TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 213, 1975

ON DEDEKIND'S PROBLEM: THE NUMBER OF ISOTONE BOOLEAN FUNCTIONS. II

BY

D. KLEITMAN[1] AND G. MARKOWSKY[2]

ABSTRACT. It is shown that $\psi(n)$, the size of the free distributive lattice on n generators (which is the number of isotone Boolean functions on subsets of an n element set), satisfies

$$\psi(n) \leq 2^{(1+O(\log n/n))}\binom{n}{[n/2]}.$$

This result is an improvement by a factor $\sqrt{n}$ in the 0 term of a previous result of Kleitman. In the course of deriving the main result, we analyze thoroughly the techniques used here and earlier by Kleitman, and show that the result in this paper is "best possible" (up to constant) using these techniques.

It was shown by D. Kleitman [4] that the number $\psi(n)$ of elements of the free distributive lattice on n generators, $FD(n)$, is bounded from above by $2^{(1+c(1/\sqrt{n})\log n)E_n}$ for some constant c, where $E_n = \binom{n}{[n/2]}$ (throughout this chapter log t means $\log_2 t$ while ln t means the natural logarithm of t). Consequently log $\psi(n)$ is asymptotic to E_n. In this paper we will improve the upper bound by showing that $\psi(n) \leq 2^{(1+c'(1/n)\log n)E_n}$ for some constant c'.

It is easy to see that $\psi(n)$ is bounded from below by 2^{E_n}. The best known lower bound for log $\psi(n)$ is $(1 + c2^{-n/2})E_n$ (see [6, Theorem 7.6]; the lower bound in [4] is larger than is warranted by the argument). Thus, the result given here narrows the gap in the second order terms. Furthermore, as we shall show later, the upper bound we obtain here for $\psi(n)$ is the best possible (up to constant) using the techniques of [4] and those used in this paper. Thus, any improvement in calculating $\psi(n)$ will require more than a minor revision of available techniques.

The following notation will be used throughout the paper. $\underline{n}$ shall denote the set $\{1, \ldots, n\}$, $2^{\underline{n}}$ the power set of $\underline{n}$, $G_{r,n}$ the set $\{S \subset \underline{n} | |S| = r\}$, τ the quantity $\sqrt{n}$ ln n, and $\{r\}$ the quantity $-[-r]$ (i.e., $\{r\}$ is the least integer not less than r). We will use iff as an abbreviation for if and only if. For our purposes it is convenient to think of $FD(n)$ as the set of all isotone (order-preserving)

Received by the editors June 5, 1973 and, in revised form, December 15, 1974.
AMS (MOS) subject classifications (1970). Primary 05A65.
Key words and phrases. Dedekind's problem, Boolean functions, free distributive lattices.
(1)Supported in part by ONR Contract N00014-67-A-0204-0063.
(2)Supported in part by ONR Contract N00014-67-A-0298-0015.

functions from $2^{\underline{n}}$ into the ordered set $\{0, 1\}$ with $0 < 1$.

Outline of proof. We partition $2^{\underline{n}}$ into disjoint chains in the way Hansel did [3]. We proceed the way Hansel did, defining isotone functions (i.e., order-preserving functions from $2^{\underline{n}}$ into $\{0, 1\}$ with $0 < 1$) successively on the chains proceeding from shorter to longer chains. Unlike Hansel, we concern ourselves with ordering all chains of the same length. Also, we allow only two choices on all but a certain number (K) of chains. We prove that we construct every monotone function at least once using every possible permutation of the original partition into chains, every ordering of chains of the same length (these will be defined later), and every possible choice of K special chains.

We prove that the procedure works by analyzing in detail the nature of the partitions utilized—we find that in most cases (we shall make this more precise below) we are able to arrange it so that the two alternatives we allow in defining our function (no more than 3 alternatives are ever necessary) are the only ones which need be considered. We do this by deriving an explicit formula for the number of exceptional chains required to construct a given monotone function using our procedure. We then show that this number is bounded by cE_n/n for some constant c, from which our theorem follows.

Of course the above is just a very sketchy outline of the proof. In the next section, we will introduce much of the machinery we will be using and give a much more detailed discussion of the argument.

Preliminaries. We now define a convention for later use. In dealing with several quantities X, Y, Z such that $X \leqslant cY$ and $Y \leqslant dZ$, where c and d are constants, we will simply write $X \leqslant cZ$ and not keep introducing a new symbol every time we change the constant. Thus, we intend to use c as a dummy symbol for a constant. Often when we state an inequality we will not bother to state that it holds only for n "sufficiently large".

We will use a basic partition of $2^{\underline{n}}$ into E_n disjoint, connected, symmetric chains. This partition has been used by *a great many* authors (DeBruijn, Hansel, Kleitman and others) in working with $2^{\underline{n}}$. We will use an explicit characterization of this partition due to C. Greene and D. Kleitman [2]. We now give an informal description of the characterization, from which it is not hard to derive a formal one.

If $S \subset \underline{n}$, we can think of S as a binary n-tuple $(a_1, \ldots, a_n)$, where $a_i = 1$ if $i \in S$ and $a_i = 0$ if $i \notin S$. If we now think of the 1's as left parentheses and of the 0's as right parentheses, we will in general be able to close parentheses and also have some open parentheses. 1's and 0's corresponding to closed parentheses are called "*bound*". Those corresponding to open parentheses are called "*free*". Consider the following example: (0, 1, 0, 1). This corresponds to)(. Thus we see that the first 0 and the last 1 are free, while the first 1 and the last 0 are bound. If we now consider two elements of $2^{\underline{n}}$ to be equivalent iff they have the same bound 1's and 0's (e.g., (0, 1, 0, 1), (0, 1, 0, 0), and (1, 1, 0, 1) are all equivalent), then one can show that the equivalence classes are connected, disjoint, symmetric chains which partition $2^{\underline{n}}$ into E_n chains. By a symmetric connected chain of $2^{\underline{n}}$ we mean a totally ordered collection of subsets $R_{n/2-j} \subseteq R_{n/2-j+1} \subseteq \cdots \subseteq R_{n/2+j}$ such that $|R_i| = i$ for each i. (Here j is half integral if n is odd.) Note that the length of a chain containing R is equal to the number of free 1's in R plus the number of free 0's in R.

This partition of $2^{\underline{n}}$ into chains was used by G. Hansel [3] to prove that $\psi(n) \leqslant 3^{E_n}$. He proved that this partition has two very important properties. First, there are exactly $\binom{n}{p} - \binom{n}{p-1}$ chains of length $n - 2p$ where $0 \leqslant p \leqslant [n/2]$. Note that by the length of a chain we mean 1 less than the number of elements in the chain. Second, given any three elements $R_1 \subsetneq R_2 \subsetneq R_3$ of $2^{\underline{n}}$, forming a connected chain (i.e., $|R_i| = |R_{i+1}| - 1$), which belong to a chain of length $n - 2p$, then the relative complement of R_2 in the interval $[R_1, R_3]$ belongs to a chain of length $n - 2p - 2$.

It follows from the second property above, that if one knows the values of an isotone Boolean function f on all chains of length $\leqslant n - 2p - 2$ of the partition, that there will be at most two elements (forming a connected chain) in each chain of length $n - 2p$ for which the values of f have not been predetermined by the monotonicity of f and the known values of 1. If $S \subsetneq T$ is a connected chain of two elements of $2^{\underline{n}}$, then since f is an isotone there are only three choices for f: $f(S) = 0 = f(T)$; $f(S) = 0$ and $f(T) = 1$; $f(S) = 1 = f(T)$. Since there are at most three choices for f on each chain, $\psi(n) \leqslant 3^{E_n}$.

