JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematics and Mathematical Physics
Vol. 69B, No. 3, July–September 1965

Some Theorems on the Permanent*

R. A. Brualdi and M. Newman

(June 9, 1965)

The purpose of this paper is to prove some miscellaneous theorems on the permanent. We define $f(k)$ to be the smallest order of a 0, 1 matrix with permanent equal to k and obtain an asymptotic formula for $\log f(k)$. A few theorems concerning the permanent of a circulant matrix are also proved.

1. Introduction

Let $A=[a_{ij}]$ be an $n \times n$ complex matrix. The permanent of A is the scalar valued function of A defined by

$$\text{per}\,(A)=\Sigma a_{1i_1}a_{2i_2}\;.\;.\;.\;a_{ni_n}$$

where the summation extends over all permutations $i_1, i_2, \ldots, i_n$ of $1, 2, \ldots, n$. Much of the current interest in the permanent is derived from a conjecture of van der Waerden, and directly or indirectly this conjecture accounts for a great deal of the research that has been done; see e.g., [1, 3, 4].[1] Our purpose here is to prove some miscellaneous theorems on the permanent. In section 2 we define a function on the positive integers by means of the permanent and obtain an asymptotic formula. In section 3 we deal with matrices which are nonnegative circulants. We derive there a congruence and upper bound for the permanent and also a theorem which would be a consequence of the van der Waerden conjecture.

2. An Asymptotic Formula

For k a positive integer define $f(k)$ to be the smallest order of a 0, 1 matrix with permanent equal to k. It of course must be verified that this definition is meaningful, and the following example shows this to be so. Define A_k to be the $k \times k$ 0, 1 matrix

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \cdot & & & & \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & & & & \\ 1 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Then it is easily seen that per $(A_k)=k$. The example also shows that $f(k)$ satisfies

$$f(k) \leqq k, \qquad k=1, 2, \ldots .$$

By taking direct sums we find that the function f also satisfies

$$f(mn) \leqq f(m)+f(n)$$

where m and n are positive integers. This function $f(k)$ is a very complicated one and how much can be said about it is not clear. However the following theorem shows that $\log f(k)$ is of the same order of magnitude as $\log \log k$.

*This work was done while the first author was a National Academy of Sciences—National Research Council Postdoctoral Resident Research Associate at the National Bureau of Standards, 1964–1965.

[1] Figures in brackets indicate the literature references at the end of this paper.

THEOREM 2.1. $\log f(k) \sim \log \log k$

PROOF. Let $A(\epsilon_0, \epsilon_1, \ldots, \epsilon_n)$ be the following $(n+2) \times (n+2)$ matrix:

$$\begin{bmatrix} 0 & \epsilon_0 & \epsilon_1 & \epsilon_2 & \ldots & \epsilon_n \\ 1 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & 0 & \ldots & 0 \\ 1 & 1 & 1 & 1 & \ldots & 0 \\ . & . & . & . & \ldots & . \\ 1 & 1 & 1 & 1 & \ldots & 1 \end{bmatrix} \tag{2.1}$$

Here we take $\epsilon_i = 0$ or 1, $i = 0, 1, \ldots, n$. We calculate the permanental minor, p_i, of ϵ_i; that is, the permanent of the $(n+1) \times (n+1)$ matrix obtained from (2.1) by striking out the row and column to which ϵ_i belongs. We have $p_0 = 1$, $p_1 = 2$, and in general that

$$p_i = 2p_{i-1}, \qquad i = 1, 2, \ldots, n.$$

Hence by induction it follows that

$$p_i = 2^i, \qquad i = 0, 1, \ldots, n.$$

Then by the Laplace expansion for the permanent we obtain

$$\text{per}\,(A(\epsilon_0, \epsilon_1, \ldots, \epsilon_n)) = \epsilon_0 + 2\epsilon_1 + \ldots + 2^n \epsilon_n \tag{2.2}$$

