[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, London 1965.

[6] J. Heading, *The discriminant of an equation of n-th degree*, Math. Gaz. 51 (1967), pp. 324–326.

[7] N. Jacobson, *Lectures in abstract algebra*, Vol, 3. *Theory of fields and Galois theory*, Van Nostrand, Princeton 1964.

[8] H. W. Knobloch, *Zum Hilbertschen Irreduzibilitätssatz*, Abh. Math. Sem. Univ. Hamburg 19 (1955), pp. 176–190.

[9] — *Die Seltenheit der reduziblen Polynome*, Jber. Deutsch. Math. Verein. 59 (1956), Abt. 1, pp. 12–19.

[10] S. Lang, *Introduction to Diophantine approximations*, Addison-Wesley, 1966.

[11] D. W. Masser, *The discriminants of special equations*, Math. Gaz. 50 (1966), pp. 158–160.

[12] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Scientific Publishers, Warszawa 1973.

[13] P. Samuel, *Algebraic theory of numbers*, Hermann, Paris 1970.

[14] W. Specht, *Zur Zahlentheorie der Polynome*, S. B. Math. Nat. Kl. Bayer. Akad. Wiss., (1951), pp. 139–146.

[15] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), pp. 1099–1106.

[16] B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. 109 (1934), pp. 13–16.

[17] — *Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt*, Monatsh. Math. 43 (1936), pp. 137–147.

[18] — *Modern algebra*, Vol. I, Ungar, New York 1953.

DEPARTMENT OF MATHEMATICS
MANHATTANVILLE COLLEGE
Purchase, New York, U.S.A.

Received on 21. 6. 1976
and in revised form on 7. 1. 1977 (856)

ACTA ARITHMETICA
XXXV (1979)

Ω-estimates in lattice point theory

by

BOHUSLAV DIVIŠ

Let $Q(u) = Q(u_1, u_2, \ldots, u_r) = \sum_{i,l=1}^{r} a_{il} u_i u_l$ be a positive definite quadratic form in $r \geqslant 2$ variables with real symmetric coefficient matrix of determinant D. Let $b = (b_1, b_2, \ldots, b_r)$ be a system of real numbers satisfying $0 \leqslant b_l < 1$ $(l = 1, 2, \ldots, r)$. For $x > 0$, let us denote by $A_Q(b; x)$ the number of lattice points $m = (m_1, m_2, \ldots, m_r)$ with integral coordinates m_l $(l = 1, 2, \ldots, r)$ satisfying the inequality $Q(m+b) \leqslant x$, that is

$$A_Q(b; x) = \sum_{Q(m+b)\leqslant x} 1.$$

Geometrically, the ellipsoid $Q(m+b) \leqslant x$ has center at the point $-b$ Obviously, $A_Q(b; x)$ is asymptotically equal to

$$V_Q(b; x) = V_Q(x) = \frac{\pi^{r/2} x^{r/2}}{\sqrt{D}\,\Gamma(\frac{1}{2}r+1)},$$

the volume of the ellipsoid $Q(u+b) \leqslant x$, which is clearly independent of b. Let us put

$$P_Q(b; x) = A_Q(b; x) - V_Q(x).$$

Since the form Q and the center $-b$ will be considered fixed, we shall simply write $A(x)$, $V(x)$ and $P(x)$ instead of $A_Q(b; x)$, $V_Q(b; x)$ and $P_Q(b; x)$. We shall study the function $P(x)$, and more generally

$$P_\varrho(x) = \frac{1}{\Gamma(\varrho)} \int_0^x P(y)(x-y)^{\varrho-1} dy \quad \text{for} \quad \varrho > 0, \quad P_0(x) = P(x).$$

The functions $A_\varrho(x)$ and $V_\varrho(x)$ are defined analogously. Finally, let us put

$$M_\varrho(x) = \int_0^x P_\varrho^2(y)\, dy \quad \text{for} \quad \varrho \geqslant 0, \quad M(x) = M_0(x)$$

and

$$\overline{P}_\varrho(x) = \sqrt{\frac{1}{x} M_\varrho(x)} \quad \text{for} \quad \varrho \geqslant 0, \quad \overline{P}(x) = \overline{P}_0(x).$$

It is evident that every Ω-estimate for $\overline{P}_\varrho$ is also an Ω-estimate for P_ϱ.

There exist at least three essentially different Ω-methods in lattice point theory. The Landau method makes no distinction between the forms Q and the centers $-b$. For sufficiently large values of ϱ, one expands $P_\varrho(x)$ into an infinite series with respect to Bessel functions and shows that at least for some values of x the first term dominates the other. Then a simple descent argument extends the result to $\varrho \geqslant 0$. One can obtain in this way

THEOREM 1.

$$\overline{P}_\varrho(x) = \Omega(x^{\frac{r-1}{4}+\frac{\varrho}{2}}).$$

Proof can be found in [6].

