ON IRREGULARITIES OF DISTRIBUTION

W. W. L. CHEN

§1. Introduction. Let $U_0 = [0, 1)$ and $U_1 = (0, 1]$. Suppose we have a distribution $\mathcal{P}$ of $N$ points in $U_0^{k+1}$, where, for $k \geq 1$, $U_0^{k+1}$ is the unit cube consisting of the points $y = (y_1, ..., y_{k+1})$ with $0 \leq y_i < 1$ ($i = 1, ..., k+1$). For $x = (x_1, ..., x_{k+1})$ in $U_1^{k+1}$, let $B(x)$ denote the box consisting of all $y$ such that $0 \leq y_i < x_i$ ($i = 1, ..., k+1$), and let $Z[\mathcal{P}; B(x)]$ denote the number of points of $\mathcal{P}$ which lie in $B(x)$. Write

$$D[\mathcal{P}; B(x)] = Z[\mathcal{P}; B(x)] - N x_1 \cdots x_{k+1}.$$ 

The irregularity of the distribution $\mathcal{P}$ can be measured in a number of ways by the behaviour of the function $D[\mathcal{P}; B(x)]$. One may consider the $L^w$-norm

$$\|D(\mathcal{P})\|_w = \left( \int_{U_1} \cdots \int_{U_1} |D(\mathcal{P}; B(x))|^w dx_1 \cdots dx_{k+1} \right)^{1/w}.$$ 

Roth [3] obtained a lower bound for the $L^2$-norm, and Schmidt [7] established the following generalization, Roth's result being the special case $W = 2$.

**Theorem 1.** (Schmidt [7]). For every $W > 1$, there exists a positive number $c_1(k, W)$, depending only on $k$ and $W$, such that

$$\|D(\mathcal{P})\|_w > c_1(k, W)(\log N)^k.$$ 

Roth's lower bound for the $L^2$-norm has been shown to be sharp, apart from the value of the constant. This was established in the special cases $k = 1$ and $k = 2$ by Davenport [1] and Roth [5] respectively, and more recently for arbitrary $k$ by Roth [6]. Different proofs for the case $k = 1$ were given by Vilenkin [8], Halton and Zaremba [2] and Roth [4].

The object of this paper is to show that Schmidt's lower bound, given in Theorem 1 above, is also sharp, apart from the value of the constant. Accordingly, we shall prove the following theorem.

**Theorem 2.** Let $W > 0$. For a suitable number $c_2(k, W)$, depending only on $k$ and $W$, there exists, corresponding to every natural number $N \geq 2$, a distribution $\mathcal{P}$, which may depend on $W$, of $N$ points in $U_0^{k+1}$ such that

$$\|D(\mathcal{P})\|_w < c_2(k, W)(\log N)^k.$$ 

The two-dimensional case, $k = 1$, of Theorem 2 can easily be deduced from the argument in Roth [4]. On the other hand, since the $L^w$-norm increases with $W$, the
case $W \leq 2$ of Theorem 2 follows immediately as a consequence of Roth [6]. Our result is therefore new only when $k \geq 2$, $W > 2$.

Our method is, as in Roth [6], based on the consideration of “translations” of the Hammersley (Halton) sequence, an average with respect to such translations being taken over a “long” interval. In the application of the Main Lemma to deduce Theorem 2 (see §7), the set $\Omega = \Omega^{(1)}$ is chosen in terms of the Hammersley (Halton) sequence† exactly as in [6]. With this choice of $\Omega$, Roth's “Basic Lemma” in [6] is the case $W = 2$ of our Main Lemma. However, to prove the Main Lemma, new ideas are required to overcome difficulties that did not arise in the case $W = 2$. The proof of the Main Lemma is new, and is based on the use of induction which was not needed in the special case $W = 2$ dealt with by Roth in [6]. To make the induction work, we have to make use of sequences (sets) (see §3) which are of a more general nature than the Hammersley (Halton) sequence, whilst retaining its relevant properties. We therefore have to introduce a wider class of sets $\Omega$ to give a formulation of our Main Lemma suitable for proof by induction. We also remark that the derivation of Lemma 5, a key identity in the proof of the Main Lemma, requires an elaboration of the idea underlying Roth's proof of his Basic Lemma (see (24) and (36)).

I am greatly indebted to Professor Roth for his constant encouragement and helpful suggestions, and for giving me manuscripts of his papers [5] and [6]. I also thank the referee for his valuable comments.

§2. Notation. By an interval $I$, we shall mean a half-open interval of the type $[\alpha_1, \alpha_2)$, while $I_1 \times I_2$ denotes the Cartesian product of $I_1$ and $I_2$.

We use $R$ to denote a residue class. In particular, $R(m, q)$ denotes the residue class of integers congruent to $m$ modulo $q$. For any real number $t$, we denote by $t + R$ the set $\{t + n : n \in R\}$, and write

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

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 $\ell(I)$ is the length of $I$. It is obvious that

$$|F[t + R ; I]| \leq 1$$

always.

Throughout, $\mathbb{Z}$ denotes the set of all integers.

§3. Generalization of the idea of the Hammersley (Halton) sequence. Let $h$ be a positive integer, and let $p_1, \ldots, p_k$ be distinct primes. For any integer $n$ satisfying $0 \leq n < (p_1 \ldots p_k)^h$ and for every $j = 1, \ldots, k$, write

$$n = \sum_{v=0}^{\alpha} a_{j,v} p_j^v \quad (0 \leq a_{j,v} < p_j),$$

where $\sum'$ signifies that there is only a finite number of non-zero terms in the sum. I
is clear that the integers \( a_{j,v} \) are uniquely determined by \( n \). We write

\[
X_j(n) = p_j^{-1} \sum_{v=0}^{\infty} a_{j,v} p_j^{-v}.
\]

Then \( X_j(n) \) lies in \( U_0 \). Let

\[
X(n) = (X_1(n), \ldots, X_k(n)).
\]

Then the vectors

\[
X(0), \ldots, X((p_1 \ldots p_k)^h - 1)
\]

are the first \((p_1 \ldots p_k)^h\) terms of the Hammersley (Halton) sequence. We extend the range of definition of \( X(n) \) over the set \( \mathbb{Z} \) of all integers by periodicity so as to ensure that

\[
X(n + (p_1 \ldots p_k)^h) = X(n)
\]

for every integer \( n \). In [6], Roth considered the set

\[
\Omega(t) = \{(X(n), n+t) : n \in \mathbb{Z}\},
\]

where \((X(n), n+t)\) stands for the point \((X_1(n), \ldots, X_k(n), n+t)\) in \((k+1)\)-dimensional space.

In this paper, we need to consider sets which are of a more general nature than (3). Let \( h \) be a positive integer, and let \( p_1, \ldots, p_k \) be distinct primes. We define a \( q \)-set of class \( h \) with respect to the primes \( p_1, \ldots, p_k \). Let \( 1 \leq j \leq k \).

**Definition.** Let \( 0 \leq s \leq h \). An interval \([\alpha_1, \alpha_2]\) is said to be an elementary \( p_j \)-type interval of order \( s \) if \( \alpha_1, \alpha_2 \) are consecutive integer multiples of \( p_j^{-s} \), and \([\alpha_1, \alpha_2]\) is contained in \( U_0 \).

