

## ON THE RANKS OF SOME (0, 1)-MATRICES WITH CONSTANT ROW SUMS

A. M. ODLYZKO

(Received 25 June 1979; revised 28 July 1980)

Communicated by W. D. Wallis

### Abstract

Let  $g(n, m)$  denote the maximal number of distinct rows in any (0, 1)-matrix with  $n$  columns, rank  $< n - 1$ , and all row sums equal to  $m$ . This paper determines  $g(n, m)$  in all cases:

$$g(n, m) = \begin{cases} \binom{n-1}{m} & \text{if } 1 < m < n/2, \\ 2 \binom{n-2}{(n-2)/2} & \text{if } m = n/2, \\ \binom{n-1}{m-1} & \text{if } n/2 < m < n. \end{cases}$$

In addition, it is shown that if  $V$  is a  $k$ -dimensional vector subspace of any vector space, then  $V$  contains at most  $2^k$  vectors all of whose coordinates are 0 or 1.

1980 *Mathematics subject classification (Amer. Math. Soc.):* 05 B 20.

### 1. Introduction

Let  $g(n, m)$  denote the maximal number of distinct rows in any (0, 1)-matrix with  $n$  columns, rank  $< n - 1$  (over any field of characteristic zero), and all row sums equal to  $m$ . In a recent paper Longstaff [1] determined  $g(n, m)$  for  $1 < m < \sqrt{n-2}$  and  $n - \sqrt{n-2} < m < n - 1$ . The purpose of this note is to present a different method that determines  $g(m, n)$  completely. (Note that  $g(n, m) = \langle n \rangle_m - 1$ , where  $\langle n \rangle_m$  is Longstaff's rotation.)

**THEOREM 1.** *If  $1 < m \leq n - 1$ , then*

$$g(n, m) = \begin{cases} \binom{n-1}{m} & \text{if } m < n/2, \\ 2 \binom{n-2}{(n-2)/2} & \text{if } n \equiv 0 \pmod{2}, m = n/2, \\ \binom{n-1}{m-1} & \text{if } m > n/2. \end{cases}$$

Results of the above type have applications in certain combinatorial problems. For example, suppose that each element  $j$  of an  $n$ -element set  $\{1, \dots, n\}$  has associated to it a real (or complex) number  $x_j$ , and that there is a family  $\mathbf{F}$  of  $m$ -element subsets of  $\{1, \dots, n\}$  and a constant  $c$  such that

$$\sum_{j \in A} x_j = c \quad \text{for all } A \in \mathbf{F}.$$

What can we conclude about the  $x_j$ ? There is always the trivial solution  $x_j = c/m$  for all  $j$ . If  $|\mathbf{F}| > g(n, m)$ , then this is the unique solution.

The restriction in the definition of  $g(n, m)$  that the rank be  $< n - 1$  over a field of characteristic zero (ranks of  $(0, 1)$ -matrices are the same over all such fields) is essential, since if the characteristic is positive and divides  $k$ , all the  $\binom{n}{k}$  vectors containing exactly  $k$  1's span a subspace of dimension  $n - 1$ . It should be possible to extend the method of this note to obtain results for non-zero characteristics which do not divide  $k$ . Also, it should be possible to extend Theorem 1 to cover the case where the rank of the matrix is restricted to be  $\leq n - 2$  for some  $n \geq 2$ , but such results would be much more complicated.

The basic tool in our proof will be provided by Lemma 1. That lemma also leads to an easy proof of the following result, which is of independent interest and answers a question posed by P. Frankl in connection with a problem of Erdős about set intersections.

**THEOREM 2.** *Let  $V$  be an  $n$ -dimensional vector subspace of some vector space  $W$  (which may be over any field). Then in any coordinate system for  $W$ ,  $V$  contains at most  $2^n$  vectors all of whose coordinates are 0 or 1.*

## 2. Proofs

**LEMMA 1.** *Let  $V$  be an  $n$ -dimensional subspace of an  $r$ -dimensional vector space  $W$  over any field. Then in any coordinate system for  $W$ , we can find a basis of  $V$  such that after permuting the coordinates of  $W$  this basis has the form*

$$(1) \quad (I_n A_{n,r-n}),$$

where  $I_n$  denotes the  $n \times n$  identity matrix,  $A_{n,r-n}$  some  $n \times (r - n)$  matrix, and the rows of the matrix represent the basis vectors,

PROOF. Let  $M$  be an  $n \times r$  matrix whose rows form a basis for  $V$ . By permuting the columns of  $M$ , if necessary, we can assume that  $M$  is of the form

$$M = (B \ C),$$

where  $B$  is a nonsingular  $n \times n$  matrix. But then the rows of

$$B^{-1}M = (I_n \ B^{-1}C)$$

generate the same space as the rows of  $M$ , namely  $V$ .