Below we will analyze the properties of this partition further with the use of two groups of permutations. The first of these groups is S_n, the symmetric group on n letters, while the second one is S_{J_n} the symmetric group on J_n letters, where J_n is the number of blocks into which our permuted partitioning chains will be broken. The detailed description of these groups and their operations will be presented below.

For convenience, let $\Omega = \{C_1, \ldots, C_{E_n}\}$ be the set of partitioning chains of $2^{\underline{n}}$ described above. Let the chains be numbered according to length, with shorter chains having smaller subscripts. S_n, being the group of permutations of $\underline{n}$, operates in a natural way on $2^{\underline{n}}$, and consequently takes members of Ω into connected symmetric chains. Thus if $\sigma \in S_n$, and $T \subset \underline{n}$, $T \in \sigma(C_i)$ iff $\sigma^{-1}(T) \in C_i$.

We wish to consider the elements of $\sigma(\Omega)$ grouped into blocks having the following property. Given any two chains, $\sigma(C_i)$ and $\sigma(C_j)$ belonging to the same block, let T_i and T_j be the unique elements of $\sigma(C_i) \cap G_{[n/2],n}$ and $\sigma(C_j) \cap$

$G_{[n/2],n}$ respectively, then $|T_i \cup T_j| > [n/2] + \tau$ or equivalently $|T_i \cap T_j| < [n/2] - \tau$.

More precisely, if $R \in G_{[n/2],n}$ then by $J(R, \rho)$ we mean the set $\{T \in G_{[n/2],n} \mid |R \cap T| = [n/2] - \rho\}$, and by $J(R)$ the set $\bigcup_{\rho=0}^{\tau} J(R, \rho)$. Of course, if $R, T \in G_{[n/2],n}$, then $|J(R)| = |J(T)|$. Finally, let J_n be the smallest integer for which there exists a partition $J^* = \{J_1, \ldots, J_{J_n}\}$ of $G_{[n/2],n}$ such that if $R, S \in J_i$, $R \neq S$, then $R \notin J(S)$. We obtain an upper bound for J_n in Lemma 3. Thus, we will say that $\sigma(C_i)$ and $\sigma(C_j)$ belong to the same block if $\sigma(C_i) \cap G_{[n/2],n}$ and $\sigma(C_j) \cap G_{[n/2],n}$ belong to the same element of J^*.

Let $(\sigma, \theta) \in S_n \times S_{J_n}$ and consider the sequence $\sigma(C_1), \ldots, \sigma(C_{E_n})$. We wish to reorder this sequence depending on the effect of θ on the sequence $J_1, \ldots, J_{J_n}$. We still wish each chain of length k to precede all chains of length $k+2$, but we will use θ to alter the order of various chains of the same length as follows. If $\sigma(C_i)$ and $\sigma(C_j)$ are of the same length and belong to the same block as defined above, then $\sigma(C_i)$ precedes $\sigma(C_j)$ if and only if $i < j$. If $\sigma(C_i)$ and $\sigma(C_j)$ are of the same length, but $\sigma(C_i) \cap G_{[n/2],n} \in J_{k_i}$ and $\sigma(C_j) \cap G_{[n/2],n} \in J_{k_j}$, where $k_i \neq k_j$, then $\sigma(C_i)$ precedes $\sigma(C_j)$ if and only if $\theta(k_i) < \theta(k_j)$.

We work our way through the chains, the $\sigma(C_i)$'s, in the order described above. Suppose that we have assigned values to a monotone function f on the first k chains $\sigma(C_{i_1}), \sigma(C_{i_2}), \ldots, \sigma(C_{i_k})$, and we wish to define f on $\sigma(C_{i_{k+1}})$. If f is already determined on $\sigma(C_{i_{k+1}})$ we simply proceed to the next chain. If f is unpredetermined at exactly one point $\sigma(C_{i_{k+1}})$, we make either of the two possible choices, and then proceed to the next chain. We know, however, that f can be unpredetermined on at most two points of $\sigma(C_{i_{k+1}})$. Suppose this is indeed the case, and let R, S $(R \subset S)$ be the two elements of $\sigma(C_{i_{k+1}})$ on which f is unpredetermined. Consider the elements $\sigma^{-1}(R)$ and $\sigma^{-1}(S)$ which belong to $C_{i_{k+1}}$. Thinking of $\sigma^{-1}(R)$ and $\sigma^{-1}(S)$ as binary n-tuples, it follows from the fact that they both belong to the same chain that $\sigma^{-1}(S)$ has a free 1 where $\sigma^{-1}(R)$ has a free 0, and that otherwise they are identical. Let this 1 be in position j. We call the position j the indicator of the triple (R, S, σ) and denote it by $\text{ind}(R, S, \sigma)$. We now count the number of *bound* 1's in $\sigma^{-1}(S)$ in the positions to the right of $\text{ind}(R, S, \sigma)$. If the number of such bound 1's is at least half the total number of bound 1's in $\sigma^{-1}(S)$, we set $f(R) = 0$. Then we make either of two permissible choices for $f(S)$, and proceed to the next chain. If, on the other hand, the total number of such bound 1's is less than half the total number of bound 1's in $\sigma^{-1}(S)$, we set $f(S) = 1$. We then make either of two permissible choices for $f(R)$, and proceed to the next chain.

The procedure described in the preceding paragraph of constructing an isotone function using the order induced by a given element of $S_n \times S_{J_n}$ shall be referred to as Procedure I.

Note that Procedure I never requires that more than two choices be made in any given chain. Unfortunately, some isotone functions cannot be constructed by Procedure I. However, we will show that modifying Procedure I slightly enables us to construct every isotone function at least once.

We modify Procedure I by simply allowing ourselves a certain number ($\leqslant K$) of chains in which we make one of three choices, the way Hansel [3] did. We will show below that there is a $K \leqslant cE_n/n$ (c a constant) for which this modified procedure (referred to Procedure II) does indeed produce every isotone function at least once.

More precisely, we claim that every isotone function will be constructed at least once by doing the following in all possible ways. Pick $(\sigma, \theta) \in S_n \times S_{J_n}$, and single out K chains from $\sigma(C_1), \ldots, \sigma(C_{E_n})$ as being special. Order them as above using θ, and begin defining an isotone function one chain at a time, allowing the full three choices (if necessary) in any special chain, while using the indicator (if necessary) to allow at most two choices in any nonspecial chain. Thus it follows that

$$|FD(n)| \leqslant |S_n| \cdot |S_{J_n}| \binom{E_n}{K} 2^{E_n - K} 3^K$$

$$\leqslant n!\, n! (2^{\sqrt{n} \ln n \log n})! \binom{E_n}{K} 2^{E_n} 2^{\log (3/2) K} \leqslant 2^{E_n (1 + (c \log n)/n)}$$

using the bound provided by Lemma 3.

We now show that we may assume that the K special chains always include all chains of length $> 2\tau$ (recall $\tau = \sqrt{n} \ln n$). There are approximately $\binom{n}{n/2+\tau}$ chains of length $> 2\tau$, which is approximately equal to

$$E_n \exp\left(-\frac{2}{n}(n(\ln n)^2)\right) = E_n \frac{1}{n^2 \ln n}$$

(see [1, p. 170, Theorem 1]) which, for large n, is negligible compared to the bound for K.