We reserve the symbol \( J \) for elementary intervals.

By an association of order \( h \) with respect to the prime \( p_j \), we shall mean the following. We associate each elementary \( p_j \)-type interval of order \( s \) with a residue class modulo \( p_j^s \) in such a way that if \( J_1 \) and \( J_2 \) are elementary \( p_j \)-type intervals, of orders \( s_1 \) and \( s_2 \) respectively, where \( 0 \leq s_2 \leq s_1 \leq h \), and if \( R_1 \) and \( R_2 \) are respectively their associated residue classes, then

\[
J_1 \subset J_2 \iff R_1 \subset R_2.
\]

Since either \( J_1 \subset J_2 \) or \( J_1 \cap J_2 = \emptyset \), and a similar relation applies to \( R_1 \) and \( R_2 \), we see, in particular, that this association sets up a one-to-one correspondence between the collection of elementary \( p_j \)-type intervals of order \( s \) and the collection of residue classes modulo \( p_j^s \) for every \( s \) satisfying \( 0 \leq s \leq h \).

Let \( Q \) be a residue class modulo \( q \), where \((q, p_1 \ldots p_k) = 1\), and suppose \( X = \{x(n) : n \in Q\} \) is a set, where for each \( n \in Q \), \( x(n) = (x_1(n), \ldots, x_k(n)) \) is a point in \( U_0 \). Consider the set

\[
\Omega(Q, X) = \{(x(n), n) : n \in Q\}.
\]

We are concerned with sets of the form (5) and having a very special property.

Our next definition is motivated by a special property of \( \Omega(0) \), where \( \Omega(t) \) is the set (3).
Definition. Suppose $\mathcal{X}$ is such that, for every integer $j = 1, \ldots, k$, we can define an association between elementary $p_j$-type intervals and residue classes modulo $p_j$ ($0 \leq s \leq h$) as follows. Given any residue class $R$ modulo $p_j$, where $0 \leq s \leq h$, there exists an elementary $p_j$-type interval $J$ of order $s$ such that $\{x(n) : n \in \mathbb{Q} \cap R\} \subset J$; in other words, the $j$-th coordinates of those points $x(n)$, for which $n$ belongs to a residue class modulo $p_j$, as well as $\mathbb{Q}$, all fall into the same elementary $p_j$-type interval of order $s$. We associate $J$ with $R$. Suppose further that, for every $j = 1, \ldots, k$, the corresponding association is of order $h$ with respect to the prime $p_j$; in other words, that for every $j = 1, \ldots, k$, the set $\mathcal{X}$ sets up an association of order $h$ with respect to the prime $p_j$. Then we say that $\Omega(Q, \mathcal{X})$ is a $q$-set of class $h$ with respect to the primes $p_1, \ldots, p_k$.

We note that, given any $q$-set $\Omega(Q, \mathcal{X})$ of class $h$ with respect to the primes $p_1, \ldots, p_k$, the association of order $h$ with respect to each prime is uniquely determined.

For the sake of simplicity, since it is important only to bear in mind the modulus $q$ of the residue class $Q$ when considering sets of the type $\Omega(Q, \mathcal{X})$, we write $\Omega(q)$ for $\Omega(Q, \mathcal{X})$. We shall consider sets of the form

$$\Omega(q)(t) = \Omega(Q, \mathcal{X}; t) = \{(x(n), n + t) : n \in \mathcal{Q}\}.$$  

Note that $\Omega(q)(0)$ is the set (5).

Definition. Suppose $\Omega(q)$ is a $q$-set of class $h$ with respect to the primes $p_1, \ldots, p_k$; and suppose $t$ is any real number. We say that the set $\Omega(q)(t)$ is a translated $q$-set of class $h$ with respect to the same primes.

It is clear that the set (3) given by the Hammersley (Halton) sequence is a translated 1-set of class $h$ with respect to the primes $p_1, \ldots, p_k$. Furthermore, if $Q$ is a residue class modulo $q$, where $(q, p_1 \cdots p_k) = 1$, the subset $\{(x(n), n + t) : n \in \mathcal{Q}\}$ of (3) is a translated $q$-set of class $h$ with respect to the primes $p_1, \ldots, p_k$. On the other hand, the following lemmas are obvious.

**Lemma 1.** Suppose $\Omega(q)(t)$ is a translated $q$-set of class $h$ with respect to the primes $p_1, \ldots, p_k$. Then, for every $s$ satisfying $1 \leq s \leq h$, $\Omega(q)(t)$ is also a translated $q$-set of class $s$ with respect to the same primes.

**Lemma 2.** Suppose $\Omega(q)(t)$ is a translated 1-set of class $h$ with respect to the primes $p_1, \ldots, p_k$. Then, for every $j = 1, \ldots, k$, the set

$$\{(x_1(n), \ldots, x_{j-1}(n), x_{j+1}(n), \ldots, x_k(n), n + t) : n \in \mathbb{Z}\}$$

is a translated 1-set of class $h$ with respect to the primes $p_1, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k$. On the other hand, if $R_j$ is a residue class modulo $q$, where $(q, p_1 \cdots p_k) = 1$, then the set $\{(x(n), n + t) : n \in \mathcal{R}_j\}$ is a translated $q$-set with respect to the primes $p_1, \ldots, p_k$.

Suppose $B = I_1 \times \cdots \times I_k \times I^*$, where $I_j \subset U_0$ ($1 \leq j \leq k$) and $I^*$ is of the type $[0, Y)$, where $Y$ is positive but otherwise unrestricted. For any $\Omega(q)(t)$ with respect to the primes $p_1, \ldots, p_k$, we define $E[\Omega(q)(t); B]$ by

$$E[\Omega(q)(t); B] = \mathbb{Z}[\Omega(q)(t); B] - q^{-1} V(B),$$

where $V(B)$ is the volume of $B$.
where $Z[\Omega^{(q)}(t) ; B]$ is the number of points of $\Omega^{(q)}(t)$ falling into $B$, and $V(B)$ is the volume of $B$. Note that $q^{-1}V(B)$ is the “expected number” of points of $\Omega^{(q)}(t)$ falling into $B$. The analogues of (7) in lower-dimensional cases are defined in the same way.

It is clear that if $B = B_1 \cup B_2$, where $B_1 \cap B_2 = \emptyset$, then

$$E[\Omega^{(q)}(t) ; B] = E[\Omega^{(q)}(t) ; B_1] + E[\Omega^{(q)}(t) ; B_2].$$

(8)

Definition. Let $0 \leq s \leq h$. Suppose further that, for each $j = 1, \ldots, k$, $I_j = [0, \eta_j)$, where $0 < \eta_j \leq 1$ and $\eta_j$ is an integer multiple of $p_j^{-s}$. Then we say that $B$ is a box of class $s$ with respect to the primes $p_1, \ldots, p_k$.

We reserve the symbol $B^*$ for such boxes.

