PACIFIC JOURNAL OF MATHEMATICS
Vol. 81, No. 2, 1979

DEDEKIND'S PROBLEM: MONOTONE BOOLEAN FUNCTIONS ON THE LATTICE OF DIVISORS OF AN INTEGER

PAUL HESS

This paper is concerned with the combinatorial problem of counting the number of distinct collections of divisors of an integer N having the property that no divisor in a collection is a multiple of any other. It is shown that if N factors into primes $N=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$ the number of distinct collections of divisors with the stated property does not exceed $(\sum_{i=1}^{n} a_i-n+3)^M$, where M is the maximum coefficient in the expansion of the polynomial

$$(1+x+x^2+\cdots+x^{a_1})(1+x+x^2+\cdots+x^{a_2})\cdots(1+x+x^2+\cdots+x^{a_n}) .$$

In the special case where N is squarefree the problem is equivalent to that of counting the number of "Sperner families" on n letters, for which G. Hansel obtained the upper bound 3^{M_n}, where M_n is the binomial coefficient $\binom{n}{[n/2]}$; the result in this paper is then a generalization of Hansel's theorem to the non-squarefree case.

The problem has also been formulated as that of counting the number of families consisting of incomparable subsets of a set of n objects (the objects of course corresponding to the primes in the number-theoretic formulation), with the variation that each object may appear in a set with a specifically limited number of repetitions (these limits corresponding to the prime exponents).

NOTATION. Given n letters $x_1, x_2, \cdots, x_n$, and n positive integers $a_1, a_2, \cdots, a_n$, consider the lattice consisting of all terms $(x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n})$ in the polynomial $\prod_{i=1}^{n}(\sum_{k=0}^{a_i} x_i^k)$, with the partial ordering defined $(x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}) \subseteqq (x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n})$ if $j_i \leqq k_i$ for all i. A single term $X = (x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n})$ in this lattice will be referred to as a "set", the empty set ϕ denoting the term with all exponents $j_1, j_2, \cdots, j_n$ equal to zero. If $X = (x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n})$, the notation (X, x_k^c) will indicate the set $(x_1^{j_1}x_2^{j_2}, \cdots x_k^{j_k+c}\cdots x_n^{j_n})$, and the exponent sum $j_1 + j_2 + \cdots + j_n$ will be written $|X|$.

A monotone Boolean function is defined to be a function taking the values 0 or 1 on each set of this lattice with the property that $f(X) \leqq f(Y)$ if $X \subseteqq Y$. The problem of counting the number of monotone Boolean functions on this lattice is then equivalent to the problem concerning collections of divisors of N stated at the beginning.

(1) The lattice defined above can be partitioned into chains, constructed inductively:

If $n = 1$, the chain covering consists of the single chain $\phi \subseteqq (x_1) \subseteqq (x_1^2) \subseteqq \cdots \subseteqq (x_1^{a_1})$.

If $n > 1$, assume the chain covering has already been constructed on the $n-1$ letters $x_1, \cdots, x_{n-1}$. Each chain $C\colon X_1 \subseteqq X_2 \subseteqq \cdots \subseteqq X_r$ of the covering on $n-1$ letters gives rise to the chains

$$X_1 \subseteqq X_2 \subseteqq \cdots \subseteqq X_r \subseteqq (X_r, x_n) \subseteqq (X_r, x_n^2) \subseteqq \cdots \subseteqq (X_r, x_n^{a_n})$$
$$(X_1, x_n) \subseteqq (X_1, x_n^2) \subseteqq \cdots \subseteqq (X_1, x_n^{a_n}) \subseteqq (X_2, x_n^{a_n}) \subseteqq \cdots \subseteqq (X_{r-1}, x_n^{a_n})$$
$$(X_2, x_n) \subseteqq (X_2, x_n^2) \subseteqq \cdots \subseteqq (X_{r-1}, x_n^{a_n-1})$$
$$\vdots$$

terminating in

$$(X_{r-1}, x_n) \subseteqq \cdots \subseteqq (X_{r-1}, x_n^{a_n-(r-2)}) \text{ if } 2 \leqq r \leqq a_n$$

or in

$$(X_{a_n}, x_n) \subseteqq (X_{a_n+1}, x_n) \subseteqq \cdots (X_{r-1}, x_n) \text{ if } r > a_n \,.$$