The main argument is best expressed in probabilistic terminology and we will use the following notation. If X is a simple space, A, B events on X and F a random variable on X, then $P(A)$ denotes the probability of A, $P(A|B)$ the conditional probability of A given B, and $E(F)$ the expectation of F. Definitions and properties of all terms can be found in Feller [1]. Our sample space shall be $S_n \times S_{J_n}$. Pick an isotone Boolean function and an element $R \in 2^n$. Consider the random variable $U_{f,r}$ defined as follows. $U_{f,r}((\sigma, \theta)) = 1$ if either:

Case (i). (a) $f(R) = 1$; (b) knowing the values of f on *all the earlier* chains of the sequence obtained from Ω by the action of (σ, θ) still leaves R and T unpredetermined, where $R \supset T$ and T belongs to the same chain $\sigma(C_j)$ (of length $\leqslant 2\tau$) as R; (c) $f(T) = 1$; (d) the number of bound 1's in $\sigma^{-1}(R)$ to the right of $\text{ind}(T, R, \sigma)$ is at least half the total number of bound 1's in $\sigma^{-1}(R)$.

Case (ii). (a) $f(R) = 0$; (b) knowing the values of f on *all the earlier* chains of the sequence obtained from Ω by the action of (σ, θ) still leaves R and T unpredetermined, where $R \subset T$ and T belongs to the same chain $\sigma(C_j)$ (of length $\leqslant 2\tau$) as R; (c) $f(T) = 0$; (d) the number of bound 1's to the right of $\text{ind}(R, T, \sigma)$ in $\sigma^{-1}(T)$ is less than half the total number of bound 1's in $\sigma^{-1}(T)$. We now define the random variable $U_f = \Sigma_{R \in 2^{\underline{n}}} U_{f,R}$.

It follows from the definitions of $U_{f,R}$ that $U_f((\sigma, \theta))$ is the number of chains on which Procedure I would force us to define f incorrectly assuming we had defined f correctly on all preceding chains, i.e., it tells us how many "special" chains (chains on which we should allow three choices) we would need if we wanted to use the ordering induced by (σ, θ) in order to be able to construct f by using Procedure II. Note that we are already counting all chains of length $> 2\tau$ as special for reasons discussed earlier. What we intend to show is that for any isotone function f $E(U_f) \leqslant cE_n/n$. This last fact implies that there exists $(\sigma_f, \theta_f) \in S_n \times S_{J_n}$ such that $U_f((\sigma_f, \theta_f)) \leqslant cE_n/n$ (this is just the method of averaging dressed up a little). But this means that every monotone function will be constructed at least once by applying Procedure II (allowing cE_n/n special chains) to every element of $S_n \times S_{J_n}$, and our result will have been proven.

We shall prove later that $E(U_f) \leqslant cE_n/n$, but at this point it might be helpful if we gave a short sketch of how we actually prove that $E(U_f) \leqslant cE_n/n$. To begin with, $E(U_f) = \Sigma_{R \in 2^{\underline{n}}} E(U_{f,R})$. Note also that if $|R| > [n/2] + \tau$ or $|R| < \{n/2\} - \tau$, then $E(U_{f,R}) = 0$, since R is in a chain of length $> 2\tau$, and we consider all such chains to be special. We now subdivide the remaining elements into two classes, those which are mapped to 1 and those mapped to 0 by f. More precisely, let

$$\Delta_{f,1} = \{R \in 2^{\underline{n}} \mid \{n/2\} - \tau \leqslant |R| \leqslant [n/2] + \tau \text{ and } f(R) = 1\},$$

$$\Delta_{f,0} = \{R \in 2^{\underline{n}} \mid \{n/2\} - \tau \leqslant |R| \leqslant [n/2] + \tau \text{ and } f(R) = 0\}.$$

Obviously,

$$E(U_f) = \sum_{R \in \Delta_{f,1}} E(U_{f,R}) + \sum_{R \in \Delta_{f,0}} E(U_{f,R}).$$

We will show in detail that $\Sigma_{R \in \Delta_{f,1}} E(U_{f,R})$ is bounded by cE_n/n for some constant c. The proof that $\Sigma_{R \in \Delta_{f,0}} E(U_{f,R})$ is bounded by a factor of the same form is similar and will be omitted. Now observe that $E(U_{f,R}) = P(U_{f,R} = 1)$.

To calculate $P(U_{f,R} = 1)$ for $R \in \Delta_{f,1}$, it is necessary to partition $\Delta_{f,1}$ into sets $L_0, \ldots, L_{[n/2]+\tau}$, where $L_i = \{R \in \Delta_{f,1} \mid R \text{ covers exactly } i \text{ elements of } \Delta_{f,1}\}$. Thus, for example, if $R \in L_0$, then $E(U_{f,R}) = 0$. Consequently,

$$\sum_{R \in \Delta_{f,1}} E(U_{f,R}) = \sum_{i=1}^{[n/2]+\tau} \sum_{R \in L_i} P(U_{f,R} = 1).$$

Hence it is sufficient to know the various $P(U_{f,R} = 1)$ for $R \in L_i$.

Basically what we do is consider three cases:

$$R \in \bigcup_{q=1}^{10 \ln n - 1} L_q, \quad R \in \bigcup_{q=10 \ln n}^{n/4} L_q, \quad \text{and} \quad R \in \bigcup_{q=n/4+1}^{[n/2]+\tau}$$

(for n sufficiently large). Lemma 9 shows that the number of elements in the first two cases cannot exceed cE_n where c is a constant. Obviously, the number of elements in the third case cannot exceed $2^{\underline{n}}$. Below, we present a *short heuristic outline* of how each case is dealt with. We begin with the second case since it is the easiest.

If $R \in \bigcup_{q=10 \ln n}^{n/4} L_q$ and $U_{f,R} = 1$, then the majority of bound ones are to the right of the indicator point (i.e., $\text{ind}(R, S, \sigma)$ where R covers S). Suppose now that by the *gap of* (R, σ) we mean the positions in $\sigma^{-1}(R)$ between $\text{ind}(R, S, \sigma)$ and the first free 1 to the right of $\text{ind}(R, S, \sigma)$ if it exists; otherwise the gap of (R, σ) is simply all of the positions of $\sigma^{-1}(R)$ to the right of $\text{ind}(R, S, \sigma)$. Since we have many bound 1's to the right of $\text{ind}(R, S, \sigma)$, either there are at least $n/100$ bound 1's in the gap, or somewhere on the order of $n/2$ bound 1's to the right of the gap. In the first case, we show that the probability f being unpredetermined on R and R covering an element of $\Delta_{f,1}$ is bounded by c/n (c a constant), since it is fairly likely some of the elements of $\Delta_{f,1}$ which are covered by R will be mapped by σ into chains of the same length as R, and in order for f to be unpredetermined on R all such elements must appear later in the ordering which is also not very probable. The second case is handled by showing that the probability that no element of $\Delta_{f,1}$ covered by R is mapped into a shorter chain by σ decreases exponentially in q, and again we get a factor of the form c/n. Putting this all together, we see that $P(U_{f,R} = 1) \leqslant c/n$ (c some constant), and the contribution of all R's for which $R \in \bigcup_{q=10 \ln n}^{n/4} L_q$ is bounded by cE_n/n (recall our convention).

