SOME PROBLEMS IN THE THEORY OF DIOPHANTINE APPROXIMATION

1967 Russ. Math. Surv. 22 80

(http://iopscience.iop.org/0036-0279/22/3/R02)

To Aleksandr Ostopovich Gel'fond on his sixtieth birthday

SOME PROBLEMS IN THE THEORY OF DIOPHANTINE APPROXIMATION

N.M. Korobov

Contents

Introduction 80
§ 1. The approximate calculation of multiple sums. 82
§ 2. The properties of optimal coefficients. 95
References 117

Introduction

In this paper we consider a number of problems in the theory of diophantine approximation that are connected with the application of number theory to the construction of formulae for many-dimensional quadrature.

In the first section the example of multiple sums is used to show how number-theoretical arguments arise in questions of numerical analysis. Formulae for approximate summation are introduced in §1.1: they are similar to the quadrature formulae I obtained in 1957–59 (see [8] and [9]). The transition to multiple sums from many-dimensional integrals permits us to use the elementary technique of finite Fourier sums, which makes the problem simpler and enables us to extend the class of functions under discussion.

In § 1.2 the same example of multiple sums is used to illustrate the method of constructing quadrature formulae for functions of bounded variation that was developed by Hlawka from 1962 onward (see [5] – [7]). At the end of the section we compare the potentialities of the two methods. Here it becomes clear that for parallelopipedal nets[1]

$$M_k=\left(\left\{\frac{a_1k}{p}\right\},\ \ldots,\ \left\{\frac{a_sk}{p}\right\}\right) \qquad (k=1,\ 2,\ \ldots,\ p) \tag{1}$$

and for the same degree of exactness in the formulae of approximate summation, the method of § 1.1 can be applied to a wider class of functions. Such a class, containing the functions of bounded variation, is the class $E_{s,p}(C)$ consisting of the functions $f(x_1,\ \ldots,\ x_s)$ for which

[1] A net (Russian: *setka*) is just the finite set of points used in an approximate computation (see the definition of [11] on p.43). The adjective parallelopipedal is applied to nets of the type (1) in the unit cube, the braces { } denoting the fractional part. (Transl.)

$$|C_p(m_1, \ldots, m_s)| \leqslant \frac{C}{\overline{m}_1 \ldots \overline{m}_s},$$

where $C_p(m_1, \ldots, m_s)$ are the finite Fourier coefficients of f, f, $\overline{m}_v = \max(1, |m_v|)$, and C is a constant independent of $m_1, \ldots, m_s$. As is shown in Theorem 2, for functions in $E_{s,p}(C)$ there is a parallelopipedal net for which the following formula of approximate summation holds:[1]

$$\frac{1}{p^s} \sum_{k_1, \ldots, k_s=0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) = \frac{1}{p} \sum_{k=1}^{p} f\left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_s k}{p}\right\}\right) + O\left(\frac{\ln^s p}{p}\right) \tag{2}$$

This result is obtained by means of optimal parallelopipedal nets, that is, nets of the form (1) where $a_1, \ldots a_s$ are integers chosen in a special way (optimal coefficients). The remainder term in (2) cannot be improved for any choice of the net (1).

In § 2 we consider the number-theoretical properties of optimal coefficients and state some problems in the theory of diophantine approximation.

In § 2.1 we investigate the connection between the optimality of parallelopipedal nets and the nature of the distribution of the points of those nets in the s-dimensional unit cube. It turns out that for optimal nets the value of the discrepancy, which characterizes the degree of uniformity of the distribution, is nearly minimal. Hence the optimal parallelopipedal nest are among the most uniformly distributed nets.

Next, in § 2.2 we consider the approximation to zero of the fractional part of the linear function

$$\alpha_1 m_1 + \ldots + \alpha_s m_s \qquad \left(\alpha_\nu = \frac{a_\nu}{p}, \quad \nu = 1, 2, \ldots, s\right) \tag{3}$$

and of the system of linear functions $\alpha_1 m, \ldots, \alpha_s m$. As the Corollaries of Theorem 7 show, a necessary and sufficient condition for the optimality of $1, a_1, \ldots, a_s$ is, in an appropriate sense, that these fractional parts are as far from zero as possible.

In § 2.3 we investigate the nature of the uniformity of distribution of the fractional parts of (3) and show that for optimal coefficients the discrepancy of the points $\{\alpha_1 m_1 + \ldots + \alpha_s m_s\}$ must be minimal.

Finally, in § 2.4 we clarify the connection between the optimality of parallelopipedal nets and the asymptotic properties of sums of fractional parts of linear functions. Let b, b_v, λ_ν be arbitrary integers and let $P \leqslant p$, $P_v \leqslant p$. Let γ be rational with denominator p and let $(\tau_1, \ldots, \tau_s) \neq (0, \ldots, 0)$ be any sequence of 0's and 1's. Denote by $N_p(\gamma_1, \ldots, \gamma_s)$ the number of the P first points of (1) that lie in $0 \leqslant x_1 < \gamma_1, \ldots, 0 \leqslant x_s < \gamma_s$, and similarly denote by $N_{p_1, \ldots, p_s}(\gamma)$

[1] Here and henceforth $\{x\}$ is the fractional part of x.

the number of fractional points of (3) lying in $[0, \gamma)$ when $m_\nu = \lambda_\nu + 1, \ldots, \lambda_\nu + P_\nu$ $(1 \leqslant \nu \leqslant s)$. The results obtained in the second section may be combined in the following pairs of dual propositions:

$$\begin{cases} \mathrm{I} & N_P(\gamma_1, \ldots, \gamma_s) = \gamma_1 \ldots \gamma_s P + O(\ln^{\beta_1} p), \\ \mathrm{I}' & N_{P_1, \ldots, P_s}(\gamma) = \gamma P_1 \ldots P_s + O(\ln^{\beta_1'} p), \end{cases}$$

$$\begin{cases} \mathrm{II} & \ll \frac{a_1 m}{p} \gg \ldots \ll \frac{a_s m}{p} \gg \geqslant \frac{1}{|m|\,(B_2 \ln^{\beta_2} p)}, \quad m \not\equiv 0 \pmod p, \\ \mathrm{II}' & \ll \frac{a_1 m_1 + \ldots + a_s m_s}{p} \gg \geqslant \frac{1}{\overline{m}_1 \ldots \overline{m}_s\,(B_2' \ln^{\beta_2'} p)}, \quad a_1 m_1 + \ldots + a_s m_s \not\equiv 0 \pmod p, \end{cases}$$

$$\begin{cases} \mathrm{III} & \sum_{m=1}^{P} \prod_{\nu=1}^{s} \left(\left\{ \frac{a_\nu m + b_\nu}{p} \right\} - \frac{p-1}{2p} \right)^{\tau_\nu} = O(\ln^{\beta_3} p), \\ \mathrm{III}' & \sum_{m_1=1}^{P_1} \cdots \sum_{m_s=1}^{P_s} \left(\left\{ \frac{a_1 m_1 + \ldots + a_s m_s + b}{p} \right\} - \frac{p-1}{2p} \right) = O(\ln^{\beta_3'} p) \end{cases}$$

Any one of these conditions is necessary and sufficient for the $1, a_1, \ldots, a_s$ to be $(s + 1)$-dimensional optimal coefficients. Hence if any one of them is satisfied, so are the others.

Observe that II and II′ can be regarded as a case of Khinchin's Transference Theorem. The results I–III′ show that for forms with rational coefficients transference theorems are only one of the possible manifestations of a connection between the fractional parts of a system of linear forms and the system of transposed forms. Other forms of this connection appear in the behaviour of the sums of fractional parts (III $\longleftrightarrow$ III′) and in the distribution of fractional parts (I $\longleftrightarrow$ I′).

The theorems proved in § 2 enable us to give values of the exponents $\beta_1, \ldots, \beta_3'$ for which I – III′ hold. However, except for $s = 1$ the question of minimal exponents remains open.

§ 1. The approximate calculation of multiple sums

1. Let $p > 1$ be an integer and let $f(x_1, \ldots, x_s)$ be defined at all rational points with common denominator p. We state the problem of the approximate calculation of the multiple sum

$$\frac{1}{p^s} \sum_{k_1, \ldots, k_s = 0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) \tag{4}$$

as follows: to find integral functions $z_1(k), \ldots, z_s(k)$ such that for every function f from some sufficiently wide class the sum

$$\frac{1}{p} \sum_{k=1}^{p} f\left(\left\{\frac{z_1(k)}{p}\right\}, \ldots, \left\{\frac{z_s(k)}{p}\right\}\right) \tag{5}$$

differs little from (4). More precisely, we look for nets

$$M_k = \left(\left\{ \frac{z_1(k)}{p} \right\}, \ldots, \left\{ \frac{z_s(k)}{p} \right\} \right) \qquad (k = 1, 2, \ldots, p),$$

for which the maximum modulus of the error R in the equation

$$\frac{1}{p^s} \sum_{k_1, \ldots, k_s = 0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p} \right) = \frac{1}{p} \sum_{k=1}^{p} f\left(\left\{ \frac{z_1(k)}{p} \right\}, \ldots, \left\{ \frac{z_s(k)}{p} \right\} \right) - R$$

tends to zero as fast as possible, as $p \to \infty$, for the class of functions in question.

In what follows we need two simple lemmas (see, for example, [11], Lemmas 1 and 15).

LEMMA 1. *Suppose that for integral m and $p > 1$ the quantity $\delta_p(m)$ is defined to be 1 if p divides m and to be 0 otherwise. Then*

$$\delta_p(m) = \frac{1}{p} \sum_k e^{2\pi i \frac{mk}{p}}, \tag{6}$$

where k runs through a complete set of residues mod p.

We define integers p_1 and p_2 by[1]

$$p_1 = \left[\frac{p-1}{2} \right], \quad p_2 = \left[\frac{p}{2} \right].$$

Then the integers of the interval $-p_1 \leqslant k \leqslant p_2$ are a complete set of residues mod p and in particular, the sum in (6) can be taken from $-p_1$ to p_2.

LEMMA 2. *Let $p > 1$ be an integer and let the function $f(x_1, \ldots, x_n)$ be defined at the points*

$$\left(\frac{z_1}{p}, \ldots, \frac{z_s}{p} \right) \qquad (z_\nu = 0, 1, \ldots, p-1;\ 1 \leqslant \nu \leqslant s).$$

Then at each of these points we have

$$f\left(\frac{z_1}{p}, \ldots, \frac{z_s}{p} \right) = \sum_{m_1, \ldots, m_s = -p_1}^{p_2} C_p(m_1, \ldots, m_s)\, e^{2\pi i \frac{m_1 z_1 + \ldots + m_s z_s}{p}}, \tag{7}$$

where

$$C_p(m_1, \ldots, m_s) = \frac{1}{p^s} \sum_{k_1, \ldots, k_s = 0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p} \right) e^{-2\pi i \frac{m_1 k_1 + \ldots + m_s k_s}{p}}. \tag{8}$$

The $C_p(m_1, \ldots, m_s)$ are called the *finite Fourier coefficients* of f and (7) is the *finite Fourier series* of f.

We now define the class of functions for which we shall discuss the question of the approximate calculation of multiple sums. We say that $f(x_1, \ldots, x_s)$ belongs to the class $E_{s,p}(C)$ if its finite Fourier

---

[1] Here and henceforth $[x]$ is the integral part of x.

coefficients satisfy

$$|C_p(m_1, \ldots, m_s)| \leqslant \frac{C}{\overline{m}_1 \ldots \overline{m}_s}, \quad \text{where } \overline{m}_\nu = \max(1, |m_\nu|).$$

The class $E_{s,p}(C)$ is very extensive. It is wider than $H_s^1(C)$ (see [11], Lemma 16) and, as will be shown below, is wider than the class of functions of bounded variation. Here we give only one example by showing that $E_{s,p}(C)$ contains the (piecewise constant) characteristic functions of rectangular domains of the form

$$0 \leqslant x_1 < \gamma_1, \ldots, 0 \leqslant x_s < \gamma_s, \tag{9}$$

where $\gamma_1, \ldots, \gamma_s$ are any numbers from $(0, 1]$.

For let Ω_s be the domain defined by (9) and let $\varphi(x_1, \ldots, x_s)$ be its characteristic function:

$$\varphi(x_1, \ldots, x_s) = \begin{cases} 1 & \text{if } (x_1, \ldots, x_s) \in \Omega_s, \\ 0 & \text{otherwise.} \end{cases}$$

Denote by $C_p(m_1, \ldots, m_s)$ the finite Fourier coefficients of φ and define the integers n_ν by

$$n_\nu = \begin{cases} [\gamma_\nu p] & \text{if } \{\gamma_\nu p\} \neq 0, \\ [\gamma_\nu p] - 1 & \text{if } \{\gamma_\nu p\} = 0 \end{cases} \qquad (\nu = 1, 2, \ldots, s).$$

Then by (8) we have

$$C_p(m_1, \ldots, m_s) = \frac{1}{p^s} \sum_{k_1, \ldots, k_s = 0}^{p-1} \varphi\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) e^{-2\pi i \frac{m_1 k_1 + \ldots + m_s k_s}{p}} =$$

$$= \frac{1}{p^s} \sum_{k_1=0}^{n_1} \cdots \sum_{k_s=0}^{n_s} e^{-2\pi i \frac{m_1 k_1 + \ldots + m_s k_s}{p}}$$

$$|C_p(m_1, \ldots, m_s)| = \frac{1}{p^s} \prod_{\nu=1}^{s} \left| \sum_{k_\nu=0}^{n_s} e^{2\pi i \frac{m_\nu k_\nu}{p}} \right|.$$

Since for $|m_\nu| \leqslant \frac{1}{2} p$ and $n_\nu \leqslant p-1$ we have (see [11], Lemma 3)

$$\left| \sum_{k_\nu=0}^{n_\nu} e^{2\pi i \frac{m_\nu k_\nu}{p}} \right| \leqslant \min\left(n_\nu + 1, \frac{1}{2 \langle\!\langle \frac{m_\nu}{p} \rangle\!\rangle}\right) \leqslant \frac{p}{\overline{m}_\nu}, \tag{10}$$

it follows clearly that

$$|C_p(m_1, \ldots, m_s)| \leqslant \frac{1}{p^s} \prod_{\nu=1}^{s} \frac{p}{\overline{m}_\nu} = \frac{1}{\overline{m}_1 \ldots \overline{m}_s}.$$

By definition it follows that φ is in $E_{s,p}(C)$ with $C = 1$.

