Acta Sci. Math., 40 (1978), 81—87

Counting additive spaces of sets

KI HANG KIM and FRED W. ROUSH

1. Introduction. In this paper we consider an asymptotic counting problem which occurs in a number of forms.

Definition 1. A family Ω of subsets of $\{1, 2, \ldots, n\}$ is an *additive space* if $\emptyset\in\Omega$ and $AB\in\Omega$ whenever $A, B\in\Omega$. Two such families are isomorphic iff they are isomorphic as semigroups under union.

Definition 2. Let V_n be the set of all n-tuples from the two-element Boolean algebra $\{0, 1\}$. A subset U of V_k is called a *Boolean subspace* iff the vector $(0, 0, \ldots, 0)$ belongs to the subspace, and whenever $u, v\in U$, the vector $u+v= =(\sup\{u_1, v_1\}, \ldots, \sup\{u_n, v_n\})$ also belongs to U. Two subspaces are isomorphic iff they are isomorphic as semigroups under $+$.

Definition 3. A lattice is of *type*-(n, m) iff it has exactly m nonzero join irreducible elements and exactly n meet irreducible elements other than its highest element.

Remark. Every Boolean subspace of V_n has a partial order given by $v\leqq w$ iff $v+w=w$. This makes the subspace into a lattice, with the join operation being Boolean sum, and the meet operation on v, w being the sum of all Boolean vectors less than or equal to both v, w.

Definition 4. By a *Boolean matrix* of order n is meant an $n\times n$ matrix over the two-element Boolean algebra $\{0, 1\}$. Let B_n denote the set of all such matrices. We consider the sum and product of members of B_n to be the sum and product over the two-element Boolean algebra $\{0, 1\}$. Then B_n is a monoid under multiplication.

Definition 5. Two Boolean matrices A, B are *$\mathscr{R}$-equivalent* iff there exist Boolean matrices X, Y such that $AX=B$, $BY=A$. They are *$\mathscr{L}$-equivalent* iff there

Received January 31, 1977.

exist matrices U, V such that $UA=B$, $VB=A$. They are *$\mathscr{D}$-equivalent* iff there exists a matrix C such that $A\mathscr{R}C$ and $C\mathscr{L}B$. They are $\mathscr{H}$-equivalent iff they are both $\mathscr{R}$-equivalent and $\mathscr{L}$-equivalent.

Remark. $\mathscr{R}, \mathscr{L}, \mathscr{H}$ are equivalence relations, by a quick computation. As a relation, $\mathscr{D}$ is the composition $\mathscr{R}\circ\mathscr{L}$. It can be shown that $\mathscr{R}\circ\mathscr{L}=\mathscr{L}\circ\mathscr{R}$, and this implies $\mathscr{D}$ is also an equivalence relation.

Definition 6. An *ideal* of B_n is a subset I of B_n such that for all $x\in I$, $a, b\in B_n$, the element axb belongs to I. Principal ideals, principal left and right ideals are defined in a similar way.

Questions.

1. What is the asymptotic number of isomorphism classes of additive spaces of subsets of $\{1, 2, \ldots, n\}$ which have m generators other than the empty set?
2. What is the asymptotic number of isomorphism classes of Boolean subspaces of V_n with m generators other than $(0, 0, \ldots, 0)$?
3. What is the asymptotic number of isomorphism classes of lattices of type-(n, m)?
4. What is the asymptotic number of $\mathscr{D}$-classes of $n\times m$ Boolean matrices?
5. What is the asymptotic number of principal ideals in B_n?

The answers to 1—4 coincide, and for $m=n$ the fifth also has the same answer. We prove that if $n, m\to\infty$ in such a way that $\frac{n}{m}$ approaches a nonzero constant, the answer to 1—4 is $\frac{2^{nm}}{n!m!}$.