Lemma 3. Suppose $\Omega^{(q)}$ is a $q$-set of class $h$ with respect to the primes $p_1, \ldots, p_k$, where $(q, p_1 \cdots p_k) = 1$; and suppose $B^*$ is a box of class $s$ with respect to the same primes, where $0 \leq s \leq h$. Then the function $E[\Omega^{(q)}(t) ; B^*]$ is periodic in $t$ with period $q(p_1 \cdots p_k)^s$.

Proof. Since $B^*$ is a box of class $s$ with respect to the primes $p_1, \ldots, p_k$, $B^*$ is a finite and mutually disjoint union of boxes of the type $B = J_1 \times \cdots \times J_k \times I^*$, where, for $j = 1, \ldots, k$, $J_j$ is an elementary $p_j$-type interval of order $s$. By (8), it suffices to prove Lemma 3 with $B^*$ replaced by such a box $B$. Consider, for any $j = 1, \ldots, k$, the set $Q_j = \{ n \in Q : x_j(n) \in J_j \}$. Then $Q_j = Q \cap R_j$, where $R_j$ is the associated residue class (modulo $p_j^s$) of $J_j$. By the Chinese Remainder Theorem, the set $R_1 \cap \cdots \cap R_k = R$ say, is a residue class modulo $(p_1 \cdots p_k)^s$. Since $(q, p_1 \cdots p_k) = 1$, we see that $Q \cap R$ is a residue class modulo $q(p_1 \cdots p_k)^s$. It follows from (1), (6) and (7) that for the above $B$,

$$E[\Omega^{(q)}(t) ; B] = F[t + (Q \cap R) ; I^*].$$

The proof of Lemma 3 is now complete, since $F[t + (Q \cap R) ; I^*]$ is clearly periodic with the desired period.

§4. Statement of the basic result and an important identity. In this section and the next two, we establish the following result from which Theorem 2 will be deduced in §7. We also assume that $W$ is an even positive integer. Let

$$M = p_1 \cdots p_k;$$

(9)

and, for $j = 1, \ldots, k$, write

$$M_j = p_1 \cdots p_{j-1} p_{j+1} \cdots p_k = Mp_j^{-1}.$$

(10)

Main Lemma. For a suitable constant $C(p_1, \ldots, p_k, W)$, depending only on $W$ and the primes $p_1, \ldots, p_k$, we have, for any $1$-set $\Omega^{(1)}$ of class $h$ with respect to the primes $p_1, \ldots, p_k$, and, for any box $B^*$ of class $h$ with respect to the same primes,

$$\int_0^M E[\Omega^{(1)}(t) ; B^*]^W dt \leq C(p_1, \ldots, p_k, W)M^h h^{khW}.$$  

(11)
The Main Lemma is in fact equivalent to the following superficially more general form.

**Alternative Form of the Main Lemma.** For the same constant \( C(p_1, \ldots, p_k, W) \) as in the Main Lemma, for any \( q \)-set \( \Omega^{(q)} \) of class \( h \) with respect to the primes \( p_1, \ldots, p_k \), where \( (q, p_1 \cdots p_k) = 1 \), and for any box \( B^* \) of class \( h \) with respect to the same primes, we have

\[
\int_0^{qM^h} E[\Omega^{(q)}(t) ; B^*]^w \, dt \leq C(p_1, \ldots, p_k, W)qM^h h^{\frac{1}{2}W}.
\]  

(12)

To see this equivalence, we first note that if \( \Omega^{(q)}(t) = \Omega(Q, \mathcal{X} ; t) \), where \( Q \) is the residue class \( n_0 \) modulo \( q \), then, by Lemma 3, the left-hand side of (12) is equal to

\[
q \int_0^{M^h} E[\Omega(Q, \mathcal{X} ; qt - n_0) ; B^*]^w \, dt,
\]

where \( \Omega(Q, \mathcal{X} ; qt - n_0) = \{(x(n), n - n_0 + qt') : n \in Q\} \). We now define \( \Omega(Z, \mathcal{X}' ; t') = \{(x'(n'), n' + t') : n' \in \mathbb{Z}\} \) by writing, for each \( n' \in \mathbb{Z} \),

\[
x'(n') = x(n_0 + qn'),
\]

so that

\[
\{(x(n), q^{-1}(n - n_0) + t') : n \in Q\} = \{(x'(n'), n' + t') : n' \in \mathbb{Z}\}.
\]  

(13)

Let \( (B')^* \) be derived from \( B^* = I_1 \times \cdots \times I_k \times [0, Y) \) by writing \( (B')^* = I_1 \times \cdots \times I_k \times [0, q^{-1} Y) \). It now suffices to show that \( \Omega(Z, \mathcal{X}' ; t') \) is a translated \( 1 \)-set of class \( h \) with respect to the primes \( p_1, \ldots, p_k \), so that by (7) and (13),

\[
E[\Omega(Q, \mathcal{X} ; qt - n_0) ; B^*] = Z[\Omega(Q, \mathcal{X} ; qt - n_0) ; B^*] - q^{-1} V(B^*)
\]

\[
= Z[\Omega(Z, \mathcal{X}' ; t') ; (B')^*] - V((B')^*)
\]

\[
= E[\Omega(Z, \mathcal{X}' ; t') ; (B')^*],
\]

and our argument is complete. It now remains to show that, for any \( j = 1, \ldots, k \), the set \( \mathcal{X}' = \{x'(n') : n' \in \mathbb{Z}\} \) sets up an association of order \( h \) with respect to the prime \( p_j \). In other words, we have to show that for any \( j = 1, \ldots, k \) and for any \( s \) satisfying \( 0 \leq s \leq h \), the set of those integers \( n' \) for which \( x'(n') \) falls into any fixed elementary \( p_j \)-type interval \( J \) of order \( s \) constitutes a residue class modulo \( p_j^s \). Since \( \Omega(Q, \mathcal{X}) \) is a \( q \)-set of class \( h \) with respect to the primes \( p_1, \ldots, p_k \), the set of those \( n \in Q \) for which \( x_j(n) \) falls into \( J \) is contained in a residue class \( R \) modulo \( p_j^s \). Then it is clear that

\[
\{n' : x_j(n') \in J\} = \{n' : n_0 + qn' \in Q \wedge x_j(n_0 + qn') \in J\}
\]

\[
= \{n' : n_0 + qn' \in Q \cap R\},
\]

where \( Q \cap R \) is a residue class modulo \( q p_j^s \). Furthermore,

\[
n_0 + qn' \in Q \cap R \iff n' \in R',
\]
where $R'$ is some residue class modulo $p^j$.

To prove the Main Lemma, we induce on $h$. For $k \geq 2$, we also make use of the corresponding results in a lower-dimensional case. We therefore begin by investigating some properties of $\Omega^{(1)}$ and $B^*$.

Let $\mathcal{A} = \{x(n) : n \in \mathbb{Z}\}$ be any arbitrary set such that the set $\Omega = \Omega^{(1)}$ defined by (5) is a 1-set of class $h$ with respect to the primes $p_1, \ldots, p_k$. We keep this set $\mathcal{A}$ fixed throughout.