We show now that for $f \in E_{s,p}(C)$ the estimation of the error made in replacing (4) by (5) reduces to the estimation of trigonometric sums of a special type depending only on the choice of the net

$$M_k = \left(\left\{ \frac{z_1(k)}{p} \right\}, \ldots, \left\{ \frac{z_s(k)}{p} \right\} \right) \qquad (k = 1, 2, \ldots, p).$$

THEOREM 1. *If f is in $E_{s,p}(C)$, then the R given by*

$$\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ldots,\frac{k_s}{p}\right)=\frac{1}{p}\sum_{k=1}^{p} f\left(\left\{\frac{z_1(k)}{p}\right\},\ldots,\left\{\frac{z_s(k)}{p}\right\}\right)-R,$$

satisfies the estimate[1]

$$|R|\leqslant\frac{C}{p}\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{|S(m_1,\ldots,m_s)|}{\overline{m}_1\ldots\overline{m}_s},$$

where

$$S(m_1,\ldots,m_s)=\sum_{k=1}^{p} e^{2\pi i\frac{m_1z_1(k)+\ldots+m_sz_s(k)}{p}}. \tag{11}$$

PROOF. Using the expression of f as a finite Fourier series and noting that

$$\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ldots,\frac{k_s}{p}\right)=C_p(0,\ldots,0),$$

we obtain

$$R=-\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ldots,\frac{k_s}{p}\right)+\frac{1}{p}\sum_{k=1}^{p} f\left(\left\{\frac{z_1(k)}{p}\right\},\ldots,\left\{\frac{z_s(k)}{p}\right\}\right)=$$

$$=-C_p(0,\ldots,0)+\frac{1}{p}\sum_{k=1}^{p}\sum_{m_1,\ldots,m_s=-p_1}^{p_2} C_p(m_1,\ldots,m_s)\,e^{2\pi i\frac{m_1z_1(k)+\ldots+m_sz_s(k)}{p}}=$$

$$=\frac{1}{p}\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' C_p(m_1,\ldots,m_s)\sum_{k=1}^{p} e^{2\pi i\frac{m_1z_1(k)+\ldots+m_sz_s(k)}{p}}$$

In the notation (11) this takes the form

$$R=\frac{1}{p}\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' C_p(m_1,\ldots,m_s)\,S(m_1,\ldots,m_s). \tag{12}$$

Since $f \in E_{s,p}(C)$, the assertion of the theorem follows:

$$|C_p(m_1,\ldots,m_s)|\leqslant\frac{C}{\overline{m}_1\ldots\overline{m}_s},$$

$$|R|\leqslant\frac{1}{p}\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' |C_p(m_1,\ldots,m_s)|\,|S(m_1,\ldots,m_s)|\leqslant$$

$$\leqslant\frac{C}{p}\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{|S(m_1,\ldots,m_s)|}{\overline{m}_1\ldots\overline{m}_s}.$$

From Theorem 1 it is clear that the better we can estimate

$$\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{|S(m_1,\ldots,m_s)|}{\overline{m}_1\ldots\overline{m}_s},$$

---

[1] Here and in what follows Σ' indicates that the term with $m_1=\ldots=m_s=0$ is omitted from the summation.

the better the results we can guarantee in the construction of approximate formulae for multiple sums. The estimate of this sum depends clearly only on the choice of the net M_k. Hence on choosing the net so that the sums $S(m_1, \ldots, m_s)$ have sufficiently good estimates we may guarantee one accuracy or another for the corresponding formulae of approximate summation. Let us choose, for example,

$$z_\nu(k) = k^\nu \qquad (\nu = 1, 2, \ldots, s)$$

and consider the corresponding non-uniform net

$$M_k = \left(\left\{\frac{k}{p}\right\}, \ldots, \left\{\frac{k^s}{p}\right\}\right) \qquad (k = 1, 2, \ldots, p).$$

The trigonometric sums $S(m_1, \ldots, m_s)$ corresponding to this net are the well-known rational trigonometric sums

$$S(m_1, \ldots, m_s) = \sum_{k=1}^{p} e^{2\pi i \frac{m_1 k + \ldots + m_s k^s}{p}}.$$

If p is a prime and at least one of the m_ν is not a multiple of by p, then results of A. Weil [4] imply that

$$|S(m_1, \ldots, m_s)| < s\sqrt{p}.$$

Taking p prime and using this estimate we obtain

$$\sum_{m_1, \ldots, m_s = -p_1}^{p_2}{}' \frac{|S(m_1, \ldots, m_s)|}{\overline{m}_1 \ldots \overline{m}_s} = O(\sqrt{p}\ln^s p).$$

Hence, by Theorem 1, for $f \in E_{s,p}(C)$ and prime p we have

$$\frac{1}{p^s} \sum_{k_1, \ldots, k_s = 0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) = \frac{1}{p} \sum_{k=1}^{p} f\left(\left\{\frac{k}{p}\right\}, \ldots, \left\{\frac{k^s}{p}\right\}\right) + O\left(\frac{\ln^s p}{\sqrt{p}}\right). \quad (13)$$

Let us now consider nets of the form

$$M_k = \left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_s k}{p}\right\}\right) \qquad (k = 1, 2, \ldots, p),$$

where $a_1, \ldots, a_s$ are integers relatively prime to p. We call such nets *parallelopipedal.* let us show that the estimate (13) can be improved essentially if instead of non-uniform nets we use parallelopipedal nets of a special type.

THEOREM 2. *There are parallelopipedal nets such that for f in $E_{s,p}(C)$*

$$\frac{1}{p^s} \sum_{k_1, \ldots, k_s = 0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) = \frac{1}{p} \sum_{k=1}^{p} f\left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_s k}{p}\right\}\right) + O\left(\frac{\ln^s p}{p}\right).$$

PROOF. For parallelopipedal nets the $z_\nu(k)$ are given by

$$z_\nu(k) = a_\nu k \qquad (\nu = 1, 2, \ldots, s),$$

and so by Lemma 1 we find

$$S(m_1, \ldots, m_s) = \sum_{k=1}^{p} e^{2\pi i \frac{m_1 z_1(k)+\ldots+m_s z_s(k)}{p}} =$$
$$= \sum_{k=1}^{p} e^{2\pi i \frac{(a_1 m_1+\ldots+a_s m_s)k}{p}} = p\delta_p(a_1 m_1 + \ldots + a_s m_s). \quad (14)$$

Hence and by Theorem 1 we have

$$\frac{1}{p^s} \sum_{k_1, \ldots, k_s=0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) = \frac{1}{p} \sum_{k=1}^{p} f\left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_s k}{p}\right\}\right) - R,$$

where

$$|R| \leqslant C \sum_{m_1, \ldots, m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1 m_1 + \ldots + a_s m_s)}{\bar{m}_1 \ldots \bar{m}_s}. \quad (15)$$

Let p be prime. Then (see [11], Lemma 20) there are integers $a_\nu = a_\nu(p)$ $(\nu = 1, 2, \ldots, s)$ prime to p such that

$$\sum_{m_1, \ldots, m_s=-(p-1)}^{p-1}{}' \frac{\delta_p(a_1 m_1 + \ldots + a_s m_s)}{\bar{m}_1 \ldots \bar{m}_s} < \frac{2(3+2\ln p)^s}{p}.$$

Hence and by (15) we have the assertion of the theorem:

$$|R| < 2C \frac{(3+2\ln p)^s}{p} = O\left(\frac{\ln^s p}{p}\right).$$

In the following theorem we show that the estimate of Theorem 2 cannot be further improved by any choice of parallelopipedal nets. Hence it turns out to be convenient to distinguish those nets for which the estimate of the error of the corresponding approximation formula either coincides with that obtained in Theorem 2 or differs from it only inessentially. This gives us the concept of optimal parallelopipedal nets

$$M_k = \left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_1 k}{p}\right\}\right) \qquad (k = 1, 2, \ldots, p)$$

and optimal coefficients $a_1, \ldots, a_s$.

Let $p > 1$ be an integer, $p_1 = \left[\frac{p-1}{2}\right]$, $p_2 = \left[\frac{p}{2}\right]$. Let $a_\nu = a_\nu(p)$ be integers relatively prime to p and let $\delta_p(m)$ denote 1 or 0 according as p divides m or not. *If there exist constants $\beta = \beta(s)$ and $B = B(s)$ such that for an infinite sequence of values of p*

$$\sum_{m_1, \ldots, m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1 m_1 + \ldots + a_s m_s)}{\bar{m}_1 \ldots \bar{m}_s} \leqslant B \frac{\ln^\beta p}{p}, \quad (16)$$

then the integers $a_1, \ldots, a_s$ are called optimal coefficients and the corresponding nets M_k are called optimal parallelopipedal nets.

From the proof of Theorem 2 it is clear that for optimal nets and for $f \in E_{s,p}(C)$ we have

$$\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ \ldots,\ \frac{k_s}{p}\right)=\frac{1}{p}\sum_{k=1}^{p} f\left(\left\{\frac{a_1k}{p}\right\},\ \ldots,\ \left\{\frac{a_sk}{p}\right\}\right)+O\left(\frac{\ln^\beta p}{p}\right).$$

For this follows from (15) and (16):

$$\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ \ldots,\ \frac{k_s}{p}\right)=\frac{1}{p}\sum_{k=1}^{p} f\left(\left\{\frac{a_1k}{p}\right\},\ \ldots,\ \left\{\frac{a_sk}{p}\right\}\right)-R,$$

$$|R|\leqslant C\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\ldots+a_sm_s)}{\overline{m}_1\ldots\overline{m}_s}\leqslant BC\frac{\ln^\beta p}{p}.$$

THEOREM 3. *There is an $f \in E_{s,p}(C)$ such that for any choice of integers $a_1, \ldots, a_s$ relatively prime to p the error in*

$$\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ \ldots,\ \frac{k_s}{p}\right)=\frac{1}{p}\sum_{k=1}^{p} f\left(\left\{\frac{a_1k}{p}\right\},\ \ldots,\ \left\{\frac{a_sk}{p}\right\}\right)-R$$

satisfies

$$|R|\geqslant C_0C\frac{\ln^s p}{p},$$

where $C_0 > 0$ is an absolute constant.

PROOF. Define f by

$$f(x_1,\ \ldots,\ x_s)=C\sum_{m_1,\ldots,m_s=-p_1}^{p_2}\frac{e^{2\pi i(m_1x_1+\ldots+m_sx_s)}}{\overline{m}_1\ldots\overline{m}_s},$$

where C is an arbitrary positive constant. Denote the finite Fourier coefficients of this function by $C_p(m_1, \ldots, m_s)$. Obviously

$$C_p(m_1,\ \ldots,\ m_s)=\frac{C}{\overline{m}_1\ldots\overline{m}_s}, \tag{17}$$

and hence $f \in E_{s,p}(C)$.

From (12) and (14) we have

$$R=\frac{1}{p}\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' C_p(m_1,\ \ldots,\ m_s)\,S(m_1,\ \ldots,\ m_s)=$$

$$=\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' C_p(m_1,\ \ldots,\ m_s)\,\delta_p(a_1m_1+\ldots+a_sm_s).$$

This together with (17) gives

$$|R|=C\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\ldots+a_sm_s)}{\overline{m}_1\ldots\overline{m}_s}. \tag{18}$$

But since $p_2 \geqslant p_1$,

$$\sum_{m_1,\ldots,m_s=1}^{p_1} \frac{1}{m_1(m_1+1)\ldots m_s(m_s+1)} \sum_{|k_1|\le m_1,\ldots,|k_s|\le m_s}' \delta_p(a_1k_1+\ldots+a_sk_s) =$$

$$= \sum_{m_1,\ldots,m_s=-p_1}^{p_1}{}' \delta_p(a_1m_1+\ldots+a_sm_s)\left(\frac{1}{\bar{m}_1}-\frac{1}{p_1+1}\right)\ldots\left(\frac{1}{\bar{m}_s}-\frac{1}{p_1+1}\right),$$

by changing the order of summation ; hence

$$\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\ldots+a_sm_s)}{\bar{m}_1\ldots\bar{m}_s} \geqslant$$

$$\geqslant \sum_{m_1,\ldots,m_s=1}^{p_1} \frac{1}{m_1(m_1+1)\ldots m_s(m_s+1)} \sum_{|k_1|\le m_1,\ldots,|k_s|\le m_s}' \delta_p(a_1k_1+\ldots+a_sk_s). \quad (19)$$

It was shown in [11] (Lemma 23) that whenever $m_1 \ldots m_s \geqslant 2p$

$$\sum_{|k_1|\le m_1,\ldots,|k_s|\le m_s}' \delta_p(a_1k_1+\ldots+a_sk_s) \geqslant \frac{(m_1+1)\ldots(m_s+1)}{2p}.$$

Hence

$$\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\ldots+a_sm_s)}{\bar{m}_1\ldots\bar{m}_s} \geqslant \frac{1}{2p} \sum_{p_1^s\geqslant m_1\ldots m_s\geqslant 2p} \frac{1}{m_1\ldots m_s} \geqslant C_0\frac{\ln^s p}{p},$$

where $C_0 > 0$ is an absolute constant. Substituting this estimate in (18) we obtain the assertion of the theorem:

$$|R| = C \sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\ldots+a_sm_s)}{\bar{m}_1\ldots\bar{m}_s} \geqslant C_0C\frac{\ln^s p}{p}.$$

Theorem 3 shows that the estimate

$$R = O\left(\frac{\ln^s p}{p}\right), \quad (20)$$

of Theorem 2 is best possible for the class of parallelopipedal nets. It is not difficult to show that the estimate cannot be essentially improved (that is, can be improved only by a logarithmic factor) for completely arbitrary nets. Apparently (20) not merely cannot be essentially improved, but cannot be improved at all for any choice of net.