The case where $R \in \bigcup_{q=1}^{10 \ln n - 1} L_q$ is handled similarly, although since q is small we must carefully analyze what happens when we have on the order of $n/2$ bound 1's to the right of the gap. However, our analysis shows that we may safely use c/n an as upper bound for $E(U_{f,R})$.

The last case is complicated by the fact that there may be on the order of 2^n such elements. Consequently, we show that for all such R, $E(U_{f,R})$ is bounded by $c/n^{3/2}$. The idea here is that since R covers so many elements on which f is 1, it becomes increasingly unlikely that R will be unpredetermined.

We realize that the above is very sketchy, but its only purpose is to help guide the reader through the technical maze ahead. In the next section, we present some lemmas which we need to prove the main result. The reader may wish to glance briefly over them. We return to the main argument later and derive an

explicit formula for $E(U_{f,R})$. The lemmas which we prove are necessary in order to derive bounds for this formula.

Some lemmas.

LEMMA 1.

$$|J(R)| \leqslant \binom{[n/2]}{\tau} \cdot \binom{\{n/2\}+\tau}{\tau}.$$

PROOF. $T \in J(R, \rho)$ for some $0 \leqslant \rho \leqslant \tau$ iff there exists $U \in G_{[n/2]-\tau,n}$ such that $U \subset R \subset T$. There exist $\binom{[n/2]}{\tau}$ U's in $G_{[n/2]-\tau,n}$ such that $U \subset R$. Each such U is contained in $\binom{\{n/2\}+\tau}{\tau}$ elements of $G_{[n/2],n}$. □

The following lemma is easily proved and hence its proof is omitted.

LEMMA 2. *Let $H \subset G_{[n/2],n}$ be nonempty, and let $J \subset H$ be a set of maximal cardinality having the following property*:

(*) *$R, S \in J, R \neq S$ imply that $R \notin J(S)$. Then $|J| > \{|H|/|J(R)|\}$.* □

LEMMA 3. $J_n \leqslant n|J(R)| \leqslant 2^{\sqrt{n} \ln n \log n}$ *where R is any element of $G_{[n/2],n}$.*

PROOF. We will prove the lemma by constructing a family of disjoint sets $\{R_1^*, \ldots, R_\lambda^*\}$, with $\lambda \leqslant n|J(R)|$ and such that each R_i^* has property (*) of Lemma 2.

Using Lemma 2, we let R_1^* be a set of cardinality $\{E_n/|J(R)|\}$ having property (*). Inductively, we let $R_k^* \subset B - \bigcup_{i=1}^{k-1} R_i^*$ be a set of cardinality $\{(E_n - \Sigma_{i=1}^{k-1} |R_i^*|)/J(R)\}$ having property (*). It is straightforward to see that

$$\sum_{i=1}^{k} |R_i^*| \geqslant \frac{E_n}{|J(R)|} \sum_{i=0}^{k-1} F^i,$$

where $F = 1 - (1/|J(R)|)$.

Consequently, we have the following inequalities:

$$E_n \geqslant \sum_{i=1}^{k} |R_i^*| \geqslant \frac{E_n}{|J(R)|}\left(\frac{1-F^k}{1-F}\right) = E_n\left(1 - \left(1 - \frac{1}{|J(R)|}\right)^k\right)$$

$$\geqslant E_n - E_n \exp\left\{-\frac{k}{|J(R)|}\right\}.$$

Hence, if $k \geqslant n|J(R)|$, $\Sigma_{i=1}^{k} |R_i^*| = E_n$. Actually, it is easy to see that the family is constructed before $n \ln 2|J(R)|$ steps are taken. A simple estimate shows that $n|J(R)| \leqslant 2^{\sqrt{n} \ln n \log n}$. □

The following lemmas are intended to provide bounds for binomial coefficients and combinations of binomial coefficients. The proof of Lemma 4 is straightforward.

LEMMA 4. *Let A, B, C be nonnegative integers. Then*

$$\frac{\binom{A-B}{C}}{\binom{A}{C}} \leqslant \left(1 - \frac{B}{A}\right)^C \leqslant e^{-BC/A}. \quad \square$$

The following lemma can be proven using the ideas in Feller [1, pp. 168–170], and will be useful for estimating binomial coefficients (see also [1, Problem 14, p. 181]).

LEMMA 5. *Let k be such that both k and $n-k$ go to ∞ as n goes to ∞. Then*

$$(*) \qquad \binom{n}{k} \sim \sqrt{\frac{n}{2\pi k(n-k)}}\, 2^n e^{-f(k)},$$

where

$$f(k) = \sum_{j=1}^{\infty} \left(\frac{2\delta_k}{n}\right)^{2j} \frac{n}{2j(2j-1)}$$

with $\delta_k = |k - \frac{1}{2}n|$.

(*Note.* If say $\ln n \leqslant k \leqslant n - \ln n$, $\binom{n}{k}$ converges uniformly to the right-hand side of (*) above throughout the entire range of values of k.) □

As consequences of Lemma 5, we have the following two lemmas.

LEMMA 6. *If k is such that $\lim_{n\to\infty} (k - \frac{1}{2}n)^4/n^3 = 0$ then*

$$\binom{n}{k} \sim \sqrt{\frac{2}{\pi n}}\, 2^n \exp\left(-\frac{2}{n}\left(k - \frac{1}{2}n\right)^2\right) \sim \binom{n}{[n/2]} \cdot \exp\left(-\frac{2}{n}\left(k - \frac{1}{2}n\right)^2\right). \quad \square$$

Note that Lemma 6 is a form of [1, Theorem 1, p. 170]. The next lemma gives us an upper bound of the same form for all binomial coefficients.

LEMMA 7. *For n sufficiently large and for $0 \leqslant k \leqslant n$,*

$$\binom{n}{k} \leqslant E_n \exp\left(-\frac{2}{n}\left(k - \frac{1}{2}n\right)^2\right)(1+\epsilon)$$

where $\epsilon \longrightarrow 0$ as $n \longrightarrow \infty$.

(*Note.* We can replace E_n by $(\sqrt{2/\pi n})(2^n)$.)

PROOF. By symmetry we need only consider $0 \leqslant k \leqslant n/2$. If $k \leqslant \ln n$, then

$$\binom{n}{k} \leqslant \left(\frac{ne}{k}\right)^k \leqslant E_n \exp\left(-\frac{2}{n}\left(k - \frac{1}{2}n\right)^2\right)(1+\epsilon)$$

for sufficiently large n and for any $\epsilon > 0$.

Now $-f(k)$ of Lemma 5 can be written as $-2(k-\frac{1}{2}n)^2/n - g(k)$, where

$$g(k) = \sum_{j=2}^{\infty} \left(\frac{2\delta_k}{n}\right)^{2j} \frac{n}{2j(2j-1)},$$

with $\delta_k = k - \frac{1}{2}n$. Note that all the terms of $g(k)$ are positive.

Now if $\ln n \leqslant k \leqslant n/2$, then

$$\binom{n}{k} \leqslant (1+\epsilon_1)\sqrt{\frac{n}{2\pi k(n-k)}}\,2^n e^{-f(k)},$$

for some $\epsilon_1 > 0$, where $\epsilon_1 \to 0$ as $n \to \infty$.

