The Annals of Probability
1979, Vol. 7, No. 2, 267–275

HAMMERSLEY'S LAW FOR THE VAN DER CORPUT SEQUENCE: AN INSTANCE OF PROBABILITY THEORY FOR PSEUDORANDOM NUMBERS[1]

BY A. DEL JUNCO AND J. MICHAEL STEELE

Ohio State University and Stanford University

The analogue of Hammersley's theorem on the length of the longest monotonic subsequence of independent, identically, and continuously distributed random variables is obtained for the pseudorandom van der Corput sequence. In this case there is no limit but the precise limits superior and inferior are determined. The constants obtained are closely related to those established in the independent case by Logan and Shepp, and Vershik and Kerov.

1. Introduction. Pseudorandom numbers form the backbone of computer simulation and Monte Carlo analysis, yet there are essentially no known theorems which make explicit the sense in which pseudorandom numbers are replacements for random numbers. There is probably no general result which can be proved, but there is still a program by which a deeper understanding of the relationship between pseudorandom numbers and random numbers can evolve.

For every pseudorandom sequence and every probabalistic theorem, there is surely some analogue of the probabalistic theorem for that pseudorandom sequence. The qualities of that analogue should then accurately reflect the random qualities of the pseudorandom sequence. By a systematic analysis of these pairs of theorems and sequences, a body of results can be obtained which is capable of resolving, or at least eroding, many of the philosophical and practical questions concerning pseudorandom sequences.

This is no overnight task and there is no obvious place to begin other than with the theorems and sequences which interest one most. We have begun with a theorem due to Hammersley and a sequence due to van der Corput.

To introduce Hammersley's theorem, let X_i, $i = 1, 2, \cdots$, be independent random variables with uniform distribution on [0, 1]. By $l_n = l(X_1, X_2, \cdots, X_n)$ we denote the cardinality of the largest monotone increasing subsequence of the values $X_1(\omega), X_2(\omega), \cdots, X_n(\omega)$. Hammersley [2] proved that

$$\lim_{n\to\infty} n^{-\frac{1}{2}} l_n = c \tag{1.1}$$

where c is a constant and the convergence is in probability. We are particularly interested in (1.1) because of the considerable effort which has been focused on the determination of c. Even before convergence had been proved in (1.1), Baer and Brock [1] had conjectured that $c = 2$ on the basis of extensive computation. Hammersley [2] gave bounds on c which were improved by Kingman [4], but the

Received September 8, 1977.
[1]Supported in part by Office of Naval Research, Contract N00014–76–C–0475.
AMS 1970 *subject classifications.* Primary 60C05; secondary 65C10.
Key words and phrases. Van der Corput sequence, monotonic subsequence.

deepest results published so far are due to Logan and Shepp [6] who proved $c \geqslant 2$. Vershik and Kerov [7] have recently announced that $c \leqslant 2$ but details of their proof have yet to appear.

In the present context Hammersley's theorem has a natural appeal as a substantive probabalistic result in which there is much current interest. The tempting prospects of obtaining c in the analogue of (1.1) for some pseudorandom sequence provide even more reason to start with Hammersley's theorem.

One natural candidate for the sequence of pseudorandom numbers is the sequence generated by the multiplicative congruential method. These are the most widely used pseudorandom numbers but there are several drawbacks to their analysis.

In the first place the sequences generated by the multiplicative congruential method are periodic. Since l_n can be properly studied only for n small compared to the period the asymptotic analysis thus is complicated not only computationally but conceptually.

Primarily for this reason we have begun with the van der Corput sequence. The sequence is generated in a manner almost as simple as multiplicative congruence, but it has the great benefit of being aperiodic. Moreover the sequence has widespread use in numerical integration [3] and considerable historical interest. (See, for example, Knuth's interesting discussion "What is a random sequence" [5] page 127–157.)