2. Let $\psi(n)$ be a function for integral n and $\Delta_n\psi(n)$ its finite differences:

$$\Delta_n\psi(n) = \psi(n+1) - \psi(n).$$

For functions of two variables the finite differences are defined by:

$$\Delta_{n_1}\psi(n_1, n_2) = \psi(n_1+1, n_2) - \psi(n_1, n_2),\ \Delta_{n_2}\psi(n_1, n_2) = \psi(n_1, n_2+1) - \psi(n_1, n_2),$$
$$\Delta_{n_1, n_2}\psi(n_1, n_2) = \Delta_{n_2}[\Delta_{n_1}\psi(n_1, n_2)].$$

Similarly finite differences are defined as follows for functions of several variables: If $1 \leqslant j_1 < \ldots < j_\nu \leqslant s \quad (2 \leqslant \nu \leqslant s)$ we put

$$\Delta_{n_j}\psi(n_1, \ldots, n_s) = \psi(n_1, \ldots, n_j+1, \ldots, n_s) - \psi(n_1, \ldots, n_s),$$
$$\Delta_{n_{j_1}, \ldots, n_{j_\nu}}\psi(n_1, \ldots, n_s) = \Delta_{n_{j_\nu}}[\Delta_{n_{j_1}, \ldots, n_{j_{\nu-1}}}\psi(n_1, \ldots, n_s)].$$

For what follows we need a special form of the n-dimensional analogue to Abel's summation formula. First of all we note that the usual Abel formula

$$\sum_{k=0}^{p-1} f\left(\frac{k}{p}\right)\varphi(k) = f(1)\sum_{k=0}^{p-1}\varphi(k) - \sum_{n=0}^{p-1}\left[f\left(\frac{n+1}{p}\right) - f\left(\frac{n}{p}\right)\right]\sum_{k=0}^{n}\varphi(k)$$

can be written in the form

$$\sum_{k=0}^{p-1} f\left(\frac{k}{p}\right)\varphi(k) = \frac{1}{p}\sum_{\tau=0}^{1}(-p)^{\tau}\sum_{n=0}^{p-1}\Delta_{n\tau}f\left[\left(\frac{n}{p}\right)^{\tau}\right]\sum_{k=0}^{n'}\varphi(k), \tag{21}$$

where n' is defined by

$$n' = n'(\tau) = \begin{cases} p-1 & \text{if } \tau = 0, \\ n & \text{if } \tau = 1. \end{cases}$$

We define n'_ν by the analogous formulae

$$n'_\nu = n'_\nu(\tau_\nu) = \begin{cases} p-1 & \text{if } \tau_\nu = 0, \\ n_\nu & \text{if } \tau_\nu = 1 \end{cases} \qquad (\nu = 1, 2, \ldots, s).$$

Then by applying (21) successively to each of the variables of summation we obtain our required multiple analogue of Abel's formula:

$$\sum_{k_1, \ldots, k_s=0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right)\varphi(k_1, \ldots, k_s) =$$
$$= \frac{1}{p^s}\sum_{\tau_1, \ldots, \tau_s=0}^{1}(-p)^{\tau_1+\cdots+\tau_s}\sum_{n_1, \ldots, n_s=0}^{p-1}\Delta_{n_1\tau_1, \ldots, n_s\tau_s}f\left[\left(\frac{n_1}{p}\right)^{\tau_1}, \ldots, \left(\frac{n_s}{p}\right)^{\tau_s}\right] \times$$
$$\times \sum_{k_1=0}^{n'_1}\cdots\sum_{k_s=0}^{n'_s}\varphi(k_1, \ldots, k_s). \tag{22}$$

We note specially the case when f is zero on the faces of the unit cube that do not contain the origin:

$$f(x_1, \ldots, x_{\nu-1}, 1, x_{\nu+1}, \ldots, x_s) = 0 \qquad (\nu = 1, 2, \ldots, s). \tag{23}$$

In this case the only term on the right of (22) that does not vanish is that with $\tau_1 = \ldots = \tau_s = 1$. Hence in this case

$$\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) \varphi(k_1, \ldots, k_s) =$$

$$= (-1)^s \sum_{n_1,\ldots,n_s=0}^{p-1} \Delta_{n_1,\ldots,n_s} f\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right) \sum_{k_1=0}^{n_1} \cdots \sum_{k_s=0}^{n_s} \varphi(k_1, \ldots, k_s). \quad (24)$$

We define the finite variation of f to be the number $V_p[f]$ given by

$$V_p[f] = \frac{1}{p^s} \sum_{\tau_1,\ldots,\tau_s=0}^{1} p^{\tau_1+\cdots+\tau_s} \times$$

$$\times \sum_{n_1,\ldots,n_s=0}^{p-1} \left| \Delta_{n_1\tau_1,\ldots,n_s\tau_s} f\left[\left(\frac{n_1}{p}\right)^{\tau_1}, \ldots, \left(\frac{n_s}{p}\right)^{\tau_s}\right]\right|.$$

For functions satisfying (23) we have a simpler expression for the finite variation:

$$V_p[f] = \sum_{n_1,\ldots,n_s=0}^{p-1} \left| \Delta_{n_1,\ldots,n_s} f\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right)\right|.$$

The class of functions of bounded finite variation, which is defined by

$$V_p[f] \leqslant C,$$

is denoted by $V_{s,p}(C)$.

For functions of one variable the definition of finite variation may be written in the form

$$V_p[f] = |f(1)| + \sum_{k=0}^{p-1} \left| f\left(\frac{n+1}{p}\right) - f\left(\frac{n}{p}\right)\right|.$$

From this it is clear that the concept of finite variation is a rational variant of the ordinary concept of the variation of a function and that any function of bounded variation has bounded finite variation.

It is easy to check that the class of functions of several variables of bounded variation, defined as in Hlawka [5], is contained in the class of functions of bounded finite variation.

We now investigate the relations between the classes $V_{s,p}(C)$ and $E_{s,p}(C)$ and show that

$$V_{s,p}(C) \subset E_{s,p}(C). \quad (25)$$

For suppose that f belongs to $V_{s,p}(C)$ and[1] that it satisfies (23). Denote by $C(m_1, \ldots, m_s)$ its finite Fourier coefficients:

---

[1] The last supposition is made for simplicity of exposition, the general case is dealt with similarly.

$$C_p(m_1, \ldots, m_s) = \frac{1}{p^s} \sum_{k_1, \ldots, k_s=0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) e^{-2\pi i \frac{m_1 k_1 + \ldots + m_s k_s}{p}}.$$

By applying the multiple Abel transformation (24) we have
$C_p(m_1, \ldots, m_s) =$

$$= \frac{(-1)^s}{p^s} \sum_{n_1, \ldots, n_s=0}^{p-1} \Delta_{n_1, \ldots, n_s} f\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right) \sum_{k_1=0}^{n_1} \ldots \sum_{k_s=0}^{n_s} e^{-2\pi i \frac{m_1 k_1 + \ldots + m_s k_s}{p}}.$$

But by (10) we have

$$\left| \sum_{k_\nu=0}^{n_\nu} e^{2\pi i \frac{m_\nu k_\nu}{p}} \right| \leqslant \frac{p}{\overline{m}_\nu},$$

and so

$$|C_p(m_1, \ldots, m_s)| \leqslant \frac{1}{\overline{m}_1 \ldots \overline{m}_s} \sum_{n_1, \ldots, n_s=0}^{p-1} \left| \Delta_{n_1, \ldots, n_s} f\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right) \right| = \frac{V_p[f]}{\overline{m}_1 \ldots \overline{m}_s}.$$

Hence it is clear that the estimate $V_p[f] \leqslant C$ implies that

$$|C_p(m_1, \ldots, m_s)| \leqslant \frac{C}{\overline{m}_1 \ldots \overline{m}_s},$$

and this proves (25). Since further we have

$$H_s^1(C) \subset E_{s,p}(C),$$

(see [11], Lemma 16) it is clear that of the three classes $H_s^1(C)$, $V_{s,p}(C)$ $E_{s,p}(C)$ the last is the most extensive.

The following theorem establishes a connection between the error in the formula for approximate summation of a function of bounded variation and the value of the discrepancy, characterizing the uniformity of distribution of the points of the net.

Let $N_p(\gamma_1, \ldots, \gamma_s)$ be the number of points of the net

$$M_k = (\xi_1(k), \ldots, \xi_s(k)) \qquad (k = 1, 2, \ldots, p),$$

lying in the domain Ω_s defined by the equations (9):

$$0 \leqslant x_1 < \gamma_1, \ldots, 0 \leqslant x_s < \gamma_s.$$

The points of M_k are said to be *uniformly distributed in the unit cube if*

$$\frac{1}{p} N_p(\gamma_1, \ldots, \gamma_s) = \gamma_1 \ldots \gamma_s + R, \tag{26}$$

where $R \to 0$ as $p \to \infty$. The number

$$D = \sup_{\gamma_1, \ldots, \gamma_s} |R| \tag{27}$$

is called the *discrepancy*. The rapidity of the decrease of the discrepancy measures the degree of uniformity of distribution of the points of M_k.

The simplest form of a connection between questions of uniform distribution and the construction of quadrature formulae is contained in (26) itself. For observing that

$$N_p(\gamma_1, \ldots, \gamma_s) = \sum_{k=1}^{p} \varphi(M_k) \text{ and } \int_{G_s} \varphi(Q)\, dQ = \gamma_1 \ldots \gamma_s,$$

where G_s is the unit s-dimensional cube and φ the characteristic function of Ω_s, we can write (26) in the form

$$\int_{G_s} \varphi(Q)\, dQ = \frac{1}{p} \sum_{k=1}^{p} \varphi(M_k) - R.$$

Hence (26), which gives the definition of uniform distribution, is itself a quadrature formula with the net M_k applied to the characteristic function of Ω_s. The quicker D decreases, the more uniform is the distribution of the points of M_k and the more precise is the quadrature formula.

Let us consider an arbitrary rational net

$$M_k = \left(\frac{z_1(k)}{p}, \ldots, \frac{z_s(k)}{p}\right) \qquad (k = 1, 2, \ldots, p).$$

It is more convenient to limit ourselves to rational values of the γ_ν:

$$\gamma_\nu = \frac{n_\nu}{p}, \quad 1 \leqslant n_\nu \leqslant p \qquad (\nu = 1, 2, \ldots, s)$$

and to change the definition of the discrepancy somewhat by writing

$$\left.\begin{aligned} \frac{1}{p} N_p\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right) &= \frac{n_1 \ldots n_s}{p^s} + R(n_1, \ldots, n_s) \\ D_p &= \max_{n_1, \ldots, n_s} |R(n_1, \ldots, n_s)|. \end{aligned}\right\} \tag{28}$$

We call D_p the finite discrepancy, or the measure of uniformity of the net M_k.

THEOREM 4. *In the formula*

$$\frac{1}{p^s} \sum_{k_1, \ldots, k_s = 0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) = \frac{1}{p} \sum_{k=1}^{p} f\left(\left\{\frac{z_1(k)}{p}\right\}, \ldots, \left\{\frac{z_s(k)}{p}\right\}\right) - R$$

of approximate summation we have

$$|R| \leqslant V_p[f]\, D_p,$$

where $V_p[f]$ is the finite variation of f and D_p is the measure of uniformity of the net M_k.

PROOF. Since

$$\frac{1}{p}\sum_{k=1}^{p} f\left(\left\{\frac{z_1(k)}{p}\right\}, \ldots, \left\{\frac{z_s(k)}{p}\right\}\right) =$$

$$= \frac{1}{p}\sum_{k=1}^{p}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right)\delta_p[z_1(k)-k_1]\ldots\delta_p[z_s(k)-k_s],$$

it is clear that

$$R = \frac{1}{p}\sum_{k=1}^{p}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right)\left(\delta_p[z_1(k)-k_1]\ldots\delta_p[z_s(k)-k_s]-\frac{1}{p^s}\right).$$

If f satisfies the condition

$$f(x_1, \ldots, x_{\nu-1}, 1, x_{\nu+1}, \ldots, x_s) = 0 \qquad (\nu = 1, 2, \ldots, s), \tag{29}$$

then by using the multiple Abel transformation (24) we find

$$R = \frac{(-1)^s}{p}\sum_{k=1}^{p}\sum_{n_1,\ldots,n_s=0}^{p-1}\Delta_{n_1,\ldots,n_s} f\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right)\sum_{k_1=0}^{n_1}\ldots\sum_{k_s=0}^{n_s}\psi_k(k_1, \ldots, k_s),$$

where $\psi_k(k_1, \ldots, k_s)$ is defined by

$$\psi_k(k_1, \ldots, k_s) = \delta_p[z_1(k)-k_1]\ldots\delta_p[z_s(k)-k_s]-\frac{1}{p^s}.$$

Hence, observing that

$$\frac{1}{p}\sum_{k=1}^{p}\sum_{k_1=0}^{n_1}\ldots\sum_{k_s=0}^{n_s}\psi_k(k_1, \ldots, k_s) =$$

$$= \frac{1}{p}\sum_{k=1}^{p}\sum_{k_1=0}^{n_1}\ldots\sum_{k_s=0}^{n_s}\delta_p[z_1(k)-k_1]\ldots\delta_p[z_s(k)-k_s]-\frac{(n_1+1)\ldots(n_s+1)}{p^s} =$$

$$= \frac{1}{p}N_p\left(\frac{n_1+1}{p}, \ldots, \frac{n_s+1}{p}\right)-\frac{(n_1+1)\ldots(n_s+1)}{p^s} = R(n_1+1, \ldots, n_s+1),$$

we obtain the assertion of the theorem:

$$|R| \leqslant \sum_{n_1,\ldots,n_s=0}^{p-1}\left|\Delta_{n_1,\ldots,n_s} f\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right)\right| |R(n_1+1, \ldots, n_s+1)| \leqslant$$

$$\leqslant D_p \sum_{n_1,\ldots,n_s=0}^{p-1}\left|\Delta_{n_1,\ldots,n_s} f\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right)\right| = V_p[f]\,D_p.$$

In the general case when (29) is not satisfied, we get the same result by using the general form (22) of Abel's transformation instead of the simpler (24).