But

$$(1+\epsilon_1)\sqrt{\frac{n}{2\pi k(n-k)}}\,2^n e^{-f(k)} \leqslant (1+\epsilon_2)E_n \exp\left(-\frac{2}{n}\left(k-\frac{1}{2}n\right)^2\right) \cdot e^{-g(k)}\sqrt{\frac{n^2}{2\pi k(n-k)}}.$$

If in addition we have that $k \leqslant n/2 - n^{9/10}$, $e^{-g(k)} < e^{-4/3n} \ll 1/n^2$, so the lemma is true in this case also. We note that in the remaining case $n/2 - n^{9/10} \leqslant k \leqslant n/2$, the factor $\sqrt{n^2/4k(n-k)}$ is bounded by something of the form $(1+\epsilon_3)$, where $\epsilon_3 \to 0$ as $n \to \infty$ regardless of the value of $e^{-g(k)}$, so again the lemma is true. □

REMARK. In using Lemma 7, we will often omit the factor of $(1+\epsilon)$ and just use the right-hand side as a bound for the left-hand side utilizing implicitly the convention introduced earlier. The reader may have observed that some of the preceding results can be sharpened and that in some cases n is sufficiently large for small values of n (e.g., 10). However, since such refinements will not improve our main result we have chosen to omit them.

LEMMA 8. *The number of distinct Boolean $(s+2t)$-tuples which can be formed from s free* 0*'s and* 1*'s $(s \geqslant 0)$ and t bound pairs of a* 1 *and a* 0 *of the form $\underline{X}\ Y\ \underline{X}\ Y\ \underline{X} \cdots \underline{X}\ Y\ \underline{X}$, where each X is either empty or some set of bound* 1-0*'s, and each Y is either a free* 0 *or a free* 1 *(all the free* 0*'s are to the left of all the free* 1*'s of course) is*

$$\binom{s+2t}{s+t} - \binom{s+2t}{s+t+1} = \frac{s+1}{s+t+1}\binom{s+2t}{s+t}.$$

PROOF. Each such element as described above belongs to a chain (of Ω_{s+2t}) of $2^{\underline{s+2t}}$ whose largest member has cardinality $s+t$. The number of such chains is the number of chains of Ω_{s+2t} which stop at level $s+t$ and is

$$\binom{s+2t}{s+t} - \binom{s+2t}{s+t+1}. \quad \square$$

A proof of the following lemma can be found in [4].

LEMMA 9. $\Sigma_{i=0}^{r} |L_i| \leqslant (\{n/2\}/([n/2] - \tau - r))E_n$.

The main argument. The following additional notation will make for increased clarity in the exposition.

Notation. For $R \in L_i$, let $b(R)$ denote the elements of $\Delta_{f,1}$ which are *covered* by R. For $\sigma \in S_n$, let $\sigma(C)_R$ denote the chain $\sigma(C_i)$ which contains R. For a given $(\sigma, \theta) \in S_n \times S_{J_n}$, let $\mathrm{ord}(\sigma(C_i))$ denote the order of $\sigma(C_i)$ as induced by σ and θ, i.e., $\mathrm{ord}(\sigma(C_i))$ is equal to one more than the number of chains considered before $\sigma(C_i)$ using Procedure II with (σ, θ). Finally, for any chain C in $2^{\underline{n}}$, let $\mathrm{len}(C)$ denote the length of C.

Fix a particular element R of some L_q $(q \geqslant 1)$ so as to avoid additional subscripts, and consider the following events defined on our sample space $S_n \times S_{J_n}$:

A_1 is the event that $\sigma(C)_R \cap b(R) \neq \varnothing$, i.e., R covers an element of $\Delta_{f,1}$ in its chain;

A_2 is the event that for all $T \in b(R) - \sigma(C)_R$, $\mathrm{ord}(\sigma(C)_T) > \mathrm{ord}(\sigma(C)_R)$, i.e., that R is unpredetermined with respect to the ordering induced by (σ, θ);

A_3 is the event that there exists an element T in $\sigma(C)_R$ covered by R, and the number of bound 1's in $\sigma^{-1}(R)$ to the right of $\mathrm{ind}(T, R, \sigma)$ is at least half the total number of bound 1's in $\sigma^{-1}(R)$;

A_4 is the event that $\mathrm{len}(\sigma(C)_R) \leqslant 2\tau$. Clearly,

$$P(U_{f,R} = 1) = P(A_1 \cap A_2 \cap A_3 \cap A_4).$$

It is necessary to subdivide the events further in order to be able effectively to compute probabilities. Let B_k $(k \geqslant 0)$ be the event that $\mathrm{len}(\sigma(C)_R) = k$. Let C_λ $(\lambda \geqslant 0)$ be the event that: (a) there exists an element T in $\sigma(C)_R$ covered by R; (b) either there is only one free 1 in $\sigma^{-1}(R)$ and λ bound 1's to the right of $\mathrm{ind}(T, R, \sigma)$, or there are at least two free 1's in $\sigma^{-1}(R)$ and λ bound 1's between $\mathrm{ind}(T, R, \sigma)$ and the next free 1 to the right of $\mathrm{ind}(T, R, \sigma)$. Finally, let D_d $(d \geqslant 0)$ be the event that there exists an element T in $\sigma(C)_R$ covered by R and d bound 1's to the right of $\mathrm{ind}(T, R, \sigma)$.

The following observations are very important in the sequel. The number of free 1's in $\sigma^{-1}(R)$ is equal to $|R| - \frac{1}{2}n + \frac{1}{2}\mathrm{len}(\sigma(C)_R)$, the number of free 0's in $\sigma^{-1}(R)$ is equal to $\frac{1}{2}\mathrm{len}(\sigma(C)_R) + \frac{1}{2}n - |R|$, and the number of bound 1's in $\sigma^{-1}(R)$ is equal to the number of bound 0's in $\sigma^{-1}(R)$, which in turn is equal to $\frac{1}{2}(n - \mathrm{len}(\sigma(C)_R))$. It now follows that

$$P(A_1 \cap A_2 \cap A_3 \cap A_4)$$

$$(1) \quad = \sum_{k=\rho(R,n)}^{2\tau} \sum_{d=1/4(n-k)}^{(n-k)/2} \sum_{\lambda=0}^{d} P(A_1 \cap A_2 \cap C_\lambda \cap D_d \cap B_k)$$

$$= \sum_{k=\rho(R,n)}^{2\tau} \sum_{d=1/4(n-k)}^{(n-k)/2} \sum_{\lambda=0}^{d} P(A_1 \cap A_2 | C_\lambda \cap D_d \cap B_k) P(D_d \cap C_\lambda | B_k) P(B_k)$$

where $\rho(R, n) = \max\{2 + n - 2|R|, 2|R| - n\}$. The lower bound for k in the preceding summation is derived from the fact that the number of free 1's in $\sigma^{-1}(R)$ must be at least one and the number of free 0's in $\sigma^{-1}(R)$ is nonnegative. We next estimate the magnitudes of the factors in (1).

Proceeding as in Lemma 8, it is easy to see that

$$P(B_k) = \frac{(2(k+1)/(n+k+2))\binom{n}{(n+k)/2}}{\binom{n}{|R|}}.$$

From Lemma 6, it follows that

$$P(B_k) \leqslant (1+\epsilon)\frac{2(k+1)}{n+k+2} \exp\left(\frac{1}{2n}((2|R|-n)^2 - k^2)\right),$$

where $\epsilon \longrightarrow 0$ as $n \longrightarrow \infty$. Note that the exponential factor is $\leqslant 1$.