Let us remark that for $r < 2\varrho+3$ and for "almost diagonal" forms also holds [3]

$$\overline{P}_\varrho(x) = O(x^{\frac{r-1}{4}+\frac{\varrho}{2}}).$$

The Hardy method uses the fact that $P_\varrho(x)$ can be expressed as an integral transformation of the generating theta function $\theta(s) = \sum_{m=-\infty}^{\infty} e^{-sQ(m+b)}$ and vice versa. If we know that $\theta(s)$ is not small then $P_\varrho(x)$ cannot be small by the inverse integral representation. A modification is needed for the function $\overline{P}_\varrho$. For details, the reader is referred to [7]. For good estimates, a good deal of information is needed about the function $\theta(s)$, and that is available again only for almost diagonal forms. One can then obtain

THEOREM 2.

$$\overline{P}_\varrho(x) = \Omega(x^{\frac{r}{2}-1-\frac{\varrho+1}{\beta}-\varepsilon}) \quad \textit{for every } \varepsilon > 0,$$

where β is a special approximation index of a system depending on the coefficients of the form Q and on the coordinates of its center.

The details and a proof can be found in [1]. If the "diagonal blocks" are large enough then also

$$P_\varrho(x) = O(x^{\frac{r}{2}-1-\frac{\varrho+1}{\beta}+\varepsilon}) \quad \text{for every } \varepsilon > 0 \ [1].$$

In this article, we shall concentrate on the third method which is due to Jarník. It is entirely elementary and in the simplest case when Q has integral coefficients, $\varrho = 0$ and $b = 0$, it runs as follows. Since Q assumes only integral values, we have for every natural number n

$$\begin{aligned} P(n+\tfrac{1}{3})-P(n+\tfrac{2}{3}) &= A(n+\tfrac{1}{3})-A(n+\tfrac{2}{3})+V(n+\tfrac{2}{3})-V(n+\tfrac{1}{3}) \\ &= V(n+\tfrac{2}{3})-V(n+\tfrac{1}{3}) \gg n^{r/2-1}. \end{aligned}$$

This shows that $P(x) = o(x^{r/2-1})$ is untenable, that is

$$P(x) = \Omega(x^{r/2-1}).$$

Jarník used his method only for ellipsoids with center at 0, for P_ϱ with integral values of ϱ and for $\overline{P}$, in which cases it yields the same estimates for P_ϱ and $\overline{P}$ as Theorem 2 ([4], [5]).

The purpose of this note is to extend the applicability of the method in several directions. Firstly, we shall drop the assumption $b = 0$. Secondly, we shall derive estimates for P_ϱ for an arbitrary $\varrho \geqslant 0$. Thirdly, we shall show that the method can be used for other regions than ellipsoids, practically for every region defined by a system of algebraic inequalities. Since we usually do not possess the knowledge needed for using the other methods, it is then the only method available. Judging from the sharpness of the estimates in case of ellipsoids, one would conjecture that the method is sharp in general. This was also confirmed by the author for polyhedra ([2]).

We shall start with a simple

LEMMA. *For $\varrho \geqslant 0$,*

$$A_\varrho(x) = \frac{1}{\Gamma(\varrho+1)} \sum_{Q(m+b)\leqslant x} (x-Q(m+b))^\varrho.$$

Proof. For $\varrho = 0$ the proof is obvious. For $\varrho > 0$, we have

$$\begin{aligned} A_\varrho(x) &= \frac{1}{\Gamma(\varrho)} \int_0^x A(y)(x-y)^{\varrho-1}dy = \frac{1}{\Gamma(\varrho)} \int_0^x \sum_{Q(m+b)\leqslant x} (x-y)^{\varrho-1}dy \\ &= \frac{1}{\Gamma(\varrho)} \sum_{Q(m+b)\leqslant x} \int_{Q(m+b)}^x (x-y)^{\varrho-1}dy = \frac{1}{\varrho\Gamma(\varrho)} \sum_{Q(m+b)\leqslant x} (x-Q(m+b))^\varrho. \end{aligned}$$

THEOREM 3. *Let $\varrho \geqslant 0$ be an integer. Let $Q(u) = \sum_{i,l=1}^{r} a_{il}u_iu_l$ be a positive definite quadratic form and let $b = (b_1, b_2, \ldots, b_r)$ be a system of real numbers. Let $\varphi(x)$ be a positive continuous strictly increasing function of a positive real variable with $\liminf_{x\to\infty} \frac{\varphi(2x)}{\varphi(x)} > 1$, i.e. in particular $\lim_{x\to\infty} \varphi(x) = \infty$, and let us denote by $\psi(x)$ its inverse. Let us suppose that the system of* *inequalities*

$$\left|q\frac{a_{il}}{a_{11}}-p_{il}\right|<\frac{1}{\varphi(q)},\qquad i,l=1,2,\ldots,r,$$

$$|q\beta_i-p_i|<\frac{1}{\sqrt{\varphi(q)}},\qquad \textit{where}\qquad \beta_i=2\sum_{l=1}^{r}\frac{a_{il}}{a_{11}}b_l,\qquad i=1,2,\ldots,r,$$