If f belongs to $V_{s,p}(C)$, Theorem 4 implies that the error in the formula of approximate summation satisfies

$$|R| \leqslant CD_p. \tag{30}$$

From this it is clear that the better the estimate for the measure D_p of uniformity of distribution, the better the accuracy that can be guaranteed for the formula of approximate summation on the class $V_{s,p}(C)$. Similarly in the construction of quadrature formulae for functions of bounded variation the useful nets are those with a minimal value of the discrepancy D.

The result of Theorem 4 is convenient in those cases when we have a direct estimate of the measure of uniformity of distribution of the net. Amongst these are the nets investigated in 1960 by Halton (see [12] and [13]). But usually we cannot estimate the discrepancy D_p directly, and then the question of estimating it reduces to estimations of trigonometric sums. It is easy to verify that such a method leads to results like those of Theorem 1, but less general, since they apply only to functions of class $V_{s,p}(C)$ and not to the wider class $E_{s,p}(C)$ considered in Theorem 1.

Indeed, by (28) we have

$$R(n_1, \ldots, n_s) = \frac{1}{p} N_p\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right) - \frac{n_1 \ldots n_s}{p^s} =$$

$$= \frac{1}{p} \sum_{k=1}^{p} \sum_{k_1=0}^{n_1-1} \cdots \sum_{k_s=0}^{n_s-1} \left(\delta_p[z_1(k) - k_1] \ldots \delta_p[z_s(k) - k_s] - \frac{1}{p^s}\right).$$

Hence by Lemma 1 and (10) we obtain

$$R(n_1, \ldots, n_s) =$$

$$= \frac{1}{p^{s+1}} \sum_{m_1, \ldots, m_s = -p_1}^{p_2}{}' \sum_{k_1=0}^{n_1-1} \cdots \sum_{k_s=0}^{n_s-1} e^{-2\pi i \frac{m_1 k_1 + \ldots + m_s k_s}{p}} \sum_{k=1}^{p} e^{2\pi i \frac{m_1 z_1(k) + \ldots + m_s z_s(k)}{p}},$$

$$D_p = \max_{n_1, \ldots, n_s} |R(n_1, \ldots, n_s)| \leqslant \frac{1}{p} \sum_{m_1, \ldots, m_s = -p_1}^{p_2}{}' \frac{|S(m_1, \ldots, m_s)|}{\overline{m}_1 \ldots \overline{m}_s}, \tag{31}$$

where $S(m_1, \ldots, m_s)$ is defined by (11). Substituting this in (30) we get, for functions of bounded finite variation $f \in V_{s,p}(C)$, the assertion of Theorem 1:

$$|R| \leqslant \frac{C}{p} \sum_{m_1, \ldots, m_s = -p_1}^{p_2}{}' \frac{|S(m_1, \ldots, m_s)|}{\overline{m}_1 \ldots \overline{m}_s}.$$

§ 2. Properties of optimal coefficients

1. Let M_k $(k = 1, 2, \ldots, p)$ be an optimal parallelopipedal net, that is, a net of the form

$$M_k = \left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_s k}{p}\right\}\right), \tag{32}$$

where $a_1, \ldots, a_s$ are optimal coefficients.

We consider the nature of the distribution of the points M_k in the s-dimensional cube. In the next theorem it is shown that the measure of uniformity of distribution of (32) satisfies

$$D_p = O\left(\frac{\ln^{\beta_1} p}{p}\right),$$

where β_1 is independent of p. It is known [1] that even for a net of the most general type this estimate cannot be improved to $O(1/p)$. Hence the optimal parallelopipedal nets belong to the class of very uniformly distributed nets. Besides, it will become clear that any parallelopipedal net whose distribution uniformity is nearly as good as it can be is necessarily optimal.

We precede the proof of the theorem by a lemma.

LEMMA 3. *Let f be defined by*

$$f(x_1, \ldots, x_s) = \sum_{m_1, \ldots, m_s = -p_1}^{p_2} \frac{e^{2\pi i(m_1 x_1 + \ldots + m_s x_s)}}{\overline{m}_1 \ldots \overline{m}_s}.$$

Then its finite variation satisfies

$$V_p[f] \leqslant C_1 \ln^s p,$$

where $C_1 = C_1(s)$ is independent of p.

PROOF. It is well known (see [11], Lemma 26) that

$$1 - 2\ln(2\sin\pi\{x\}) = \sum_{m=-p_1}^{p_1} \frac{e^{2\pi i m x}}{\overline{m}} + \frac{\theta}{p_1 \ll x \gg}, \tag{33}$$

for $\{x\} \neq 0$. where $|\theta| \leqslant 1$.

We define a function $\varphi(x)$ by

$$\varphi(x) = \sum_{m=-p_1}^{p_2} \frac{e^{2\pi i m x}}{\overline{m}}.$$

Then on applying (33) we get

$$\varphi\left(\frac{n}{p}\right) = 1 - 2\ln\left(2\sin\pi\frac{n}{p}\right) + \frac{2\theta_1}{p_1 \ll \frac{n}{p} \gg} \qquad (1 \leqslant n < p),$$

$$\sum_{n=0}^{p-1} \left|\Delta_n \varphi\left(\frac{n}{p}\right)\right| = 2\sum_{n=1}^{p-2} \left|\Delta_n \ln\sin\pi\frac{n}{p}\right| + O(\ln p)$$

for some $|\theta_1| \leqslant 1$. Hence, observing that $\ln\sin\pi x$ is monotone on (0 $(0, \frac{1}{2})$ and $(\frac{1}{2}, 1)$ we get

$$\sum_{n=0}^{p-1} \left|\Delta_n \varphi\left(\frac{n}{p}\right)\right| = O(\ln p).$$

Since, further, $\varphi(1) = O(\ln p)$, we clearly have

$$\sum_{n=0}^{p-1} \left|\Delta_{n\tau} \varphi\left[\left(\frac{n}{p}\right)^\tau\right]\right| \leqslant C_0 p^{1-\tau} \ln p,$$

where C_0 is an absolute constant and τ is 0 or 1. But then, on putting $C_1 = (2C_0)^s$ and noting that $f(x_1, \ldots, x_s) = \varphi(x_1) \ldots \varphi(x_s)$, we get the assertion of the lemma:

$$V_p[f] = \frac{1}{p^s} \sum_{\tau_1, \ldots, \tau_s = 0}^{1} p^{\tau_1 + \ldots + \tau_s} \sum_{n_1, \ldots, n_s = 0}^{p-1} \left| \Delta_{n_1\tau_1, \ldots, n_s\tau_s} f\left[\left(\frac{n_1}{p}\right)^{\tau_1}, \ldots, \left(\frac{n_s}{p}\right)^{\tau_s}\right]\right| =$$

$$= \frac{1}{p^s} \sum_{\tau_1, \ldots, \tau_s = 0}^{1} p^{\tau_1 + \ldots + \tau_s} \sum_{n_1, \ldots, n_s = 0}^{p-1} \left|\Delta_{n_1\tau_1}\varphi\left[\left(\frac{n_1}{p}\right)^{\tau_1}\right]\right| \cdots \left|\Delta_{n_s\tau_s}\varphi\left[\left(\frac{n_s}{p}\right)^{\tau_s}\right]\right| \leqslant$$

$$\leqslant C_1 \ln^s p.$$

THEOREM 5.[1] *A necessary and sufficient condition for the optimality of the parallelopipedal nets* (32) *is the inequality*

$$D_p \leqslant \frac{B_1 \ln^{\beta_1} p}{p},$$

where D_p is the measure of uniformity of its distribution and B_1, β_1 are constants independent of p.

PROOF. For any net of the type

$$M_k = \left(\left\{\frac{z_1(k)}{p}\right\}, \ldots, \left\{\frac{z_s(k)}{p}\right\}\right) \qquad (k = 1, 2, \ldots, p)$$

(31) gives the following estimate for the measure of uniformity of distribution:

$$D_p \leqslant \frac{1}{p} \sum_{m_1, \ldots, m_s = -p_1}^{p_2}{}' \frac{|S(m_1, \ldots, m_s)|}{\overline{m}_1 \ldots \overline{m}_s},$$

where

$$S(m_1, \ldots, m_s) = \sum_{k=1}^{p} e^{2\pi i \frac{m_1 z_1(k) + \ldots + m_s z_s(k)}{p}}$$

On applying this to the parallelopipedal nets

$$M_k = \left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_s k}{p}\right\}\right) \qquad (k = 1, 2, \ldots, p) \tag{34}$$

and using (14), that is,

$$S(m_1, \ldots, m_s) = p\delta_p(a_1 m_1 + \ldots + a_s m_s),$$

we find

$$D_p \leqslant \sum_{m_1, \ldots, m_s = -p_1}^{p_2}{}' \frac{\delta_p(a_1 m_1 + \cdots + a_s m_s)}{\overline{m}_1 \ldots \overline{m}_s}. \tag{35}$$

[1] A more complicated proof of a similar proposition on the discrepancy of optimal parallelopipedal nets was given earlier in [11] (Theorem 22).

If (32) is an optimal net, the definition of optimality of the coefficients implies (16), that is:

$$\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\cdots+a_sm_s)}{\overline{m}_1\ldots\overline{m}_s} \leqslant \frac{B\ln^\beta p}{p},$$

which, by (35), proves the necessity of the condition of the theorem with $B_1 = B$ and $\beta_1 = \beta$:

$$D_p \leqslant \frac{B_1 \ln^{\beta_1} p}{p}. \tag{36}$$

Now we suppose that (36) is satisfied for some parallelopipedal net (32). We define f as in Lemma 3:

$$f(x_1,\ldots,x_s) = \sum_{m_1,\ldots,m_s=-p_1}^{p_2} \frac{e^{2\pi i(m_1x_1+\ldots+m_sx_s)}}{\overline{m}_1\ldots\overline{m}_s}.$$

Then we get

$$\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ldots,\frac{k_s}{p}\right) = \frac{1}{p}\sum_{k=1}^{p} f\left(\left\{\frac{a_1k}{p}\right\},\ldots,\left\{\frac{a_sk}{p}\right\}\right) - R,$$

where, according to (18),

$$|R| = \sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\ldots+a_sm_s)}{\overline{m}_1\ldots\overline{m}_s}.$$

But by Theorem 4

$$|R| \leqslant V_p[f]\cdot D_p.$$

Therefore, on using Lemma 3 and (36) we obtain

$$\sum_{m_1,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(a_1m_1+\ldots+a_sm_s)}{\overline{m}_1\ldots\overline{m}_s} \leqslant V_p[f]\,D_p \leqslant \frac{B_1C_1\ln^{\beta_1+s}p}{p}.$$

Thus, $a_1, \ldots, a_s$ are optimal coefficients. This proves the sufficiency part of the theorem.

Using Theorem 5 it is easy to show that optimal parallelopipedal nets, and only they, satisfy

$$N_p(\gamma_1,\ldots,\gamma_s) = \gamma_1\ldots\gamma_s p + O(\ln^{\beta_1}p), \tag{37}$$

where $N_p(\gamma_1, \ldots, \gamma_s)$ is the number of points of (34) lying in any domain of the form

$$0 \leqslant x_1 < \gamma_1, \ldots, 0 \leqslant x_s < \gamma_s \quad (0 < \gamma_\nu \leqslant 1). \tag{38}$$

For rational $\gamma_\nu = \frac{n_\nu}{p}$ this follows at once from Theorem 5 and (28); and the general case reduces to the rational one by means of the equations

$$\gamma_\nu = \frac{n_\nu}{p} + \frac{\theta_\nu}{p} \qquad (0 \leqslant \theta_\nu < 1, \ \nu = 1, 2, \ldots, s).$$

Now we choose integers a_ν so that $1, a_1, \ldots, a_s$ are $(s + 1)$-dimensional optimal coefficients. We show that in this case a good distribution is characteristic not merely for all points of the optimal parallelopipedal net

$$M_k = \left(\left\{ \frac{a_1 k}{p} \right\}, \ldots, \left\{ \frac{a_s k}{p} \right\} \right) \quad (k = 1, 2, \ldots, p), \tag{39}$$

but also for the first P points of the net for any P in the interval $1 \leqslant P \leqslant p$.

We denote by $N_p(\gamma_1, \ldots, \gamma_s)$ the number of the points M_k $(k = 1, 2, \ldots, P)$ that lie in (38) or, what is the same, the number of solutions of the system of inequalities

$$\left.\begin{array}{l} 0 \leqslant \left\{ \frac{a_1 k}{p} \right\} < \gamma_1, \\ \cdots\cdots\cdots \\ 0 \leqslant \left\{ \frac{a_s k}{p} \right\} < \gamma_s \end{array}\right\} \quad (k = 1, 2, \ldots, P).$$

THEOREM 6. *The equation*

$$N_P(\gamma_1, \ldots, \gamma_s) = \gamma_1 \ldots \gamma_s P + O(\ln^\beta p)$$

is satisfied for the points of (39) *for any* $P \leqslant p$ *if and only if the integers* $1, a_1, \ldots, a_s$ *are an optimal system of coefficients.*

PROOF. Clearly, as in (37), it is enough to prove the assertion for rational γ_ν:

$$\gamma_\nu = \frac{n_\nu}{p}, \quad 1 \leqslant n_\nu \leqslant p \quad (\nu = 1, 2, \ldots, s). \tag{40}$$

Consider the system of inequalities

$$\left.\begin{array}{l} 0 \leqslant \left\{ \frac{k}{p} \right\} < \frac{P}{p}, \\ 0 \leqslant \left\{ \frac{a_1 k}{p} \right\} < \frac{n_1}{p}, \\ \cdots\cdots\cdots \\ 0 \leqslant \left\{ \frac{a_s k}{p} \right\} < \frac{n_s}{p} \end{array}\right\} \quad (k = 1, 2, \ldots, p). \tag{41}$$

The number of solutions is clearly $N_p(\gamma_0, \ldots, \gamma_s)$ where $\gamma_0 = \frac{P}{p}$, and the values of $\gamma_1, \ldots, \gamma_s$ are given by (40). Comparing (41) with the system

$$\left.\begin{array}{l} 0 \leqslant \left\{ \frac{a_1 k}{p} \right\} < \frac{n_1}{p}, \\ \cdots\cdots\cdots \\ 0 \leqslant \left\{ \frac{a_s k}{p} \right\} < \frac{n_s}{p} \end{array}\right\} \quad (k = 1, 2, \ldots, P),$$

we note that

$$N_P(\gamma_1, \ldots, \gamma_s) = N_p(\gamma_0, \ldots, \gamma_s) + O(1). \tag{42}$$

Let $1, a_1, \ldots, a_s$ be optimal coefficients. Then (37) gives

$$N_p(\gamma_0, \ldots, \gamma_s) = \gamma_0 \ldots \gamma_s p + O(\ln^\beta p). \tag{43}$$

Hence using (42) with our choice of γ_0 we get

$$N_P(\gamma_1, \ldots, \gamma_s) = \gamma_1 \ldots \gamma_s P + O(\ln^\beta p),$$

which shows the necessity of the condition in the theorem.