The next factor which we consider is $P(A_1 \cap A_2 | C_\lambda \cap D_d \cap B_k)$. If we know that $C_\lambda \cap D_d \cap B_k$ has occurred, then $\sigma^{-1}(R)$ must look like $(X, 1, \lambda$ bound 1-0 pairs, $Y)$ where X consists of $\frac{1}{2}k + \frac{1}{2}n - |R|$ free 0's intermixed with $\frac{1}{2}(n-k) - d$ bound 1-0 pairs, while Y simply consists of $|R| - \frac{1}{2}n + \frac{1}{2}k - 1$ free 1's with $d - \lambda$ bound 1-0 pairs intermixed. It is necessary to determine the number of elements S covered by R such that $\operatorname{ord}(\sigma(C)_S) \geqslant \operatorname{ord}(\sigma(C)_R)$. Let H be the set $\{j \in \underline{n} |$ there is a 1 in the jth position of $\sigma^{-1}(R)\}$. For $j \in H$, let $Z_j \in 2^{\underline{n}}$ be such that $\sigma^{-1}(Z_j)$ is the same as $\sigma^{-1}(R)$ except that there is a 0 in the jth position of $\sigma^{-1}(Z_j)$. Clearly, the set of the Z_j's is exactly the set of elements covered by R. If $j < \operatorname{ind}(T, R, \sigma)$, $\operatorname{len}(\sigma(C)_{Z_j}) = \operatorname{len}(\sigma(C)_R) + 2$, and consequently $\operatorname{ord}(\sigma(C)_{Z_j}) \not\leqslant \operatorname{ord}(\sigma(C)_R)$. If $j > \operatorname{ind}(T, R, \sigma) + 2\lambda$, $\operatorname{len}(\sigma(C)_{Z_j}) = \operatorname{len}(\sigma(C)_R) - 2$, and consequently $\operatorname{ord}(\sigma(C)_{Z_j}) < \operatorname{ord}(\sigma(C)_R)$. Of course, $Z_{\operatorname{ind}(T,R,\sigma)} = T$. Finally, we note that for $\operatorname{ind}(T, R, \sigma) < j \leqslant \operatorname{ind}(T, R, \sigma) + 2\lambda$, $\operatorname{len}(\sigma(C)_{Z_j}) = \operatorname{len}(\sigma(C)_R)$ and the ordering depends on θ. It is here that we use the partition $J^* = \{J_1, \ldots, J_{J_n}\}$ defined earlier. Namely, for $\operatorname{ind}(T, R, \sigma) < j_1, j_2 \leqslant \operatorname{ind}(T, R, \sigma) + 2\lambda$, $\sigma(C)_{Z_{j_1}}$, $\sigma(C)_{Z_{j_2}}$ and $\sigma(C)_R$ must belong to different blocks, and consequently S_{J_n} acts as if it were the symmetric permutation group of the set $X = \{\sigma(C)_R\} \cup \{\sigma(C)_{Z_j} | \operatorname{ind}(T, R, \sigma) < j \leqslant \operatorname{ind}(T, R, \sigma)\}$ in the sense that if we look at the orderings induced by S_{J_n} on X we will see that any permutation

of the elements of X is just as frequent as any other. Now for $A_1 \cap A_2$ to occur, T must belong to $\Delta_{f,1}$, no $Z_j \notin \Delta_{f,1}$ for $j > \operatorname{ind}(T, R, \sigma) + 2\lambda$ or for those j, $\operatorname{ind}(T, R, \sigma) < j \leqslant \operatorname{ind}(T, R, \sigma) + 2\lambda$, such that $\operatorname{ord}(\sigma(C)_{Z_j}) < \operatorname{ord}(\sigma(C)_R)$.

Consider the event $F_{q'}$, which is that there are exactly q' j's, $\operatorname{ind}(T, R, \sigma) < j \leqslant \operatorname{ind}(T, R, \sigma) + 2\lambda$, such that $Z_j \in \Delta_{f,1}$. It follows that

$$P(A_1 \cap A_2 | C_\lambda \cap D_d \cap B_k) = \sum_{q'=0}^{\min\{q-1,\lambda\}} P(A_1 \cap A_2 | C_\lambda \cap D_d \cap B_k \cap F_{q'}) P(F_{q'} | C_\lambda \cap D_d \cap B_k).$$

Consider the factor $P(A_1 \cap A_2 | C_\lambda \cap D_d \cap B_k \cap F_{q'})$. If $(\sigma, \theta) \in C_\lambda \cap D_d \cap B_k \cap F_{q'}$, then there exist q' j's, $\{j_1, \ldots, j_{q'}\}$, $\operatorname{ind}(T, R, \sigma) < j \leqslant \operatorname{ind}(T, R, \sigma) + g$, such that $Z_{j_l} \in \Delta_{f,1}$. By symmetry we may assume that we are only considering those pairs (σ, θ), such that for a fixed set $\{T_1, \ldots, T_{q'}\} \subset b(R) \cap \Delta_{f,1}$, $Z_{j_{\operatorname{ind}(T,R,\sigma)+i}} = T_i$, $1 \leqslant i \leqslant q'$. Actually, we may concentrate our attention only on the pairs for which $\sigma^{-1}(R)$ is some fixed element. In this case S_n can be viewed rather as $S_{|R|}$.

Pick such a pair (σ, θ). In order for A_1 to occur (recall $F_{q'}$ has occurred), of the remaining $|R| - q'$ elements of $b(R)$ whose images under σ^{-1} have not yet been determined, σ must map exactly one of the remaining $q - q'$ elements of $b(R) \cap \Delta_{f,1} - \{T_1, \ldots, T_{q'}\}$ into the same chain as R and map no additional element of $b(R) \cap \Delta_{f,1}$ into a chain of length k. Thus A_1 will occur only in the proportion $(q - q')/(|R| - \lambda)$. In order for A_2 to occur simultaneously, it is necessary and sufficient that the remaining $q - q' - 1$ elements of $b(R) \cap \Delta_{f,1} - \{T_1, \ldots, T_{q'}, T_{q'+1}\}$ (where $T_{q'+1}$ is in the same chain as R) be mapped into the Z_j's for $j < \operatorname{ind}(T, R, \sigma) = 3n/2 - k/2 - 2d - |R|$. There are $\frac{1}{2}(n-k) - d$ such Z_j's and $\operatorname{ord}(\sigma(C)_{Z_{\operatorname{ind}(T,R,\sigma)+i}}) > \operatorname{ord}(\sigma(C)_R)$ for $1 \leqslant i \leqslant q'$.

The first condition only affects the first component of (σ, θ) and gives a factor of

$$\frac{\binom{(n-k)/2-d}{q-q'-1}}{\binom{|R|-\lambda-1}{q-q'-1}}.$$

The second condition only affects the second component of (σ, θ) and gives a factor of $1/(q' + 1)$. Thus we see that

$$P(A_1 \cap A_2 | C_\lambda \cap D_d \cap B_k \cap F_{q'}) = \frac{1}{q'+1} \frac{q-q'}{|R|-\lambda} \frac{\binom{(n-k)/2-d}{q-q'-1}}{\binom{|R|-\lambda-1}{q-q'-1}}$$

It is not hard to see, reasoning as above, that

$$P(F_{q'} | C_\lambda \cap D_d \cap B_k) = \binom{\lambda}{q'} \frac{\binom{|R|-\lambda}{q-q'}}{\binom{|R|}{q}}.$$

(*Note.* This is the hypergeometric distribution, see [1, p. 41].) Thus we know the value of $P(A_1 \cap A_2 | C_\lambda \cap D_d \cap B_k)$.

