

## ACTA ARITHMETICA XXXVII (1980)

## On irregularities of distribution, IV

bу

## K. F. ROTH (London)

Dedicated to the memory of Paul Turán

1. Introduction. Let k be a natural number and let  $U_0^{k+1}$ ,  $U_1^{k+1}$  denote the unit cubes consisting respectively of points  $\boldsymbol{\beta}=(\beta^{(1)},\ldots,\beta^{(k+1)})$  with  $0\leqslant \beta^{(j)}<1$   $(j=1,\ldots,k+1)$  and points  $\boldsymbol{\alpha}=(\alpha^{(1)},\ldots,\alpha^{(k+1)})$  with  $0<\alpha^{(j)}\leqslant 1$   $(j=1,\ldots,k+1)$ . Let  $\mathscr P$  be a finite set in  $U_0^{k+1}$ . For  $\boldsymbol{\alpha}$  in  $U_1^{k+1}$ , write  $Z(\mathscr P,B(\boldsymbol{\alpha}))$  for the number of points of  $\mathscr P$  lying in the box  $B(\boldsymbol{\alpha})$  consisting of all  $\boldsymbol{\beta}$  satisfying  $0\leqslant \beta^{(j)}<\alpha^{(j)}$   $(j=1,\ldots,k+1)$ ; and put

$$D(\mathscr{P}; B(a)) = Z(\mathscr{P}; B(a)) - |\mathscr{P}| V(B(a)),$$

where  $|\mathscr{P}|$  is the number of elements of  $\mathscr{P}$  and V(B(a)) is the volume of B(a).

Roth [5] proved (1) the following result.

THEOREM 1. There exists a positive number c'(k), depending only on k, such that for every  $\mathscr P$  in  $U_0^{k+1}$ ,

$$(1.1) \qquad \int\limits_{U_1^{k+1}} |D(\mathscr{P}; B(a))|^2 da > c'(k) (\log |\mathscr{P}|)^k.$$

The purpose of the present paper is to establish the following complementary result.

THEOREM 2. For a suitable number e''(k) (depending only on k) there exists, corresponding to every natural number  $N\geqslant 2$ , a set  $\mathscr P$  in  $U_0^{k+1}$  such that  $|\mathscr P|=N$  and

(1.2) 
$$\int_{U_1^{k+1}} |D(\mathscr{P}; B(a))|^2 da < c''(k) (\log |\mathscr{P}|)^k.$$

<sup>(1)</sup> We use  $\int_{U_1^{k+1}} da$  to signify  $\int_{U_1} \dots \int_{U_1} da^{(1)} \dots da^{(k+1)}$ .

This shows that (apart from the value of the constant) Theorem 1 is best possible.

The case k+1=2 of Theorem 2 (the 2 dimensional case) was established by Davenport [1], and different proofs were given by Vilenkin [8], Halton-Zaremba [3] and Roth [6] (but see [7] Appendix for a simplification of this last proof). The case k+1=3 was established by Roth in [7], but the method used there fails to generalize to larger k+1. Our present result is therefore new when  $k+1 \ge 4$ .

We shall make use of the Hammersley sequence (see [4]) and ideas from Halton's proof of a result (see [2]) which implies that for certain sets  $\mathscr P$  derived from the Hammersley sequence,

(1.3) 
$$\sup_{\alpha \in U_1^{k+1}} \left| D(\mathscr{P}; B(\alpha)) \right| < c(k) (\log |\mathscr{P}|)^k.$$

I am indebted to a copy of notes of lectures given by Prof. Wolfgang M. Schmidt (Boulder 1973) for an exposition of the proof of inequalities of type (1.3).

For further discussion and references, see [6], [7].

2. Notation. Although our final result concerns k+1 dimensional space, the k dimensional subspace corresponding to the first k coordinates will play an important role. Accordingly, we shall be dealing with both k dimensional vectors and k+1 dimensional vectors; we reserve bold type for vectors of either kind.

By an "interval" I we shall mean a half-open interval of type  $[a_1, a_2)$ . Thus, for some pair  $a_1, a_2$  satisfying  $a_1 < a_2$ , the interval I consists of all  $\beta$  satisfying  $a_1 \leq \beta < a_2$ .