Suppose
\[ B^* = B^*(\eta, Y) = [0, \eta_1) \times \ldots \times [0, \eta_k) \times [0, Y) \]  

is a box of class $h$ with respect to the primes $p_1, \ldots, p_k$. For $j = 1, \ldots, k$ and $s = 0, \ldots, h$, let $\xi_{j,s}$ denote the greatest integer multiple of $p_j^{-s}$ not exceeding $\eta_j$; furthermore, for $s \neq 0$, write
\[ v_{j,s} = p_j^s(\xi_{j,s} - \xi_{j,s-1}) . \]

Then $v_{j,s}$ is an integer and $0 \leq v_{j,s} < p_j$ for $j = 1, \ldots, k$ and $s = 1, \ldots, h$. Let
\[ I^* = [0, Y) . \]

For $s = 0, \ldots, h$, let
\[ B^*_s = [0, \xi_{1,s}) \times \ldots \times [0, \xi_{k,s}) \times I^* , \]

so that $B^*_s$ is the largest box of class $s$ with respect to the primes $p_1, \ldots, p_k$ which is contained in $B^*$. We now consider the complement of $B^*_{s-1}$ in $B^*_s$. We let $B^*_{1,s}$ denote the part of this which is contained in $[\xi_{1,s-1}, \xi_{1,s}) \times [0, 1]^{k-1} \times I^*$, $B^*_{2,s}$ denote the part of the remainder which is contained in $[0, 1) \times [\xi_{2,s-1}, \xi_{2,s}) \times [0, 1]^{k-2} \times I^*$, and so on. In other words, for $j = 1, \ldots, k$ and $s = 1, \ldots, h$, we let
\[ B^*_{j,s} = [0, \xi_{1,s-1}) \times \ldots \times [0, \xi_{j-1,s-1}) \times [\xi_{j,s-1}, \xi_{j,s}) \times [0, 1]^{k-j} \times I^* , \]

Then, it follows that, for $s = 1, \ldots, h$,
\[ B^*_s = B^*_{s-1} \cup B^*_{1,s} \cup \ldots \cup B^*_s , \]

and that the union is pairwise disjoint; so it follows from (8) that, for $s = 1, \ldots, h$,
\[ E[\Omega(t); B^*_{s-1}] + \sum_{j=1}^k E[\Omega(t); B^*_{j,s}] . \]

If, for some $j, s$ with $1 \leq j \leq k$ and $1 \leq s \leq h$, $B^*_{j,s} = \emptyset$, then obviously $E[\Omega(t); B^*_{j,s}] = 0$, and we may omit reference to $E[\Omega(t); B^*_{j,s}]$ in (19). So we may suppose that all $B^*_{j,s}$ are non-empty. Then the interval $[\xi_{j,s-1}, \xi_{j,s})$ in (17) is a union of exactly $v_{j,s}$ disjoint elementary $p_j$-type intervals of order $s$. We denote them by $J_{j,s,a}$ ($a = 1, \ldots, v_{j,s}$), and, for future reference, we suppose they correspond
respectively to the residue classes $R(m(j, s, \alpha), p_j^s)$. For $\alpha = 1, \ldots, v_{j,s}$, we write

$$B_{j,s,\alpha} = [0, \xi_{1,s-1}] \times \ldots \times [0, \xi_{j-1,s-1}] \times J_{j,s,\alpha} \times [0, \xi_{j+1,s}] \times \ldots \times [0, \xi_{k,s}] \times I^*.$$  \hfill (20)

Then we see that, for $j = 1, \ldots, k$ and $s = 1, \ldots, h$,

$$B_{j,s} = \bigcup_{\alpha = 1}^{v_{j,s}} B_{j,s,\alpha},$$

and the union is pairwise disjoint, so that by (8),

$$E[\Omega(t); B_{j,s}] = \sum_{\alpha = 1}^{v_{j,s}} E[\Omega(t); B_{j,s,\alpha}].$$ \hfill (21)

For $j = 1, \ldots, k$ and $s = 1, \ldots, h-1$, let

$$\bar{J}_{j,s} = \left[\xi_{j,s}, \xi_{j,s} + p_j^{-s}\right),$$ \hfill (22)

so that $\bar{J}_{j,s}$ is the elementary $p_j$-type interval of order $s$ containing the complement of $[0, \xi_{j,s}]$ in $[0, \eta_j]$. We modify $B_{j,h}$ (see (17) with $s = h$) by replacing $[\xi_{{j},h-1}, \xi_{j,h})$ by $\bar{J}_{j,s}$, which is the elementary $p_j$-type interval of order $s$ containing $[\xi_{{j},h-1}, \xi_{j,h})$. Accordingly, for $j = 1, \ldots, k$ and $s = 1, \ldots, h-1$, we let the modification $\bar{B}_{j,s}$ be defined by

$$\bar{B}_{j,s} = [0, \xi_{1,h-1}] \times \ldots \times [0, \xi_{j-1,h-1}] \times \bar{J}_{j,s} \times [0, \xi_{j+1,h}] \times \ldots \times [0, \xi_{k,h}] \times I^*.$$ \hfill (23)

Note that $B_{j,h}$ has $h-1$ modifications, namely $\bar{B}_{j,1}, \ldots, \bar{B}_{j,h-1}$.

Our next lemma contains the key idea underlying Roth's proof of his Basic Lemma in [6].

**Lemma 4.** For $j = 1, \ldots, k$ and for $\alpha = 1, \ldots, v_{j,h}$, we have

$$\sum_{a = 0}^{p_j-1} E[\Omega(t + aM_j^hp_j^{-1}); B_{j,h,\alpha}] = E[\Omega(t); \bar{B}_{j,h-1}].$$ \hfill (24)

Also, for $j = 1, \ldots, k$ and $s = 2, \ldots, h-1$, we have

$$\sum_{a = 0}^{p_j-1} E[\Omega(t + aM_j^hp_j^{-1}); \bar{B}_{j,s}] = E[\Omega(t); \bar{B}_{j,s-1}].$$ \hfill (25)

**Proof.** We first prove (24). Recall the definitions of $B_{j,h,\alpha}$ (see (20) with $s = h$) and $\bar{B}_{j,h-1}$ (see (23) with $s = h-1$). We note that the only difference is that $J_{j,h,\alpha}$ in the former is replaced by $\bar{J}_{j,h-1}$ in the latter. By (22), we see that $\bar{J}_{j,h-1}$ is the elementary $p_j$-type interval of order $h-1$ containing $J_{j,h,\alpha}$. Hence, by (4), the associated residue class $R(m(j, h, \alpha), p_j^s)$ of $J_{j,h,\alpha}$ is contained in the associated
residue class, \( R_0 \) say, of \( J_{j, h-1} \). So \( R_0 \) is the residue class modulo \( p_j^{h-1} \) containing \( R(m(j, h, \omega), p_j^h) \). Let \( J_i, i = 1, \ldots, j-1, j+1, \ldots, k, \) denote any elementary \( p_t \)-type interval of order \( h \). Then we see that, since \([0, \xi_{i,h-1})\) and \([0, \xi_{i,h})\) are the union of a finite number of mutually disjoint intervals of the type \( J_1 \), it follows from (8) that to prove (24), it suffices to prove that

\[
\sum_{a=0}^{p_j-1} E[\Omega(t + aM_j^h p_j^{h-1}) ; J_1 \times \cdots \times J_{j-1} \times J_{j,h,A} \times J_{j+1} \times \cdots \times J_k \times I^*] = E[\Omega(t) ; J_1 \times \cdots \times J_{j-1} \times J_{j,h} \times J_{j+1} \times \cdots \times J_k \times I^*].
\] (26)

