MATHEMATICS

N. M. KOROBOV

1960

SovietRxiv

Abstract

Full Text

MATHEMATICS

N. M. KOROBOV

PROPERTIES AND COMPUTATION OF OPTIMAL COEFFICIENTS

(Presented by Academician I. M. Vinogradov, 5 II 1960)

We shall say that the function

$$f(x_1, \dots, x_s) = \sum_{m_1, \dots, m_s = -\infty}^{\infty} C(m_1, \dots, m_s) e^{2\pi i (m_1 x_1 + \dots + m_{sx} s)} \tag{1}$$

belongs to the class E_s^α, if $C(m_1, \dots, m_s) = O((\overline{m}_1 \cdots \overline{m}_s)^{-\alpha})$, where $\alpha > 1$ and $\overline{m}_\nu = \max(1, |m_\nu|)$. Denote by $-R$ the error of the quadrature formula

$$\int_0^1 \cdots \int_0^1 f(x_1, \dots, x_s)\, dx_1 \cdots dx_s = \frac{1}{p} \sum_{k=1}^{p} f\left(\frac{ka_1}{p}, \dots, \frac{ka_s}{p}\right) - R. \tag{2}$$

According to ([1],[2]), the integers $a_\nu = a_\nu(p)$ $(\nu = 1, 2, \dots, s)$ are called **optimal coefficients** if, for functions $f \in E_s^\alpha$, the estimate $R = O(p^\beta \ln^\beta p)$ holds, where β and the constant in O do not depend on p.

In paper ([1]) the existence was proved and a method was given for finding optimal coefficients for which $\beta = \alpha s$. In the present paper other methods for computing optimal coefficients are indicated, and some of their properties are presented, with applications both in approximate analysis and directly in number theory.

Let z be an integer, $p > s$ a prime, $[A]$ the integral part and $\{A\}$ the fractional part of the number A. Define the function $H(z)$ by the equality

$$H(z) = \frac{3^s}{p} \sum_{k=1}^{p} \left(1 - 2\left\{\frac{k}{p}\right\}\right)^2 \cdots \left(1 - 2\left\{\frac{kz^{s-1}}{p}\right\}\right)^2. \tag{3}$$

Theorem 1. *If the minimum of the function $H(z)$ on the interval $1 \le z < p$ is attained at $z = a$, then the integers $1, a, \dots, a^{s-1}$ will be optimal coefficients for those classes E_s^α for which $\alpha \ge 2$.*

Proof. Denote by $\delta_p(m)$ one or zero according as the congruence $m \equiv 0 \pmod p$ holds or not. We use the equalities

$$\delta_p(m)=\frac{1}{p}\sum_{k=1}^{p}e^{\frac{2\pi imk}{p}},\qquad 3(1-2\{x\})^2=\sum_{m=-\infty}^{\infty}\frac{e^{2\pi imx}}{\psi(m)},\tag{4}$$

where, for $m\neq 0$, $\psi(m)=\frac{\pi^2}{6}m^2$, and $\psi(0)=1$. From (3), after transformations analogous to those carried out in ([1]), since $\psi(m)\geq\overline{m}^2$, we obtain

$$H(z)-1=\sum_{-\infty}^{\infty}{}'\frac{\delta_p(m_1+\cdots+m_sz^{s-1})}{\psi(m_1)\cdots\psi(m_s)}\leq\sum_{-(p-1)}^{p-1}{}'\frac{\delta_p(m_1+\cdots+m_sz^{s-1})}{(\overline{m}_1\cdots\overline{m}_s)^2}+O\left(\frac{1}{p^2}\right),$$

where $\sum'$ means summation over systems $(m_1,\ldots,m_s)\neq(0,\ldots,0)$, in which respectively $|m_\nu|<\infty$ or $|m_\nu|\leq p-1$ $(\nu=1,2,\ldots,s)$.