To define the van der Corput sequence we first write, for $n \geqslant 0$, $n = \sum_{i=0}^{\infty} a_i 2^i$ where $a_i = 0$ or 1. The $n+1$st element of the sequence is $\varphi_2(n) = \sum_{i=0}^{\infty} a_i 2^{-i-1}$. One can see that $\varphi_2(0) = 0$, $\varphi_2(1) = \frac{1}{2}$, $\varphi_2(2) = \frac{1}{4}$, $\varphi_2(3) = \frac{3}{4}$, etc. The nature of $\varphi_2(n)$ is more easily seen in binary notation where $\varphi_2(n)$ is the "the reflection of n in the decimal point." As the subscript suggests one can define a similar sequence by $\varphi_p(n) = \sum_{i=0}^{\infty} a_i p^{-i-1}$ where $n = \sum_{i=0}^{\infty} a_i p^1$, $0 \leqslant a_i < p$ and $p \geqslant 2$ is an integer.

We now have the theorem:

If $l(n)$ is the cardinality of the largest monotone increasing subsequence of $\{\varphi_p(0), \varphi_p(1), \cdots, \varphi_p(n-1)\}$ then

$$\text{(1.2)} \quad \liminf_{n\to\infty} n^{-\frac{1}{2}} l(n) = 2^{\frac{1}{2}}, \qquad \limsup_{n\to\infty} n^{-\frac{1}{2}} l(n) = \tfrac{3}{2} \qquad \textit{for } p = 2,$$

and

(1.3)

$$\liminf_{n\to\infty} n^{-\frac{1}{2}} l(n) = 2(1-p^{-1})^{\frac{1}{2}}, \qquad \limsup_{n\to\infty} n^{-\frac{1}{2}} l(n) = p^{\frac{1}{2}} \qquad \textit{for } p > 2.$$

This result is as precise an analogue to (1.1) as one could realistically expect. Also, the Logan-Shepp lower bound on c makes it particularly noteworthy that

$$\text{(1.4)} \qquad \lim_{p\to\infty} \liminf_{n\to\infty} n^{-\frac{1}{2}} l(n) = 2.$$

For digestibility, the proof of these results has been divided into four parts. First we obtain a geometrical characterization of the monotone subsequences of van der Corput's sequence. Upper and lower bounds are then obtained for $l(n)$. Finally the required limits are identified.

2. The geometrical representation. Our first goal is to obtain a representation from which detailed information about $\{\varphi_p(0), \varphi_p(1), \cdots, \varphi_p(n-1)\}$ can be deduced. We define σ_n to be the unique permutation of $\{0, 1, \cdots, n-1\}$ which puts $\varphi_p(i)$, $0 \leqslant i \leqslant n-1$ in increasing order, i.e.,

$$\varphi_p(\sigma_n(0)) < \varphi_p(\sigma_n(1)) < \cdots < \varphi_p(\sigma_n(n-1)).$$

This permutation will be written as a sequence

$$\sigma_n = (\sigma_n(0), \sigma_n(1), \cdots, \sigma_n(n-1))$$

and our reason for introducing σ_n is the elementary fact that the length of the longest monotone increasing subsequence of σ_n is equal to $l(n)$.

We also have the following *law of formation* of σ_{mp^n} which will be crucial.

LEMMA 2.1. *One obtains σ_{mp^n} from σ_{p^n} by replacing the entry $\sigma_{p^n}(i)$ of σ_{p^n} by the sequence $\sigma_{p^n}(i) + p^n\sigma_m$.*

REMARK. Here and in the following if x is a sequence then $a + bx$ is a sequence with the same domain as x defined by $(a + bx)(i) = a + bx(i)$.

PROOF OF LEMMA. Notice that there are two things we must show:

$$\varphi_p(\sigma_{p^n}(i) + p^n\sigma_m(j)) < \varphi_p(\sigma_{p^n}(i) + p^n\sigma_m(j+1)), \tag{2.1}$$

and

$$\varphi_p(\sigma_{p^n}(i) + p^n\sigma_m(j)) < \varphi_p(\sigma_{p^n}(i+1) + p^n\sigma_m(j')), \tag{2.2}$$

for any j, j'.