For \( i = 1, \ldots, j-1, j+1, \ldots, k, \) let \( R_i \) denote the associated residue class of \( J_i \). Then the summand on the left-hand side of (26) is, by (1) and (7), equal to

\[
F[(t + aM_j^h p_j^{h-1}) + \left( R_1 \cap \cdots \cap R_{j-1} \cap R(m(j, h, \omega), p_j^h) \cap R_{j+1} \cap \cdots \cap R_k \right) ; I^*] = F\left[ t + \left( R_1 \cap \cdots \cap R_{j-1} \cap \left( aM_j^h p_j^{h-1} + R(m(j, h, \omega), p_j^h) \right) \cap R_{j+1} \cap \cdots \cap R_k \right) ; I^* \right].
\] (27)

On the other hand,

\[
\bigcup_{a=0}^{p_j-1} \left( aM_j^h p_j^{h-1} + R(m(j, h, \omega), p_j^h) \right) = R_0.
\] (28)

It follows from (27) and (28) that the left-hand side of (26), and so also the right-hand side, is equal to

\[
F[t + (R_1 \cap \cdots \cap R_{j-1} \cap R_0 \cap R_{j+1} \cap \cdots \cap R_k) ; I^*].
\]

This completes the proof of (24). Equation (25) follows similarly, for if \( R_s \) and \( R_{s-1} \) are respectively the associated residue classes of \( J_{j,s} \) and \( J_{j,s-1} \), then the analogue of (28) is

\[
\bigcup_{a=0}^{p_j-1} \left( aM_j^h p_j^{s-1} + R_s \right) = R_{s-1}.
\]

This completes the proof of Lemma 4.

For \( s = 1, \ldots, h \), write, for the sake of simplicity,

\[
G_s(t) = \sum_{j=1}^{k} E[\Omega(t) ; B_{j,s}] .
\] (29)

Let

\[
T_0 = \int_0^{M_j^h} E[\Omega(t) ; B_{h-1}^*] \, dt ;
\] (30)
and, for \( w = 2, \ldots, W \),

\[
T_w = \int_0^{M^h} E[\Omega(t) ; B_{h-1}^*]^{W-w} G_h^w(t) dt .
\] (31)

For \( j = 1, \ldots, k \), we write

\[
S_j = \int_0^{M^h} E[\Omega(t) ; B_j^*]^{W-1} E[\Omega(t) ; B_{j,1}] dt ;
\] (32)

further, for \( s = 1, \ldots, h-1 \) and \( w = 1, \ldots, W-1 \), we write

\[
S_{j,s,w} = \int_0^{M^h} E[\Omega(t) ; B_{s-1}^*]^{W-w-1} G_s^w(t) E[\Omega(t) ; B_{j,s}] dt .
\] (33)

Our proof of the Main Lemma is based on the following identity.

**Lemma 5.** We have, for \( h \geq 2 \), that

\[
\int_0^{M^h} E[\Omega(t) ; B^*]^W dt = T_0 + \sum_{w=2}^W \binom{W}{w} T_w + W \sum_{j=1}^k v_{j,h} p_j^{-(h-1)} S_j
\]

\[+ W \sum_{j=1}^k v_{j,h} \sum_{s=1}^{h-1} p_j^{-(h-s)} \sum_{w=1}^{W-1} \binom{W-1}{w} S_{j,s,w} .
\] (34)

**Proof.** We note, by (14), (15) and (16), that \( B^* = B^*_1 \); so, by taking \( W \)-th powers on both sides of (19) with \( s = h \), and using binomial expansion on the right-hand side, we have, in view of (29),

\[
E[\Omega(t) ; B^*]^W = E[\Omega(t) ; B_{h-1}^*]^W + W \sum_{j=1}^k E[\Omega(t) ; B_{h-1}^*]^{W-1} E[\Omega(t) ; B_{j,h}]
\]

\[+ \sum_{w=2}^W \binom{W}{w} E[\Omega(t) ; B_{h-1}^*]^{W-w} G_h^w(t) .
\]

By (30) and (31), we see that to prove Lemma 5, it remains to show that, for \( j = 1, \ldots, k \),

\[
\int_0^{M^h} E[\Omega(t) ; B_{h-1}^*]^{W-1} E[\Omega(t) ; B_{j,h}] dt
\]

\[= v_{j,h} p_j^{-(h-1)} S_j + v_{j,h} \sum_{s=1}^{h-1} p_j^{-(h-s)} \sum_{w=1}^{W-1} \binom{W-1}{w} S_{j,s,w} .
\] (35)
Now since $B^*_h - 1$ is a box of class $h - 1$ with respect to the primes $p_1, \ldots, p_k$, we know, by Lemma 3, that $E[\Omega(t); B^*_h - 1]$ is periodic in $t$ with period $M^{h - 1}$, and therefore also periodic with period $M^s p_j^{h - 1}$, for every $j = 1, \ldots, k$. So, by (21) with $s = h$ and (24), we have, for $j = 1, \ldots, k$ and writing $V_j$ for the left-hand side of (35),

$$V_j = \sum_{x = 1}^{M^h} E[\Omega(t); B^*_h - 1]^{w - 1} E[\Omega(t); B_{j, h}] dt$$

$$= v_{j, h} p_j^{-1} \int_0^{M^h} E[\Omega(t); B^*_h - 1]^{w - 1} E[\Omega(t); B_{j, h - 1}] dt . \quad (36)$$

Now, by (19) and (29), we have, for $s = 1, \ldots, h - 1$,

$$E[\Omega(t); B^*_s]^{w - 1} = E[\Omega(t); B^*_s - 1]^{w - 1} + \sum_{w = 1}^{W - 1} \left( \frac{W - 1}{w} \right) E[\Omega(t); B^*_s - 1]^{w - 1} G_s^w(t) . \quad (37)$$

On combining (36) and the case $s = h - 1$ of (37) and (33), we have, for $j = 1, \ldots, k$,

$$v_{j, h}^{-1} V_j = p_j^{-1} \int_0^{M^h} E[\Omega(t); B^*_h - 2]^{w - 1} E[\Omega(t); B_{j, h - 1}] dt$$

$$+ p_j^{-1} \sum_{w = 1}^{W - 1} \left( \frac{W - 1}{w} \right) S_{j, h, w} . \quad (38)$$

For $s = 1, \ldots, h - 2$, we know that $B^*_s$ is a box of class $s$ with respect to the primes $p_1, \ldots, p_k$, and so, by Lemma 3, (25), (37) and (33), we have, for $j = 1, \ldots, k$ and $s = 1, \ldots, h - 2$,

$$\int_0^{M^h} E[\Omega(t); B^*_s]^{w - 1} E[\Omega(t); B_{j, s + 1}] dt$$

$$= p_j^{-1} \int_0^{M^h} E[\Omega(t); B^*_s]^{w - 1} E[\Omega(t); B_{j, s}] dt$$

$$= p_j^{-1} \int_0^{M^h} E[\Omega(t); B^*_s - 1]^{w - 1} E[\Omega(t); B_{j, s}] dt + p_j^{-1} \sum_{w = 1}^{W - 1} \left( \frac{W - 1}{w} \right) S_{j, s, w} . \quad (39)$$

In view of (32) the result (35) now follows from (38) by repeated application of (39). This completes the proof of Lemma 5.
§5. The case \( k = 1 \). The following lemma is only applicable for the case \( k = 1 \).