has infinitely many integer solutions p_{il}, p_i $(i,l=1,2,\ldots,r)$ *and* q *with* $q\to\infty$. *Then*

$$P_\varrho(b;x)=\Omega\left(\frac{x^{r/2-1}}{\psi^{\varrho+1}(x)}\right).$$

Proof. Let us first start with $\varrho=0$. There is a positive constant C depending only on the form Q such that

$$Q(u)\geqslant C\Big(\sum_i|u_i|\Big)^2.$$

We shall restrict ourselves to q sufficiently large. If particular, we assume that

$$Q(u+b)>\frac{C}{60}\varphi(q)-\frac{a_{11}}{q}$$

implies

$$(1)\qquad \frac{10}{9}Q(u+b)>Q(u)>\frac{C}{64}\varphi(q).$$

Let us put $M=\left[\dfrac{Cq\varphi(q)}{60a_{11}}\right]$.

We shall show that there are no lattice points in the region

$$(2)\qquad a_{11}\frac{M+\frac{1}{3}}{q}+Q(b)\leqslant Q(u+b)\leqslant a_{11}\frac{M+\frac{2}{3}}{q}+Q(b).$$

Let us suppose that (2) holds. Then

$$Q(u+b)>a_{11}\frac{M}{q}>\frac{a_{11}}{q}\left(\frac{Cq\varphi(q)}{60a_{11}}-1\right)=\frac{C}{60}\varphi(q)-\frac{a_{11}}{q},$$

and hence (1) holds. We have obviously

$$Q(u+b)=\sum_{i,l}a_{il}(u_i+b_i)(u_l+b_l)=a_{11}\sum_{i,l}\frac{a_{il}}{a_{11}}u_iu_l+a_{11}\sum_i\beta_iu_i+Q(b).$$

Put

$$Q^*(u)=a_{11}\sum_{i,l}\frac{p_{il}}{q}u_iu_l+a_{11}\sum_i\frac{p_i}{q}u_i+Q(b).$$

If u were a lattice point, then $Q^*(u)$ would have to be of the form $a_{11}\dfrac{m}{q}+Q(b)$, where m is an integer. Now we have

$$\begin{aligned}|Q(u+b)-Q^*(u)|&\leqslant a_{11}\sum_{i,l}\left|\frac{a_{il}}{a_{11}}-\frac{p_{il}}{q}\right|\cdot|u_i|\cdot|u_l|+a_{11}\sum_i\left|\beta_i-\frac{p_i}{q}\right|\cdot|u_i|\\ &<\frac{a_{11}}{q\varphi(q)}\Big(\sum_i|u_i|\Big)^2+\frac{a_{11}}{q\sqrt{\varphi(q)}}\sum_i|u_i|\\ &\leqslant\frac{a_{11}}{Cq\varphi(q)}Q(u)+\frac{a_{11}}{q}\frac{Q(u)}{C\varphi(q)}\sqrt{\frac{C\varphi(q)}{Q(u)}}\\ &<\frac{9a_{11}}{Cq\varphi(q)}Q(u)<10\frac{a_{11}}{Cq\varphi(q)}Q(u+b)\qquad\text{by (1).}\end{aligned}$$

This implies

$$Q(u+b)\left(1-10\frac{a_{11}}{Cq\varphi(q)}\right)<Q^*(u)<Q(u+b)\left(1+10\frac{a_{11}}{Cq\varphi(q)}\right).$$

Using (2), we have

$$\begin{aligned}Q(u+b)\left(1+10\frac{a_{11}}{Cq\varphi(q)}\right)&\leqslant a_{11}\frac{M+\frac{2}{3}}{q}+Q(b)+a_{11}\frac{M}{q}\cdot10\frac{a_{11}}{Cq\varphi(q)}+O\left(\frac{1}{q\varphi(q)}\right)\\ &=a_{11}\frac{M+\frac{2}{3}}{q}+Q(b)+\frac{a_{11}}{q}\frac{Cq\varphi(q)}{60a_{11}}\cdot10\frac{a_{11}}{Cq\varphi(q)}+O\left(\frac{1}{q\varphi(q)}\right)\\ &=a_{11}\frac{M+\frac{5}{6}}{q}+Q(b)+O\left(\frac{1}{q\varphi(q)}\right)<a_{11}\frac{M+1}{q}+Q(b)\end{aligned}$$

for q large enough.

Analogously,

$$\begin{aligned}Q(u+b)\left(1-10\frac{a_{11}}{Cq\varphi(q)}\right)&\geqslant a_{11}\frac{M+\frac{1}{3}}{q}+Q(b)-a_{11}\frac{M+1}{q}\cdot10\frac{a_{11}}{Cq\varphi(q)}+O\left(\frac{1}{q\varphi(q)}\right)\\ &\geqslant a_{11}\frac{M+\frac{1}{3}}{q}+Q(b)-\frac{a_{11}}{q}\frac{Cq\varphi(q)}{60a_{11}}\cdot10\frac{a_{11}}{Cq\varphi(q)}+O\left(\frac{1}{q\varphi(q)}\right)\\ &\geqslant a_{11}\frac{M+\frac{1}{6}}{q}+Q(b)+O\left(\frac{1}{q\varphi(q)}\right)>a_{11}\frac{M}{q}+Q(b)\end{aligned}$$

for q large enough.