If $r = 1$, the chain C gives rise only to the chain

$$X_1 \subseteqq (X_1, x_n) \subseteqq \cdots \subseteqq (X_1, x_n^{a_n}) \,.$$

EXAMPLES. If $n = 1$, $a_1 = 2$, the covering consists of the single chain $\phi \subseteqq (x_1) \subseteqq (x_1^2)$.

If $n = 2$, $a_1 = 2$, $a_2 = 4$, the covering consists of the three chains

$$\phi \subseteqq (x_1) \subseteqq (x_1^2) \subseteqq (x_1^2 x_2) \subseteqq (x_1^2 x_2^2) \subseteqq (x_1^2 x_2^3) \subseteqq (x_1^2 x_2^4)$$
$$(x_2) \subseteqq (x_2^2) \subseteqq (x_2^3) \subseteqq (x_2^4) \subseteqq (x_1 x_2^4)$$
$$(x_1 x_2) \subseteqq (x_1 x_2^2) \subseteqq (x_1 x_2^3) \,.$$

An easy induction on n suffices to show that each chain contains a set X for which the exponent sum

$$|X| = \begin{cases} \sum_{i=1}^{n} a_i/2 & \text{if } \sum_{i=1}^{n} a_i \text{ is even} \\ \left(\sum_{i=1}^{n} a_i + 1\right)\Big/2 & \text{if } \sum_{i=1}^{n} a_i \text{ is odd} \end{cases}$$

and that all sets in the lattice appear once and only once in the coverning. It follows that the number of chains in the covering is given by M, the maximum coefficient in the expansion of the polynomial $\prod_{i=1}^{n} (\sum_{k=0}^{a_i} x_i^k)$. (The coefficient of x^j in this polynomial is the number of sets in the lattice with exponent sum j.)

A theorem of Dilworth [2], states that a partially ordered set with k but not $k+1$ incomparable elements can be covered by k

chains. The chain covering defined above is the covering whose existence is guaranteed by Dilworth's theorem.

The set function σ. If three sets $X \subseteqq Y \subseteqq Z$ appear in succession within a chain, we define $\sigma(X)$ to be the set $X + (Z - Y)$. $\sigma(X)$ is undefined if X is not at least three places from the end of its chain.

EXAMPLES. $\phi \subseteqq (x_1) \subseteqq (x_1^2);\ \sigma(\phi) = (x_1)$

$$(x_1^2 x_2^3) \subseteqq (x_1^2 x_2^4) \subseteqq (x_1^2 x_2^4 x_3);\ \sigma(x_1^2 x_2^3) = (x_1^2 x_2^3 x_3)\ .$$

If $X \subseteqq Y \subseteqq Z$ are three sets in succession within a chain in the covering, it is easy to see that if $\sigma(X) = Y$, then all the letters in Z are also letters in Y. This situation will be abbreviated "$\sigma(X) =$ next", and we note that the length l of the longest possible sequence in a chain of the form $\cdots X_{i+1} \subseteqq X_{i+2} \subseteqq \cdots \subseteqq X_{i+l} \cdots$ where $X_{i+1} \neq \phi$ and all X in the sequence are composed of the same letters, is $\sum_{i=1}^{n} a_i - n + 1$.