We first suppose $j < p^n$ and k is any integer. Setting $j = \sum_{i=0}^{n-1} a_i p^i$, $k = \sum_{i=-n}^{m} a_k p^{i-n}$ we have $j + p^n k = \sum_{i=0}^{m} a_i p^1$, and consequently

$$\begin{aligned} \varphi_p(j + p^n k) &= \textstyle\sum_{i=0}^{m} a_i p^{-(i+1)} \\ &= \textstyle\sum_{i=0}^{n-1} a_i p^{-(i+1)} + p^{-n}\sum_{i=n}^{m} a_i p^{-(i+1)} \\ &= \varphi_p(j) + p^{-n}\varphi_p(k) \quad \text{for} \quad j < p^n. \end{aligned} \tag{2.3}$$

Now by (2.3) we see (2.1) is equivalent to

$$p^{-n}\varphi_p(\sigma_m(j)) < p^{-n}\varphi_p(\sigma_m(j+1)),$$

which is just the definition of σ_m. Similarly, (2.2) is equivalent to

$$\varphi_p(\sigma_{p^n}(i)) + p^{-n}\varphi_p(\sigma_m(j)) < \varphi_p(\sigma_{p^n}(i+1)) + p^{-n}\varphi_p(\sigma_m(j')). \tag{2.4}$$

To check (2.4) we note that, as i runs through $\{0, 1, \cdots, p^n - 1\}$, $\varphi_p(i)$ runs through $\{0, p^{-n}, 2p^{-n}, \cdots, (p^n - 1)p^{-n}\}$ so that, in fact, $\varphi_p(\sigma_{p^n}(i+1)) = p^{-n} + \varphi_p(\sigma_{p^n}(i))$. The proof of the lemma is thus complete.

In many ways it is easier to work with the permutation matrix A_n associated with σ_n. We recall that A_n is an $n \times n$ matrix defined by

$$\begin{aligned} A_n(i, j) &= 1 \quad \text{if} \quad i = \sigma_n(j) \\ &= 0 \quad \text{otherwise.} \end{aligned}$$

To rephrase Lemma 2.1 in terms of matrices we define m different $p^n \times mp^n$ matrices $\bar{A}^0_{p^n}, \bar{A}^1_{p^n}, \cdots, \bar{A}^{m-1}_{p^n}$ by

$$\bar{A}^0_{p^n}(i,j) = A_{p^n}(i, jm^{-1}) \quad \text{if} \quad m|j$$
$$= 1 \quad \text{otherwise}$$

and

$$\bar{A}^l_{p^n}(i,j) = \bar{A}^0_{p^n}(i, (j-l) \bmod m).$$

Intuitively, we get $\bar{A}^0_{p^n}$ by inserting $m-1$ columns of 0's after each column of A_{p^n} and then shift $\bar{A}^0_{p^n}$ by l places to the right to get $\bar{A}^l_{p^n}$.

Finally we can phrase Lemma 2.1 by the following formula for A_{mp^n} as a block matrix:

$$A_{mp^n} = \begin{bmatrix} \bar{A}^{\sigma_m^{-1}(1)}_{p^n} \\ \bar{A}^{\sigma_m^{-1}(2)}_{p^n} \\ \vdots \\ \bar{A}^{\sigma_m^{-1}(m)}_{p^n} \end{bmatrix} \tag{2.5}$$

This matrix representation of the permutation permits a geometrical view of the decreasing subsequences. Formally an increasing subsequence of σ_n is a sequence of integers $P = \{j_1 < j2 < \cdots < j_l\}$ such that $\sigma(j_i) < \sigma(j_{i+1})$. Such a subsequence can be identified in A_n as a path of 1's which goes down and to the right. The set of integers $[j_1, j_l] = \{k : j_1 \leqslant k \leqslant j_l\}$ will be called the domain of the path P and will be denoted by dom(P). The integer interval $[\sigma_n(j_1), \sigma_n(j_l)] = \{k : \sigma_n(j_1) \leqslant k \leqslant \sigma_n(j_l)\}$ will be called the range of the path, and naturally $l(P)$ will be called the length of P.