PROOF OF THEOREM 2. We may assume that  $W$  is of finite dimension  $r$ , since if  $V$  had more than  $2^n$  (0, 1)-vectors in an infinite-dimensional space  $W$ , then we could find a subspace  $V'$  of a finite-dimensional space  $W'$  such that  $\dim(V') < n = \dim(V)$ , and  $V'$  would contain  $> 2^n$  (0, 1)-vectors. Suppose therefore that  $\dim(W) = r$ . By Lemma 1, we can find a basis of  $V$  such that after a suitable permutation of the coordinates, it has the form (1). Let  $v_1, \dots, v_n$  denote the rows of the matrix (1). If  $v$  is any (0, 1)-vector in  $V$ , then

$$v = \sum_{j=1}^n a_j v_j.$$

Since  $v$  has only 0's and 1's as coordinates, we conclude that each  $a_j$  is 0 or 1. Hence there are no more than  $2^n$  possibilities for  $v$ . Q.E.D.

PROOF OF THEOREM 1. This proof is considerably more involved than that of Theorem 2. We first prove that  $g(n, m)$  is at least as large as the values given in Theorem 1. If  $m < n/2$ , consider an  $(n - 1) \times n$  matrix

$$A = \begin{pmatrix} & 0 \\ & \vdots \\ I_{n-1} & \vdots \\ & 0 \end{pmatrix}.$$

Then the  $\binom{n-1}{m}$  choices of  $m$  rows of  $A$  give distinct  $n$ -vectors with sum of entries equal to  $m$ , and they all lie in the  $(n - 1)$ -dimensional subspace spanned by the rows of  $A$ . Hence  $g(n, m) \geq \binom{n-1}{m}$  (a bound which is actually valid for all  $m$ ). If  $m > n/2$ , we replace each 0 in the last column of  $A$  by  $1/(m - 1)$  and consider choices of  $m - 1$  rows of  $A$  at a time. This shows that  $g(n, m) \geq \binom{n-1}{m-1}$ . Finally, suppose that  $2|n, m = n/2$ . In this case we replace the last column of  $A$  by the transpose of the vector  $((m - 1)^{-1}, (m - 1)^{-1}, \dots, (m - 1)^{-1}, -1)$  of length  $n - 1$ . Then adding up any choice of  $m - 1$  of the first  $n - 2$  rows of  $A$  will yield an  $n$ -vector with sum equal to  $m$ . This same sum, however, will also be

obtained by choosing any  $m - 1$  of the first  $n - 2$  rows of  $A$  and the last row of  $A$ . Thus we obtain  $2\binom{n-2}{m-1}$  distinct choices in this case, which concludes the proof that the values given in Theorem 1 are actually lower bounds for  $g(n, m)$ .

We now proceed to obtain upper bounds for  $g(n, m)$ . Let us suppose that  $V$  is a vector subspace of a vector space  $W$  (over a field of characteristic 0 this time),  $\dim(W) = n, \dim(V) = n - 1$ . Let  $V_m$  be the set of  $(0, 1)$ -vectors in  $V$  which have exactly  $m$  1's. If  $m = 1$ , then the assertion of the theorem is trivial. Hence we can take  $m \geq 2$ . By Lemma 1, we can find a basis for  $V$  which, after suitable coordinate permutations, has the form

$$(2) \quad \begin{pmatrix} & a_1 \\ & \vdots \\ I_{n-1} & \vdots \\ & a_{n-1} \end{pmatrix}.$$