Within the chain covering (1), define an ordering of the chains as follows: If $n = 1$, C_1 is the single chain $\phi \subseteqq (x_1) \subseteqq (x_1^2) \subseteqq \cdots \subseteqq (x_1^{a_1})$, and inductively if $n > 1$, and $C_1', C_2', \cdots C_k'$ are the ordered chains in the covering for the $n - 1$ letters $x_1, \cdots, x_{n-1}$, and if C_j' gives rise to the chains $C_{j_1}, C_{j_2}, \cdots, C_{jl_j}$ in the covering on n letters in the sequence in which they appear in the definition (1), then let $C_{11}, C_{12}, \cdots, C_{1l_1}; C_{21}, C_{22}, \cdots, C_{2l_2}; \cdots; C_{k1}, C_{k2}, \cdots, C_{kl_k}$ be the ordering of the chains $C_1, C_2, \cdots, C_M$ in the n-letter covering. (In other words, simply order the chains as they appear in the inductive definition). An easy induction on n then establishes the following property of the function σ: (2) If $\sigma(X)$ is defined and "$\neq$ next", and X appears in chain C_i, $\sigma(X)$ in chain C_j, then $j > i$.

Proof of (2). Induction on n. The statement is true for $n = 1$ vacuously. Consider the chain on $n - 1$ letters $X_1 \subseteqq X_2 \subseteqq \cdots \subseteqq X_r$ giving rise to the chains on n letters

$$X_1 \subseteqq X_2 \subseteqq \cdots \subseteqq X_r \subseteqq (X_r, x_n) \subseteqq \cdots \subseteqq (X_r, x_n^{a_n})$$
$$(X_1, x_n) \subseteqq (X_1, x_n^2) \subseteqq \cdots \subseteqq (X_1, x_n^{a_n}) \subseteqq (X_2, x_n^{a_n}) \subseteqq \cdots \subseteqq (X_{n-1}, x_n^{a_n})$$
$$\vdots$$
$$(X_{j-1}, x_n) \subseteqq \cdots (X_{j-1}, x_n^{a_n-(j-2)}) \subseteqq (X_j, x_n^{a_n-(j-2)}) \subseteqq \cdots \subseteqq (X_{r-1}, x_n^{a_n-(j-2)})\ .$$

In the first chain above, if $\sigma(X_k)$ is defined and "$\neq$ next", $k \leqq r-2$, so that $\sigma(X_k)$ is in a later $n - 1$ chain by induction, therefore in a later n-chain. $\sigma(X_r)$ "$=$ next" and the same holds for $\sigma(X_r, x_n)$, $\sigma(X_r, x_n^2)$, etc. $\sigma(X_{r-1}) = (X_{r-1}, x_n)$ which is in a later n-chain. In subsequent chains, $\sigma(X_{j-1}, x_n^{a_n-(j-1)}) = (X_j, x_n^{a_n-(j-1)})$ which appears in the chain immediately following. $\sigma(X_i, x_n^{a_n-(j-2)})$, where $i \geqq j-1$, if defined and "$\neq$ next", is the set $(\sigma(X_i), x_n^{a_n-(j-2)})$ where $\sigma(X_i)$ "$\neq$ next". By induction, $\sigma(X_i)$ is in a later $n-1$ chain so that $(\sigma(X_i), x_n^{a_n-(j-2)})$ is in a later n-chain, which completes the proof of the assertion.

(3) If C is a chain in the covering and f is a monotone Boolean function already defined on all sets $\sigma(W)$, where W is any set in the chain C for which $\sigma(W)$ is defined and "$\neq$ next", then the number of possible definitions for f on the chain C does not exceed $\sum_{i=1}^n a_i - n + 3$.