Suppose now that this condition is satisfied for any $P \leqslant p$. Then (42) shows that (43) is satisfied with any $\gamma_0, \ldots, \gamma_s$. Consequently, by Theorem 5, the coefficients $1, a_1, \ldots, a_s$ are optimal, which shows the sufficiency of the condition in the theorem.

2. Let us consider the congruence

$$m_0 + a_1 m_1 + \ldots + a_s m_s \equiv 0 \pmod p \tag{44}$$

and the system of congruences

$$\left.\begin{array}{l} a_1 k_0 \equiv k_1, \\ \cdots\cdots \\ a_s k_0 \equiv k_s \end{array}\right\} \pmod p, \tag{45}$$

where $a_1, \ldots, a_s$ are relatively prime to p. We call the solutions $m_0 = \ldots = m_s = 0$ and $k_0 = \ldots = k_s = 0$ *trivial*. We denote by q and Q, respectively, the minimum of the product $\overline{m}_0 \ldots \overline{m}_s$ and $|k_0| \ldots |k_s|$, the minimum being taken over the non-trivial solutions of (44) and (45).

It is easy to see that inside the hyperbolic domain

$$\overline{m}_0 \ldots \overline{m}_s \leqslant q, \quad -p_1 \leqslant m_\nu \leqslant p_2, \tag{46}$$

there are no points of the integral lattice, other than the origin, that satisfy (44). The region

$$|k_0| \ldots |k_s| \leqslant Q, \quad -p_1 \leqslant k_\nu \leqslant p_2 \tag{47}$$

has the same property with respect to (45).

The following theorem shows that there is a close connection between the optimality of the $(s+1)$-dimensional parallelopipedal nets

$$M_k = \left(\left\{ \frac{k}{p} \right\}, \left\{ \frac{a_1 k}{p} \right\}, \ldots, \left\{ \frac{a_s k}{p} \right\} \right) \quad (k = 1, 2, \ldots, p)$$

and the size of the hyperbolic regions (46) and (47). For the proof we need a result of A.O. Gel'fond, which is a special form of a transference theorem for congruences.

LEMMA 4. *(A.O. Gel'fond). There is a positive constant $C_1 = C_1(s)$ such that for prime p the inequalities $Q \geqslant C_1 q^s$ and $q \geqslant C_1 \dfrac{Q^s}{p^{2s-1}}$ hold.*

PROOF. Let $k_0, \ldots, k_s$ be a solution of (45) for which $|k_0| \ldots |k_s| = Q$, and let z_ν be arbitrary integers such that

$$0 \leqslant z_\nu \leqslant \frac{[(2s+3)Q]^{\frac{1}{s}}}{|k_\nu|} \quad (\nu = 0, 1, \ldots, s). \tag{48}$$

Clearly

$$\left| \sum_{\nu=0}^{s} k_\nu z_\nu \right| \leqslant (s+1)[(2s+3)Q]^{\frac{1}{s}}.$$

Hence $\sum k_\nu z_\nu$ can take no more than t distinct values, where

$$t \leqslant 2(s+1)[(2s+3)Q]^{\frac{1}{s}} + 1 < (2s+3)^{1+\frac{1}{s}} Q^{\frac{1}{s}}.$$

Since the number of distinct systems $z_0, \ldots, z_s$ is not less than

$$\frac{[(2s+3)Q]^{\frac{s+1}{s}}}{|k_0| \ldots |k_s|} = (2s+3)^{1+\frac{1}{s}} Q^{\frac{1}{s}},$$

there must be systems $(z_0, \ldots, z_s) \neq (z_0', \ldots, z_s')$ such that

$$\sum_{\nu=0}^{s} k_\nu z_\nu = \sum_{\nu=0}^{s} k_\nu z_\nu'.$$

Using this equation and our choice of $k_0, \ldots, k_s$ we derive from the identity

$$k_0 \left(m_0 + \sum_{\nu=1}^{s} a_\nu m_\nu\right) = \sum_{\nu=0}^{s} k_\nu m_\nu + \sum_{\nu=1}^{s} m_\nu (a_\nu k_0 - k_\nu) \tag{49}$$

with $m_\nu = z_\nu - z_\nu'$ that

$$k_0 \left(m_0 + \sum_{\nu=1}^{s} a_\nu m_\nu\right) = \sum_{\nu=1}^{s} m_\nu (a_\nu k_0 - k_\nu) \equiv 0 \pmod{p}.$$

Hence, since p is prime and $k_0 \not\equiv 0 \pmod{p}$, we have

$$m_0 + \sum_{\nu=1}^{s} a_\nu m_\nu \equiv 0 \pmod{p}.$$

Thus, the $m_0 = z_0 - z_0', \ldots, m_s = z_s - z_s'$ form a non-trivial solution of (44); and by (48) we have

$$\overline{m}_0 \ldots \overline{m}_s = \overline{z_0 - z_0'} \ldots \overline{z_s - z_s'} \leqslant (2s+3)^{1+\frac{1}{s}} Q^{\frac{1}{s}}. \tag{50}$$

Put $C_1 = \frac{1}{(2s+3)^{s+1}}$. Then observing that $q \leqslant \overline{m}_0 \ldots \overline{m}_s$, we obtain by (50) the first assertion of the Lemma:

$$q \leqslant (2s+3)^{1+\frac{1}{s}} Q^{\frac{1}{s}}, \quad Q \geqslant \frac{q^s}{(2s+3)^{s+1}} = C_1 q^s.$$

Now let y_ν be arbitrary integers from the intervals

$$0 \leqslant y_\nu \leqslant \frac{[(2s+3)\,qp^{s-1}]^{\frac{1}{s}}}{\bar{m}_\nu} \qquad (\nu = 0,\ 1,\ \dots,\ s), \tag{51}$$

where $m_0, \dots, m_s$ is a solution of (44) for which $\bar{m}_0 \dots \bar{m}_s = q$. Since $m_0, \dots, m_s$ is a non-trivial solution, at least one of $m_0, \dots, m_s$ is not a multiple of p. For definiteness we assume that $m_s \not\equiv 0 \pmod p$.
Define $n,\ n_1,\ \dots,\ n_{s-1}$ by

$$\sum_{\nu=0}^{s} m_\nu y_\nu = n, \quad a_\nu y_0 - y_\nu \equiv n_\nu \pmod p, \quad 0 \leqslant n_\nu < p \quad (\nu = 1,\ 2,\ \dots,\ s-1).$$

Since

$$|n| \leqslant \sum_{\nu=0}^{s} |m_\nu| \frac{[(2s+3)\,qp^{s-1}]^{\frac{1}{s}}}{\bar{m}_\nu} \leqslant (s+1)\,[(2s+3)\,qp^{s-1}]^{\frac{1}{s}},$$

the integer n can take not more than

$$2\,(s+1)\,[(2s+3)\,qp^{s-1}]^{\frac{1}{s}} + 1 < (2s+3)^{1+\frac{1}{s}}\,(qp^{s-1})^{\frac{1}{s}}$$

values, and so the number of distinct systems $n,\ n_1,\ \dots,\ n_{s-1}$ is less than

$$(2s+3)^{1+\frac{1}{s}}\,(qp^{s-1})^{\frac{1}{s}}\,p^{s-1} = (2s+3)^{1+\frac{1}{s}}\,q^{\frac{1}{s}}\,p^{s-\frac{1}{s}}.$$

But the number of distinct systems $y_0,\ \dots,\ y_s$ is not less than

$$\frac{[(2s+3)\,qp^{s-1}]^{\frac{s+1}{s}}}{\bar{m}_0 \dots \bar{m}_s} = (2s+3)^{1+\frac{1}{s}}\,q^{\frac{1}{s}}\,p^{s-\frac{1}{s}}.$$

Consequently there are two systems $(y_0,\ \dots,\ y_s) \neq (y_0',\ \dots,\ y_s')$ corresponding to the same system $n, n_1,\ \dots,\ n_{s-1}$:

$$\sum_{\nu=0}^{s} m_\nu y_\nu = \sum_{\nu=0}^{s} m_\nu y_\nu',$$

$$a_\nu y_0 - y_\nu \equiv a_\nu y_0' - y_\nu' \pmod p \quad (\nu = 1,\ 2,\ \dots,\ s-1).$$

We take $k_\nu = y_\nu - y_\nu'$ $(\nu = 0,\ 1,\ \dots,\ s)$ and write these relations in the form

$$\sum_{\nu=0}^{s} m_\nu k_\nu = 0, \quad a_\nu k_0 - k_\nu \equiv 0 \pmod p \quad (\nu = 1,\ 2,\ \dots,\ s-1). \tag{52}$$

Then by (49) and the choice of $m_0,\ \dots,\ m_s$ we get

$$m_s\,(a_s k_0 - k_s) = k_0\Bigl(m_0 + \sum_{\nu=1}^{s} a_\nu m_\nu\Bigr) - \sum_{\nu=1}^{s-1} m_\nu\,(a_\nu k_0 - k_\nu) \equiv 0 \pmod p.$$

Hence, since p is prime and $m_s \not\equiv 0 \pmod{p}$, we get

$$a_s k_0 - k_s \equiv 0 \pmod{p}.$$

From this congruence and from (52) it is clear that $k_0, \ldots, k_s$ form a non-trivial solution of (45), and (51) implies that

$$|k_0| \ldots |k_s| = |y_0 - y_0'| \ldots |y_s - y_s'| \leqslant (2s+3)^{1+\frac{1}{s}} q^{\frac{1}{s}} p^{s-\frac{1}{s}}.$$

Hence observing that $Q \leqslant |k_0| \ldots |k_s|$, we get the second assertion of the lemma:

$$Q \leqslant (2s+3)^{1+\frac{1}{s}} q^{\frac{1}{s}} p^{s-\frac{1}{s}}, \quad q \geqslant \frac{Q^s}{(2s+3)^{s+1} p^{s^2-1}} = \frac{C_1 Q^s}{p^{s^2-1}}.$$

We note that in Lemma 4 the requirement that p is a prime is connected only with the method of proof. It can be shown that similar propositions are true for any integer $p > 1$.

Now we turn to the question of the size of the hyperbolic domains (46) and (47)

$$\overline{m}_0 \ldots \overline{m}_s \leqslant q, \quad |k_0| \ldots |k_s| \leqslant Q, \tag{53}$$

corresponding to the parallelopipedal net

$$M_k = \left(\left\{ \frac{k}{p} \right\}, \left\{ \frac{a_1 k}{p} \right\}, \ldots, \left\{ \frac{a_s k}{p} \right\} \right) \quad (k = 1, 2, \ldots, p). \tag{54}$$

As was already remarked above, these domains contain no non-trivial solutions of the congruence

$$m_0 + a_1 m_1 + \ldots + a_s m_s \equiv 0 \pmod{p} \tag{55}$$

and of the system

$$a_\nu k_0 \equiv k_\nu \pmod{p} \quad (\nu = 1, 2, \ldots, s) \tag{56}$$

of congruences, respectively.

By Theorem 2 the results of the approximate calculations of $(s+1)$-dimensional sums for the class $E_{s+1,p}(C)$ by means of (54) are the more precise the smaller the value of the sum

$$\sum_{m_0, \ldots, m_s = -p_1}^{p_2}{}' \frac{\delta_p(m_0 + a_1 m_1 + \ldots + a_s m_s)}{\overline{m}_0 \ldots \overline{m}_s},$$

involving the optimal coefficients $1, a_1, \ldots, a_s$. Since the summands are non-negative and at least one of them is equal to $1/q$, we cannot get a better estimate above than $1/q$. This gives rise to a connection between the error in the formula for approximate summation and size of the first of the hyperbolic domains (53). By Lemma 4 this connection extends to the second domain : optimal parallelopipedal nets correspond to large domains (53).

THEOREM 7. *Let q and Q be the least values of $\bar{m}_0, \ldots, \bar{m}_s$ and $|k_0| \ldots |k_s|$, for non-trivial solutions of the congruence* (55) *and the system* (56) *of congruences, respectively. A necessary and sufficient condition for* $1, a_1, \ldots, a_s$ *to be optimal coefficients is that either of the inequalities*

$$q \geqslant \frac{p}{B \ln^{\beta} p} \quad or \quad Q \geqslant \frac{p^s}{B_1 \ln^{\beta_1} p} \tag{57}$$

holds, where $B > 0$, $B_1 > 0$, $\beta \geqslant 0$, $\beta_1 \geqslant 0$ *are constants independent of* p.