Denote the rows of this matrix by  $\underline{v}_1, \dots, \underline{v}_{n-1}, \underline{v}_n = (v_{k,1}, \dots, v_{k,n})$ . Any vector  $\underline{v} \in V_m$  must be the sum (with coefficients 1) of either  $m - 1$  or  $m$  of the  $\underline{v}_j$ . Let

$$S_h = \left\{ \{ \underline{v}_{i_1}, \dots, \underline{v}_{i_k} \}; 1 \leq i_1 < \dots < i_k \leq n - 1, \sum \underline{v}_{i_j} \in V_m \right\}.$$

If we could show that none of the sets in  $S_{m-1}$  is a subset of any set in  $S_m$ , we would be done very quickly. Unfortunately no such result is valid in general. However, our proof will be based on a somewhat related observation. If  $A \in S_{m-1}, B \in S_m$ , then

$$\sum_{\underline{v}_k \in A} v_{k,n} = 1, \quad \sum_{\underline{v}_k \in B} v_{k,n} = 0,$$

so that if  $B = A \cup \{ \underline{v}_p \}$ , then  $v_{p,n} = -1$ . Thus the vectors  $\underline{v}_p$  with  $v_{p,n} = -1$  play a special role, and we will treat them in a special way.

Let  $t$  be the number of vectors  $\underline{v}_p, 1 \leq p \leq n - 1$ , such that  $v_{p,n} = -1$ , and  $T = \{ \underline{v}_p; v_{p,n} = -1 \}$ . By permuting rows and columns of the matrix (2), if necessary, we may assume that  $v_{n-t,n} = v_{n-t+1,n} = \dots = v_{n-1,n} = -1$ . (We do not exclude the possibility that  $t = 0$ .) We let  $s = n - 1 - t$ , so that  $v_{k,n} \neq -1$  for  $1 \leq k \leq s$ . We also define

$$S^*(k) = \left\{ \underline{v}; \underline{v} = (v_1, \dots, v_n), \underline{v} = \sum_{j=1}^{m-k} \underline{v}_{i_j}, 1 \leq i_1 < \dots < i_{m-k} \leq s, v_n = k \right\},$$

$$s(k) = |S^*(k)|.$$

We now observe that if  $\underline{v} \in V_m, \underline{v} = (v_1, \dots, v_n)$  has  $v_n = 0$ , then for some nonnegative integer  $r, \underline{v}$  must be a sum of  $r$  distinct vectors  $\underline{v}_p \in T$ , and of a vector in  $S^*(r)$ . Similarly, if  $\underline{v} \in V_m$  has  $v_n = 1$ , then for some  $r$ , it is the sum of  $r$  distinct vectors from  $T$  and of a vector in  $S^*(r + 1)$ . Moreover, each such

representation is unique. Hence

$$(3) \quad |V_m| = \sum s(r) \binom{t}{r} + \sum s(r+1) \binom{t}{r} \\ = \sum s(r) \binom{t+1}{r},$$

where  $r$  ranges between 0 and  $\min(t+1, m-1)$ .

To bound the sum in (3) we now need to obtain some additional information about the  $S^*(k)$ . In fact we only need to show that not all of the  $S^*(r)$  can be large simultaneously. Since  $v_{p,n} \neq -1$  for any  $v_p$  with  $1 \leq p \leq s$ , we conclude that if  $\underline{v} \in S^*(v+1)$ ,  $\underline{v} = v_{i_1} + \dots + v_{i_{m-r-1}}$ , then  $\underline{v} + v_p \notin S^*(r)$  for any  $p$  with  $1 \leq p \leq s$ ,  $p \neq i_1, \dots, i_{m-r-1}$ . Thus for each  $\underline{v} \in S^*(r+1)$ , there are  $s - (m - r - 1)$  vectors which cannot be in  $S^*(r)$  even though they are sums of  $m - r$  of the  $v_k$ ,  $1 \leq k \leq s$ . Furthermore, since each vector  $\underline{w}$  which is a sum of the  $v_k$ ,  $1 \leq k \leq s$ , can be expressed in at most  $m - r$  ways as  $\underline{w} = \underline{v} + v_p$  for  $\underline{v} \in S^*(r+1)$ ,  $1 \leq p \leq s$ , we conclude that

$$(4) \quad s(r) + \frac{s - m + r + 1}{m - r} s(r+1) \leq \binom{s}{m - r}$$

for  $0 \leq r \leq \min(t, m - 2)$ . We will conclude the proof by showing that the system (4) of inequalities yields the desired bound for  $V_m$ .