**Lemma 6.** For \( s = 1, \ldots, h \),

\[
|G_s(t)| = |E[\Omega(t); B_{1,s}]| < p_1 ; \tag{40}
\]

also, for \( s = 1, \ldots, h - 1 \),

\[
|E[\Omega(t); \bar{B}_{1,s}]| \leq 1 . \tag{41}
\]

**Proof.** Recall (21) with \( j = 1 \). For \( s = 1, \ldots, h \),

\[
E[\Omega(t); B_{1,s}] = \sum_{\alpha = 1}^{v_{1,s}} E[\Omega(t); B_{1,s,\alpha}] .
\]

Since \( v_{1,s} < p_1 \), we see that to prove (40) it suffices to show that, for each \( \alpha = 1, \ldots, v_{1,s} \),

\[
|E[\Omega(t); B_{1,s,\alpha}]| \leq 1 . \tag{42}
\]

Now on recalling (20), we know, for \( s = 1, \ldots, h \) and \( \alpha = 1, \ldots, v_{1,s} \), that \( B_{1,s,\alpha} = J_{1,s,\alpha} \times I^* \), where \( J_{1,s,\alpha} \) is an elementary \( p_1 \)-type interval of order \( s \). It follows from (1), (7) and the remark before (20) that

\[
E[\Omega(t); B_{1,s,\alpha}] = F[t + R(m(1,s,\alpha), p_1^s); I^*] . \tag{43}
\]

(42) now follows from (43) and (2). Inequality (41) follows similarly, since, for \( s = 1, \ldots, h - 1 \), we know, by (23) and (22), that \( \bar{B}_{1,s} = \bar{J}_{1,s} \times I^* \), and \( \bar{J}_{1,s} \) is an elementary \( p_1 \)-type interval of order \( s \). This completes the proof of Lemma 6.

We shall prove by induction on \( h \) that the Main Lemma for \( k = 1 \) holds for a constant \( C \) satisfying

\[
C = C(p_1, W) = (2^{W+1} p_1^W) . \tag{44}
\]

Note that, in particular,

\[
C > p_1^W . \tag{45}
\]

Suppose \( B^* = I_1 \times I^* \), where \( I_1 = [0, 1) \). Then by (1), (7) and (2),

\[
|E[\Omega(t); B^*]| = |F[t + Z; I^*]| \leq 1 ,
\]

and the Main Lemma for \( k = 1 \) is proved. We may therefore suppose that \( I_1 \neq [0, 1) \), and hence, by (16), that \( B_0^* = \emptyset \). For \( h = 1 \), we know, by (18) and (40), that

\[
|E[\Omega(t); B^*]| = |E[\Omega(t); B_{1,1}^*]| = |E[\Omega(t); B_{1,1}]| < p_1 .
\]

So in view of (45), the Main Lemma for \( k = 1 \) holds for \( h = 1 \). Suppose now that \( h > 1 \) and that the Main Lemma for \( k = 1 \) holds, when \( h \) is replaced by any smaller
positive integer, so that in particular, for any \( s = 2, \ldots, h \), we have, in view of Lemma 3,

\[
\int_0^{M_1} \left[ E[\Omega(t) ; B_{s-1}^*] \right]^W dt \leq C M^h (s-1)^{\frac{1}{W}}. \tag{46}
\]

Applying Hölder’s inequality, (40) and (46) to (31), we have, for \( w = 2, \ldots, W \),

\[
T_w \leq C^{(W-w)W} p^w_1 M^h (h-1)^{\frac{1}{W}}. \tag{47}
\]

in view of (45), so that

\[
\sum_{w=2}^{W} \binom{W}{w} T_w \leq C^{\frac{1}{1/W}} 2^w p^w_1 M^h (h-1)^{\frac{1}{W}}. \tag{48}
\]

On the other hand, since \( B_0^* = \emptyset \), we have \( E[\Omega(t) ; B_0^*] = 0 \), and so, by (32),

\[
S_1 = 0. \tag{49}
\]

Applying Hölder’s inequality, (40), (41) and (46) to (33), we have, for \( s = 2, \ldots, h-1 \) and \( w = 1, \ldots, W-1 \), in view of (45),

\[
S_{1,s,w} \leq C^{(W-w-1)W} p^w_1 M^h (s-1)^{\frac{1}{W}} \leq C^{\frac{1}{W}} W p^w_1 M^h (h-1)^{\frac{1}{W}}. \tag{50}
\]

Furthermore

\[
S_{1,1,w-1} \leq p^w_1 M^h \leq C^{1-W} M^h (h-1)^{\frac{1}{W}}. \tag{51}
\]

For \( w = 1, \ldots, W-2 \), we have \( S_{1,1,w} = 0 \). It follows that

\[
W_{1,h} \sum_{s=1}^{h-1} p^-(h-s) \sum_{w=1}^{W-1} \binom{W-1}{w} S_{1,s,w} \leq C^{1-W} W p^w_1 M^h (h-1)^{\frac{1}{W}}. \tag{52}
\]

On the other hand, by (30) and (46),

\[
T_0 \leq C M^h (h-1)^{\frac{1}{W}}. \tag{53}
\]

Combining (34), (47), (48), (49) and (50),

\[
\int_0^{M_1} \left[ E[\Omega(t) ; B^*] \right]^W dt \leq C M^h (h-1)^{\frac{1}{W}} + C^{1-W} (2^W + 2^{W-1} W) p^w_1 M^h (h-1)^{\frac{1}{W}}
\]

\[
\leq C M^h (h-1)^{\frac{1}{W}} + C^{1-W} 2^W W p^w_1 (h-1)^{\frac{1}{W}}
\]

\[
= C M^h (h-1)^{\frac{1}{W}} + \frac{1}{2} W (h-1)^{\frac{1}{W}}
\]

\[
\leq C M^h h^{\frac{1}{W}},
\]

in view of (44). The proof of the Main Lemma for \( k = 1 \) is now complete.
§6. The case $k \geq 2$. We suppose, for every $j = 1, \ldots, k$, that the corresponding Main Lemma for $q$-sets and boxes with respect to the primes $p_1, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k$ holds with $C_j(p_1, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k, W)$ and $M_j$ in place of $C(p_1, \ldots, p_k, W)$ and $M$ respectively, and with the exponent of $h$ replaced by $\frac{1}{2}(k-1)W$. We let $C_0 = C_0(p_1, \ldots, p_k, W)$ be defined by

$$C_0 = 1 + \max_{1 \leq j \leq k} C_j(p_1, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k, W).$$

(51)

We shall prove, by induction on $h$, that the Main Lemma holds for a constant $C$ satisfying

$$C = C(p_1, \ldots, p_k, W) = 2^{kW^2 + W}(p_1 \ldots p_k)^{W+1}C_0(p_1, \ldots, p_k, W).$$

(52)

Clearly

$$C > (p_1 \ldots p_k)^{W+1}C_0$$

(53)

and

$$C > (p_1 \ldots p_k)^W.$$  

(54)

First of all, we must establish a link which enables us to use the analogues of the Main Lemma in lower-dimensional cases.