PROOF. Let $\varphi(m)$ be a non-negative function for which

$$\sum_{m=-p_1}^{p_2} \varphi(m) \leqslant 1.$$

Using Abel's summation formula we obtain

$$\sum_{m=-p_1}^{p_2} \frac{\varphi(m)}{\bar{m}} = \sum_{m=1}^{p_1} \frac{1}{m(m+1)} \sum_{|k| \leqslant m} \varphi(k) + O\left(\frac{1}{p}\right).$$

Successive application of this inequality gives

$$\sum_{m_0, \ldots, m_s = -p_1}^{p_2}{}' \frac{\delta_p(m_0 + a_1 m_1 + \ldots + a_s m_s)}{\bar{m}_0 \ldots \bar{m}_s} = \sum_{m_1, \ldots, m_{s+1}=1}^{p_1} \frac{1}{m_1(m_1+1) \ldots m_{s+1}(m_{s+1}+1)} \times$$
$$\times \sum_{|k_1| \leqslant m_1, \ldots, |k_{s+1}| \leqslant m_{s+1}}{}' \delta_p(a_1 k_1 + \ldots + a_s k_s + k_{s+1}) + O\left(\frac{1}{p}\right). \tag{58}$$

But, as was shown in [11] (Lemma 27), we have for arbitary integers λ, λ_v and $n_v \geqslant 1$

$$\sum_{k_1=\lambda_1+1}^{\lambda_1+n_1} \cdots \sum_{k_s=\lambda_s+1}^{\lambda_s+n_s} \delta_p(a_1 k_1 + \ldots + a_s k_s) \leqslant \begin{cases} 1 & \text{for } n_1 \ldots n_s \leqslant q_0, \\ \dfrac{4 n_1 \ldots n_s}{q_0} & \text{for } n_1 \ldots n_s > q_0, \end{cases}$$

where q_0 is the least value of $\bar{m}_1 \ldots \bar{m}_s$ for non-trivial solutions of

$$a_1 m_1 + \ldots + a_s m_s \equiv 0 \pmod{p}.$$

Hence, when we substitute $s+1$ for s and put $a_{s+1} = 1$, $\lambda = 0$, $\lambda_\nu = -m_\nu - 1$, $n_\nu = 2m_\nu + 1$ $(\nu = 1, 2, \ldots, s+1)$, we obtain

$$\sum_{|k_1| \leqslant m_1, \ldots, |k_{s+1}| \leqslant m_{s+1}}{}' \delta_p(a_1 k_1 + \ldots + a_s k_s + k_{s+1}) \leqslant 4 \cdot 3^{s+1} \frac{m_1 \ldots m_{s+1}}{q}.$$

Now (58) gives

$$\sum_{m_0,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(m_0+a_1m_1+\ldots+a_sm_s)}{\overline{m}_0\ldots\overline{m}_s} = O\left(\frac{\ln^{s+1}p}{q}\right).$$

If $q \geqslant \frac{p}{B\ln^{\beta}p}$, then

$$\frac{\ln^{s+1}p}{q} \leqslant \frac{B\ln^{\beta+s+1}p}{p},$$

consequently

$$\sum_{m_0,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(m_0+a_1m_1+\ldots+a_sm_s)}{\overline{m}_0\ldots\overline{m}_s} = O\left(\frac{\ln^{\beta+s+1}p}{p}\right), \tag{59}$$

and this by the definition of optimal coefficients proves the sufficiency[1] of the first of the conditions (57).

If $Q \geqslant \frac{p^s}{B_1\ln^{\beta_1}p}$, then by Lemma 4 we have

$$q \geqslant C_1\frac{Q^s}{p^{s^2-1}} \geqslant \frac{p}{B\ln^{\beta}p},$$

where $B = \frac{B_1^s}{C_1}$ and $\beta = \beta_1 s$. But then (59) holds with $\beta = \beta_1 s$; this proves the sufficiency of the second of the conditions (57).

To prove the necessity of these conditions we assume that $1, a_1, \ldots, a_s$ are optimal coefficients. Then

$$\sum_{m_0,\ldots,m_s=-p_1}^{p_2}{}' \frac{\delta_p(m_0+a_1m_1+\ldots+a_sm_s)}{\overline{m}_0\ldots\overline{m}_s} \leqslant \frac{B\ln^{\beta}p}{p}.$$

When we take here the summand corresponding to a solution of

$$m_0+a_1m_1+\ldots+a_sm_s \equiv 0 \pmod p$$

with $\overline{m}_0\ldots\overline{m}_s = q$, we find

$$\frac{1}{q} \leqslant \frac{B\ln^{\beta}p}{p},$$

which is just the first of the conditions (57):

$$q \geqslant \frac{p}{B\ln^{\beta}p}.$$

Finally, by means of Lemma 4 it is easy to see that for $B_1 = \frac{B^s}{C_1}$ and $\beta_1 = \beta_s$ the second of the conditions holds:

1 The sufficiency of this condition was obtained earlier in a different way, as a consequence of a theorem of Bakhvalov (see [2] and [11], Corollary to Theorem 19).

$$Q \geqslant C_1 q^s \geqslant \frac{p^s}{B_1 \ln^{\beta_1} p}.$$

We now give some consequences of Theorem 7.

COROLLARY 1. *Let $a_1, \ldots, a_s$ be optimal coefficients. For $1, a_1, \ldots, a_s$ to be $(s+1)$-dimensional optimal coefficients it is necessary and sufficient that*

$$\ll \frac{a_1 m_1 + \ldots + a_s m_s}{p} \gg \geqslant \frac{1}{\overline{m}_1 \ldots \overline{m}_s (B \ln^\beta p)}, \tag{60}$$

whenever $a_1 m_1 + \ldots + a_s m_s \not\equiv 0 \pmod p$, where $B > 0$ and $\beta \geqslant 0$ are constants depending only on s.

For define m_0 by

$$m_0 + a_1 m_1 + \ldots + a_s m_s \equiv 0 \pmod p, \quad -p_1 \leqslant m_0 \leqslant p_2. \tag{61}$$

Then clearly

$$\ll \frac{a_1 m_1 + \ldots + a_s m_s}{p} \gg = \frac{|m_0|}{p}. \tag{62}$$

Suppose that $a_1 m_1 + \ldots + a_s m_s \not\equiv 0 \pmod p$. Rewriting (60) in the form

$$\frac{|m_0|}{p} \geqslant \frac{1}{\overline{m}_1 \ldots \overline{m}_s (B \ln^\beta p)}$$

and noting that $|m_0| = \overline{m}_0 \neq 0$ we get

$$\overline{m}_0 \ldots \overline{m}_s \geqslant \frac{p}{B \ln^\beta p}. \tag{63}$$

But if $a_1 m_1 + \ldots + a_s m_s \equiv 0 \pmod p$, then Theorem 7 implies that for $(m_1, \ldots, m_s) \neq (0, \ldots, 0)$ we have

$$\overline{m}_1 \ldots \overline{m}_s \geqslant \frac{p}{B \ln^\beta p}. \tag{64}$$

In this case $m_0 = 0$ and $\overline{m}_0 = 1$, and so (63) and (64) coincide. Hence (63) is satisfied for all non-trivial solutions of (61) and so $1, a_1, \ldots a_s$ is an optimal system by another application of Theorem 7.

We now proceed to prove the necessity of the condition of the corollary. Let $1, a_1, \ldots, a_s$ be optimal coefficients. Then

$$\sum_{m_0, \ldots, m_s = -p_1}^{p_2}{}' \frac{\delta_p (m_0 + a_1 m_1 + \ldots + a_s m_s)}{\overline{m}_0 \ldots \overline{m}_s} \leqslant \frac{B \ln^\beta p}{p}.$$

Hence for $m_0 = 0$ we obtain

$$\sum_{m_1, \ldots, m_s = -p_1}^{p_2}{}' \frac{\delta_p (a_1 m_1 + \ldots + a_s m_s)}{\overline{m}_1 \ldots \overline{m}_s} \leqslant \frac{B \ln^\beta p}{p}.$$

Therefore $a_1, \ldots, a_s$ are s-dimensional optimal coefficients. Further, by Theorem 7 every non-trivial solution of (61) satisfies

$$\bar{m}_0 \ldots \bar{m}_s \geqslant \frac{p}{B \ln^\beta p}. \tag{65}$$

If $a_1 m_1 + \ldots + a_s m_s \not\equiv 0 \pmod p$, then $m_0 \neq 0$ and $m_0 = |\bar{m}_0|$. Rewriting (65) in the form

$$\frac{|m_0|}{p} \geqslant \frac{1}{\bar{m}_1 \ldots \bar{m}_s (B \ln^\beta p)},$$

and using (62) we get (60).

We remark that if the estimate

$$\ll \alpha_1 m_1 + \ldots + \alpha_s m_s \gg \ \geqslant \frac{1}{B\bar{m}_1 \ldots \bar{m}_s \ln^\beta (\bar{m}_1 \ldots \bar{m}_s + 1)} \tag{66}$$

analogous to (60) holds for $(m_1, \ldots, m_s) \neq (0, \ldots, 0)$ and some system $\alpha_1, \ldots, \alpha_s$ of irrational numbers, then the quadrature formula

$$\int_0^1 \cdots \int_0^1 f(x_1, \ldots, x_s)\, dx_1 \ldots dx_s = \frac{1}{p} \sum_{k=1}^{p} f(\{\alpha_1 k\}, \ldots, \{\alpha_s k\}) + O\left(\frac{1}{p}\right)$$

holds for $f \in E_s^\alpha(C)$ (see [11], Theorem 11). The estimate (66) is known to hold for almost all points of the s-dimensional unit cube G_s, but for $s > 1$ not one specimen of such a point is known. All that has been said also holds for points $\alpha_1, \ldots, \alpha_s$ for which

$$\ll \alpha_1 m \gg \ldots \ll \alpha_s m \gg \ \geqslant \frac{1}{B |m| \ln^\beta (|m| + 1)}$$

for all integers $m \neq 0$. We discuss the rational variant of this inequality in the second Corollary to Theorem 7.

A result like (66) but with $\ln^\beta(\bar{m}_1 \ldots \bar{m}_s + 1)$ replaced by a function growing faster than any power of a logarithm was obtained recently by Baker [3]. The combination of this result with the corresponding theorems in [2] and [11] permits us to construct many-dimensional quadrature formulae.

COROLLARY 2. *The numbers* $1, a_1, \ldots, a_s$ *are an* $(s + 1)$*-dimensional set of optimal coefficients if and only if for* $k \neq 0$ *and* $-p_1 \leqslant k \leqslant p_2$ *the inequality*

$$\ll \frac{a_1 k}{p} \gg \ldots \ll \frac{a_s k}{p} \gg \ \geqslant \frac{1}{(B_1 \ln^{\beta_1} p)\, |k|} \tag{67}$$

holds, where $B_1 > 0$ *and* $\beta_1 \geqslant 0$ *depend only on* s.

For define integers $k_1, \ldots, k_s$ by

$$\left.\begin{array}{l} a_1 k \equiv k_1, \\ \cdots\cdots \\ a_s k \equiv k_s \end{array}\right\} \pmod p, \qquad -p_1 \leqslant k_\nu \leqslant p_2 \quad (\nu = 1, 2, \ldots, s). \tag{68}$$

Then clearly

$$\ll\frac{a_1k}{p}\gg=\frac{|k_1|}{p},\ \ldots,\ \ll\frac{a_sk}{p}\gg=\frac{|k_s|}{p},$$

and so (67) can be written in the form

$$|k||k_1|\ldots|k_s|\geqslant\frac{p^s}{B_1\ln^{\beta_1}p},\tag{69}$$

where k, k_1, ..., k_s is any non-trivial solution of (68). It is easy to see that (69) holds if and only if

$$Q\geqslant\frac{p^s}{B_1\ln^{\beta_1}p}.$$

Hence we can derive the Corollary by Theorem 7.

By the definitions of q and Q it is easy to show that for any parallelopipedal net

$$M_k=\left(\left\{\frac{k}{p}\right\},\ \left\{\frac{a_1k}{p}\right\},\ \ldots,\left\{\frac{a_sk}{p}\right\}\right)\quad(k=1,\ 2,\ \ldots,\ p)\tag{70}$$

we have the estimates

$$\ll\frac{a_1m_1+\ldots+a_sm_s}{p}\gg\geqslant\frac{q}{p\overline{m}_1\ldots\overline{m}_s},\qquad a_1m_1+\ldots+a_sm_s\not\equiv 0\ (\mathrm{mod}\ p),$$

$$\ll\frac{a_1k}{p}\gg\ldots\ll\frac{a_sk}{p}\gg\geqslant\frac{Q}{p^s|k|},\qquad k\not\equiv 0\ (\mathrm{mod}\ p),$$

similar to those in the Corollaries to Theorem 7 for optimal parallelopipedal nets. The larger the values of

$$q=q\,(1,\ a_1,\ \ldots,\ a_s)\ \text{and}\ Q=Q\,(1,\ a_1,\ \ldots,\ a_s),$$

the stronger are the estimates.

We define q^* and Q^* by

$$q^*=\max_{a_1,\ \ldots,\ a_s}q\,(1,\ a_1,\ \ldots,\ a_s),\qquad Q^*=\max_{a_1,\ \ldots,\ a_s}Q\,(1,\ a_1,\ \ldots,\ a_s).$$

To the parallelopipedal nets (70) for which $q = q^*$ or $Q = Q^*$ there correspond, clearly, the largest hyperbolic domains of the type (53).

We estimate q^* and Q^*. It is easy to see that

$$q^*\leqslant\frac{1}{2}p\ \text{and}\ Q^*\leqslant\frac{1}{2^s}p^s.\tag{71}$$

For when we set $m_1= \ldots =m_s = 1$ and use

$$\sum_{m_0=-p_1}^{p_2}\delta_p\,(m_0+a_1m_1+\ldots+a_sm_s)=1$$

we obtain the first estimate of (71). The second follows for $k_0 = 1$ from

$$\sum_{k_1,\ \ldots,\ k_s=-p_1}^{p_2}\delta_p\,(a_1k_0-k_1)\ldots\delta_p\,(a_sk_0-k_s)=1.$$

On the other hand, it is not difficult to show that

$$q^* \geqslant \frac{p}{B \ln^s p} \text{ and } Q^* \geqslant \frac{p^s}{B_1 \ln^s p}, \tag{72}$$

for prime p, where B and B_1 are positive constants depending only on s. The first of these estimates was obtained by Bakhvalov [2]. The second estimate in (72) follows from the fact that for sufficiently large $B_1 = B_1(s)$ we have

$$\min_{a_1, \ldots, a_s} \sum_{1 \leq |k_0| \ldots |k_s| < \frac{p^s}{B_1 \ln^s p}} \delta_p(a_1 k_0 - k_1) \ldots \delta_p(a_s k_0 - k_s) = 0. \tag{73}$$

This equation is obtained by obvious calculations after majorizing the minimum of the sum in (73) by its mean.