Suppose  $k_1 = k$  or  $k_1 = k+1$ . We shall be concerned with boxes in  $k_1$  dimensional space of the type consisting of all points  $(\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(k_1)})$  satisfying  $\beta^{(j)} \in I^{(j)}$   $(j = 1, 2, \ldots, k_1)$ , where  $I^{(j)}$  is an interval  $[\alpha_1^{(j)}, \alpha_2^{(j)})$ . We shall use the Cartesian product  $I^{(1)} \times I^{(2)} \times \ldots \times I^{(k_1)}$  to represent such a box.

We use R to denote a residue class; or, more precisely, the set of all integers in a residue class. Thus, for some natural number q and some integer a, the set R consists of all integers congruent to a modulo q. For every real t, we use t+R to denote the set  $\{t+n; n \in R\}$ .

If t+R has the above meaning and I is an "interval" of the kind described, we define F[t+R;I] by

$$(2.1) F[t+R;I] = Z(t+R;I) - q^{-1}l(I),$$

where Z(t+R;I) denotes the number of elements of t+R falling into I, q is the modulus of the residue class R, and l(I) is the length of I. We note that

$$(2.2) |F[t+R;I]| \leq 1 \text{always.}$$

3. Preparatory definitions and remarks. Let h be a natural number, and let  $p_1, p_2, \ldots, p_k$  be the first k primes. We write

$$(3.1) M = M(h) = (p_1 p_2 \dots p_k)^h.$$

For n = 0, 1, ..., M-1 and for each j = 1, 2, ..., k, we express n in the scale  $p_j$  by writing

(3.2) 
$$n = \sum_{r=0}^{\infty} a_r^{(j)} p_j^r \quad (0 \leqslant a_r < p_j),$$

where  $\sum'$  signifies that there are only a finite number of non-zero terms in the sum. The  $a_r^{(j)}$  are of course uniquely determined by n. We write

(3.3) 
$$x_n^{(j)} = p_j^{-1} \sum_{r=0}^{\infty} a_r^{(j)} p_j^{-r}.$$

We note that the  $x_n^{(j)}$  lie in  $U_0$ . We write

$$(3.4) x_n = (x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(k)}).$$

The vectors

$$(3.5) x_0, x_1, ..., x_{M-1}$$

are the first M terms<sup>(2)</sup> of the Halton sequence.

We extend the range of definition of  $x_n$  over the set of all integers n so as to ensure that

$$(3.6) x_{n+M} = x_n for every integer n.$$

There is, of course, precisely one such extension of the set (3.5).

LEMMA 1. Suppose that I is a subinterval of  $U_0$  of the type

$$vp_j^{-s} \leqslant \beta < (v+1)p_j^{-s},$$

where v, s are integers and  $0 \le s \le h$ . Then the set of all those n for which  $x_n^{(j)}$  lies in I constitutes a residue class R modulo  $p_i^s$ .

Proof. When s=0 we must have  $I=U_0$  and the result is trivial, so we suppose s>0. For  $0 \le n < M$  the condition  $x_n^{(j)} \in I$  determines  $a_0^{(j)}, \ldots, a_{s-1}^{(j)}$  uniquely, but leaves the remaining  $a_r^{(j)}$  arbitrary. Since  $p_j^s$  is a divisor of the period M appearing in (3.6), the result follows.

In view of the above lemma it is convenient to introduce the following terminology.

DEFINITION. An interval  $[a_1, a_2)$  is said to be an elementary  $p_j$  type

<sup>(2)</sup> Strictly speaking, it is more customary to commence the Halton sequence with  $x_1$ .

interval of order s if  $a_1$ ,  $a_2$  are consecutive integer multiples of  $p_j^{-s}$ . We reserve the symbol J for elementary intervals.

For every real t we define the set  $\varOmega(t)=\varOmega(h,t)$  in k+1 dimensional space by

(3.7) 
$$\Omega(t) = \{(x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(k)}, n+t); n \in \mathbb{Z}\}.$$

In other words,  $\Omega(t)$  consists of all points  $(x_n, n+t)$  as n ranges through the integers.