We also obtain information about related questions: the number of subspaces of V_n with m generators (not just isomorphism classes), the number of $\mathscr{R}, \mathscr{L}, \mathscr{H}$-classes. Also on the number of matrices X such that for some non-identity permutation matrices P, Q, $PXQ=X$ (for instance if X were a *projective plane*, such P, Q would give a collineation, the existence of P, Q is an unsolved problem [2], [5]).

2. Facts about Boolean matrices; lemmas. Equivalence of questions 1 and 2 is by an isomorphism of semigroups. Equivalence to question 3 follows by results about lattices involving duality, regarding lattices as idempotent abelian semigroups [1].

The *row space* of an $m\times n$ Boolean matrix is the subspace of V_n generated by its rows, with $(0, 0, \ldots, 0)$. Likewise there is a column space. It is known that the row space (as a subset of V_n) determines the $\mathscr{L}$-class of a matrix and the column space determines the $\mathscr{R}$-class [3]. Every subspace of V_n has a unique smallest generating set excluding $(0, 0, \ldots, 0)$. Such a set is called a *basis*. A basis for the row space of a matrix is called a *row basis*, and a basis for the column space of a matrix is called a *column basis*. It is known [3] that the isomorphism class of the row space determines the $\mathscr{L}$-class showing that questions 2, 4 have the same answer. It follows by semigroup theory [4] that for $n=m$ questions 4, 5 have the same answer.

We will begin to answer question 4. The *row rank* of a Boolean matrix is the number of elements in a row basis; likewise for the column rank. For any two Boolean matrices A, B we say $A \leqq B$ if $a_{ij}=1$ implies $b_{ij}=1$ for all i, j.

Lemma 1. *Let n, m tend to infinity in such a way that*

$$\frac{\log n}{m} \to 0, \quad \frac{\log m}{n} \to 0.$$

Then the proportion of $m \times n$ Boolean matrices which have both row rank m and column rank n tends to 1.

Proof. For a Boolean matrix A, let A_{i*} be its i^{th} row, and A_{*j} be its j^{th} column. Let N_{ij} denote the number of $m \times n$ Boolean matrices with $A_{i*} \geqq A_{j*}$ and M_{ij} the number with $A_{*i} \geqq A_{*j}$. Let N denote 2^{mn}, the number of all $m \times n$ Boolean matrices. Then for fixed $i \neq j$ we have

$$\frac{N_{ij}}{N} = \left(\frac{3}{4}\right)^n \quad \text{and} \quad \frac{M_{ij}}{N} = \left(\frac{3}{4}\right)^m.$$

Thus the number of matrices having no row greater than or equal to any other, and no column greater than or equal to any other is at least

$$\left(1-(n^2-n)\left(\frac{3}{4}\right)^m-(m^2-m)\left(\frac{3}{4}\right)^n\right)2^{mn}.$$

All these matrices have row rank m and column rank n. Under the given hypotheses this number divided by 2^{mn} will tend to 1. The proof of Lemma 1 is completed.

If two matrices of row rank m are $\mathscr{L}$-equivalent their rows must be permutations of each other by the uniqueness of a row basis. So $A=PB$. Likewise for $\mathscr{R}$-equivalence if the column rank is n. So for X of the type of this lemma, the only matrices $\mathscr{D}$-equivalent to it will be of the form PXQ. Thus such $\mathscr{D}$-classes have at most $n!m!$ members, and asymptotically the number of $\mathscr{D}$-classes is at least $\dfrac{2^{nm}}{n!m!}$. The proof of the reverse inequality will be based on a study of the equation $PXQ=X$.

Lemma 2. *If P or Q have no more than k cycles the number of solutions X of $PXQ=X$ is no more than 2^{kn} or 2^{km}, respectively.*

Proof. Let P have no more than k cycles. Choose one row from each cycle, and specify it. This can be done in 2^{kn} ways, and these rows determine the rest. Similarly for Q.

Lemma 3. *If a permutation P has at least k cycles, it will fix at least $m-2(m-k)$ numbers from* $\{1, 2, \dots, m\}$.

Proof. Immediate.