Let d be the greatest common divisor of the numbers $m_1,\ldots,m_s$, and let $A(m_1,\ldots,m_s)$ be the number of solutions of the congruence $m_1+\cdots+m_sz^{s-1}\equiv 0 \pmod p$. Thus

since for $d\not\equiv 0 \pmod p$ the estimate $A(m_1,\ldots,m_s)\leqslant s-1$ is valid, we have

$$\min_{1\leqslant z<p}\sum_{-(p-1)}^{p-1}{}'\frac{\delta_p(m_1+\cdots+m_sz^{s-1})}{\bar{m}_1\cdots\bar{m}_s}\leqslant\frac{1}{p-1}\sum_{-(p-1)}^{p-1}{}'\frac{1}{\bar{m}_1\cdots\bar{m}_s}\sum_{z=1}^{p-1}\delta_p(m_1+\cdots$$

$$\cdots+m_sz^{s-1})\leqslant\frac{1}{p-1}\sum_{-(p-1)}^{p-1}{}'\frac{A(m_1,\ldots,m_s)}{\bar{m}_1\cdots\bar{m}_s}=O\left(\frac{\ln^s p}{p}\right)$$

and, consequently,

$$H(a)-1\leqslant\left[\min_{1\leqslant z<p}\sum_{-(p-1)}^{p-1}{}'\frac{\delta_p(m_1+\cdots+m_sz^{s-1})}{\bar{m}_1\cdots\bar{m}_s}\right]^2+O\left(\frac{1}{p^2}\right)=O\left(\frac{\ln^{2s}p}{p^2}\right).\tag{5}$$

For $\alpha\geqslant 2$, from (1) and (2), applying the first of the equalities (4), we obtain

$$R=\sum_{m_1,\ldots,m_s=-\infty}^{\infty}{}'C(m_1,\ldots,m_s)\delta_p(a_1m_1+\cdots+a_{sm}s),\tag{6}$$

$$|R|\leqslant C\sum_{-\infty}^{\infty}{}'\frac{\delta_p(a_1m_1+\cdots+a_{sm}s)}{(\bar{m}_1\cdots\bar{m}_s)^\alpha}\leqslant C\left[\sum_{-\infty}^{\infty}{}'\frac{\delta_p(a_1m_1+\cdots+a_{sm}s)}{(\bar{m}_1\cdots\bar{m}_s)^2}\right]^{\alpha/2},$$

where $C = C(\alpha, s)$. Hence, since $\bar{m}^2 \geqslant \frac{6}{\pi^2}\psi(m)$, for $a_\nu = a^{\nu-1}$, by virtue of (5) the assertion of the theorem follows:

$$\sum_{-\infty}^{\infty}{}' \frac{\delta_p(m_1 + \cdots + m_{sa}^{s-1})}{(\bar{m}_1 \cdots \bar{m}_s)^2} \leqslant \left(\frac{\pi^2}{6}\right)^s \sum_{-\infty}^{\infty}{}' \frac{\delta_p(m_1 + \cdots + m_{sa}^{s-1})}{\psi(m_1)\cdots\psi(m_s)} = \left(\frac{\pi^2}{6}\right)^s [H(a)-1], \tag{7}$$

$$|R| \leqslant C\left(\frac{\pi^2}{6}\right)^{\alpha s/2} [H(a)-1]^{\alpha/2} = O\left(\frac{\ln^{\alpha s} p}{p^\alpha}\right).$$

Corollary. For $s \geqslant 2$, the incomplete quotients of the expansions of the numbers

$$\left\{\frac{a^2}{p}\right\}, \ldots, \left\{\frac{a^{s-1}}{p}\right\}$$

into continued fractions are bounded by $C \ln^s p$, where the constant C depends only on s.