This means that for q large enough

$$a_{11}\frac{M}{q}+Q(b)<Q^*(u)<a_{11}\frac{M+1}{q}+Q(b),$$

and thus $Q^*(u)$ is not of the form $a_{11}\dfrac{m}{q}+Q(b)$.

Hence, there are no lattice points in the region (2).

It follows that

$$\left|P\left(b;\, a_{11}\frac{M+\frac{2}{3}}{q}+Q(b)\right)-P\left(b;\, a_{11}\frac{M+\frac{1}{3}}{q}+Q(b)\right)\right|$$

$$=\left|V\left(b;\, a_{11}\frac{M+\frac{2}{3}}{q}+Q(b)\right)-V\left(b;\, a_{11}\frac{M+\frac{1}{3}}{q}+Q(b)\right)\right|$$

$$\geqslant\left(\frac{M+\frac{2}{3}}{q}+\frac{Q(b)}{a_{11}}\right)^{r/2}-\left(\frac{M+\frac{1}{3}}{q}+\frac{Q(b)}{a_{11}}\right)^{r/2}\geqslant\left(\frac{M+\frac{1}{3}}{q}+\frac{Q(b)}{a_{11}}\right)^{r/2-1}\frac{1}{q}$$

$$\geqslant\left(\frac{M+1}{q}\right)^{r/2-1}\frac{1}{\psi\left(\frac{M+1}{q}\right)}\,\frac{\psi\left(\frac{M+1}{q}\right)}{q}\geqslant\left(\frac{M+1}{q}\right)^{r/2-1}\frac{1}{\psi\left(\frac{M+1}{q}\right)}\,\frac{\psi\left(\frac{C\varphi(q)}{60\,a_{11}}\right)}{q}$$

$$\geqslant\left(\frac{M+1}{q}\right)^{r/2-1}\psi^{-1}\left(\frac{M+1}{q}\right),$$

since $\liminf\limits_{x\to\infty}\dfrac{\varphi(2x)}{\varphi(x)}>1$ implies $\psi\left(\dfrac{C\varphi(q)}{60\,a_{11}}\right)\geqslant q$ for sufficiently large q. This means that at least one of the numbers

$$\left|P\left(b;\, a_{11}\frac{M+\frac{2}{3}}{q}+Q(b)\right)\right|,\qquad\left|P\left(b;\, a_{11}\frac{M+\frac{1}{3}}{q}+Q(b)\right)\right|$$

must be

$$\geqslant\left(\frac{M+1}{q}\right)^{r/2-1}\psi^{-1}\left(\frac{M+1}{q}\right).$$

Since $M/q\to\infty$ with $q\to\infty$, this proves

$$P(b;x)=\Omega\left(\frac{x^{r/2-1}}{\psi(x)}\right).$$

Now, let us assume that $\varrho>0$. It will be convenient to reformulate the statement for $\varrho=0$. Let us denote by λ_n $(n=1,2,\ldots)$, $0\leqslant\lambda_1<\lambda_2<\ldots$ the sequence of all distinct values of $Q(m+b)$ where m is a lattice point and let us write a_n for the number of solutions of $Q(m+b)=\lambda_n$. We can then write by our lemma

$$P_\varrho(x)=P_\varrho(b;x)=\frac{1}{\Gamma(\varrho+1)}\sum_{\lambda_n\leqslant x}a_n(x-\lambda_n)^\varrho-\frac{\pi^{r/2}x^{r/2+\varrho}}{\sqrt{D}\,\Gamma(r/2+\varrho+1)}\quad\text{for }\varrho\geqslant 0,$$

and the function $P_\varrho(x)$ is infinitely many times differentiable for $\lambda_n<x<\lambda_{n+1}$. We have always either $|P(\lambda_n+)|\geqslant\lambda_n^{r/2-1}(\lambda_{n+1}-\lambda_n)$ or $|P(\lambda_{n+1}-)|$

$\geqslant\lambda_n^{r/2-1}(\lambda_{n+1}-\lambda_n)$ or both. What we have proved above is simply

$$\lambda_{n+1}-\lambda_n=\Omega\left(\frac{1}{\psi(\lambda_n)}\right).$$

Let us choose an integer $k\geqslant\varrho+1$ and put $z=\dfrac{\lambda_{n+1}-\lambda_n}{k+2}$. For each $n\geqslant 1$, let us define the differences $\Delta_{n,z}P_\varrho(x)$ as follows:

$$\Delta_{1,z}P_\varrho(x)=P_\varrho(x+z)-P_\varrho(x),$$
$$\Delta_{l+1,z}P_\varrho(x)=\Delta_{l,z}P_\varrho(x+z)-\Delta_{l,z}P_\varrho(x)\quad\text{for}\quad l\geqslant 1.$$