We now regard the  $s(r)$  as nonnegative real numbers subject only to the inequalities (4). Since the system (4) gives an absolute bound for each of the  $s(r)$ , there is a choice of the  $s(r)$  which achieves the maximum possible value of

$$(5) \quad \sum_{r=0}^{\min(t+1, m-1)} s(r) \binom{t+1}{r}.$$

We now claim that for this optimal choice of the  $s(r)$ , equality must hold in (4) for all  $r$ . This is clearly true for  $r = 0$  and  $r = \min(t, m - 2)$ , since in each case the corresponding inequality contains an  $s(k)$  that appears only in that inequality. Suppose therefore that for some  $r$ ,  $0 < r < \min(t, m - 2)$ , we have the inequalities

$$(6a) \quad s(r-1) + \frac{s - m + r}{m - r + 1} s(r) < \binom{s}{m - r + 1},$$

$$(6b) \quad s(r) + \frac{s - m + r + 1}{m - r} s(r+1) < \binom{s}{m - r},$$

$$(6c) \quad s(r+1) + \frac{s - m + r + 2}{m - r - 1} s(r+2) < \binom{s}{m - r - 1}.$$

We wish to show that the strict inequality in (6b) enables us to find another set of  $s(k)$ 's which will increase the sum in (5). If we increase  $s(r)$  by  $\epsilon > 0$ , then in order to keep (6a) satisfied we will need to decrease  $s(r-1)$  by

$\epsilon(s - m + r)/(m - r + 1)$ . This change will add to (5) the quantity

$$x_1 = \epsilon \binom{t + 1}{r} - \epsilon \frac{s - m + r}{m - r + 1} \binom{t + 1}{r - 1}.$$

If we instead increase  $s(r + 1)$  by  $\epsilon$ , then in order to keep (6c) satisfied we will need to decrease  $s(r + 2)$  by  $\epsilon(m - r - 1)/(s - m + r + 2)$  which will have the effect of adding to (5) the quantity

$$x_2 = \epsilon \binom{t + 1}{r + 1} - \epsilon \frac{m - r - 1}{s - m + r + 2} \binom{t + 1}{r + 2}.$$

We now show that either  $x_1 > 0$  or  $x_2 > 0$ . After simplifying the above expression we discover that  $x_1 > 0$  precisely when

$$y_1 = mt - rt - rs - 3r + t + 2m + 2 > 0$$

and that  $x_2 > 0$  when

$$y_2 = -mt + rt + rs + 3r + t - 2m + 2s + 4 > 0.$$

However,

$$y_1 + y_2 = 2t + 2s + 6 = 2n + 4 > 0,$$

so at least one of  $y_1$  and  $y_2$  is positive, and hence at least one of  $x_1$  and  $x_2$  is positive. This shows that the  $s(r)$  do not maximize (5), which is a contradiction. Thus we have proved our claim that equality must hold in (4) for all  $r$ .

The rest of the proof is relatively straightforward. Since we have

$$(7) \quad s(r) + \frac{s - m + r + 1}{m - r} s(r + 1) = \binom{s}{m - r}$$

for  $0 \leq r \leq \min(t, m - 2)$ , the value of  $s(0)$  determines all the other  $s(r)$ , and in fact any solution  $(s(0), s(1), \dots)$  of (7) is a convex combination of the extremal solutions obtained when  $s(0) = 0$  and when  $s(0) = \binom{s}{m}$ . Therefore (5), and hence also  $|V_m|$ , is bounded by the maximum of the values of (5) at those two choices of the  $s(r)$ . If  $s(0) = 0$ , we obtain  $s(r) = 0$  for  $r \equiv 0 \pmod{2}$ ,  $s(r) = \binom{s}{m-r}$  for  $r \equiv 1 \pmod{2}$ , and so

$$|V_m| \leq \sum s(r) \binom{t + 1}{r} = \sum_{r \equiv 1(2)} \binom{s}{m - r} \binom{t + 1}{r}.$$

If  $s(0) = \binom{s}{m}$ , then  $s(r) = 0$  for  $r \equiv 1 \pmod{2}$ ,  $s(r) = \binom{s}{m-r}$  for  $r \equiv 0 \pmod{2}$ , and so

$$|V_m| \leq \sum s(r) \binom{t + 1}{r} = \sum_{r \equiv 0(2)} \binom{s}{m - r} \binom{t + 1}{r}.$$

Theorem 1 now easily follows from the following binomial coefficient inequality.