Proof of (3). Let the chain C consist of l sets $W_1 \subsetneqq W_2 \subsetneqq \cdots \subsetneqq W_l$. Suppose $\sigma(W)$ is undefined or " = next" for all W in the chain C. Then if $l \geqq 3$, $W_2 \neq \phi$ and $W_2 \cdots W_l$ are sets consisting of the same letters. Then the number of ways of defining a monotone Boolean function on the chain is at most $l + 1 \leqq \sum_{i=1}^n a_i - n + 3$. Otherwise, let W_m be the W farthest to the right in the chain for which $f(\sigma(W)) = 0$, and W_k the W farthest to the left for which $f(\sigma(W)) = 1$. Either m or k exists. If k does not exist, then m does. In this case $f(\sigma(W_m)) = 0$ and since $W_m \subseteqq \sigma((W_m))$, f is undetermined only on the portion of the chain $W_{m+1}, W_{m+2}, \cdots, W_{m+l}$. But σ is undefined or "=next" on these sets, so that $W_{m+2} \cdots W_l$ are sets consisting of the same letters (or $W_{m+1} \cdots W_l$ is shorter than 3 sets in length). Thus f is undetermined on at most $\sum_{i=1}^n a_i - n + 2$ sets and the number of ways of defining f is at most $\sum_{i=1}^n a_i - n + 3$ (either 0 throughout the chain, or $\sum_{i=1}^n a_i - n + 2$ choices for the position of the 1 farthest to the left). A similar argument takes care of the case where m does not exist and k does. If m and k both exist, first suppose $m < k$. Then we have $f = 0$ on the sets $W_m, W_{m-1}, \cdots$, down to W_1, and $f = 1$ on the sets $W_{k+2}, W_{k+3}, \cdots$ up to W_l. In this case $W_{m+2} \cdots W_{k-1} W_k W_{k+1}$ are all sets consisting of the same letters, so that the length of the segment on which f is undetermined, $(k+1) - (m+1) + 1$, is at most $\sum_{i=1}^n a_i - n + 2$, and as before the number of possible definitions of f on the chain is at most $\sum_{i=1}^n a_i - n + 3$. The final possibility is $m \geqq k$, but by definition of m and k, $m \neq k$ and obviously m cannot exceed $k+1$. The situation is then: $W_1 \subsetneqq \cdots \subsetneqq W_k \subsetneqq W_m \subsetneqq W_{m+1} \subsetneqq \cdots \subsetneqq W_l$, $m = k+1$, $f(\sigma(W_k)) = 1$ and $f(\sigma(W_m)) = 0$ so that $f = 1$ on the sets $W_{m+1} \cdots W_l$, $f = 0$ on the sets $W, \cdots, W_k, W_m$, and f is completely predetermined on the chain in this case.

Conclusion. $(\sum_{i=1}^n a_i - n + 3)^M$, where M is the maximal coefficient in the expansion of $(1 + x + \cdots + x^{a_1})(1 + x + \cdots + x^{a_2})\cdots(1 + x + \cdots + x^{a_n})$ is an upper bound on the number of monotone Boolean functions on the lattice of divisors of $N = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$.

Proof. Let $C_1, C_2, \cdots, C_M$ be the ordered chains in the covering. On the last chain, the function σ is undefined or "=next" throughout. (Otherwise, according to (2), for X in the chain C_M, $\sigma(X)$ would appear in a later chain which is impossible.) It then follows from (3) that the number of ways of defining f on C_M does not exceed $\sum_{i=1}^{n} a_i - n + 3$. On chain C_{M-1}, if X is a set in this chain for which $\sigma(X)$ is defined and "$\neq$ next", then according to (2) $\sigma(X)$ appears in the chain C_M. Thus $f(\sigma(X))$ is already defined for all such X in the chain C_{M-1}, and from (3) there are at most $\sum_{i=1}^{n} a_i - n + 3$ possible definitions of f on C_{M-1}. Continuing in this way to the first chain C_1 gives the upper bound stated.

References

1. G. Hansel, *Sur le nombre des fonctions booléennes monotones de n variables*, C. R. Acad. Sci. Paris, **262**, 1088.

2. R. P. Dilworth, *A decomposition theorem for partially ordered sets*, Annals of Mathematics, January, 1950.

Not cited in this paper, but related:

3. D. Kleitman, *On Dedekind's Problem: The Number of Monotone Boolean Functsons*, Proc. Amer. Math. Soc., **21** (1969), 677-682.

4. H. N. Shapiro, *On the counting problem for Monotone Boolean functions*, Comm. Pure and Applied Math., XXIII, (1970), 299-312.

Received April 6, 1978 and in revised form September 14, 1978.

COOPER UNION
EIGHTH STREET AND FOURTH AVENUE
NEW YORK, NY 10003