Since the function $P_\varrho(x)$ is sufficiently smooth for $\lambda_n+z\leqslant x\leqslant\lambda_n+(k+1)z$, there exists an x_n, $\lambda_n+z<x_n<\lambda_n+(k+1)z$ such that $P_\varrho^{(k)}(x_n)=z^{-k}\Delta_{k,z}P_\varrho(\lambda_n+z)$, i.e.

$$\frac{1}{\Gamma(\varrho-k+1)}\sum_{\lambda_m\leqslant x_n}a_m(x_n-\lambda_m)^{\varrho-k}-\frac{\pi^{r/2}x_n^{r/2+\varrho-k}}{\sqrt{D}\,\Gamma(r/2+\varrho-k+1)}=(k+2)^k(\lambda_{n+1}-\lambda_n)^{-k}\Delta_{k,z}P_\varrho(\lambda_n+z).\tag{3}$$

Now, if $\varrho>0$ is an integer, put $k=\varrho+1$. From (3) then follows

$$|\Delta_{\varrho+1,z}P_\varrho(\lambda_n+z)|\geqslant x_n^{r/2-1}(\lambda_{n+1}-\lambda_n)^{\varrho+1}.\tag{4}$$

If we had $P_\varrho(x)=o\left(\dfrac{x^{r/2-1}}{\psi^{\varrho+1}(x)}\right)$, the left-hand side of (4) would be $o\left(\dfrac{\lambda_n^{r/2-1}}{\psi^{\varrho+1}(\lambda_n)}\right)$. Since $\lambda_{n+1}-\lambda_n=\Omega\left(\dfrac{1}{\psi(\lambda_n)}\right)$, this is a contradiction. This completes the proof of Theorem 3.

THEOREM 4. *Let $\varrho>0$ be not an integer and let otherwise the assumptions of Theorem 3 be satisfied. If*

$$P(x)=O\left(x^{r/2-1}\frac{1}{\psi^{1-\varepsilon}(x)}\right)\quad\textit{for an }1>\varepsilon>0,$$

then

$$P_\varrho(x)=\Omega\left(x^{r/2-1}\frac{1}{\psi^{\varrho+1+2\varepsilon}(x)}\right).$$

Proof. Let us first consider $0<\varepsilon<\frac{1}{2}$. We shall use the relation (3) again and restrict ourselves to those n for which $\lambda_{n+1}-\lambda_n\geqslant 1/\psi(\lambda_n)$. Let k be the smallest integer greater than $\varrho+1$. If we assume that

$$P_\varrho(x)=o\left(x^{r/2-1}\frac{1}{\psi^{\varrho+1+2\varepsilon}(x)}\right),$$

then

$$(\lambda_{n+1}-\lambda_n)^{-k}\Delta_{k,z}P_\varrho(\lambda_n+z)=o\left(\lambda_n^{r/2-1}\frac{1}{\psi^{\varrho+1-k+2\varepsilon}(\lambda_n)}\right)$$
$$=o\left(\lambda_n^{r/2-1}\psi^{(1-2\varepsilon)(k-\varrho-1)}(\lambda_n)\right).$$

Further,

$$x_n^{r/2+\varrho-k}\ll\lambda_n^{r/2-1}\psi^{(1-2\varepsilon)(k-\varrho-1)}(\lambda_n)\left(\lambda_n\psi^{1-2\varepsilon}(\lambda_n)\right)^{\varrho+1-k}$$
$$=o\left(\lambda_n^{r/2-1}\psi^{(1-2\varepsilon)(k-\varrho-1)}(\lambda_n)\right).$$

Finally, let us look at the last term in (3). We have

$$\sum_{\lambda_m\leqslant x_n}a_m(x_n-\lambda_m)^{\varrho-k}\geqslant\sum_{\lambda_m\leqslant\lambda_n}a_m(\lambda_{n+1}-\lambda_m)^{\varrho-k}$$
$$\geqslant\sum_{\lambda_n-\psi^{2\varepsilon-1}(\lambda_n)<\lambda_m\leqslant\lambda_n}a_m(\lambda_{n+1}-\lambda_m)^{\varrho-k}.$$