Now let k be any positive integer and write k in binary form,

$$k = \epsilon_0 + 2\epsilon_1 + \ldots + 2^n \epsilon_n$$

where $\epsilon_i = 0$ or 1 for $i = 0, 1, \ldots, n-1$ and $\epsilon_n = 1$. Then by the above calculation $A(\epsilon_0, \epsilon_1, \ldots, \epsilon_n)$ is an $(n+2) \times (n+2)$ 0, 1 matrix with permanent equal to k, so that $f(k) \leqq n+2$. Since $k \geqq 2^n$, this implies that

$$f(k) \leqq \frac{\log k}{\log 2} + 2.$$

Thus there is a constant $a > 0$ such that

$$\frac{\log f(k)}{\log \log k} < 1 + \frac{a}{\log \log k}. \tag{2.3}$$

Now let r be the uniquely determined integer such that

$$(r-1)! < k \leqq r!.$$

Then it is clear that $f(k) \geqq r$. An easy application of Stirling's formula shows that for a suitable constant $b > 0$,

$$r > b \, \frac{\log k}{\log \log k}$$

and thus

$$f(k) > b \, \frac{\log k}{\log \log k}.$$

Hence there is a constant $c > 0$ such that

$$\frac{\log f(k)}{\log \log k} > 1 - c \, \frac{\log \log \log k}{\log \log \text{k.}} \tag{2.4}$$

The two inequalities (2.3) and (2.4) imply the theorem upon passage to the limit.

Now let $\mathfrak{A}(n)$ denote the class of all $n \times n$ 0, 1 matrices. The permanent restricted to $\mathfrak{A}(n)$ is a function mapping $\mathfrak{A}(n)$ into the set of integers $0, 1, \ldots, n!$. The following corollary gives some information about its range.

COROLLARY 2.2. *Let* k *be an integer with* $0 \leqq \text{k} \leqq 2^{n-1}$. *Then there exists a matrix* A *in* $\mathfrak{A}(\text{n})$ *with permanent equal to* k.

PROOF. Let $k < 2^{n-1}$. Then the binary expansion of k is

$$k = \epsilon_0 + 2\epsilon_1 + \ldots + 2^{n-2} \epsilon_{n-2}$$

with $\epsilon_i = 0$ or 1 for $i = 0, 1, \ldots, n-2$. But then $\text{A}(\epsilon_0, \epsilon_1, \ldots, \epsilon_{n-2})$ is a matrix in $\mathfrak{A}(n)$ with permanent equal to k. The $n \times n$ matrix in $\mathfrak{A}(n)$ which is obtained from $A(1, 1, \ldots, 1)$ by replacing the 0 in the (1, 1) position by a 1 has permanent equal to 2^{n-1}. This establishes the corollary.

3. Nonnegative Circulants

Let C be an $n \times n$ nonnegative circulant matrix so that

$$C = [c_{ij}] = c_0 P^0 + c_1 P^1 + \ldots + c_{n-1} P^{n-1}, \; P^0 = I,$$

where

$$P = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & . & . & \ldots & . \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}, \tag{3.1}$$

the $n \times n$ full cycle permutation matrix, and $c_i \geqq 0$, $i = 0, 1, \ldots, n-1$. Then the permanent of C is

$$\text{per}\,(C) = \sum_\sigma c_{1\sigma(1)} c_{2\sigma(2)} \ldots c_{n\sigma(n)},$$

where the summation extends over all permutations σ of $1, 2, \ldots, n$. Suppose that for $k = 0, 1, \ldots, n-1$ there are precisely x_k integers i from $1, 2, \ldots,$

n such that

$$\sigma(i)-i\equiv k \qquad (\mathrm{mod}\ n). \tag{3.2}$$

Then from the definition of a circulant it follows that

$$c_{1\sigma(1)}c_{2\sigma(2)}\ .\ .\ .\ c_{n\sigma(n)}=c_0^{x_0}c_1^{x_1}\ .\ .\ .\ c_{n-1}{}^{x_{n-1}}$$

The x_k are nonnegative integers satisfying

$$x_0+x_1+.\ .\ .+x_{n-1}=n. \tag{3.3}$$

By summing (3.2) over all $i=1, 2, \ldots, n$ they also satisfy

$$0\cdot x_0+1\cdot x_1+.\ .\ .+(n-1)x_{n-1}\equiv 0\ (\mathrm{mod}\ n). \tag{3.4}$$

Hence we may write

$$\mathrm{per}\ (C)=\Sigma\mu(x_0, x_1, \ldots, x_{n-1})c_0^{x_0}c_1^{x_1}\ .\ .\ .\ c_{n-1}{}^{x_{n-1}} \tag{3.5}$$

where the summation extends over all nonnegative integers $x_0, x_1, \ldots, x_{n-1}$ satisfying (3.3) and (3.4). Here $\mu(x_0, x_1, \ldots, x_{n-1})$ is a nonnegative integer.

Theorem 3.1. *If* C *is an* $n\times n$ *nonnegative circulant, then*

$$\mathrm{per}\ (C)\leqq\frac{\mathrm{tr}\ (C^n)}{n}, \tag{3.6}$$

where tr (X) *denotes the trace of* X.