The inequalities (71) show that (72) cannot be improved essentially. But except for $s = 1$ the true order of q^* and Q^* is unknown. For $s = 1$ the estimate (72) gives the true order, since it is known (see [11], Lemma 5 and Theorem 20) that $q \geqslant p/8M$, where M is an upper bound for the partial quotients of a/p.

3. At the beginning of this subsection we established a connection between the nature of the uniformity of distribution of the points of the parallelopipedal nets

$$M_k = \left(\left\{ \frac{a_1 k}{p} \right\}, \ldots, \left\{ \frac{a_s k}{p} \right\} \right) \tag{74}$$

and the optimality of those nets. Now we show that the optimality of the nets is also connected with the nature of the uniformity of distribution of the fractional parts of the linear form $\alpha_1 m_1 + \ldots + \alpha_s m_s$, where $\alpha_\nu = \frac{a_\nu}{p}$ $(\nu = 1, 2, \ldots, s)$.

Suppose that $0 < \gamma \leqslant 1$, that λ_ν are arbitrary integers, that $1 \leqslant P_\nu \leqslant p$ and that $N_{p_1 \ldots p_s}(\gamma)$ denotes the number of solutions of

$$0 \leqslant \left\{ \frac{a_1 m_1 + \ldots + a_s m_s}{p} \right\} < \gamma,$$

when the m_ν independently run through integral values from the intervals

$$\lambda_\nu + 1 \leqslant m_\nu \leqslant \lambda_\nu + P_\nu \qquad (\nu = 1, 2, \ldots, s).$$

We precede the proof of the main theorem by the following lemma.

LEMMA 5. *A necessary and sufficient condition for the integers* $1, a_1, \ldots, a_s$ *to be optimal coefficients is that*

$$\sum_{1 \leq |k_0|, \ldots, |k_s| \leq p_2} \frac{\delta_p(a_1 k_0 - k_1) \ldots \delta_p(a_s k_0 - k_s)}{|k_0| \ldots |k_s|} \leqslant \frac{B_2 \ln^{\beta_2} p}{p^s}, \tag{75}$$

where $B_2 > 0$ *and* $\beta_2 \geqslant 0$ *are constants depending only on* s.

PROOF. It is easy to see that the summands in (75) are different from zero only for those systems $k_0, \ldots, k_s$ that give a non-trivial solution of the system of congruences

$$\left.\begin{array}{l} a_1k_0 \equiv k_1, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_sk_0 \equiv k_s \end{array}\right\} \pmod p. \tag{76}$$

Hence the range of summation may be written in the form

$$1 \leqslant |k_0|, \ldots, |k_s| \leqslant p_2, \quad |k_0| \ldots |k_s| \geqslant Q,$$

where Q is the minimal product $|k_0| \ldots |k_s|$ over non-trivial solutions of (76). Define r by $2^{r-1} \leqslant p_2 < 2^r$ and split the range of summation for k_j into the parts

$$2^{\nu_j} \leqslant |k_j| < 2^{\nu_j+1}, \quad 0 \leqslant \nu_j < r \quad (j = 0, 1, \ldots, s). \tag{77}$$

Denoting the sum (75) by σ and using

$$\frac{1}{|k_j|} \leqslant \frac{1}{2^{\nu_j}},$$

we obtain

$$\sigma \leqslant \sum_{\nu_0, \ldots, \nu_s} \frac{1}{2^{\nu_0+\cdots+\nu_s}} \sum_{k_0, \ldots, k_s} \delta_p(a_1k_0 - k_1) \ldots \delta_p(a_sk_0 - k_s), \tag{78}$$

where the range of summation is defined by (77) and the supplementary condition

$$2^{\nu_0+\ldots+\nu_s} \geqslant \frac{1}{2^{s+1}} Q. \tag{79}$$

Suppose that 1, a_1, ..., a_s are optimal coefficients. Then observing that

$$\sum_{k_0=1}^{P} \sum_{k_1=0}^{n_1-1} \cdots \sum_{k_s=0}^{n_s-1} \delta_p(a_1k_0 - k_1) \ldots \delta_p(a_sk_0 - k_s) = N_P\left(\frac{n_1}{p}, \ldots, \frac{n_s}{p}\right),$$

and using Theorem 7 we find

$$\sum_{2^{\nu_0} \leqslant |k_0| < 2^{\nu_0+1}} \cdots \sum_{2^{\nu_s} \leqslant |k_s| < 2^{\nu_s+1}} \delta_p(a_1k_0 - k_1) \ldots \delta_p(a_sk_0 - k_s) \leqslant$$

$$\leqslant 2^{s+1} N_{2^{\nu_0+1}}\left(\frac{2^{\nu_1+1}}{p}, \ldots, \frac{2^{\nu_s+1}}{p}\right) \leqslant C\left(\frac{2^{\nu_0+\ldots+\nu_s}}{p^s} + \ln^\beta p\right),$$

where C is a constant depending only on s and β is determined by the choice of optimal coefficients. Now (78) and (79) imply that

$$\sigma \leqslant C\left(\frac{r^{s+1}}{p^s} + \frac{r^{s+1}\ln^\beta p}{Q}\right) = O\left(\frac{\ln^{\beta+s+1} p}{Q}\right).$$

Since by Theorem 7,

$$Q \geqslant \frac{p^s}{B_1 \ln^{\beta_1} p},$$

we arrive at

$$\sigma = O\left(\frac{\ln^{\beta_2} p}{p^s}\right),$$

with $\beta_2 = \beta + \beta_1 + s + 1$, and this proves the necessity of the condition of the lemma. The sufficiency follows immediately from Theorem 7,

because $\sigma \geqslant \frac{1}{Q}$, and (75) gives

$$Q \geqslant \frac{p^s}{B_2 \ln^{\beta_2} p}.$$

THEOREM 8. *A necessary and sufficient condition for* 1, a_1, ... a_s *to be optimal coefficients is that*

$$N_{P_1, \ldots, P_s}(\gamma) = \gamma P_1 \ldots P_s + O(\ln^\beta p) \tag{80}$$

for any rational γ *with denominator* p.

PROOF. Let $\gamma = u/p$, where $1 \leqslant n \leqslant p$. Clearly

$$N_{P_1, \ldots, P_s}(\gamma) = \sum_{m_0=0}^{n-1} \sum_{n_1=\lambda_1+1}^{\lambda_1+P_1} \ldots \sum_{m_s=\lambda_s+1}^{\lambda_s+P_s} \delta_p(-m_0 + a_1 m_1 + \ldots + a_s m_s).$$

Using the equation

$$\delta_p(-m_0 + a_1 m_1 + \ldots + a_s m_s) = \frac{1}{p} + \frac{1}{p} \sum_{k_0=-p_1}^{p_2}{}' e^{2\pi i \frac{(-m_0 + a_1 m_1 + \ldots + a_s m_s) k_0}{p}}$$

and the estimate

$$\left| \sum_{m_\nu=\lambda_\nu+1}^{\lambda_\nu+P_\nu} e^{2\pi i \frac{a_\nu k_0 m_\nu}{p}} \right| \leqslant \frac{1}{\left\langle\!\left\langle \frac{a_\nu k_0}{p} \right\rangle\!\right\rangle},$$

after some obvious transformation we get

$$N_{P_1, \ldots, P_s}(\gamma) = \gamma P_1 \ldots P_s + R,$$

where

$$|R| \leqslant \sum_{1 \leqslant |k_0| \leqslant p_2} \frac{1}{|k_0| \left\langle\!\left\langle \frac{a_1 k_0}{p} \right\rangle\!\right\rangle \ldots \left\langle\!\left\langle \frac{a_s k_0}{p} \right\rangle\!\right\rangle} \leqslant$$

$$\leqslant p^s \sum_{1 \leqslant |k_0|, \ldots, |k_s| \leqslant p_2} \frac{\delta_p(a_1 k_0 - k_1) \ldots \delta_p(a_s k_0 - k_s)}{|k_0| \ldots |k_s|}.$$

If 1, a_1, ..., a_s are optimal coefficients, then this together with Lemma 5 gives

$$|R| \leqslant B_2 \ln^{\beta_2} p,$$

which proves the necessity of the condition in the theorem.

Suppose now that (80) is fulfilled:

$$N_{P_1, \ldots, P_s}(\gamma) = \gamma P_1 \ldots P_s + R, \qquad |R| \leqslant C \ln^\beta p. \tag{81}$$

Define β_1 and t by

$$\beta_1 = (\beta+1)s+1, \qquad t = [\ln^{\beta+1} p]. \tag{82}$$

Let us assume that there are integers $n_1, \ldots, n_s$ such that $a_1 n_1 + \ldots + a_s n_s \not\equiv 0 \pmod p$ and

$$\ll \frac{a_1 n_1 + \ldots + a_s n_s}{p} \gg < \frac{1}{\bar{n}_1 \ldots \bar{n}_s \ln^{\beta_1} p}. \tag{83}$$

Then for $k = 1, 2, \ldots, 2t$ we get

$$\ll \frac{a_1 n_1 k + \ldots + a_s n_s k}{p} \gg < \frac{2t}{\bar{n}_1 \ldots \bar{n}_s \ln^{\beta_1} p}. \tag{84}$$

Let $P_\nu = 2\bar{n}_\nu t$ and λ_ν be chosen so that

$$\lambda_\nu + 1 \leqslant n_\nu k \leqslant \lambda_\nu + P_\nu \qquad (1 \leqslant \nu \leqslant s, \ k = 1, 2, \ldots, 2t), \tag{85}$$

and put $\gamma = \frac{n}{p}$, where the integer n is determined by

$$\frac{n-1}{p} \leqslant \frac{2t}{\bar{n}_1 \ldots \bar{n}_s \ln^{\beta_1} p} < \frac{n}{p}.$$

It follows from (84) that for $\lambda_\nu + 1 \leqslant m_\nu \leqslant \lambda_\nu + P_\nu$ at least one of the intervals $(0, \gamma)$ or $(1-\gamma, 1)$ contains at least t fractional parts $\left\{\frac{a_1 m_1 + \ldots + a_s m_s}{p}\right\}$.

Suppose that this interval[1] is $(0, \gamma)$.

Then (81) and (82) give

$$t \leqslant N_{P_1, \ldots, P_s}(\gamma) \leqslant \frac{2t+1}{\bar{n}_1 \ldots \bar{n}_s \ln^{\beta_1} p} P_1 \ldots P_s + C \ln^\beta p = O(\ln^\beta p),$$

which is impossible by our choice of t. Therefore the assumption (83) is contradictory, that is,

$$\ll \frac{a_1 m_1 + \ldots + a_s m_s}{p} \gg \geqslant \frac{1}{\bar{m}_1 \ldots \bar{m}_s \ln^{\beta_1} p} \tag{86}$$

for all $m_1, \ldots, m_s$ for which $a_1 m_1 + \ldots + a_s m_s \not\equiv 0 \pmod p$.

Now let $t = [2C \ln^\beta p]$ and let $n_1, \ldots, n_s$ be any solution of

$$a_1 m_1 + \ldots + a_s m_s \equiv 0 \pmod p. \tag{87}$$

Clearly for $k = 1, 2, \ldots, t$ the numbers $n_1 k, \ldots, n_s k$ are also a solution. Put $\gamma = \frac{1}{p}$, $P_\nu = \bar{n}_\nu t$ and define the λ_ν so that as in (85).

$$\lambda_\nu + 1 \leqslant n_\nu k \leqslant \lambda_\nu + P_\nu \qquad (1 \leqslant \nu \leqslant s).$$

[1] The case $(1-\gamma, 1)$ is treated similarly.

Since here the number $N_{p_1 \ldots p_s}(\gamma)$ is equal to the number of solutions of (87), by (81) we have

$$t \leqslant N_{p_1, \ldots, p_s}(\gamma) \leqslant \frac{\bar{n}_1 \ldots \bar{n}_s (2t)^s}{p} + C \ln^\beta p.$$

Hence by our choice of t it follows that

$$\bar{n}_1 \ldots \bar{n}_s \geqslant C_1 \frac{p}{\ln^{\beta_1} p},$$

where $\beta_1 = (s-1)\beta$ and $C_1 = C_1(s)$. Thus, by Theorem 7 the numbers $a_1, \ldots, a_s$ are s-dimensional optimal coefficients. But then by (86) and Theorem 7, Corollary 1 the numbers 1, $a_1, \ldots, a_s$ are $(s + 1)$-dimensional optimal coefficients.

4. In this subsection we consider the connection between optimal parallelopipedal nets and the asymptotic behaviour of sums of fractional parts. Particular cases of this connection are used in the construction of algorithms for the computation of optimal systems of coefficients. For example, it is known (see [10] and [11], Theorem 23) that if

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

attains its minimum at $z = a$, then 1, $a, \ldots, a^{s-1}$ are s-dimensional optimal coefficients to the prime modulus p. The proof of this depends on the equation

$$H(a) = 1 + O\left(\frac{\ln^{2s} p}{p^2}\right),$$

which, clearly, is equivalent to the asymptotic formula

$$\sum_{k=1}^{p} \left(1 - 2\left\{\frac{k}{p}\right\}\right)^2 \cdots \left(1 - 2\left\{\frac{a^{s-1}k}{p}\right\}\right)^2 = \frac{p}{3^s} + O\left(\frac{\ln^{2s} p}{p}\right).$$

Suppose that $b_1, \ldots, b_s$ be arbitrary integers and that each of $\tau_1, \ldots, \tau_s$ take the values 0 or 1.

THEOREM 9. *A necessary and sufficient condition for $a_1, \ldots, a_s$ to be optimal coefficients is that*

$$\sum_{k=1}^{p} \left(\left\{\frac{a_1 k + b_1}{p}\right\} - \frac{p-1}{2p}\right)^{\tau_1} \cdots \left(\left\{\frac{a_s k + b_s}{p}\right\} - \frac{p-1}{2p}\right)^{\tau_s} = O(\ln^\beta p) \qquad (88)$$

for all $b_1, \ldots, b_s$ and for any system $(\tau_1, \ldots, \tau_s) \neq (0, \ldots, 0)$.