Now, we shall use the assumption $P(x)=O\left(x^{r/2-1}\psi^{\varepsilon-1}(x)\right)$. In particular, we have $\lambda_{n+1}-\lambda_n=o\left(\psi^{2\varepsilon-1}(\lambda_n)\right)$. This gives us

$$\sum_{\lambda_m\leqslant x_n}a_m(x_n-\lambda_m)^{\varrho-k}\geqslant\left(\lambda_{n+1}-\lambda_n+\psi^{2\varepsilon-1}(\lambda_n)\right)^{\varrho-k}\sum_{\lambda_n-\psi^{2\varepsilon-1}(\lambda_n)<\lambda_m\leqslant\lambda_n}a_m$$
$$\geqslant\psi^{(2\varepsilon-1)(\varrho-k)}(\lambda_n)\left(\lambda_n^{r/2}-\left(\lambda_n-\psi^{2\varepsilon-1}(\lambda_n)\right)^{r/2}+O\left(\lambda_n^{r/2-1}\psi^{\varepsilon-1}(\lambda_n)\right)\right)$$
$$\geqslant\psi^{(2\varepsilon-1)(\varrho-k)}(\lambda_n)\lambda_n^{r/2-1}\psi^{2\varepsilon-1}(\lambda_n)=\lambda_n^{r/2-1}\psi^{(1-2\varepsilon)(k-\varrho-1)}(\lambda_n\ ),$$

which is a contradiction.

Let us remark that we have in fact proved

$$P_\varrho(x)=\Omega\left(x^{r/2-1}\frac{1}{\psi^{\varrho+1+2\varepsilon(k-\varrho-1)}(x)}\right)\quad\text{for}\quad 0<\varepsilon<\tfrac{1}{2}.$$

The proof of Theorem 4 in the case $\frac{1}{2}\leqslant\varepsilon<1$ is contained in

THEOREM 5. *Let $\varrho>0$ be not an integer and let otherwise the assumptions of Theorem 3 be satisfied. If $P(x)=o(x^{r/2-1})$, then*

$$P_\varrho(x)=\Omega\left(x^{r/2-1}\frac{1}{\psi^{\varrho+2}(x)}\right).$$

Proof. Let again be $\varrho+1<k<\varrho+2$ and let us consider the relation (3). We shall restrict ourselves to those n for which $\lambda_{n+1}-\lambda_n\geqslant 1/\psi(\lambda_n)$. Let us remark that $\lambda_{n+1}-\lambda_n=o(1)$ since $P(x)=o(x^{r/2-1})$. If we assume $P_\varrho(x)=o\left(x^{r/2-1}\dfrac{1}{\psi^{\varrho+2}(x)}\right)$, then

$$(\lambda_{n+1}-\lambda_n)^{-k}\Delta_{k,z}P_\varrho(\lambda_n+z)=o\left(\lambda_n^{r/2-1}\frac{1}{\psi^{\varrho+2-k}(\lambda_n)}\right)=o(\lambda_n^{r/2-1}).$$

Also,

$$x_n^{r/2+\varrho-k}\ll\lambda_n^{r/2-1}\lambda_n^{\varrho+1-k}=o(\lambda_n^{r/2-1}).$$

On the other hand,

$$\sum_{\lambda_m\leqslant x_n}a_m(x_n-\lambda_m)^{\varrho-k}\geqslant\sum_{\lambda_n-1\leqslant\lambda_m\leqslant\lambda_n}a_m(\lambda_{n+1}-\lambda_m)^{\varrho-k}\geqslant\sum_{\lambda_n-1\leqslant\lambda_m\leqslant\lambda_n}a_m$$
$$=\lambda_n^{r/2}-(\lambda_n-1)^{r/2}+o(\lambda_n^{r/2-1})\geqslant\lambda_n^{r/2-1},$$

a contradiction.

THEOREM 6. *If $Q(u)=\sum_{i,j=1}^{r}a_{ij}u_iu_j$ is a rational quadratic form and if all the numbers b_j $(j=1,2,\ldots,r)$ are rational then*

$$P_\varrho(x)=\Omega(x^{r/2-1})\quad\textit{for}\quad\varrho\geqslant 0.$$

Proof. We have clearly $\lambda_{n+1}-\lambda_n\geqslant 1$ in this case. From this, $P(x)=\Omega(x^{r/2-1})$ immediately follows. If $\varrho>0$ is an integer, we can argue as in the proof of Theorem 3. Namely, if we had $P_\varrho(x)=o(x^{r/2-1})$, the left-hand side of (3) would be $\Omega(\lambda_n^{r/2-1})$, whereas the right-hand side would be $o(\lambda_n^{r/2-1})$ $(k=\varrho+1)$. If $\varrho>0$ is not an integer, we take $k>\varrho+1$ in (3). Assuming $P_\varrho(x)=o(x^{r/2-1})$, we get

$$(\lambda_{n+1}-\lambda_n)^{-k}\Delta_{k,z}P_\varrho(\lambda_n+z)=o(\lambda_n^{r/2-1}),$$
$$x_n^{r/2+\varrho-k}\ll\lambda_n^{r/2-1}\lambda_n^{\varrho+1-k}=o(\lambda_n^{r/2-1}).$$

On the other hand,

$$\sum_{\lambda_m\leqslant x_n}a_m(x_n-\lambda_m)^{\varrho-k}\geqslant a_n(\lambda_{n+1}-\lambda_n)^{\varrho-k}.\tag{5}$$

In order to get a contradiction we shall change the meaning of the numbers λ_n. These are rational numbers with a finite common denominator d, say. We shall write $\lambda_n=n/d$. In this way, some of the numbers a_n become zero but that does not matter. We have $\lambda_{n+1}-\lambda_n=1/d$ and $a_n=\Omega(\lambda_n^{r/2-1})$, since $\sum_{m\leqslant n}a_m\geqslant\lambda_n^{r/2}$. If we use this in (5), we get finally a contradiction.