Lemma 4. *Let a permutation group G act on a set T of letters. If for any element g of G, g fixes at least $|T|-a$ letters with $a>0$, then there is a set of $|T|-2a+1$ letters fixed by every element of G.*

Proof. The action of G on T gives a linear representation R of G by permutation matrices. Let $o_1, \dots, o_f, o_{f+1}, \dots, o_{f+t}$ be the G-orbits contained in T, where $o_1, \dots, o_f$ contain only one element each, and the rest contain more than one element. Corresponding to this orbit decomposition we have a direct sum decomposition $R=R_1\oplus\dots\oplus R_f\oplus R_{f+1}\oplus\dots\oplus R_{f+t}$. A theorem in group representation theory (see [6], p. 280) states that

$$\sum_{g\in G} Tr(g) = (f+t)\,|G|.$$

But $Tr(g) \geqq |T|-a$ for any $g\in G$, and assuming $a>0$, $Tr(I) > |T|-a$. Therefore $|T|-a<f+t$. Yet $|T|\geqq f+2t$. Therefore

$$|T|-a<f+\frac{|T|-f}{2}$$

which yields the desired inequality on f.

3. Main results

Theorem 5. *Let n, m tend to infinity such that $\frac{n}{m}$ tends to a nonzero constant. Then the number of $\mathcal{D}$-classes of $m\times n$ matrices is asymptotically equal to* $\frac{2^{mn}}{m!\,n!}$.

Proof. By Lemma 1 and the considerations after its proof we need only prove this formula gives an asymptotic upper bound. Let $k=\sup\left\{\lim \frac{n}{m}, \lim \frac{m}{n}\right\}$.

Case 1. $\mathcal{D}$-classes containing some X such that $PXQ=X$ for some P, Q such that P has no more than $m-(4k+1)\log m$ cycles. (All logarithms are base 2.) For fixed P, Q with P satisfying the hypothesis of this case, there are at most

$$2^{(m-(4k+1)\log m)\,n}$$

matrices X such that $PXQ=X$, by Lemma 2. The number of possibilities for P, Q cannot exceed $n!m!$. Thus the number of possibilities for X in the present case is at most

$$2^{(m-(4k+1)\log m)\,n}\,n!\,m!.$$

Therefore also the number of $\mathscr{D}$-classes containing at least one such X is at most

$$2^{(m-(4k+1)\log m)n}n!m!.$$

The ratio of this number to $\frac{2^{nm}}{n!m!}$ will approach zero.

Case 2. $\mathscr{D}$-classes containing some matrix X such that $PXQ=X$ for some P, Q such that Q has no more than $n-(4k+1)\log n$ cycles. This case is treated like Case 1.

Case 3. $\mathscr{D}$-classes containing a matrix X such that $PXQ=X$ for some P, Q not both the identity, but such that $PXQ=X$ does not hold for any P, Q with P having no more than $m-(4k+1)\log m$ cycles or Q having no more than $n-(4k+1)\log n$ cycles. For such an X, choose a pair P, Q satisfying $PXQ=X$ such that $\sup\{m-\text{number of cycles in } P, n-\text{number of cycles in } Q\}$ is a maximum. Let s denote this maximum. We have $0<s<(4k+1)\sup\{\log m, \log n\}$. For a given X the set $\{P:PXQ=X \text{ for some } Q\}$ forms a group [2]. Each element of this group will fix at least $m-2s$ letters by Lemma 3. Therefore by Lemma 1 the whole group will fix at least $m-4s$ letters. There is a similar group of Q's which fixes at least $n-4s$ letters.