3. The lower bound lemma. The main result of this section is the following:

LEMMA 3.1. *For $p^{n-2} \leqslant m \leqslant p^{n-1}$ we have*

$$l(mp^n) \geqslant p^{n-1} + m(p-1) - (3p-1), \tag{3.1}$$

and for $p^{n-3} \leqslant m \leqslant p^{n-2}$ we have

$$l(mp^n) \geqslant p^{n-3}(p-1) + mp - (p^2 + 2p - 1). \tag{3.2}$$

PROOF. First we will consider m such that $p^{n-2} \leqslant m \leqslant p^{n-1}$ and construct an explicit path through A_{mp^n}. By setting $m_1 = (p^{n-1} - m)/(p-1)$ and $m_2 = m - m_1$ we have $m_1 p^2 + m_2 p = p^n$. For $0 \leqslant i < [m_1]$ we can define a path P_i through A_{p^n} of length $2p-1$ and domain $[p^2 i, p^2(i+1) - 1]$ by

$$P_i = (p^2 i, p^2 i + p, p^2 i + 2p, \cdots, p^2(i+1) - p,$$
$$p^2(i+1) - p + 1, \cdots, p^2(i+1) - 1).$$

For $0 \leqslant i < [m_2]$ we then define a path $P_{[m_1]+i}$ through A_{p^n} with length p and domain $\left[[m_1]p^2 + ip, [m_1]p^2 + (i+1)p - 1\right]$ by

$$P_{[m_1]+i} = \left([m_1]p^2 + ip, [m_1]p^2 + ip + 1, \cdots, [m_1]p^2 + (i+1)p - 1\right).$$

Now we consider the paths $\bar{P}_i$ in $\bar{A}_{p^n}^{\sigma_m^{-1}(i)}$ which correspond to P_i. These paths are defined by $\bar{P}_i = mP_i + \sigma_m^{-1}(i)$. Finally we define our desired path P through A_{mp^n} as the concatenation of the $\bar{P}_i$,

$$P = \bar{P}_0\bar{P}_1 \cdots \bar{P}_{[m_1]+[m_2]-1}.$$

To make certain that the path P is properly defined we have to check that for each $k \in \operatorname{dom} \bar{P}_{i+1}$ and $l \in \operatorname{dom} \bar{P}_i$ we have $k > l$. This condition will be abbreviated by $\operatorname{dom} \bar{P}_{i+1} > \operatorname{dom} \bar{P}_i$, and it follows immediately from the corresponding fact that $\operatorname{dom} P_{i+1} > \operatorname{dom} P_i$. By our construction we finally have

$$\begin{aligned} l(mp^n) \geqslant l(P) &= [m_1](2p-1) + [m_2]p \\ &\geqslant m_1(2p-1) + m_2p - (3p-1) \\ &= p^{n-1} + m(p-1) - (3p-1) \end{aligned}$$

which completes the proof of (3.1).

We now consider $m, p^{n-3} \leqslant m \leqslant p^{n-2}$ and begin by setting $m_1 = (p^{n-2} - m)/(p-1)$ and $m_2 = m - m_1$. This time we have $m_1p^3 + m_2p^2 = p^n$. As in our previous construction there is a path of length p^2 through A_{p^3}, so for $0 \leqslant i < [m_1]$ there is a path P_i of length p^2 through A_{p^n} with domain $[ip^3, (i+1)p^3 - 1]$. For $0 \leqslant i < [m_2]$ there is a path $P_{[m_1]+i}$ of length $2p-1$ through A_{p^n} with domain $\big[[m_1]p^3 + ip^2, [m_1]p^3 + (i+1)p^2 - 1\big]$. Next we set $\bar{P}_i = mP_i + \sigma_m^{-1}(i)$ and obtain a path through $\bar{A}_{p^n}^{\sigma_m^{-1}(i)}$ by letting

$$P = \bar{P}_0\bar{P}_1 \cdots \bar{P}_{[m_1]+[m_2]-1}.$$

Finally we calculate as before:

$$\begin{aligned} l(mp^n) \geqslant l(P) &= [m_1]p^2 + [m_2](2p-1) \\ &\geqslant m_1p^2 + m_2(2p-1) - (p^2 + 2p - 1) \\ &= p^{n-2}(p-1) + mp - (p^2 + 2p - 1) \end{aligned}$$

which completes the proof of (3.2).

REMARK. The preceding proof probably appears more involved than an examination of an example would indicate. By calculating A_{mp^n} for $p = 3$ and several small values of m and n one can easily find the path P and see how it evolves as m and n increase. Similarly in the arguments which follow one should keep the example $p = 3$ clearly in mind, perhaps by keeping a small table of the A_{mp^n}.