Indeed, since for $|m_1| \leqslant p/2$, from the congruence $-m_1 \equiv a^\nu m_{\nu+1} \pmod p$ there follows the equality

$$|m_1| = p\left(\frac{a^\nu m_{\nu+1}}{p}\right),$$

where (A) is the distance from A to the nearest integer, by virtue of (7) and (5) we obtain

$$\frac{1}{p^2} \sum_{|m_{\nu+1}| \not\equiv 0 \pmod p} \left(\left(\frac{a^\nu m_{\nu+1}}{p}\right) m_{\nu+1}\right)^{-2} = \sum_{1 \leqslant |m_1| < p/2} \sum_{|m_{\nu+1}|=1}^{\infty} \frac{\delta_p(m_1 + a^\nu m_{\nu+1})}{(|m_1|\,|m_{\nu+1}|)^2} \leqslant$$

$$\leqslant \sum_{-\infty}^{\infty}{}' \frac{\delta_p(m_1 + \cdots + m_{sa}^{s-1})}{(\bar{m}_1 \cdots \bar{m}_s)^2} = O\left(\frac{\ln^{2s} p}{p^2}\right).$$

Hence, for any integer $m_{\nu+1}$ not divisible by p, for some $C = C(s)$ we obtain the inequalities

$$\left(\frac{a^\nu}{p} m_{\nu+1}\right) \geqslant \frac{1}{C|m_{\nu+1}| \ln^s p} \qquad (\nu = 1, 2, \ldots, s-1), \tag{8}$$

which are equivalent to the assertion of the corollary.

The following theorem somewhat strengthens this result.

Theorem 2. For $s \geqslant 2$, for each sufficiently large prime p one can indicate no fewer than $2^{-s+1}p$ integers $a = a(p)$ such that the in-

the incomplete quotients $\dfrac{a}{p}, \left\{\dfrac{a^2}{p}\right\}, \ldots, \left\{\dfrac{a^{s-1}}{p}\right\}$ are bounded respectively by the quantities $2(5\ln p), 2(5\ln p)^2, \ldots, 2(5\ln p)^{s-1}$.

Proof. For $\nu = 1, 2, \ldots, s-1$ introduce the notation

$$p_\nu = \left[\frac{p}{2^\nu}\right], \qquad q_\nu = \left[\frac{p}{2\cdot 5^\nu \ln^\nu p}\right] + 1, \qquad S_\nu(z) = \sum_{\overline{m_1}\ldots\overline{m_{\nu+1}}<q_\nu}{}' \delta_p(m_1 + \cdots + m_{\nu+1}z^\nu).$$

Let $z_1, \ldots, z_{p-1}$ be such a permutation of the numbers $1, 2, \ldots, p-1$ for which

$$S_1(z_1) \geq S_1(z_2) \geq \cdots \geq S_1(z_{p-1}).$$

Then, for sufficiently large p,

$$S_1(z_{p_1}) \leq \frac{1}{p_1}\sum_{j=1}^{p_1} S_1(z_j) \leq \frac{1}{p_1}\sum_{\overline{m_1 m_2}<q_1}{}' 1 < 1,$$

and, by the definition of $S_\nu(z)$, we obtain

$$S_1(z_{p_1}) = \cdots = S_1(z_{p-1}) = 0.$$

It follows that for $a = z_j$, where $p_1 \leq j < p$, for nontrivial solutions of the congruence

$$m_1 + am_2 \equiv 0 \pmod p$$

the inequality $\overline{m_1 m_2} \geq q_1$ is satisfied. But then, since

$$|m_1| = \left(\frac{am_2}{p}\right)p,$$

for $m_2 \not\equiv 0 \pmod p$ we obtain

$$\left(\frac{am_2}{p}\right) \geq \frac{q_1}{p|m_2|} > \frac{1}{10|m_2|\ln p}.$$

From this inequality, since $p - p_1 \geq p_1$, we obtain the assertion of the theorem for the case $s = 2$.