Fix s. We first choose a set of $4s$ letters which is to contain the set of all non-fixed letters under $\{P:PXQ=X \text{ for some } Q\}$. There are $\binom{m}{4s}$ such choices. There are $\binom{n}{4s}$ choices for a similar set for $\{Q:PXQ=X \text{ for some } P\}$. Provided these sets are chosen, we can choose P in $(4s)!$ ways to act on its set and Q in $(4s)!$ ways to act on its set. Once P, Q are chosen we can choose X in at most

$$2^{nm-s\min\{n,m\}}$$

ways by Lemma 2. Thus for a given s, there are at most

$$\binom{m}{4s}\binom{m}{4s}(4s)!(4s)!\,2^{nm-s\min\{n,m\}}$$

choices of X having the required value of s. However these X's do not all lie in different $\mathscr{D}$-classes. For any permutation matrices R, S, RXS will lie in the same $\mathscr{D}$-class and have the same value of s.

How many different matrices RXS are there for a given X? We have a group action of the product of two symmetric groups on such matrices, sending Y to RYS^{-1}. The isotropy group of X has order at most $((4s)!)^2$ by the remarks above about choosing P, Q such that $PXQ=X$. Thus a $\mathscr{D}$-class containing one X also contains at least

$$\frac{n!m!}{(4s)!(4s)!}$$

other matrices with the same s. Therefore the number of $\mathcal{D}$-classes containing matrices of this type for a given s is at most

$$\frac{m^{4s}n^{4s}2^{nm-s\min\{n,m\}}((4s)!)^2}{n!m!}.$$

Allowing any value of s we have at most

$$\max_{1\leq s\leq(4k+1)n_1}\frac{m^{4s}n^{4s}2^{nm-sn_2}((4s)!)^2(4k+1)\log n_1}{n!m!}$$

where $n_1=\max\{n, m\}$ and $n_2=\min\{n, m\}$. The ratio of this quantity to $\frac{2^{nm}}{n!m!}$ tends to zero.

Case 4. All PXQ are distinct so the $\mathcal{D}$-classes have at least $n!m!$ elements. There are at most $\frac{2^{nm}}{n!m!}$ $\mathcal{D}$-classes of this type. This proves the theorem.

Corollary 6. *Let N be the number of matrices X such that $PXQ=X$ for some P, Q not both the identity. Then if $n, m\to\infty$ in such a way that $\frac{n}{m}$ approaches a nonzero constant, $\frac{N}{2^{nm}}$ approaches* 0.

Theorem 7. *Under the hypotheses of Lemma* 1, *the number of $\mathcal{R}$ and $\mathcal{L}$-classes of $m\times n$ matrices are asymptotically equal to $\frac{2^{nm}}{n!}$, $\frac{2^{nm}}{m!}$ respectively. The number of $\mathcal{H}$-classes is asymptotically equal to 2^{nm}.*

Proof. For an upper bound, for instance for $\mathcal{R}$-classes, we have

$$\binom{2^m}{n}+\binom{2^m}{n-1}+\dots+\binom{2^m}{1}$$

by, for column rank k, choosing a set of k column vectors to be a column basis. This is less than or equal to

$$\binom{2^m}{n}\sum_{i=1}^{\infty}\left(\frac{n}{2^m-n}\right)^i$$

which gives the theorem. Similar methods apply in the other cases.

The authors would like to thank András Ádám for a very constructive criticism of the original draft of this paper.

References

[1] G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloq. Pub. Vol. 25 (Providence, R. I., 1967).

[2] Ki Hang Kim, *Subgroups of binary relations*, Proc. Second International Conference on Theory Groups, Canberra, Australia, August 1973, 188—196. MR 51 # 774.

[3] Ki Hang Kim, Combinatoral properties of binary semigroups, *Periodica Mathematica Hungarica*, 5 (1974), 3—46.

[4] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. 1, Math. Surveys No. 7, Amer. Math. Soc. (Providence, R. I., 1961).

[5] H. J. Ryser, *Combinatorial mathematics*, Carus Math. Monographs, Math. Assoc. of Amer., Wiley (New York, 1963).

[6] M. Hall, *The theory of groups*, Macmillan (New York, 1959).

DEPARTMENT OF MATHEMATICS
ALABAMA STATE UNIVERSITY
MONTGOMERY, ALABAMA 36 101, USA