4. The upper bound lemma. The recursive nature of A_{mp^n} provides the key to the following, Lemma 4.1. For any positive integer m we have

$$l(mp^{n-1}) \leqslant p^{n-1} + m(p-1) \tag{4.1}$$

and

$$l(mp^n) \leqslant p^{n-1} - p^{n-2} + mp. \tag{4.2}$$

PROOF. For any path P through A_{mp^n} we can decompose P as a concatenation

$$P = \bar{P}_0\bar{P}_1 \cdots \bar{P}_{m-1}$$

where $\bar{P}_i$ is a path through $\bar{A}_p^{\sigma_m^{-1}(i)}$. Here one should note that the range of $\bar{P}_i$ is a subset of $[ip^n, (i+1)p^n - 1]$.

We now let P_i be the corresponding path in A_{p^n} of $\bar{P}_i$. That is, we let $P_i = m^{-1}(\bar{P}_i - \sigma_m^{-1}(i))$. We do not have dom $P_i <$ dom P_{i+1} but we obviously do have dom $P_i \leqslant$ dom P_{i+1} so the two paths have at most one common point. If dom $P_i \cap$ dom $P_{i+1} \neq \varnothing$ we shall say P_i and P_{i+1} are linked. Since $l(P) \leqslant \Sigma_{i=0}^{m-1} l(P_i)$ the lemma would follow from $\Sigma_{i=0}^{m-1} l(P_i) \leqslant \min(p^{n-1} + m(p-1), p^{n-1} - p^{n-2} + mp)$. This fact will be proved using only the inequality dom $P_i \leqslant$ dom P_{i+1}.

First we decompose A_{p^n} into p^n blocks of height p^{n-1} and width p. We note that each block has exactly one 1, and the pattern of 1's in each column of blocks is the same as the pattern in A_p.

The block width $w(P)$ of a path P is defined as the number of distinct columns of blocks which intersect P. The block height $h(P)$ is defined correspondingly. Further, we let μ equal the number of integers i such that P_i is linked to P_{i+1}.

If P_i and P_{i+1} are linked we define their linkage as the concatenation $P_iP_{i+1}^*$ where P_{i+1}^* denotes P_i with its first entry removed. By forming the successive linkage of the P_i we obtain $m - \mu$ paths $\hat{P}_1, \hat{P}_2, \cdots, \hat{P}_{m-\mu}$ which are unlinked and for which

$$\mu + \Sigma_{i=1}^{m-\mu} l(\hat{P}_i) = \Sigma_{i=0}^{m-1} l(P_i). \tag{4.3}$$

Next we form all possible concatenations of successive $\hat{P}_i$ to get s paths $P_1', P_2', \cdots, P_s'$ which allow no further concatenation. One then has $s \leqslant m - \mu$ and

$$\Sigma_{i=1}^{s} l(P_i') = \Sigma_{i=1}^{m-\mu} l(\hat{P}_i). \tag{4.4}$$

Moreover, one notes that no two P_i' share a common column of blocks for the simple reason that dom $P_i <$ dom P_{i+1} and the 1 in any block is to the right of the 1 in any block above it.

The crucial observation is that for each path P_i' we have

$$l(P_i') \leqslant h(P_i') + w(P_i') - 1 \leqslant p + w(P_i') - 1$$

which by summing over i yields

$$\Sigma_{i=1}^{s} l(P_i') \leqslant \Sigma_{i=1}^{s} w(P_i') + s(p-1). \tag{4.5}$$

Since no two P_i' share a column of blocks we have

$$\Sigma_{i=1}^{s} w(P_i') \leqslant p^{n-1}. \tag{4.6}$$

By the inequality (4.5) we obtain

$$\Sigma_{i=1}^{s} l(P_i') \leqslant p^{n-1} + s(p-1) \tag{4.7}$$

which by setting $s = m - \mu - \lambda$ with $\lambda \geqslant 0$ using (4.3) and (4.4) becomes

$$\Sigma_{i=0}^{m-1} l(P_i) \leqslant p^{n-1} + (m-\lambda)(p-1) - \mu(p-2). \tag{4.8}$$

This completes the proof of (4.1) since $\lambda \geqslant 0$ and $\mu \geqslant 0$. On the other hand (4.6) also yields $s \leqslant p^{n-1}$ so $-\mu \leqslant p^{n-1} - (m - \lambda)$ which by (4.8) implies

$$\Sigma_{i=0}^{m-1} l(P_i) \leqslant p^{n-1} + (m - \lambda)(p - 1) + (p^{n-1} - (m - \lambda))(p - 2)$$
$$\leqslant p^n - p^{n-1} + m.$$

This implies $l(mp^n) \leqslant p^n - p^{n-1} + m$ and by replacing n by $n - 1$ and m by mp we obtain the proof of (4.2). This completes our proof of the upper bound lemma.