THEOREM 7. *For an arbitrary positive definite quadratic form Q,*

$$\overline{P}_0(x)=\overline{P}(x)=\Omega\left(\frac{x^{r/2-1}}{\psi(x)}\right),$$

where $\psi(x)$ has the same meaning as in Theorem 3.

Proof follows from a careful study of the proof of Theorem 3. Namely, we have there shown in fact, that

$$|P(x)|\geqslant\frac{(M/q)^{r/2-1}}{\psi(M/q)}$$

for x from an interval of length $\geqslant 1/q$ contained in the interval $\left(a_{11}\dfrac{M}{q}+Q(b),\, a_{11}\dfrac{M+1}{q}+Q(b)\right)$. The reader can easily see that we get the same result if we take an arbitrary integer M from the interval $I=\left(\dfrac{Cq\varphi(q)}{61\,a_{11}},\dfrac{Cq\varphi(q)}{60\,a_{11}}\right)$.

It follows that

$$\left(\frac{1}{\varphi(q)}\int\limits_0^{c\varphi(q)} P^2(x)\,dx\right)^{1/2} \geqslant \left(\frac{1}{\varphi(q)}\sum_{M\in I}\frac{(M/q)^{r-2}}{\psi^2(M/q)}\,\frac{1}{q}\right)^{1/2}$$
$$\geqslant \left(\frac{1}{\varphi(q)}\,q\varphi(q)\,\frac{\varphi^{r-2}(q)}{\psi^2\big(\varphi(q)\big)}\,\frac{1}{q}\right)^{1/2} = \frac{\varphi^{r/2-1}(q)}{\psi\big(\varphi(q)\big)}.$$

If we write x_q for $c\varphi(q)$, we get

$$\overline{P}(x_q) \geqslant \frac{x_q^{r/2-1}}{\psi(x_q)}.$$

This proves our assertion.

In this way, we obtained the estimate given by Theorem 2 for $\overline{P}$ and for P_ϱ, $\varrho \geqslant 0$. It suffices to take $\varrho(x) = x^\delta$, $\delta < \beta$ and specialize the form Q. If ϱ is not an integer then we use O-estimates found in [1] in order to meet the assumptions of Theorems 4 and 5. We did not succeed in extending the method to $\overline{P}_\varrho$ when $\varrho > 0$.

In the introduction, we mentioned that the Ω-method considered here can be applied to very general regions defined by algebraic inequalities. As an example of this kind, let us consider the biquadratic form B defined by

$$B(u) = \sum_{j=1}^{r} a_j u_j^4, \qquad a_j > 0, \qquad j = 1, 2, \ldots, r.$$

If $b = (b_1, \ldots, b_r)$ is a system of real numbers, let us write $A(b;x)$ for the number of lattice points $m = (m_1, \ldots, m_r)$ in the region

$$B(m+b) \leqslant x.$$

Analogously as above, let us write $V(x)$ for the volume of this region and put

$$P(b;x) = A(b;x) - V(x).$$

We have clearly

$$V(x) = C_B x^{r/4},$$

where C_B is a positive constant. Using the method of Theorem 3, we obtain

$$P(b;x) = \Omega(x^{r/4-1-1/\delta}),$$

where δ is any positive number such that the system

$$\left\|\frac{a_j}{a_1}q\right\| < q^{-\delta}, \quad \left\|\frac{a_j}{a_1}b_j q\right\| < q^{-3\delta/4}, \quad \left\|\frac{a_j}{a_1}b_j^2 q\right\| < q^{-\delta/2}, \quad \left\|\frac{a_j}{a_1}b_j^3 q\right\| < q^{-\delta/4},$$
$$j = 1, 2, \ldots, r,$$

has infinitely many solutions in integers $q \to \infty$.

The reader will find it easy to generalize the last result to other forms of even degree. Let us consider now forms of odd degree. An example of this kind would be the linear form

$$L(u) = \sum_{j=1}^{r} a_j |u_j|, \qquad a_j > 0, \qquad j = 1, 2, \ldots, r.$$

If $b = (b_1, b_2, \ldots, b_r)$ is a system of real numbers, $0 \leqslant b_j < 1$ $(j = 1, 2, \ldots, r)$, let us write $A(b;x)$ for the number of lattice points $m = (m_1, \ldots, m_r)$ in the region

$$L(m+b) \leqslant x.$$

Again, let us put

$$P(b;x) = A(b;x) - V(x),$$

where $V(x)$ is the volume of the region $L(u+b) \leqslant x$, that is

$$V(x) = \frac{2^r x^r}{a_1 a_2 \ldots a_r \Gamma(r+1)}.$$

Making a little modification in the method of proof of Theorem 3, we obtain for integral values of ϱ