We now derive an expression for $P(D_d \cap C_\lambda | B_k)$. We proceed much the same way as above. We first observe that $P(D_d \cap C_\lambda | B_k) = P(C_\lambda | B_k \cap D_d) \cdot P(D_d | B_k)$.

Now $P(D_d | B_k) = N_1 N_2 / N_3$, where N_3 is the number of chains of length k, N_1 is the number of ways of intermixing $\frac{1}{2}(n-k) - d$ bound 1-0 pairs with $\frac{1}{2}k + \frac{1}{2}n - |R|$ free 0's, and N_2 is the number of ways of intermixing d bound 1-0 pairs with $|R| - \frac{1}{2}n + \frac{1}{2}k - 1$ free 1's. We know N_3 from the calculation of $P(B_k)$, while N_1 and N_2 can be calculated by Lemma 8.

Thus

$$P(D_d|B_k) = \frac{\frac{\frac{1}{2}(n+k) - |R| + 1}{(n - |R| - d + 1)} \binom{3n/2 - \frac{1}{2}k - |R| - 2d}{n - |R| - d}}{\frac{2(k+1)}{2 + k + 2}\binom{n}{((n+k)/2)}} \cdot \frac{(|R| - \frac{1}{2}(n-k))}{(|R| \frac{1}{2}(n-k) + d)} \binom{|R| - \frac{1}{2}(n-k) + 2d - 1}{|R| - \frac{1}{2}(n-k) + d - 1}.$$

Again with the help of Lemma 8, we see that

$$P(C_\lambda | B_k \cap D_d) = \frac{\frac{1}{\lambda+1}\binom{2\lambda}{\lambda} \frac{(|R| - \frac{1}{2}(n-k) - 1)}{(|R| - \frac{1}{2}(n-k) + (d-\lambda) - 1)} \binom{|R| - \frac{1}{2}(n-k) + 2(d-\lambda) - 2}{|R| - \frac{1}{2}(n-k) + (d-\lambda) - 2}}{\frac{(|R| - \frac{1}{2}(n-k))}{(|R| - \frac{1}{2}((n-k) + d))} \binom{|R| - \frac{1}{2}(n-k) + 2d - 1}{|R| - \frac{1}{2}(n-k) + d - 1}}$$

(unless $|R| = \frac{1}{2}(n-k) + 1$, when the numerator $= 1$ when $d = \lambda$, 0 otherwise).

From (1) and the above, we get

$$E(U_{f,R}) = \sum_k \sum_d \sum_\lambda \sum_{q'} Q_1 Q_2 Q_3 Q_4 Q_5, \tag{2}$$

where the indices k, d, λ, q' have the same ranges as above and

$$Q_1 = P(A_1 | C_\lambda \cap D_d \cap B_{k'}), \quad Q_2 = 1/(q'+1),$$

$$Q_3 = P(A_2 | C_\lambda \cap D_d \cap B_k \cap F_{q'} \cap A_1)/Q_2, \quad Q_4 = P(F_{q'} | C_\lambda \cap D_d \cap B_k \cap A_1),$$

and

$$Q_5 = P(C_\lambda \cap D_d \cap B_k).$$

We can simplify (2) to get

$$\sum_k \sum_d \sum_\lambda Q_5 \frac{1}{\lambda+1} \frac{\binom{\frac{1}{2}(n-k)-(d-\lambda)+1}{q}}{\binom{|R|}{q}} \sum_{q'} \frac{\binom{\lambda+1}{q'+1}\binom{\frac{1}{2}(n-k)-d}{q-q'-1}}{\binom{\frac{1}{2}(m-k)-(d-\lambda)+1}{q}}$$

(where we only sum for those k, λ, d such that $q \leqslant \frac{1}{2}((n-k) - (d-\lambda) + 1)$). The terms inside $\Sigma_{q'}$ are those of a hypergeometric series, and hence their sum does not exceed 1.

Lemma 4 implies that $E(U_{f,R}) \leqslant \Sigma_k \Sigma_d \Sigma_\lambda Q$, where

$$Q = (1/(\lambda+1)) \exp(-q(|R| - \tfrac{1}{2}(n-k) + (d-\lambda) + 1)/|R|) P(C_\lambda \cap D_d \cap B_k).$$

First consider those R for which $10 \ln n \leqslant q \leqslant n/4$. Then

$$E(U_{f,R}) \leqslant \sum_k \sum_d \sum_{\lambda > n/100} Q + \sum_k \sum_d \sum_{\lambda < n/100} Q.$$

If $\lambda \geqslant n/100$, then $Q \leqslant cP(C_\lambda \cap D_d \cap B_k)/n$ (where c is a constant on the order of 100) and $\Sigma_k \Sigma_d \Sigma_{\lambda > n/100} Q \leqslant c/n$. If $\lambda < n/100$, then $|R| - (n-k)/2 + (d-\lambda) + 1 > |R|/10$ for n sufficiently large since $d \geqslant (n-k)/4$ and $k \leqslant 2\tau$. Consequently, the exponential term is not greater than $1/n$, and as before $\Sigma_k \Sigma_d \Sigma_{\lambda < n/100} Q \leqslant 1/n$. Thus $E(U_{f,R}) \leqslant c/n$ (recall the convention that c is a dummy constant). From Lemma 9 it follows that the number of R's for which q is in the range we are considering is less than $10E_n$ (for n sufficiently large). Hence

$$\sum_{i=10 \ln n}^{n/4} \sum_{R \in L_i} E(U_{f,R}) \leqslant \frac{c}{n} E_n.$$

Thus it only remains for us to deal with the cases where $q < 10 \ln n$ and $q > n/4$.

In the first case, the summand $\Sigma_k \Sigma_d \Sigma_{\lambda > n/100} Q$ is not greater than c/n for the same reasons as above. To calculate the contribution of the terms for $\lambda < n/100$ we return to (2). We rewrite it slightly as follows:

$$\frac{1}{|R|} \sum_k \sum_d \sum_{\lambda < n/100} Q_5 \sum_{q'} \frac{q}{q'+1} Q_3 Q_4.$$

We claim that there exists a constant r, such that if $q \geqslant r$, $qQ_3/(q'+1) \leqslant 1$ (for $|R|$, i.e., sufficiently large). Once we prove this, our bound of c/n will be obtained as follows. For $q \geqslant r$, the sum over q' is $\leqslant 1$, as is the sum of Q_5 over k, d, λ. Thus $1/|R|$ would be our bound. But $1/|R| < c/n$ for sufficiently large n, since $[n/2] - \tau \leqslant |R| \leqslant [n/2] + \tau$. For $q \leqslant r$, the sum over q' is $\leqslant r$, and thus the factor is bounded by $r/|R|$. Again using Lemma 9, we can show that

$$\sum_{i=1}^{10 \ln n} \sum_{R \in L_i} E(U_{f,R}) \leqslant \frac{c}{n} E_n.$$

Now we prove the existence of r. By Lemma 4, $Q_3 \leqslant \exp(-h(q - q' - 1))$ for some constant $h > 0$ and all $|R|$ sufficiently large. It is easy to see that for any $h > 0$, there exists an $r \geqslant 1$ such that for all a and b, such that $a \geqslant r$ and $a \geqslant b \geqslant 1$, $(a/b) \exp(-h(a-b)) \leqslant 1$.