Suppose B is a box in k+1 dimensional space of the type  $(I^{(1)} \times I^{(2)} \times ... \times I^{(k)}) \times I^*$ , where  $I^{(j)}$  is a subinterval of  $U_0$  (for  $j=1,\ldots,k$ ) and  $I^*$  is of the type [0, Y) where Y is positive (but otherwise unrestricted). We define  $E[\Omega(t); B]$  by

(3.8) 
$$E[\Omega(t); B] = Z(\Omega(t); B) - V(B),$$

where  $Z(\Omega(t); B)$  is the number of points of  $\Omega(t)$  falling into B and V(B) is the volume of B.

4. The basic result. We prove the following result from which Theorem 2 will be deduced in the subsequent section.

Basic Lemma. Let Y > 0 and, for each j = 1, 2, ..., k, let  $\eta^{(j)}$  be an integer multiple of  $p_j^{-h}$  lying in  $U_1$ . Let  $B^*$  be the box

$$B^*(\eta, Y) = I^{(1)} \times I^{(2)} \times \ldots \times I^{(k)} \times I^*.$$

where  $I^{(j)} = [0, \eta^{(j)})$  and  $I_{,j}^* = [0, Y)$ . Then

(4.1) 
$$\int_{0}^{M} |E[\Omega(t); B^{*}]|^{2} dt < (4h)^{k} (p_{1} \dots p_{k})^{2} M.$$

Proof. If  $\eta^{(j)} < 1$ , it can be seen by considering the expansion of  $\eta^{(j)}$  as a decimal in the scale  $p_j$  that  $I^{(j)}$  can be represented as a union of disjoint elementary  $p_j$  type intervals of various positive orders not exceeding h; the union being such that there are at most  $p_j-1$  intervals in the union having any given order. If  $\eta^{(j)}=1$ , we may think of  $I^{(j)}$  as being a union consisting of a single elementary interval of order 0.

Suppose that, in either event, the elementary intervals constituting the union are

$$J_1^{(j)}, J_2^{(j)}, \dots, J_{L_i}^{(j)}$$

of orders s(j, 1), s(j, 2), ...,  $s(j, L_j)$  respectively, and that the numbering is such that

$$s(j, 1) \leqslant s(j, 2) \leqslant \ldots \leqslant s(j, L_j).$$

In view of our above remarks, the situation is as follows.

LEMMA 2. Either  $L_i = 1$  and s(j, 1) = 0, or

$$(4.3) 1 \leqslant s(j,1) \leqslant s(j,2) \leqslant \ldots \leqslant s(j,L_i) \leqslant h$$

and there are at most  $p_j - 2$  consecutive equalities in (4.3) (not, of course, counting equalities possibly implicit in  $1 \leq s(j, 1)$  or  $s(j, L_j) \leq h$ ).

It follows from Lemma 1 that the *n* for which  $x_n^{(i)}$  lies in  $J_l^{(i)}$  form a residue class modulo  $p_i^{e(i,l)}$ ; we denote this residue class by  $R^{(i)}(l)$ .

For any given  $l_1, \ldots, l_k$  satisfying  $1 \leqslant l_j \leqslant L_j$   $(j = 1, \ldots, k)$ , the n for which  $x_n$  lies in the box

$$B_{l_1,\ldots,l_k} = J_{l_1}^{(1)} \times J_{l_2}^{(2)} \times \ldots \times J_{l_k}^{(k)}$$

constitute the residue class R(l) defined by

(4.4) 
$$R(l) = R(l_1, ..., l_k) = \bigcap_{j=1}^k R^{(j)}(l_j).$$

Thus, by (2.1), (3.7), (3.8) and the Chinese Remainder Theorem,

$$[E[\Omega(t); (B_{l_1,...,l_k}) \times I^*] = F[t + R(l_1,...,l_k); I^*].$$

It follows from what has been said above that

$$E[\mathit{Q}(t);\mathit{B}^*] = \sum_{l_1=1}^{L_1} \ldots \sum_{l_k=1}^{L_k} \!\! F[t\!+\!R(l);\mathit{I}^*].$$