By applying the preceding lemmas, we should note that in certain cases the inequalities can be made to provide equality. By inspecting the proof of (3.1) in the cases of $m = p^{n-1}$ and $m = p^{n-2}$ one sees that it is not necessary to estimate greatest integers so that the $3p - 1$ disappears from the right of (3.1). Combining this with (4.1) we have the identities

$$l(p^{2n-1}) = p^n \quad \text{and} \quad l(p^{2n-2}) = p^{n-2}(2p - 1). \tag{4.9}$$

By similar analysis for $p = 2$ we also have the identity

$$l(m2^n) = 2^{n-1} + m \quad \text{for} \quad 2^{n-2} \leqslant m \leqslant 2^{n-1} \tag{4.10}$$
$$= 2^{n-1} + 2m \quad \text{for} \quad 2^{n-3} \leqslant m \leqslant 2^{n-2}.$$

5. Identification of the limits. To complete the proof of our theorem, we first identify $\limsup_{n\to\infty} N^{-\frac{1}{2}} l(N)$ where N is restricted to $S = \{mp^n : p^{n-3} \leqslant m \leqslant p^{n-1}\}$.

LEMMA 5.1. *Setting* $K = \max(2(1 - p^{-1})^{\frac{1}{2}}, p^{\frac{1}{2}}, 2 - p^{-1})$ *and* $k = \min(2(1 - p^{-1})^{\frac{1}{2}}, p^{\frac{1}{2}}, 2 - p^{-1})$, *we have*

$$\limsup_{N \in S} N^{-\frac{1}{2}} l(N) = K, \tag{5.1}$$

and

$$\liminf_{N \in S} N^{-\frac{1}{2}} l(N) = k. \tag{5.2}$$

PROOF. As in Section 3 we deal with $p^{n-2} \leqslant m \leqslant p^{n-1}$ (case 1) and $p^{n-3} \leqslant m \leqslant p^{n-2}$ (case 2) separately. This time we begin with case 2. By (3.2) and (4.2) we have

$$g_n(m) - (p^2 + 2p + 1)(mp^n)^{-\frac{1}{2}} \leqslant l(mp^n)(mp^n)^{-\frac{1}{2}} \leqslant g_n(m)$$

where $g_n(x) = (p^{n-2}(p - 1) + xp)(xp^n)^{-\frac{1}{2}}$. Consequently we have

$$\liminf l(mp_n)(mp^n)^{-\frac{1}{2}} = \liminf g_n(m), \tag{5.3}$$

where the lim inf is taken over the set $S_1 = \{mp^n : p^{n-3} \leqslant m \leqslant p^{n-2}, 1 \leqslant n\}$. One has the same equation as (5.3) for the lim sup.

Next observe $g_n(m)$ has its minimum at $a_n = p^{n-3}(p - 1)$ and g_n is decreasing for $p^{n-3} \leqslant x \leqslant a_n$ and increasing for $a_n \leqslant x \leqslant p^{n-2}$. One easily checks that $g_n(p^{n-3}) = p^{\frac{1}{2}}$, $g_n(p^{n-2}) = 2 - p^{-1}$, and $g_n(a_n) = 2(1 - p^{-1})^{\frac{1}{2}}$ so we have

$$\liminf_{mp^n \in S_1} g_n(m) = k \quad \text{and} \quad \limsup_{mp^n \in S_1} g_n(m) = K. \tag{5.4}$$

