе* $(\mathbf{N}^n, +)$ *можно указать 2-редкое подмножество множества* $\mathbf{Z}_m^n$, *имеющее мощность* $O(m^{n/2})$, *если выполняется одно из условий*:

1) $n=1$ *или* n *четно, а* $m\to\infty$;

2) m — *фиксированное простое число, а* $n\to\infty$.

(v) *В полугруппе* $(\mathbf{N}^n, +)$ *можно указать 3-редкое подмножество множества* $\mathbf{Z}_m^n$, *имеющее мощность* $O(m^{2n/3})$, *если* 1) m — *фиксированное простое, большее 2,* $n\to\infty$, *либо* 2) n *кратно 3,* $m\to\infty$.

(vi) *Для некоторого* $\varepsilon>0$ *в полугруппе* $(\mathbf{N}^n, +)$ *можно указать 3-редкое подмножество множества* $\mathbf{Z}_m^n$, *имеющее мощность* $O(m^{n(1/2+\varepsilon)})$, *если* 1) $m>2$, $n\to\infty$, *либо* 2) $n>4$, $m\to\infty$.

Утверждение (i) следует из теоремы [11, с. 280]; утверждение (ii) — из теоремы Зингера [12, с. 179]; утверждение (iii) — из теоремы Брауна [13] и задачи [14, с. 458]; утверждение (iv) из (i), (ii); утверждение (v) — из (iii), изоморфизма $(GF(q), +)\simeq(\mathbf{Z}_p^n, +)$, где $q=p^n$, и асимптотической теоремы о простых; утверждение (vi) — из (v) и асимптотической теоремы о простых.

Следствие. (i) *Для некоторого* $\varepsilon>0$ *и любых* $m>2$ *и* n *можно указать многочлен с коэффициентами 0 и 1 от* n *переменных, каждая из которых имеет степень не выше* $m-1$, *такой, что при* $n\to\infty$

$$L_+(f)\geqslant O_{n,}(m^{n\left(\frac{1}{2}+\varepsilon\right)}).$$

(ii) *Можно указать многочлен с коэффициентами* 0 *и* 1, *у которого* $L_+(f) \geqslant O(3^{3^{\deg f}})$.

(iii) *Можно указать многочлены* f_1, f_2, f_3 *степени* n *от одной, двух и трех переменных соответственно, у которых*

$$L_+(f_1) \geqslant O(n^{1/2}), \quad L_+(f_2) \geqslant O(n), \quad L_+(f_3) \geqslant O(n^2),$$

$$L_\times(f_1) \geqslant O(n^{1/3}), \quad L_\times(f_2) \geqslant O(n^{2/3}), \quad L_\times(f_3) \geqslant O(n^{6/5}).$$

Замечание 1. М. И. Гринчук доказал существование k-редких подмножеств $(\mathbf{N}_n, +)$, лежащих в $\mathbf{Z}_m^n$ и имеющих мощность $m^n/k^{O(1)}$, где $k=(n\log m)^{O(1)}$ (работа вскоре будет опубликована). Из этого неэффективного результата вытекает существование множества $\operatorname{mon} f \subset \subset \mathbf{Z}_m^n$, для которого

$$L_+(f) \geqslant \frac{m^n}{(n\log m)^{O(1)}}, \quad L_\times(f) \geqslant \frac{m^{n/2}}{(n\log m)^{O(1)}}.$$

Так как для любого множества $\operatorname{mon} f \subset \mathbf{Z}_m^n$ $L_+(f) \leqslant m^n$ и $L_\times(f) \leqslant \leqslant O(m^{n/2})$, то предыдущие оценки довольно близки к точным.

Замечание 2. Из одного неравенства Д. Клейтмена (см., например, [7, с. 126]) вытекает, что в лемме 7 оценку 2^{k-1} можно заменить на $C_k^{[k/2]}(1+o(1))$. Поэтому утверждение (ii) теоремы 1 справедливо для некоторой последовательности $\alpha(k) \sim C_{k-1}^{\left[\frac{k-1}{2}\right]}$.

Замечание 3. Можно эффективно построить в группе $(\mathbf{Z}_2^n, +)$ k-редкое подмножество мощности $O(2^{2n/3})$ при $k=315$. Для этого достаточно заметить, что поверхность $x^3+y^7+z^{15}=1$ над конечным полем $GF(2^{2m+1})$ имеет 2^{4m+2} точек и является k-редким подмножеством аддитивной группы трехмерного пространства над этим полем при $k=315$.

Из теоремы 1 тогда вытекает, что неравенство (ii) следствия из теоремы 2 для некоторых эффективно конструируемых многочленов f можно усилить до следующего: $L_+(f) \geqslant O(2^{\frac{2}{3}\deg f})$.