Since  $I^*$  remains fixed throughout the proof of the Basic Lemma, we shall henceforth write simply F[t+R(l)] for  $F[t+R(l); I^*]$ . We now have

(4.5) 
$$\int_{0}^{M} |E[\Omega(t); B^{*}]|^{2} dt = \sum_{l=1}^{L_{1}} \dots \sum_{l'_{k}=1}^{L_{k}} \sum_{l''_{k}=1}^{L_{1}} \dots \sum_{l''_{k}=1}^{L_{k}} H(l', l''),$$

where

(4.6) 
$$H(l', l'') = \int_{0}^{M} F[t + R(l')] F[t + R(l'')] dt.$$

We consider the integrand on the right hand side of (4.6). For each j = 1, 2, ..., k, let

(4.7) 
$$q_{j}(l', l'') = \min(p_{j}^{s(j,l'_{j})}, p_{j}^{s(j,l'_{j})}),$$

(4.8) 
$$Q_{j}(l', l'') = \max(p_{j}^{s(j, l'_{j})}, p_{j}^{s(j, l'_{j})}),$$

and 
$$A_j(l', l'') = Q_j(l', l'')/q_j(l', l'')$$
. We note that

(4.9) 
$$A_i(l', l'') = p_i^d$$
, where  $d = |s(j, l_i') - s(j, l_i'')|$ .

Write

(4.10) 
$$M_{j} = Mp_{j}^{-h} = \prod_{\substack{i=1\\i\neq j}}^{k} p_{i}^{h} \quad (j = 1, 2, ..., k).$$

Since the integrand in (4.6) is periodic with period M in t, and M is the length of the range of integration, we are entitled (for any integer a) to replace t by

$$(4.11) t + a \mathcal{M}_1 q_1(\mathbf{l}', \mathbf{l}'')$$

in (4.6). After replacing t by (4.11) in (4.6), we shall sum over the values

$$(4.12)^{n} \qquad a = 1, 2, ..., A_1(l', l'').$$

We note that, since  $(M_1, p_1) = 1$ , as a runs through the set (4.12) the numbers  $aM_1q_1(l', l'')$  represent all the residue classes modulo  $Q_1(l', l'')$  that are congruent to 0 modulo  $q_1(l', l'')$ .

If  $R^{(j)}(l)$  is a residue class modulo  $p_j^{s(i,l)}$  of the type introduced earlier, and  $0 \le b \le s(j,l)$ , we denote by  $R^{(j)}(l;p_j^b)$  the (unique) residue class modulo  $p_j^b$  which contains  $R^{(j)}(l)$ . We denote by  $R_1(l'|l'')$  the modification of the residue class R(l') obtained by replacing  $R^{(1)}(l_1')$  by  $R^{(1)}[l_1';q_1(l',l'')]$  in the representation of  $R(l_1',\ldots,l_k')$  as an intersection of k residue classes with prime power moduli (whilst leaving the remaining k-1 residue classes in the intersection unchanged). Similarly  $R_1(l''|l')$  denotes the modification of the residue class R(l'') obtained by interchanging the roles of l' and l'' above.

Now if  $s(1, l'_1) \ge s(1, l''_1)$  the assertion (A') below is true.

$$F[t + a M_1 q_1(l', l'') + R(l'')] = F[t + R_1(l''|l')] \quad \text{ for every } a.$$

If  $s(1, l'_1) \leq s(1, l''_1)$ , the assertion (A''), obtained from (A') by interchanging the roles of l', l'', is true. (If  $s(1, l'_1) = s(1, l''_1)$  the assertions (A') and (A'') are of course identical.)