LEMMA 2. *If  $m, n,$  and  $k$  are positive integers, and*

$$f_j(m, n, k) = \sum_{r \equiv j(2)} \binom{n}{m-r} \binom{k}{r}$$

for  $j = 0$  or  $1,$  then

$$f_j(m, n, k) \leq \begin{cases} \binom{n+k-1}{m}, & m < (n+k)/2, \\ \binom{n+k-1}{m-1}, & m > (n+k)/2, \\ 2\binom{n+k-2}{m-1}, & m = (n+k)/2. \end{cases}$$

PROOF. We first prove the lemma for  $n+k$  odd,  $m = (n+k-1)/2.$  Let us first assume that  $n \geq 4, k \geq 4.$  Since  $f_j(m, n, k)$  is the coefficient of  $z^m$  in

$$\frac{1}{2}(1+z)^k(1+z)^n + \frac{1}{2}(-1)^j(1-z)^k(1+z)^n,$$

it will suffice to prove that if  $A_m =$  coefficient of  $z^m$  in  $(1-z)^k(1+z)^n,$  then

$$(8) \quad |A_m| < 2\binom{n+k-1}{m} - \binom{n+k}{m} = \frac{1}{m+1}\binom{n+k-1}{m} = \frac{1}{m+1}\binom{2m}{m}.$$

Now by Cauchy's theorem,

$$A_m = \frac{1}{2\pi i} \int_{|z|=1} (1-z)^k(1+z)^k z^{-m-1} dz,$$

so as  $\theta$  runs over the real numbers,

$$|A_m| \leq \max_{\theta} |1 - e^{i\theta}|^k |1 + e^{i\theta}|^n = \max_{\theta} 2^{n+k} \left| \sin \frac{1}{2} \theta \right|^k \left| \cos \frac{1}{2} \theta \right|^n.$$

Letting  $x = (\sin(\theta/2))^2,$  we find that

$$|A_m|^2 \leq \max_{0 < x < 1} 4^{n+k} x^k (1-x)^n.$$

By setting the derivative of  $x^k(1-x)^n$  equal to 0, we discover that the maximum above is attained at  $x = k/(n+k),$  and equals

$$\frac{k^k n^n 4^{n+k}}{(n+k)^{n+k}} = \frac{k^k n^n 4^{2m+1}}{(2m+1)^{2m+1}}.$$

To obtain (8), it will therefore suffice to prove that for  $4 < k < 2m-1,$

$$(9) \quad k^k (2m+1-k)^{2m+1-k} < 4^{-2m-1} \frac{(2m+1)^{2m+1}}{(m+1)^2} \binom{2m}{m}^2.$$

The maximum of the quantity on the left side above is achieved at the endpoints of the interval  $[4, 2m - 3]$ , so it will suffice to prove (9) for  $k = 4$ , which reduces to

$$(10) \quad 4^{2m+5}(2m - 3)^{2m-3} \frac{(m + 1)^2}{(2m + 1)^{2m+1}} < \binom{2m}{m}^2.$$

Since

$$\binom{2m}{m} \geq \frac{4^m}{2\sqrt{m}} \quad \text{for } m > 1,$$

(10) will follow if we can show that

$$(11) \quad m(m + 1)^2(2m - 3)^{2m-3}(2m + 1)^{-2m-1} < 4^{-6}.$$

But

$$\begin{aligned} m(m + 1)^2 \frac{(2m - 3)^{2m-3}}{(2m + 1)^{2m+1}} &= \frac{m(m + 1)^2}{(2m - 3)^4} \left(1 - \frac{4}{2m + 1}\right)^{2m+1} \\ &< \frac{m(m + 1)^2}{(2m - 3)^4} e^{-4} \quad \text{for } m > 1, \end{aligned}$$

and  $m(m + 1)^2(2m - 3)^{-4} < 11 \cdot 12^2 \cdot 19^{-4} < e^4 \cdot 4^{-6}$  for  $m > 11$ , which proves (11), and therefore also (10) for  $m \geq 11$ . Finally, it is easily checked that (10) holds for  $7 \leq m \leq 10$ . We have thus proved the lemma in the special case  $m = (n + k - 1)/2$ ,  $4 \leq k \leq 2m - 3$ ,  $m \geq 7$ . If  $m = (n + k - 1)/2$ ,  $4 \leq k \leq 2m - 3$ , but  $4 \leq m \leq 6$ , then we check by direct computation that the lemma holds.