We apply induction. Suppose the theorem is true for some $s = k$ $(k \geq 2)$. Then on the interval $[1, p-1]$ there exist p_{k-1} values of a for which, for $\nu =$

$1, 2, \dots, k-1$, the incomplete quotients $\left\{\frac{a^\nu}{p}\right\}$ are bounded respectively by the quantities $2 \cdot 5^\nu \ln^\nu p$. Arranging these values a so that the inequalities

$$S_k(z'_1) \geq \cdots \geq S_k(z'_{p_{k-1}})$$

hold, as above, we obtain

$$S_k(z'_{p_k}) = \cdots = S_k(z'_{p_{k-1}}) = 0.$$

Choose $a = z'_j$, where $p_k \leq j \leq p_{k-1}$. Then for nontrivial solutions of the congruence

$$m_1 + \cdots + m_{k+1}a^k \equiv 0 \pmod{p}$$

the inequality $\overline{m_1 \cdots m_{k+1}} \geq q_k$ will be satisfied. In particular, for solutions in which

$$m_2 + \cdots + m_{k+1}a^{k-1} \not\equiv 0 \pmod{p},$$

for $p > p_0$ we obtain

$$\left(\frac{a}{p}m_2 + \cdots + \frac{a^k}{p}m_{k+1}\right) \geq \frac{q_k}{p\overline{m_2} \cdots \overline{m_{k+1}}} > \frac{1}{2 \cdot 5^k \overline{m_2} \cdots \overline{m_{k+1}} \ln^k p}. \qquad (9)$$

Hence, putting $m_2 = \cdots = m_k = 0$, it follows that the incomplete quotients

$$\left\{\frac{a^k}{p}\right\}$$

are bounded by the quantity $2 \cdot 5^k \ln^k p$, and, since $p_{k-1} - p_k + 1 > p_k$, we obtain the assertion of the theorem.

Inequalities (8) and (9) may be regarded as consequences of a more general assertion connecting the concept of optimal coefficients with questions of linear Diophantine approximations.

Theorem 3. Let $(a_\nu, p) = 1$ and $a_\nu b_\nu \equiv 1 \pmod{p}$ $(\nu = 1, 2, \dots, s)$. A necessary and sufficient condition for the quantities $a_1, \dots, a_s$ to be optimal coefficients is the fulfillment of the inequalities

$$\left|\frac{b_{\nu-1}a_\nu}{p}m_\nu + \cdots + \frac{b_{\nu-1}a_s}{p}m_s - n\right| > \frac{B}{\overline{m_\nu} \cdots \overline{m_s}^1 \ln^\gamma p} \qquad (\nu = 2, 3, \dots, s) \quad (10)$$

for any integers $n, m_\nu, \dots, m_s$ satisfying the condition

$$a_\nu m_\nu + \cdots + a_s m_s \not\equiv 0 \pmod{p},$$

where $B = B(s) > 0$ and $\gamma = \gamma(s) \geq 0$.

The proof is based on the use of the relation

$$R = \sum_{-\infty}^{\infty} \frac{\delta_p(a_1 m_1 + \cdots + a_{sm} s)}{(\overline{m_1} \cdots \overline{m_s})^{\alpha}},$$

which is obtained from (6) with

$$C(m_1, \ldots, m_s) = (\overline{m_1} \cdots \overline{m_s})^{-\alpha};$$

in proving the sufficiency of conditions (10), Theorem 2 of the paper ([3]) is also used.

Corollary. Let $(a, p) = 1$, $s \geqslant 2$, $B = B(s) > 0$, $\gamma = \gamma(s) \geqslant 0$, and let $m_2, \ldots, m_s$ be arbitrary integers for which $m_2 + \cdots + a^{s-2} m_s \not\equiv 0 \pmod{p}$. The integers $1, a, \ldots, a^{s-1}$ will then and only then be optimal coefficients when the condition

$$\left(\frac{a}{p} m_2 + \cdots + \frac{a^{s-1}}{p} m_s \right) > -\frac{B}{\overline{m}_2 \ldots \overline{m}_s \ln^{\gamma} p} \tag{11}$$

is satisfied.

Remark 1. Using Theorem 3, it is easy to show that the optimality property of the coefficients indicated in Theorem 1 for $\alpha \geqslant 2$ extends to all classes E_s^{α} with $\alpha > 1$.