Thus, in any event,

$$(4.13) A_1(l', l'')H(l', l'') = H_1(l', l''),$$

where

(4.14) 
$$H_1(l', l'') = \int_0^M F[t + R_1(l'|l'')] F[t + R_1(l''|l')] dt.$$

We now replace t by  $t+aM_2q_2(l', l'')$  in (4.14) and sum over  $a=1, 2, \ldots, A_2(l', l'')$ . We obtain

$$A_2(l', l'')H_1(l', l'') = H_2(l', l''),$$

where

$$H_2(l',l'') = \int\limits_0^M F[t+R_{1,2}(l'|l'')]F[t+R_{1,2}(l''|l')]dt$$

and, for example,  $R_{1,2}(l'|l'')$  is the modification of the residue class  $R_1(l'|l'')$  obtained by replacing  $R^{(2)}(l_2')$  by  $R^{(2)}(l_2'; q_2(l', l''))$  in the representation of  $R_1(l'|l'')$  as an intersection of k residue classes with prime power moduli. After k applications of this procedure, we finally obtain

(4.15) 
$$H(l', l'') = P^{-1} \int_{0}^{M} F[t+R'] F[t+R''] dt,$$

where

(4.16) 
$$P = \prod_{j=1}^{k} A_{j}(l', l'')$$

and R', R'' are residue classes. We have already noted in (2.2) that  $|F(t+R)| \le 1$  for every real t and every residue class R. Thus, by (4.9), (4.5) yields

$$(4.17) M^{-1} \int_{0}^{M} |E[\Omega(t); B^*]|^2 dt \leqslant \sigma_1 \sigma_2 \dots \sigma_k,$$

where, for j = 1, 2, ..., k,

(4.18) 
$$\sigma_{j} = \sum_{l'_{j}=1}^{L_{j}} \sum_{l'_{j}=1}^{L_{j}} p_{j}^{-|s(j,l'_{j})-s(j,l''_{j})|}.$$

We write  $\sigma_j = \sum_b \sigma_{j,b}$ , where

$$\sigma_{j,b} = \sum_{l'_j=1}^{L_f} \sum_{l''_j=1}^{L_f} p_j^{-|s(j,l'_j)-s(j,l''_j)|},$$

$$(4.19)$$

the new condition of summation being

(4.19) 
$$\min(s(j, l_i), s(j, l_i')) = b.$$

If  $L_j=1$  we have  $\sigma_j=1$ , and if  $L_j>1$  it follows from Lemma 2 that

$$\sigma_{j} = \sum_{b=1}^{h} \sigma_{j,b} < 2h(p_{j}-1)^{2} \sum_{d=0}^{\infty} p_{j}^{-d} < 4hp_{j}^{2}.$$

Thus (4.17) yields the desired inequality (4.1).

5. Proof of Theorem 2. Let the natural number  $N \geqslant 2$  be given, and choose

$$(5.1) h = \lceil \log_2 N \rceil + 1,$$

(934)

so that

$$(5.2) N \leq p_j^h (j = 1, 2, ..., k).$$

For any  $\theta$  in  $U_1^k$ , and any real Y satisfying

$$(5.3) 0 < Y \leqslant N,$$

we use  $B^*(\theta, Y)$  to denote the Cartesian product of the k+1 intervals

$$[0, \theta^{(1)}), [0, \theta^{(2)}), ..., [0, \theta^{(k)}), [0, Y).$$

Write

(5.4) 
$$S(t; \theta, Y) = E[\Omega(t); B^*(\theta, Y)]$$

and

$$(5.5) T(t; \theta, \Upsilon) = S(t; \eta(\theta), \Upsilon),$$

where  $\eta = \eta(\theta)$  is defined by taking  $\eta^{(j)}$  to be the least integer multiple of  $p_j^{-h}$  that is not less than  $\theta^{(j)}$ . Written symbolically,

(5.6) 
$$\eta^{(j)}(\theta) = -p_j^{-h}[-p_j^h \theta^{(j)}] \quad (j = 1, ..., k).$$

It follows from the Basic Lemma that

(5.7) 
$$\int_{0}^{M} \int_{U_{1}^{k}}^{N} |T(t; \theta, Y)|^{2} dt d\theta dY \leq h^{k} MN,$$

where the implicit constant depends only on k.