To prove the comparable identities for case 1 one sets $f_n(x) = (p^{n-1} + x(p-1))(xp^n)^{-\frac{1}{2}}$ and obtains from (3.1) and (4.1) that

$$\liminf_{mp^n \in S_2} l(mp^n)(mp^n)^{-\frac{1}{2}} = \limsup_{mp^n \in S_2} f_n(m)$$

where $S_2 = \{mp^n : p^{n-2} \leqslant mp^{n-1}, n \geqslant 1\}$. The same equality holds for the limsup, and we note as before that f_n has a minimum at $p^{n-1}(p-1)^{-1} = b_n$, decreases for $p^{n-2} \leqslant x \leqslant b_n$ and increases for $b_n \leqslant x \leqslant p^{n-1}$. Finally we note $f_n(b_n) = 2(1 - p^{-1})^{\frac{1}{2}}$, $f_n(p^{n-1}) = p^{\frac{1}{2}}$, and $f_n(p^{n-2}) = 2 - p^{-1}$. Hence, we have

$$\liminf_{mp^n \in S_2} f_n(m) \geqslant k \quad \text{and} \quad \limsup_{mp^n \in S_2} f_n(m) \leqslant K. \tag{5.5}$$

One has inequality in (5.5) since b_n is not an integer. Actually equality can be proved but is not required for the rest of the proof. By (5.3), (5.4) and (5.5) we have completed the proof of (5.1) and (5.2) as required by the lemma.

The proof of our theorem can now be completed in a routine way. For an arbitrary integer N we write

$$N = mp^n + r \quad \text{with} \quad p^{n-3} \leqslant m \leqslant p^{n-1} \quad \text{and} \quad 0 \leqslant r \leqslant p^{n+2}. \tag{5.6}$$

Letting $l(i, j)$ denote the cardinality of the largest increasing subsequence of $(\varphi_p(i), \varphi_p(i+1), \cdots, \varphi_p(j-1))$ we see

$$l(ip^k, (i+1)p^k) = l(p^k) \tag{5.7}$$

as a consequence of (2.3). There is also the obvious fact that $l(i, j)$ is subadditive,

$$l(i, k) \leqslant l(i, j) + l(j, k) \qquad \text{for} \quad i \leqslant j \leqslant k.$$

By choosing an integer t such that $tp^{n+2} \leqslant mp^n$ and $mp^n + p^{n+2} \leqslant (t+2)p^{n+2}$ one has by (5.6) that

$$\begin{aligned} l(N) &\leqslant l(mp^n + p^{n+2}) \\ &\leqslant l(mp^n) + l(mp^n, mp^n + p^{n+2}) \\ &\leqslant l(mp^n) + l(tp^{n+2}, (t+2)p^{n+2}) \\ &\leqslant l(mp^n) + 2l(p^{n+2}). \end{aligned}$$

Hence we have

$$l(mp^n) \leqslant l(N) \leqslant l(mp^n) + 2l(p^{n+2}). \tag{5.8}$$

Since for large N one has N/mp^n is near 1 and $l(p^{n+2})/(mp^n)^{\frac{1}{2}}$ is near 0, the inequality (5.8) together with Lemma 5 completes the proof of the theorem.

REFERENCES

[1] BAER, R. M. and BROCK, P. (1968). Natural sorting over permutation spaces. *Math. Comp.* **22** 385–410.

[2] HAMMERSLEY, J. M. (1972). A few seedlings of research. *Proc. Sixth Berkeley Symp. Math. Statist. Probability* **1** 345–394. Univ. of California Press.

[3] HAMMERSLEY, J. M. and HANDSCOMB, D. C. (1964). *Monte Carlo Methods*. Methuen, London.

[4] KINGMAN, J. F. C. (1973). Subadditive ergodic theory. *Ann. Probability* **1** 883–899.
[5] KNUTH, D. E. (1969). *The Art of Computer Programming*, **2** (*Seminumerical Algorithms*). Addison-Weslay, Palo Alto.
[6] LOGAN, B. F. and SHEPP, L. A. (1975). A variational problem for random Young tableaux. *Advances in Math.* **26** 206–222.
[7] VERSHIK, A. M. and KEROV, S. V. (1977). Asymptotics of the Plancherel measure of the symmetric group and the limiting form of Young tables. *Soviet Math. Dokl.* **18** 527–531.

DEPARTMENT OF MATHEMATICS
OHIO STATE UNIVERSITY
COLUMBUS, OHIO 43210

DEPARTMENT OF STATISTICS
STANFORD UNIVERSITY
STANFORD, CALIFORNIA 94305