To complete the proof of the lemma for  $m = (n + k - 1)/2$ , we next consider  $1 \leq k \leq 3$ . As an example, we have

$$\begin{aligned} f_1((n + 2)/2, n, 3) &= 3 \binom{n}{n/2} + \binom{n}{n/2 - 2} \\ &= 6 \binom{n - 1}{n/2 - 1} + \binom{n}{n/2 - 2} + \binom{n}{n/2 - 3}. \end{aligned}$$

On the other hand,

$$\binom{n + 2}{(n + 2)/2} = 6 \binom{n - 1}{n/2 - 1} + 2 \binom{n}{n/2 - 2} > f_1((n + 2)/2, n, 3).$$

The verification of the other cases is even more routine and is omitted. Finally, the case  $2m - 2 \leq k \leq 2m$  reduces to the case  $1 \leq k \leq 3$ , since

$$f_j(m, n, k) = f_{j'}(m, k, n),$$

where  $j = j'$  if  $m \equiv 0 \pmod{2}$ , and  $j = 1 - j'$  otherwise.

The above discussion proves the lemma whenever  $m = (n + k - 1)/2$ . The remaining cases follow quite easily. We use induction on  $m + n$ . Suppose that

the lemma is true for  $m + n < M$ . Since the lemma is trivially true if any of  $m, n,$  and  $k$  equals 1, this assumption is certainly true for  $M = 2$ . Now suppose  $m + n = M + 1$ , and that  $m \geq 2, n \geq 2$ . Then

$$(12) \quad \begin{aligned} f_j(m, n, k) &= \sum_{r \equiv j(2)} \left\{ \binom{n-1}{m-r} + \binom{n-1}{m-1-r} \right\} \binom{k}{r} \\ &= f_j(m, n-1, k) + f_j(m-1, n-1, k). \end{aligned}$$

We now apply the induction hypothesis to

$$f_j(m, n-1, k) \quad \text{and} \quad f_j(m-1, n-1, k).$$

If  $m < (n + k - 1)/2$ , then we obtain

$$f_j(m, n, k) < \binom{n+k-2}{m} + \binom{n+k-2}{m-1} = \binom{n+k-1}{m},$$

which is the claim of the lemma. Similarly if  $m > (n + k + 1)/2$ , then

$$f_j(m, n, k) < \binom{n+k-2}{m-1} + \binom{n+k-2}{m-2} = \binom{n+k-1}{m-1}.$$

If  $m = (n + k)/2$ , then (12) and the induction hypothesis give

$$f_j(m, n, k) < 2 \binom{n+k-2}{m-1}.$$

To complete the proof, we thus only have to consider  $m = (n + k \pm 1)/2$ . If  $m = (n + k - 1)/2$ , then the claim of the lemma follows from the discussion at the beginning of the proof. The case  $m = (n + k + 1)/2$ , on the other hand, follows from the case  $m = (n + k - 1)/2$  and the observation that

$$f_j(m, n, k) = \sum_{r \equiv j(2)} \binom{n}{n-m+r} \binom{k}{k-r} = \sum_{n \equiv k+j(2)} \binom{n}{n+k-m-s} \binom{k}{s},$$

so that  $f_j(m, n, k) = f_{j'}(n + k - m, n, k)$ , where  $j' \equiv k + j \pmod{2}$ .

### References

[1] W. E. Longstaff, "Combinatorial solution of certain systems of linear equations involving (0, 1) matrices", *J. Austral. Math. Soc. Ser. A* **23**, (1977), 266–274.

Bell Laboratories  
 Murray Hill  
 New Jersey 07974  
 U.S.A.