For any fixed t,  $\theta$ , Y, we consider the effect on

(5.8) 
$$S(t; \theta^{(1)}, \theta^{(2)}, ..., \theta^{(k)}, Y)$$

of replacing  $\theta^{(1)}$  by  $\eta^{(1)}(\theta)$ , whilst leaving  $\theta^{(2)}, \ldots, \theta^{(k)}$  unchanged. On applying (5.4), we must recall the definition (3.8) of  $\mathcal{B}$ . The error introduced in

(5.9) 
$$Z(\Omega(t); B^*(\theta^{(1)}, \theta^{(2)}, ..., \theta^{(k)}, Y))$$

on replacing  $\theta^{(1)}$  by  $\eta^{(1)}(\theta)$  does not exceed the number of n in [-t, Y-t) for which  $x_n^{(1)}$  lies in

$$[\eta^{(1)}(\theta)-p_1^{-h}, \eta^{(1)}(\theta)].$$

Since this is an interval of the type to which Lemma 1 is applicable, it follows from Lemma 1 (with s = h) in conjunction with (5.2), (5.3) that the difference between

(5.10) 
$$Z(\Omega(t); B^*(\eta^{(1)}(\theta), \theta^{(2)}, ..., \theta^{(k)}, Y))$$

and (5.9) is at most 1. Again using (5.2), (5.3), we see that the increase in  $V(B^*)$  is also at most 1. Thus the absolute value of the error introduced in (5.8) is also at most 1.

Clearly, the above argument can also be used to show that the replacement of  $\theta^{(2)}$  by  $\eta^{(2)}(\theta)$  in (5.10) increases the value of the expression by at most 1; and so on. Thus on replacing  $\theta^{(1)}$ ,  $\theta^{(2)}$ , ...,  $\theta^{(k)}$  successively by  $\eta^{(1)}(\theta)$ ,  $\eta^{(2)}(\theta)$ , ...,  $\eta^{(k)}(\theta)$  in (5.8), we see that

$$|S(t, \theta, Y) - T(t, \theta, Y)| \leq k$$

for every t,  $\theta$ , Y relevant to (5.7). Since  $|S-T| \le k$  implies  $|S|^2 \le 2|T|^2 + 2k^2$ , it follows from (5.7) and (5.1) that there exists a real number  $t^*$ , satisfying  $0 \le t^* < M$ , such that

(5.11) 
$$\int_{U_1^k} \int_0^N |S(t^*, \theta, Y)|^2 d\theta dY \leq (\log N)^k N.$$

On recalling (5.4) and the definition (3.7) of  $\Omega(t)$ , we see from (5.11) that the set

$$\mathscr{P} = \{(x_n^{(1)}, x_n^{(2)}, \ldots, x_n^{(k)}, N^{-1}(n+t^*)); \ 0 \leqslant n+t^* < N\}$$

fulfils the requirements of Theorem 2.

## References

- H. Davenport, Note on irregularities of distribution, Mathematika 3 (1956), pp. 131-135.
- [2] J. H. Halton, On the efficiency of certain quasirandom sequences of points in evaluating multidimensional integrals, Num. Math. 2 (1960), pp. 84-90.
- [3] J. H. Halton and S. K. Zaremba, The extreme and L<sup>2</sup> discrepancies of some plane sets, Monatsch. Math. 73 (1969), pp. 316-328.
- [4] J. M. Hammersley, Monte Carlo methods for solving multivariable problems, Ann. New York Acad. Sci. 86 (1960), pp. 844-874.
- [5] K. F. Roth, On irregularities of distribution, Mathematika 1 (1954), pp. 73-79.
- [6] On irregularities of distribution, II, Comm. Pure Appl. Math. 29 (1976), pp. 749-754.
- [7] On irregularities of distribution, III, Acta Arith. 35 (1979), pp. 373-384.
- [8] I. V. Vilenkin, Plane nets of integration (in Russian), Ž. Vyčisl. Mat. i Mat. Fiz. 7 (1967), pp. 189-196; Engl. transl. in U.S.S.R. Comp. Math. and Phys. 7 (1) (1967), pp. 258-267,

IMPERIAL COLLEGE London, S.W. 7, England