$$P_\varrho(b;x) = \Omega(x^{r-1-(\varrho+1)/\delta}),$$

where $\delta > 0$ is such that the system

$$\left\|\frac{a_j}{a_1}q\right\| < q^{-\delta}$$

has infinitely many solutions in integers $q \to \infty$. A modification is necessary because of the presence of the absolute values. First we note that if m_j is an integer then $|m_j + b_j| = |m_j| \pm b_j$ according as $m_j \geqslant 0$ or $m_j < 0$. We have thus

$$L(m+b) = \sum_{j=1}^{r} a_j |m_j| + \sum_{j=1}^{r} \pm a_j b_j;$$

where the combination of the ± signs depends on the lattice point m. Let us put then

$$L^*(m) = \sum_{j=1}^{r} \frac{p_j}{q} |m_j| + \sum_{j=1}^{r} \pm a_j b_j,$$

where the combination of the ± signs is the same as in the representation of $L(m+b)$. The rest of the argument is already as in the proof of the Theorem 3. For O-estimates see [2].

If we have a region defined by a system of algebraic inequalities then the order of the error term is usually determined by a single piece of the boundary, that is by just one of the inequalities. In this sense, we will not be getting much new.

Let us also mention that all estimates still hold if we restrict ourselves to lattice points with square-free (or cube-free etc.) coordinates as considered by Lursmanašvili or Podsypanin.

Note added in proof by the editor. Similar results have been obtained by B. Novák. However he has notified the editors that his paper *Remarks on Jarník Ω-method in lattice point theory*, announced in J. Number Theory 8(1976), p. 39, will not appear.

References

[1] B. Diviš, *Lattice point theory of irrational ellipsoids with an arbitrary center*, Mh. Math. 83(1977), pp. 279–307.

[2] — *Lattice point theory in polyhedra*, to appear.

[3] — *Mean value estimates in lattice point theory*, Mh. Math. 84(1977), pp. 21–28.

[4] V. Jarník, *Über Gitterpunkte in mehrdimensionalen Ellipsoiden*, Math. Ann. 100 (1928), pp. 699–721; Tôhoku Math. J. 30(1929), pp. 354–371.

[5] — *Bemerkungen zu Landauschen Methoden in der Gitterpunktlehre*, Abh. aus Zahlentheorie und Analysis zur Erinnerung an E. Landau, Berlin 1968, pp. 139–156.

[6] B. Novák, *Mean value theorems in the theory of lattice points with weight II*, Comm. Math. Univ. Carol. 11 (1970), pp. 53–81.

[7] — *Über eine Methode der Ω-Abschätzungen*, Czech. Math. J. 21 (1971), pp. 257–279.

Received on 29. 7. 1976 (862)

ACTA ARITHMETICA
XXXV (1979)

Weak equivalence of functions over a finite field

by

Gary L. Mullen (Sharon, Pa.)

1. Introduction. In a series of papers [1], [3], and [8], L. Carlitz, S. Cavior, and the author studied right equivalence of functions over a finite field. In [3] and [7] S. Cavior and the author studied properties of left equivalence of functions over a finite field, while in [3] Cavior considered the notion of weak equivalence.

In this paper we study a form of weak equivalence which generalizes all of the above types of equivalence of functions over a finite field. Even though we restrict our study to functions of one variable, it will be clear that our results are readily extendable to several variables and in fact, may be extended to functions from one finite set to another.

In Section 1 we are concerned with preliminaries while in Section 2 we present the general theory of weak equivalence. In Section 3 the theory of weak equivalence is applied in the case where the groups of permutations are cyclic. In Section 4, as a special case of weak equivalence, we present an application to similarity of functions over a finite field as considered by Cavior in [3]. Finally in Section 5 we give several applications of weak equivalence to permutation polynomials over a finite field.

Let $K = \mathrm{GF}(q)$ denote the finite field of order q where $q = p^n$. Let $K[x]$ represent the ring of polynomials over K. Two polynomials $f, g \in K[x]$ are equal if they are equal as functions. By the Lagrange Interpolation Formula ([5], p. 55), each function from K into K can be expressed uniquely as a polynomial of degree less than q so that $K[x]$ consists of exactly q^q functions. The group of all permutations of K will be denoted by Φ so that Φ is isomorphic to S_q, the symmetric group of order $q!$. That Ω is an arbitrary subgroup of Φ will be denoted by $\Omega < \Phi$, $|\Omega|$ will denote the order of Ω, and $[\Phi : \Omega]$ will represent the index of Ω in Φ.

2. General theory. We begin with

Definition 2.1. Let $\Omega_1, \Omega_2 < \Phi$ and $f, g \in K[x]$. Then f is *weakly equivalent* to g relative to Ω_1 and Ω_2 if there exists $\varphi_1 \in \Omega_1$ and $\varphi_2 \in \Omega_2$ such that $\varphi_1 f \varphi_2 = g$.