Remark 2. The process of finding integers $a = a(p)$ leading to inequality (9) can be used in computing optimal coefficients. To simplify the computations, we modify this process as follows. Let

$$\sigma_{\nu}(z) = \sum_{\overline{m}1 \ldots \overline{m}_s = \nu} \delta_p(m_1 + \cdots + m_s z^{s-1}),$$

where $p > s$ is prime. Those of the integers $z \in [1, p-1]$ for which $\sigma_1(z) = 0$ we denote by z_1. Next, those among the z_1 for which $\sigma_2(z_1) = 0$ we denote by z_2. In general, those among the $z_{\nu-1}$ for which $\sigma_{\nu}(z_{\nu-1}) = 0$ we denote by z_{ν}. Obviously, $\sigma_1(z_{\nu}) = \cdots = \sigma_{\nu}(z_{\nu}) = 0$. The process terminates after obtaining quantities z_n, for each of which $\sigma_{n+1}(z_n) > 0$. It is easy to verify that if a is equal to any of the quantities z_n, then, by virtue of (11), the integers $1, a, \ldots, a^{s-1}$ will be optimal coefficients.

The number of operations necessary for computing optimal coefficients can be significantly reduced by passing to quantities $p = p'p''$, where p' and p'' are prime and p'' has order $\sqrt{p'}$. Let, for example,

$$\widetilde{H}(z) = \frac{3^s}{p'p''} \sum_{k=1}^{p'p''} \left(1 - 2\left\{\frac{p' + p''}{p'p''} k\right\}\right)^2 \cdots \left(1 - 2\left\{\frac{p' z^{s-1} + p'' a^{s-1}}{p'p''} k\right\}\right)^2,$$

where a is defined as in Theorem 1 for $p = p'$. Let, further, $\widetilde{H}(b) = \min_{1 \leqslant z < p''} \widetilde{H}(z)$. It can be shown that for $p = p'p''$ the integers $p' + p'', \ldots, p'b^{s-1} + p''a^{s-1}$ will be optimal coefficients; to compute them it is enough to carry out $O(p^{1+1/3})$ elementary operations (the number of operations in Theorem 1 and in Remark 2 is respectively $O(p^2)$ and $O(p^2 \ln^{s-1} p)$).

In conclusion we note one property of cubature formulas constructed with the aid of optimal coefficients. Let us call the degree of the finite trigonometric polynomial

$$P(x_1, \ldots, x_s) = \sum_{m_1, \ldots, m_s} C(m_1, \ldots, m_s) e^{2\pi i (m_1 x_1 + \cdots + m_{sx} s)}$$

the maximum of the product $\overline{m}_1 \cdots \overline{m}_s$. By virtue of (11), from (9), for $k = s-1$ it follows that the integers $1, a, \ldots, a^{s-1}$ obtained in Theorem 2 will be optimal coefficients. We shall assume that $\max \overline{m}_1 \cdots \overline{m}_s \leqslant \frac{1}{2} p (5 \ln p)^{-s+1}$. Using the equality $\delta_p(m_1 + \cdots + m_s a^{s-1}) = 0$, valid for systems $(m_1, \ldots, m_s) \neq (0, \ldots, 0)$ satisfying the condition $\overline{m}_1 \cdots \overline{m}_s \leqslant \frac{1}{2} p (5 \ln p)^{-s+1}$, for $f = P$ by virtue of (6) we obtain $R = 0$. Thus, cubature formulas constructed with the aid of these optimal coefficients, for sufficiently large prime p, will be exact for trigonometric polynomials whose degree does not exceed $\frac{1}{2} p (5 \ln p)^{-s+1}$. By virtue of Theorem 3, an analogous assertion with $\frac{1}{2} p (5 \ln p)^{-s+1}$ replaced by $Bp \ln^{-\gamma} p$ is also valid for an arbitrary choice of optimal coefficients.

Mathematical Institute named after V. A. Steklov
Academy of Sciences of the USSR

Received
4 II 1960

REFERENCES

1. N. M. Korobov, DAN, **124**, No. 6, 1207 (1959).
2. N. M. Korobov, Vestn. MGU, No. 4 (1959).
3. N. S. Bakhvalov, Vestn. MGU, No. 4 (1959).

Note: Figure translations are in progress. See original paper for figures.