For $j = 1, \ldots, k$, $s = 1, \ldots, h$ and $\alpha = 1, \ldots, v_{j,s}$, we define the set $\Omega_{j,s,\alpha}(t)$ of points in $k$-dimensional space by

$$\Omega_{j,s,\alpha}(t) = \{(x_1(n), \ldots, x_{j-1}(n), x_{j+1}(n), \ldots, x_k(n), n + t : n \in R(m(j, s, \alpha), p_j^s)\},$$

where $R(m(j, s, \alpha), p_j^s)$ is the associated residue class modulo $p_j^s$ of $J_{j,s,\alpha}$. Then, for every real number $t$, we know, by Lemma 2, that $\Omega_{j,s,\alpha}(t)$ is a translated $p_j^s$-set of class $h$ with respect to the primes $p_1, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k$. On the other hand, let $B_{j,s}^*$ be defined for the above values of $j$ and $s$ by

$$B_{j,s}^* = [0, \xi_{1,s-1}] \times \ldots \times [0, \xi_{j-1,s-1}] \times [0, \xi_{j+1,s}] \times \ldots \times [0, \xi_{k,s}] \times I^*.$$  

Then $B_{j,s}^*$ is a box of class $s$ with respect to the primes $p_1, \ldots, p_{j-1}, p_{j+1}, \ldots, p_k$. It is easy to see that, for $j = 1, \ldots, k$, $s = 1, \ldots, h$ and $\alpha = 1, \ldots, v_{j,s}$,

$$E[\Omega(t) ; B_{j,s,\alpha}] = E[\Omega_{j,s,\alpha}(t) ; B_{j,s}^*].$$

(55)

It follows, on our assumption of the lower-dimensional cases of the Main Lemma, and hence its alternative form, in view of (55), (51), Lemma 3, (9) and (10), that for every $j = 1, \ldots, k$, $s = 1, \ldots, h$ and $\alpha = 1, \ldots, v_{j,s}$,

$$\int_0^{M_j^s} E[\Omega(t) ; B_{j,s,\alpha}]^W dt = M_j^{h-s} \int_0^{M_j^s} E[\Omega_{j,s,\alpha}(t) ; B_{j,s}^*]^W dt \leq C_j M_j^{h^s \frac{1}{2}(k-1)W} C_0 M_j^{h^s \frac{1}{2}(k-1)W}.  $$

(56)
Similarly, for $j = 1, \ldots, k$ and $s = 1, \ldots, h-1$, on relating $E[\Omega(t); \tilde{B}_{j,s}]$ to the discrepancy of certain translated $p_j^*$-set with respect to the primes $p_1, \ldots, p_{j-1}$, $p_{j+1}, \ldots, p_k$ in the box $B_{j,k}^*$, we have

$$\int_0^{M^h} E[\Omega(t); \tilde{B}_{j,s}]^W dt < C_0 M^h h^{\frac{1}{4}(k-1)W}. \quad (57)$$

We know, by (29) and (21), that, for $s = 1, \ldots, h$,

$$\int_0^{M^h} G^w_s(t) dt = \int_0^{M^h} \left( \sum_{j=1}^k \sum_{\xi=1}^{\nu_j,s} E[\Omega(t); B_{j,s}\xi] \right)^W dt \leq \left( \sum_{j=1}^k \nu_j,s \right)^W \left( \sum_{j=1}^k \sum_{\xi=1}^{\nu_j,s} E[\Omega(t); B_{j,s}\xi] \right)^W dt; \quad (58)$$

so that, on combining (56) and (58), we have, for $s = 1, \ldots, h$,

$$\int_0^{M^h} G^w_s(t) dt \leq (p_1 + \ldots + p_k)^{W+1} C_0 M^h s^{\frac{1}{2}(k-1)W} \leq (p_1 \ldots p_k)^{W+1} C_0 M^h s^{\frac{1}{2}(k-1)W}. \quad (59)$$

We may assume that $B^* = I_1 \times \ldots \times I_k \times I^*$, where for some $j = 1, \ldots, k$, $I_j \neq [0, 1)$. Otherwise, by (1), (7) and (2), we know that $|E[\Omega(t); B^*]| = |F[t + Z; I^*]| \leq 1$, and the Main Lemma follows. By (16), we see that $B_0^* = \emptyset$. On the other hand, it is easy to see, from the definition of $\Omega(t)$, that for any fixed $t$ and $\eta$, $E[\Omega(t); B^*(\eta, Y)]$ is periodic in $Y$ with period $p_1 \ldots p_k$, so that we may assume that $0 \leq Y < p_1 \ldots p_k$ when estimating $E[\Omega(t); B^*]$. With this restriction on $Y$, $Z[\Omega(t); B_1^*] \leq p_1 \ldots p_k$ and $V(B^_1) < p_1 \ldots p_k$, so, by (7), $|E[\Omega(t); B^*]| \leq p_1 \ldots p_k$. Hence, by (54), we see that the Main Lemma holds for $h = 1$ with $C$ defined by (52).

Suppose now that $h \geq 2$, and that the Main Lemma holds when $h$ is replaced by any smaller positive integer, so that, in particular, for $s = 2, \ldots, h$, in view of Lemma 3,

$$\int_0^{M^h} E[\Omega(t); B_{s-1}^*] \leq CM^h(s-1)^{\frac{1}{2}W}. \quad (60)$$

Applying Hölder's inequality, (59) and (60) to (31), for $w = 2, \ldots, W$, we obtain

$$T_w \leq C^{(W-w)/W} C_0^{w/W} (p_1 \ldots p_k)^{(W+1)/W} M^h(h-1)^{\frac{1}{2}(W-w)/W} h^{\frac{1}{2}(k-1)W} \leq C^{(W-w)/W} C_0^{w/W} (p_1 \ldots p_k)^{(W+1)/W} 2^{(k-1)W} M^h(h-1)^{\frac{1}{2}W-1}.$$
by (53). Hence

\[
\sum_{w=2}^{W} \binom{W}{w} T_w \leq C^{1-1/W} C_0^{1/W} (p_1 \ldots p_k)^{(W+1)/W} 2^{W} M^b (h-1)^{1/kW-1}.
\] (61)

On the other hand, since \( B_0^* = \emptyset \), we know that \( E[\Omega(t); B_0^*] = 0 \), and so by (32), we deduce that for every \( j = 1, \ldots, k \),

\[
S_j = 0.
\] (62)