Proof. We have that

$$C^n=\sum\frac{n!}{x_0!x_1!\ .\ .\ .\ x_{n-1}!}c_0^{x_0}c_1^{x_1}\ .\ .\ .\ c_{n-1}{}^{x_{n-1}}\ P^{0\cdot x_0}P^{1\cdot x_1}\ .\ .\ .\ P^{(n-1)x_{n-1}},$$

where the summation extends over all nonnegative integers $x_0, x_1, \ldots, x_{n-1}$ satisfying $x_0+x_1+\ldots+x_{n-1}=n$. Consider

$$P^{0\cdot x_0}P^{1\cdot x_1}\ .\ .\ .\ P^{(n-1)x_{n-1}}=P^a.$$

Now $tr(P^a)=0$ unless $P^a=I$ in which case $tr(P^a)=n$. But $P^a=I$ if and only if

$$a=0\cdot x_0+1\cdot x_1+.\ .\ .+(n-1)x_{n-1}\equiv 0\ (\mathrm{mod}\ n).$$

Hence we may write

$$\frac{tr(C^n)}{n}=\sum\frac{n!}{x_0!x_1!\ .\ .\ .\ x_{n-1}!}c_0^{x_0}c_1^{x_1}\ .\ .\ .\ c_{n-1}{}^{x_{n-1}}$$

where the summation extends over all nonnegative integers $x_0, x_1, \ldots, x_{n-1}$ satisfying (3.3) and (3.4). But clearly

$$\mu(x_0, x_1, \ldots, x_{n-1})\leqq\binom{n}{x_0}\binom{n-x_0}{x_1}\ .\ .\ .\ \binom{n-x_0-\ldots-x_{n-1}}{x_n}=\frac{n!}{x_0!x_1!\ .\ .\ .\ x_{n-1}!}.$$

Since the c_i are nonnegative numbers, inequality (3.6) now follows.

We now assume that the circulant is of prime order.

Theorem 3.2. *Let* p *be a prime and* $C=c_0P^0+c_1P^1+\ldots+c_{p-1}P^{p-1}$, *a* $p\times p$ *circulant with* $c_0, c_1, \ldots, c_{p-1}$ *nonnegative integers. Then*

$$\mathrm{per}\ (C)\equiv c_0+c_1+\ldots+c_{p-1}\ (\mathrm{mod}\ p).$$

Proof. Let t be the permutation of $1, 2, \ldots, p$ corresponding to the permutation matrix P given in (3.1); that is, $t(i)\equiv i+1\ (\mathrm{mod}\ p)$. Let σ be a permutation distinct from $t^0=1, t, \ldots, t^{p-1}$. Suppose σ corresponds to the term $c_0^{x_0}c_1^{x_1}\ .\ .\ .\ c_{p-1}{}^{x_{p-1}}$ in per (C), so that there are precisely x_r i's with $\sigma(i)-i\equiv r\ (\mathrm{mod}\ p)$. Consider the permutation $t^k\sigma t^{-k}$ for $k=0, 1, \ldots, p-1$. We have that

$$\begin{aligned} t^k\sigma t^{-k}(i)-i &\equiv t^k\sigma(i-k)-i && (\mathrm{mod}\ p)\\ &\equiv \sigma(i-k)+k-i && (\mathrm{mod}\ p)\\ &\equiv \sigma(i-k)-(i-k) && (\mathrm{mod}\ p). \end{aligned}$$

Here $(i-k)$ is to be interpreted as its residue mod p in the complete residue system $1, 2, \ldots, p$. But then as i varies over the integers $1, 2, \ldots, p$, $(i-k)$ varies over $1, 2, \ldots, p$. Hence σ and $t^k\sigma t^{-k}$ give rise to equal summands $c_0^{x_0}c_1^{x_1}\ .\ .\ .\ c_{p-1}{}^{x_{p-1}}$ in per (C). Suppose $t^k\sigma t^{-k}=\sigma$ for some $k=1, 2, \ldots, p-1$. Then inductively it follows that $t^{jk}\sigma t^{-jk}=\sigma$ for $j=1, 2, \ldots$. Thus

$$t^{jk}\sigma(1)=\sigma t^{jk}(1),$$

and therefore

$$\sigma(1)+jk\equiv\sigma(1+jk) \qquad (\mathrm{mod}\ p)$$

or

$$\sigma(1)-1\equiv\sigma(1+jk)-(1+jk)\ (\mathrm{mod}\ p), \qquad j=1, 2, \ldots$$