In the remaining case ($q > n/4$), our strategy is to show that $E(U_{f,R}) < c/n^{3/2}$, since we can no longer use Lemma 9 to bound the number of R's. For

$\lambda < n/100, Z << 1/n^{3/2}$ where

$$Z = \exp\left(-q\left(|R| - \frac{1}{2}(n-k) + (d-\lambda) + 1\right)\Big/|R|\right),$$

and we can proceed as before. For $\lambda \geqslant n/100$, $(1/(\lambda+1))Z \leqslant c/n^{3/2}$ for k, λ, d such that $|R| - (n-k)/2 + (d-\lambda) + 1 \geqslant (3 \ln n)/2$, since $q/|R| > 1/3$ (for n sufficiently large).

Thus it is only necessary to consider the case where $\lambda \geqslant n/100$, and $|R| - (n-k)/2 + (d-\lambda) \leqslant (3 \ln n)/2$. To make the following discussion more readable we introduce the new variables $\alpha = |R| - \frac{1}{2}(n-k) \geqslant \max\{1, 2|R| - n\} = \gamma_R$ and $\beta = (d-\lambda) \geqslant 0$. Thus in our summation we need only consider terms for which $\alpha + \beta \leqslant (3 \ln n)/2$. Hence we are considering

$$\sum_{k \text{ (such that } \gamma_R \leqslant \alpha \leqslant (3 \ln n)/2)} \sum_{d} \sum_{\lambda=d-(3 \ln n)/2+\alpha}^{d} \frac{1}{\lambda+1} e^{-(\alpha+\beta)/3} P(C_\lambda | D_d \cap B_k).$$

$$P(D_d|B_k) \cdot P(B_k) \leqslant \frac{c}{n} \sum_k \sum_d P(D_d|B_k)P(B_k) \sum_\lambda P(C_\lambda|D_d \cap B_k)$$

$$\leqslant \frac{c}{n} \sum_k \sum_d P(D_d|B_k)P(B_k).$$

We consider the expressions derived earlier for $P(D_d|B_k)$ and $P(B_k)$ with α and β substituted where appropriate.

$\binom{n}{|R|}$ and $\binom{\alpha+2d-1}{\alpha+d-1}$, which appear in the sum above, can both be estimated (to within a multiplicative constant) by Lemma 6. We now assume that $|R| \leqslant n/2$ (we will shortly discuss what changes need to be made for the case $|R| > n/2$). It follows from Lemma 7 that

$$\binom{n-\alpha-2d}{n-|R|-d} \leqslant \frac{c}{\sqrt{(n-\alpha)-2d}} 2^{n-\alpha-2d} \cdot \exp\left(-\frac{2}{n-\alpha-2d}\left(\frac{1}{2}n + \frac{1}{2}\alpha - R\right)^2\right).$$

Note that for $|R| \leqslant n/2$, $n - \alpha - 2d \geqslant 1$ for all possible d and α. It follows from the above and some straightforward analysis that the sum in question is bounded by

$$M \underset{\text{def}}{=} (c \ln n/n^2) \sum_{\alpha=\gamma_R}^{(3 \ln n)/2} (n - 2|R| + \alpha + 1) \cdot \sum_{d=(|R|-\alpha)/2}^{|R|-\alpha} ((n - |R| + 1 - d)(n - \alpha - 2d)^{1/2})^{-1}.$$

However, the interior sum in M is bounded by $\int_{(|R|-\alpha)/2}^{|R|-\alpha} f(t)dt + f(|R| - \alpha)$, where $f(t) = ((n - |R| + 1 - t)\sqrt{n - \alpha - 2t})^{-1}$. Integration shows that M can be bounded by $c(\ln n)^2(2\tau + (3 \ln n)/2 + 1)^{1/2}/n^2$, which is bounded by $c/n^{3/2}$.

Essentially the same argument works for the case $(n/2) + (3/4) \ln n \geqslant |R| > (n/2)$, except that a little more care must be taken to evaluate the bounds. The exponential term in W is bounded by a constant again since

$$\frac{2}{n}\left(|R| - \frac{1}{2}n\right)^2 \leqslant \frac{9}{8}\frac{(\ln n)^2}{n},$$

which goes to 0 as $n \to \infty$. The rest of the estimating procedure is exactly the same except for the following exception. When we are summing for $\alpha = \gamma_R = 2|R| - n \geqslant 2$, we can use the above summation procedure for all the cases except $d = |R| - \alpha$, since in that case we will get 0 in the denominator of the upper bound. However, this case can easily be evaluated directly from (2) and it only contributes a factor of $(c \ln n)/n^2$. Again we conclude that $E(U_{f,R}) \leqslant c/n^{3/2}$. Actually, we can do better, since it is easy to show that we actually get $E(U_{r,R}) \leqslant c(\ln n)^3/n^2$ for all such R that we have just been considering

Thus the proof of the theorem is completed.

REMARK. We will now show that we have produced the best possible bound (up to a constant multiple) for Procedure II, by showing that there exist isotone functions f for which $E(U_f) \geqslant dE_n/n$ for some constant d. Suppose $|R|$ is approximately $[n/2]$ and $R \in L_1$. It is easy to show by direct evaluation of (2) that $E(U_{f,R}) \geqslant a/|R|$ where a is on the order of $\frac{1}{2}$. Thus we need only show that there exist monotone functions f for which $|L_1|$ is on the order of E_n, since then it would follow that $E(U_f) \geqslant dD_n/n$. Knuth shows [5] by the use of Hamming codes that there exist arbitrarily large odd integers n, for which there exists a subset I of $G_{[n/2],n}$ of size at least $E_n/(n+1)$ such that for any $S, T \in I$, $|S \cup T| > [n/2] + 1$. Let f be a function such that $f(Z) = 1$ if $|Z| > [n/2]$ or $Z \in I$, and $f(Z) = 0$ otherwise. Then $L_1 = \{Y \in G_{[n/2]+1,n} | Y \supset S \text{ for some } S \in I\}$. It is easy to see that $|L_1| \simeq \frac{1}{2}E_n$, and thus $E(U_f) \geqslant (d/n)E_n$.

REFERENCES

1. W. K. Feller, *An introduction to probability theory and its applications.* Vol. I, Wiley, New York; Chapman & Hall, London, 1957. MR 19, 466.

2. C. Greene and D. J. Kleitman, *Strong versions of Sperner's theorem,* J. Combinatorial Theory (to appear).

3. G. Hansel, *Sur le nombres des fonctions booléennes monotones de n variables,* C. R. Acad. Sci. Paris Sér. A-B 262 (1966), A1088–A1090. MR 36 #7439.

4. D. J. Kleitman, *On Dedekind's problem: The number of monotone Boolean functions,* Proc. Amer. Math. Soc. 21 (1969), 677–682. MR 39 #2674.

5. D. E. Knuth, *The asymptotic number of geometries,* Discrete Math. (to appear).

6. G. Markowsky, *Combinatorial aspects of lattice theory with applications to the enumeration of free distributive lattices*, Ph. D. Thesis, Harvard University, 1973.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139 (Current address of D. J. Kleitman)

DEPARTMENT OF MATHEMATICAL SCIENCES, IBM T. J. WATSON RESEARCH CENTER, YORKTOWN HEIGHTS, NEW YORK 10598 (Current address of G. Markowsky)