PROOF. Define f by

$$f\left(\frac{k_1}{p}, \ldots, \frac{k_s}{p}\right) = \left(\left\{\frac{k_1 + b_1}{p}\right\} - \frac{p-1}{2p}\right)^{\tau_1} \cdots \left(\left\{\frac{k_s + b_s}{p}\right\} - \frac{p-1}{2p}\right)^{\tau_s}.$$

By Theorem 4

$$\frac{1}{p^s}\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ldots,\frac{k_s}{p}\right)=\frac{1}{p}\sum_{k=1}^{p}\prod_{\nu=1}^{s}\left(\left\{\frac{a_\nu k+b_\nu}{p}\right\}-\frac{p-1}{2p}\right)^{\tau_\nu}-R,$$

$$|R|\leqslant V_p[f]\,D_p, \tag{89}$$

where $V_p[f]$ is the finite variation of f and D_p is the measure of uniformity of distribution of the net

$$M_k=\left(\left\{\frac{a_1k}{p}\right\},\ldots,\left\{\frac{a_sk}{p}\right\}\right)\quad (k=1,2,\ldots,p). \tag{90}$$

Since at least one of the τ_ν is 1, on noting that

$$\sum_{k_\nu=0}^{p-1}\left(\left\{\frac{k_\nu+b_\nu}{p}\right\}-\frac{p-1}{2p}\right)=0,$$

we get

$$\sum_{k_1,\ldots,k_s=0}^{p-1} f\left(\frac{k_1}{p},\ldots,\frac{k_s}{p}\right)=0,$$

and so

$$\sum_{k=1}^{p}\left(\left\{\frac{a_1k+b_1}{p}\right\}-\frac{p-1}{2p}\right)^{\tau_1}\cdots\left(\left\{\frac{a_sk+b_s}{p}\right\}-\frac{p-1}{2p}\right)^{\tau_s}=pR.$$

Let $a_1, \ldots, a_s$ be optimal coefficients. Then by Theorem 5

$$D_p\leqslant\frac{B_1\ln^{\beta_1}p}{p},$$

and since f is a function of bounded finite variation (this is easy to check directly), we now derive from (89) the estimate.

$$R=O\left(\frac{\ln^{\beta_1}p}{p}\right).$$

But then

$$\sum_{k=1}^{p}\left(\left\{\frac{a_1k+b_1}{p}\right\}-\frac{p-1}{2p}\right)^{\tau_1}\cdots\left(\left\{\frac{a_sk+b_s}{p}\right\}-\frac{p-1}{2p}\right)^{\tau_s}=O(\ln^{\beta_1}p),$$

and this proves the necessity of the condition of the theorem.

Now suppose that (88) is fulfilled. Define $\varphi(x_1, \ldots, x_s)$ by

$$\varphi_\gamma(x)=\{x-\gamma\}-\{x\}+\gamma,\quad \varphi(x_1,\ldots,x_s)=\prod_{\nu=1}^{s}\varphi_{\gamma_\nu}(x_\nu). \tag{91}$$

Since clearly $\varphi_\gamma(x)=\begin{cases}1 & \text{if}\quad \{x\}<\gamma,\\ 0 & \text{if}\quad \{x\}\geqslant\gamma,\end{cases}$ the function $\varphi(x_1, \ldots, x_s)$ is the characteristic function of the domain $0\leqslant x_1<\gamma_1, \ldots, 0\leqslant x_s<\gamma_s$. Hence for the number of points of the net (90) lying in this domain we find

$$N_p(\gamma_1, \ldots, \gamma_s) = \sum_{k=1}^{p} \varphi\left(\left\{\frac{a_1 k}{p}\right\}, \ldots, \left\{\frac{a_s k}{p}\right\}\right).$$

Let us choose the γ_ν to be rational with common denominator p:

$$\gamma_\nu = \frac{n_\nu}{p}, \quad 1 \leqslant n_\nu \leqslant p \quad (\nu = 1, 2, \ldots, s). \tag{92}$$

Then by (91) we have

$$N_p(\gamma_1, \ldots, \gamma_s) = \sum_{k=1}^{p} \prod_{\nu=1}^{s} \left(\left\{\frac{a_\nu k - n_\nu}{p}\right\} - \left\{\frac{a_\nu k}{p}\right\} + \frac{n_\nu}{p}\right) = \gamma_1 \ldots \gamma_s p + R,$$

where

$$|R| \leqslant 2^s \max_{(\tau_1, \ldots, \tau_s)'} \left|\sum_{k=1}^{p} \prod_{\nu=1}^{s} \left(\left\{\frac{a_\nu k - n_\nu}{p}\right\} - \left\{\frac{a_\nu k}{p}\right\}\right)^{\tau_\nu} \left(\frac{n_\nu}{p}\right)^{1-\tau_\nu}\right|.$$

Hence, observing that $\left|\frac{n_\nu}{p}\right| \leqslant 1$, and using

$$\left\{\frac{a_\nu k - n_\nu}{p}\right\} - \left\{\frac{a_\nu k}{p}\right\} = \left(\left\{\frac{a_\nu k - n_\nu}{p}\right\} - \frac{p-1}{2p}\right) - \left(\left\{\frac{a_\nu k}{p}\right\} - \frac{p-1}{2p}\right),$$

and (88) we obtain

$$|R| \leqslant 4^s \max_{(\tau_1, \ldots, \tau_s)'} \left|\sum_{k=1}^{p} \prod_{\nu=1}^{s} \left(\left\{\frac{a_\nu k + b_\nu}{p}\right\} - \frac{p-1}{2p}\right)^{\tau_\nu}\right| = O(\ln^\beta p).$$

But then for any γ_v of the form (92) we have

$$N_p(\gamma_1, \ldots, \gamma_s) = \gamma_1 \ldots \gamma_s p + O(\ln^\beta p),$$

and by (37) this proves the sufficiency of the condition of the theorem.

Note that if the condition

$$\sum_{k=1}^{P} \left(\left\{\frac{a_1 k + b_1}{p}\right\} - \frac{p-1}{2p}\right)^{\tau_1} \ldots \left(\left\{\frac{a_s k + b_s}{p}\right\} - \frac{p-1}{2p}\right)^{\tau_s} = O(\ln^\beta p) \tag{93}$$

is satisfied not merely for $P = p$, as was the case in Theorem 9, but also for any $P \leqslant p$, then 1, a_1, ..., a_s are $(s + 1)$-dimensional optimal coefficients. The condition (93) is also necessary and sufficient for optimality of these numbers. We do not carry out the proof, as it is essentially the same as that of Theorem 9.

THEOREM 10. *A necessary and sufficient condition for* 1, 1, a_1, ..., a_s *to be* $(s + 1)$ *-dimensional optimal coefficients is that*

$$\sum_{m_1=1}^{P_1} \cdots \sum_{m_s=1}^{P_s} \left\{\frac{a_1 m_1 + \ldots + a_s m_s + b}{p}\right\} = \frac{p-1}{2p} P_1 \ldots P_s + O(\ln^\beta p) \tag{94}$$

for all $P_v \leqslant p$ *and any integer* b.

PROOF. Let $\varphi_\gamma(x)$ be defined as in (91): $\varphi_\gamma(x)=\{x-\gamma\}-\{x\}+\gamma$. Since $\varphi_\gamma(x)$ is the characteristic function of the interval $[0,\gamma)$, for $\gamma=\frac{n}{p}$ $(1\leqslant n\leqslant p)$ we obtain

$$N_{P_1,\dots,P_s}(\gamma)=\sum_{m_1=1}^{P_1}\dots\sum_{m_s=1}^{P_s}\left(\left\{\frac{a_1m_1+\dots+a_sm_s-n}{p}\right\}-\right.$$
$$\left.-\left\{\frac{a_1m_1+\dots+a_sm_s}{p}\right\}+\frac{n}{p}\right)=\gamma P_1\dots P_s+R,$$

where by (94).

$$R=\sum_{m_1=1}^{P_1}\dots\sum_{m_s=1}^{P_s}\left(\left\{\frac{a_1m_1+\dots+a_sm_s-n}{p}\right\}-\left\{\frac{a_1m_1+\dots+a_sm_s}{p}\right\}\right)=O(\ln^\beta p).$$

Thus, $N_{P_1,\dots,P_s}(\gamma)=\gamma P_1\dots P_s+O(\ln^\beta p)$, and this proves the sufficiency of (94) by Theorem 8.

To prove the necessity of the condition we note that the function $\{x\}$ has bounded finite variation so that its finite Fourier coefficients satisfy $|C_p(m)|\leqslant\frac{C}{\overline{m}}$, where C is an absolute constant. Since clearly

$$C_p(0)=\frac{1}{p}\sum_{k=0}^{p-1}\left\{\frac{k}{p}\right\}=\frac{p-1}{2p},$$ on developing $\{x\}$ in a finite

Fourier series we obtain

$$\sum_{m_1=1}^{P_1}\dots\sum_{m_s=1}^{P_s}\left\{\frac{a_1m_1+\dots+a_sm_s+b}{p}\right\}=\frac{p-1}{2p}P_1\dots P_s+R,\tag{95}$$

where

$$|R|=\left|\sum_{m_0=-p_1}^{p_2}{}'\,C_p(m_0)\sum_{m_1=1}^{P_1}\dots\sum_{m_s=1}^{P_s}e^{2\pi i\frac{(a_1m_1+\dots+a_sm_s+b)m_0}{p}}\right|\leqslant$$
$$\leqslant C\sum_{m_0=-p_1}^{p_2}{}'\frac{1}{|m_0|\left\langle\!\left\langle\frac{a_1m_0}{p}\right\rangle\!\right\rangle\dots\left\langle\!\left\langle\frac{a_sm_0}{p}\right\rangle\!\right\rangle}\leqslant$$
$$\leqslant Cp^s\sum_{1\leqslant|m_0|,\dots,|m_s|\leqslant p_2}\frac{\delta_p(a_1m_0-m_1)\dots\delta_p(a_sm_0-m_s)}{|m_0|\,\dots|m_s|}$$

If 1, $a_1,\dots,a_s$ are optimal coefficients, we have $R=O(\ln^{\beta_2}p)$ by Lemma 5. Substituting this in (95) we see that the condition of the theorem is necessary.

We now turn to the computation of optimal coefficients. It is easy to see that the algorithm mentioned at the beginning of this subsection, which reduces the problem to finding the minimum of the function

$$H(z)=\frac{3^s}{p}\sum_{k=1}^{p}\left(1-2\left\{\frac{k}{p}\right\}\right)^2\cdots\left(1-2\left\{\frac{z^{s-1}k}{p}\right\}\right)^2, \tag{96}$$

requires $O(p^2)$ elementary arithmetical operations. For the minimum of $H(z)$ can be found by comparing its values for $z = 1, 2, \ldots, p-1$. Since (96) contains p terms, for given z the computation of $H(z)$ requires $O(p)$ elementary operations. Thus, the total number of operations required is $O(p^2)$. There exist more economical algorithms in which the number of elementary operations is $O(p^{1+\frac{1}{3}})$ (see [11], Theorem 24). By using the Corollaries to Theorem 7 we can reduce this to $O(p)$. The question whether this can be further diminished for arbitrary dimension s seems to present considerable difficulties. But it is encouraging that for $s = 2$ the search for optimal coefficients requires only $O(\ln p)$ elementary arithmetical operations (see [11], § 10).

In conclusion we mention another problem connected with the construction of algorithms for computing optimal coefficients. It is easy to show that if $a_1, \ldots, a_s$ is an s-dimensional optimal system, then for $1 < r < s$ any r of them form an r-dimensional optimal system. This gives a necessary condition for optimality. The question whether this condition is sufficient remains open. In particular, it is not known whether $1, a, b$ is an optimal 3-dimensional system when $1, a$; $1, b$ and a, b are all 2-dimensional optimal systems.

Received by the Editors October 11, 1966.

REFERENCES

[1] T. von Aardenne-Ehrenfest, On the impossibility of a just distribution, Indag. Math. 11 (1949), 264–269.

[2] N.S. Bakhvalov, The approximate computation of multiple integrals, Vestnik Moskov. Univ. Ser. Mat. Mekh. Astr. Fiz. Khim. 1959 no. 4, 3–18.

[3] A.C. Baker, On some diophantine inequalities involving the exponential function, Canad. J. Math. 17 (1965), 616–626.

[4] A. Weil, On some exponential sums. Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.

[5] E. Hlawka, Zur angenäherten Berechnung mehrfacher Integrale. Monatshefte Math. 66 (1962), 140–151.

[6] E. Hlawka, Lösung von Integralgleichungen mittels zahlentheoretischer Methoden I. Österreich. Akad. Wiss. Math.-Nat. Kl. S.-B. II 171 (1962), 103–123.

[7] E. Hlawka, Uniform distribution modulo 1 and numerical analysis. Comp. Math. 16 (1964), 92–105.

[8] N.M. Korobov. The approximate calculation of multiple integrals using number-theoretic methods, Dokl. Akad. Nauk SSSR 115 (1957), 1062–1065.

[9] N.M. Korobov. The approximate calculation of multiple integrals, Dokl. Akad. Nauk SSSR 124 (1959), 1207-1210.

[10] N.M. Korobov. Properties and computation of optimal coefficients Dokl. Akad. Nauk SSSR. 132 (1960), 1009–1012.
= Soviet Math. Doklady 1 (1960), 696–700.

[11] N.M. Korobov. *Teoretiko-chislovye metody v priblizhennom analize* (Number-theoretical methods in approximate analysis) Fizmatgiz., Moscow 1963.
[12] J.H. Halton. On the efficiency of certain quasi-random sequences of points in evaluating multidimensional integrals. Numerische Math. 2 (1960), 84–90.
[13] J.M. Hammersley. Monte Carlo methods for solving multivariable problems. Ann. New. York Acad. Sci. 86 (1960), 844–874.

Translated by J.W.S. Cassels