СПИСОК ЛИТЕРАТУРЫ

1. Касим-заде О. М. О сложности монотонных многочленов//Сб. тр. семинара по дискретной математике и ее приложениям. М., 1986.
2. Шнорр К. П. Нижняя оценка числа сложений в монотонных вычислениях//Кибернет. сб. Нов. сер. М., 1981. № 18. 5—20.
3. Кузнецов С. Е. Монотонные вычисления полиномов и схемы без нулевых цепей: Тез. докл. VII Всесоюз. конф. «Проблемы теоретической кибернетики», ч. I. Иркутск, 1985. 108—109.
4. Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций. Препринт № 248 Ин-та пробл. механ. АН СССР. 1985.
5. Нигматуллин Р. Г. Сложность булевых функций. Казань, 1983.
6. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. М., 1984.
7. Эрдеш П., Спенсер Дж. Вероятностные методы в комбинаторике. М., 1976.
8. Шнорр К. П. Улучшенные нижние оценки умножений (делений), необходимых для вычисления многочленов//Кибернет. сб. Нов. сер. М., 1983. № 20. 30—45.
9. Хайнц И., Зивекинг М. Нижние оценки для многочленов с алгебраическими коэффициентами//Там же. 46—58.
10. Фонцур Гатен И., Штрассен Ф. Некоторые многочлены, имеющие высокую сложность вычисления//Там же. 59—63.
11. Дискретная математика и математические вопросы кибернетики. М., 1974.
12. Холл М. Комбинаторика. М., 1970.

13. Браун В. Дж. О графах, не содержащих графа Томсена//Кибернет. сб. Нов. сер. М., 1981. № 18. 34—38.
14. Боревич З. И., Шафаревич И. Р. Теория чисел. М., 1985.

Поступила в редакцию
15.10.85

ВЕСТН. МОСК. УН-ТА. СЕР. 1, МАТЕМАТИКА. МЕХАНИКА. 1987. № 5

УДК 511

В. А. Плаксин

О СУММЕ КВАДРАТИЧНОЙ ФОРМЫ И СТЕПЕНИ ЦЕЛОГО ЧИСЛА

1. Введение. Разрешимость диофантова уравнения $N=x^2+y^2+Dz^2$ для последовательности натуральных чисел N положительной плотности установила Е. П. Голубева [1]. Пусть $k\geqslant 2$ и $\psi(x, y)$ — любая невырожденная квадратичная форма с целыми постоянными коэффициентами. В настоящей работе изучается разрешимость уравнения $N=\psi(x, y)+Dz^k$ для почти всех чисел $N\leqslant X$, за исключением $\ll X^{1-\zeta_k}$, где $\zeta_k>0$.

Для простоты изложения рассмотрим уравнение

$$N=\psi(x, y)+n^k \tag{1}$$

с положительно определенной квадратичной формой ψ фундаментального дискриминанта $-\tau$ в целых числах x, y и $0<n$. Обозначим $\varkappa(N)$ число решений уравнения (1), $u(m, N)$ — число решений сравнения

$$N\equiv\psi(x, y)+z^k \pmod m.$$

Пусть $\zeta={}^1/_{61}k^3\ln k$, π_ψ — площадь области $\psi(x, y)\leqslant 1$ и

$$A(N, Q)=\sum_{q\leqslant Q} v(q, N),\quad v(q, N)=\sum_{d\mid q}\mu(d)u(q/d, N)(q/d)^{-2}. \tag{2}$$

Теорема. *Чисел $N\leqslant X$, для которых формула*

$$\varkappa(N)=\pi_\psi A(N, X^{1/2k^2})N^{1/k}+O(X^{1/k-\zeta})$$

неверна, всего $\ll X^{1-\zeta}$.

В дальнейшем p обозначает простое число, $p^\nu\|N$, $p^\theta\|k$, $p^\delta\|\tau$, $\beta=\nu+\max\{\theta+1;\ \delta\}$ и $G=\prod_{p\mid\tau}p^\beta$.

Следствие. *Чисел $N\leqslant X$ с условием $u(G, N)>0$, не представимых в виде* (1), *всего $\ll X^{1-\zeta}$.*

Доказательство теоремы (п. 2—4) использует круговой метод Харди—Литтлвуда—Рамануджана в форме тригонометрических сумм И. М. Виноградова [2, 3], доказательство следствия (п. 5—6) — рассуждения Дэвенпорта и Хейлбронна [4] и Ю. В. Линника [5].

2. Круговой метод. Малые дуги. Введем обозначения: $\rho={}^1/_{40}k^2\ln k$, $\varepsilon=10^{-3}$, $c>k$; $X\geqslant X_c$, $P=X^{1/k}$, $R=P^{k-1/k}$, $Q=P^{1/2k}$, $\Delta=1/qR$, $\mathscr{L}=\ln X$. Пусть $e(\alpha)=\exp(2\pi i\alpha)$,

$$S_\psi(\alpha)=\sum_{\psi(x, y)\leqslant X} e(\alpha\psi(x, y))\ \text{и}\ S_k(\alpha)=\sum_{n^k\leqslant X} e(\alpha n^k). \tag{3}$$

Согласно [2], $\varkappa(N)$ представляется в виде интеграла по интервалу $(-1/R;\ 1-1/R]$ от произведения сумм (3). Разбиение области интегри-