Applying Hölder's inequality, (57), (59) and (60) to (33), for \( j = 1, \ldots, k \), \( s = 2, \ldots, h-1 \) and \( w = 1, \ldots, W-1 \), in view of (53), we obtain

\[
S_{j,s,w} \leq C^{(W-s)/W} C_0^{(s+1)/W} (p_1 \ldots p_k)^{(W+1)/W} M^b (s-1)^{1/k(W-s-1)} 2^{(k-1)/W} h^{1/(k-1)}
\]

\[
\leq C^{1-1/W} C_0^{1/W} 2^{1/k(k-1)} M^b (h-1)^{1/kW-1}.
\]

Furthermore,

\[
S_{1,1,w-1} \leq C_0 (p_1 \ldots p_k)^{(W-1)/(W+1)/W} M^b 2^{1/k(k-1)}
\]

\[
\leq C^{1-1/W} C_0^{1/W} 2^{1/k(k-1)} M^b (h-1)^{1/kW-1}.
\]

For \( j = 1, \ldots, k \) and \( w = 1, \ldots, W-2 \), we know that \( S_{j,1,w} = 0 \). It follows that

\[
\sum_{j=1}^{k} \sum_{h=1}^{h-1} \sum_{s=1}^{W-1} \binom{W-1}{w} S_{j,s,w} \leq C^{1-1/W} C_0^{1/W} (p_1 + \ldots + p_k) 2^{1/k(k-1)} 2^{W-1} W M^b (h-1)^{1/kW-1}
\]

\[
\leq C^{1-1/W} C_0^{1/W} (p_1 \ldots p_k)^{(W+1)/W} 2^{W} M^b (h-1)^{1/kW-1},
\] (63)

since \( 2^{1/k(k-1)} 2^{W-1} W \leq 2^{1/k(k-1)+1} 2^{W-2} < 2^{kW} \). Also, by (30) and (60), we deduce that

\[
T_0 \leq C M^h (h-1)^{1/kW}.
\] (64)

Combining (34), (61), (62), (63) and (64), in view of (52), we obtain

\[
\int_0^M E[\Omega(t); B^*] W dt \leq C M^h \{(h-1)^{1/kW} + 2C^{-1/W} C_0^{1/W} (p_1 \ldots p_k)^{(W+1)/W} 2^{W} (h-1)^{1/kW-1}\}
\]

\[
= C M^h \{(h-1)^{1/kW} + (h-1)^{1/kW-1}\}
\]

\[
< C M^h h^{1/kW}.
\]

This completes the proof of the Main Lemma.

§7. Proof of Theorem 2. We now take \( p_1, \ldots, p_k \) to be the first \( k \) primes. For any
natural number \( N \geq 2 \), let
\[
h = \lfloor \log_2 N \rfloor + 1. \tag{65}
\]
Then, for every \( j = 1, \ldots, k \), we have
\[
N \leq p_j^h. \tag{66}
\]
For any \( \theta = (\theta_1, \ldots, \theta_k) \) in \( U_1^k \), and, for any real \( Y \) satisfying
\[
0 < Y < N, \tag{67}
\]
let \( B(\theta, Y) \) be the box defined by
\[
B(\theta, Y) = [0, \theta_1] \times \cdots \times [0, \theta_k] \times [0, Y).
\]
Let \( \eta = \eta(\theta) = (\eta_1, \ldots, \eta_k) \) be defined such that, for every \( j \) satisfying \( 1 \leq j \leq k \),
\[
\eta_j = \eta_j(\theta_j) = -p_j^{-h}[-p_j^h \theta_j], \tag{68}
\]
i.e. \( \eta_j \) is the least integer multiple of \( p_j^{-h} \) not less than \( \theta_j \).

Let \( \Omega(t) = \Omega(t) \), where \( \Omega(t) \) is defined by (3) in terms of the first \( M^n \) terms of the Hammersley (Halton) sequence.

**Lemma 7.** For any \( \theta \) in \( U_1^k \) and any \( Y \) satisfying (67),
\[
|E[\Omega(t); B(\theta, Y)] - E[\Omega(t); B^*(\eta(\theta), Y)]| \leq k. \tag{69}
\]

**Proof.** For \( j = 0, \ldots, k \), for any fixed \( \theta \) in \( U_1^k \) and for any fixed \( Y \) satisfying (67), let
\[
B^{(j)} = B^{(j)}(\theta, Y) = [0, \eta_1] \times \cdots \times [0, \eta_j] \times [0, \eta_{j+1}] \times \cdots \times [0, \theta_k] \times [0, Y).
\]
Then clearly \( B^{(0)} = B(\theta, Y) \) and \( B^{(k)} = B^*(\eta(\theta), Y) \). It is easy to see that to prove Lemma 7, it suffices to prove that, for every \( j = 1, \ldots, k, \)
\[
|E[\Omega(t); B^{(j)}] - E[\Omega(t); B^{(j-1)}]| \leq 1.
\]
For each \( j = 1, \ldots, k \), we know, by (68), that \( \eta_j \geq \theta_j \) and \( \eta_j - \theta_j < p_j^{-h} \). It follows from (66) and (67) that
\[
0 \leq V(B^{(j)}) - V(B^{(j-1)}) < 1.
\]
By (7) with \( q = 1 \), it remains to show, for \( j = 1, \ldots, k, \) that
\[
0 \leq Z[\Omega(t); B^{(j)}] - Z[\Omega(t); B^{(j-1)}] \leq 1. \tag{69}
\]
The first inequality of (69) is obvious. On the other hand, the difference in question in (69) does not exceed the number of \( n \) in \([-t, Y-t)\) for which \( X(n) \) lies in
This interval is an elementary \( p_j \)-type interval of order \( h \), so that, in view of (66) and (67), and, since \( \Omega(t) \) is of class \( h \), the difference is either 0 or 1. This proves (69), and the proof of Lemma 7 is now complete.

For any even positive integer \( W \), we know, by Lemma 7, that for any \( \theta \) in \( U^k \) and any real \( Y \) satisfying \( 0 < Y \leq N \),

\[
E[\Omega(t); B(\theta, Y)]^w \leq 2^w E[\Omega(t); B^*(\eta(\theta), Y)]^w + (2k)^w. \tag{70}
\]

By the Main Lemma, we have

\[
\int_0^{M^h} \int_0^N \int_{U^k} E[\Omega(t); B^*(\eta(\theta), Y)]^w \, dt \, d\theta \, dY \ll_{k, W} M^h h^{kW} N. \tag{71}
\]

Combining (70) and (71), we see that there is a real number \( t^* \), satisfying \( 0 < t^* < M^h \), such that

\[
\int_{U^k} E[\Omega(t^*); B(\theta, Y)]^w \, d\theta \, dY \ll_{k, W} (\log N)^{kW} N. \tag{72}
\]

in view of (65). Note that the value of \( t^* \) may depend on the value of \( W \). On recalling the definition of \( \Omega(t) \) and (6), we see from (72) that the set

\[
\mathcal{P} = \{(X_1(n), ..., X_k(n), N^{-1}(n+t^*)): 0 \leq n+t^* < N\} \tag{73}
\]

gives a proof of Theorem 2 for even positive integers \( W \).

The case for general positive \( W \) follows immediately.

References