Here again $1+jk$ is to be interpreted as the residue in the appropriate residue system mod p. But as j varies over $1, 2, \ldots, p$ so does the residue of $1+jk$. For

$$1+jk\equiv 1+j'k\ (\mathrm{mod}\ p), \qquad 1\leqslant j<j'\leqslant p,$$

implies $p\,|\,(j'-j)k$, the latter being impossible for p a prime. Therefore $\sigma(i)-i\equiv\sigma(1)-1\equiv a\ (\mathrm{mod}\ p)$, for $i=1, 2, \ldots, p$, and this implies $\sigma=t^a$ which is a contradiction. Hence the permutations σ, $t\sigma t^{-1}$, . . ., $t^{p-1}\sigma t^{-(p-1)}$ are all distinct. Therefore the coefficient of $c_0^{x_0} c_1^{x_1} \ldots c_{p-1}^{x_{p-1}}$ in per (C) is congruent to zero modulo P. Since this is true for all terms arising from a permutation $\sigma \neq t^0, t^1, \ldots, t^{p-1}$, we can conclude that

$$\text{per}\,(C) \equiv c_0^p + c_1^p + \ldots + c_{p-1}^p \pmod p$$

$$\equiv c_0 + c_1 + \ldots + c_{p-1} \pmod p,$$

the second congruence following from Fermat's theorem.

Let $\mathfrak{A}(n;\,k)$ denote the class of all $n\times n$ 0, 1 matrices with precisely k 1's in each row and column. It has been conjectured by Marshall Hall that

$$\lim_{n\to\infty} \min_{A\in\mathfrak{A}(n;\,k)} \text{per}\,(A) = \infty, \qquad k \geqq 3. \tag{3.7}$$

This conjecture would be a consequence of the validity of the van der Waerden conjecture which asserts for $A\in\mathfrak{A}(n;\,k)$ that

$$\text{per}\,(A) \geqq k^n \frac{n!}{n^n}.$$

Hall's conjecture appears to be about as difficult as that of van der Waerden. The following theorem shows that (3.7) is valid if instead of considering the class $\mathfrak{A}(n;\,k)$ we consider the subclass $\mathfrak{C}(n;\,k)$ of all $n\times n$ 0, 1 circulant matrices with $k \geqq 3$ 1's in each row and column.

THEOREM 3.3. *For* $k \geqq 3$,

$$\lim_{n\to\infty} \min_{C\in\mathfrak{C}(n;\,k)} \text{per}\,(C) = \infty. \tag{3.8}$$

PROOF. Clearly we need only prove (3.8) for the case $k=3$. Thus let $C\in\mathfrak{C}(n;\,3)$. Without loss of generality we may assume that

$$C = I + P^i + P^j,\ 1 \leqq i < j \leqq n-1, \tag{3.9}$$

where P is defined as in (3.1). We define a permutation σ of 1, 2, . . ., n in the following way:

$$\sigma(r) = r \qquad ,\qquad r = 1, \ldots, j-i$$

$$\sigma(j-i+r) = j+r \qquad ,\qquad r = 1, \ldots, n-j$$

$$\sigma(n-i+r) = j-i+r, \qquad r = 1, \ldots, i.$$

It is easy to verify that σ is indeed a permutation of 1, 2, . . ., n.

Now

$$\sigma(r) - r \equiv 0 \pmod n \qquad ,\qquad r = 1, \ldots, j-i$$

$$\sigma(j-i-r) - (j-i-r) \equiv i \pmod n, \qquad r = 1, \ldots, n-j$$

$$\sigma(n-i+r) - (n-i+r) \equiv j \pmod n, \qquad r = 1, \ldots, i.$$

Hence the term in per (C) corresponding to the permutation σ is equal to

$$c_0^{j-i} c_i^{n-j} c_j^i \tag{3.10}$$

which, when C is given by (3.9), is equal to 1.

Let t be the permutation defined by $t(i) \equiv i+1 \pmod n$. As in the proof of the preceding theorem (the primeness was not used in this part) it follows that the permutations σ, $t\sigma t^{-1}$, . . ., $t^{(n-1)}\sigma t^{-(n-1)}$ all give rise to equal summands (3.10) in per (C). But

$$t^k \sigma t^{-k} \neq \sigma, \qquad k = 1, 2, \ldots, n-1$$

since the fixed elements of the permutation σ are 1, 2, . . ., $j-i$ while those of $t^k\sigma t^{-k}$ are $1+k, 2+k, \ldots, j-i+k \pmod n$. Hence the permutations σ, $t\sigma t^{-1}$, . . ., $t^{(n-1)}\sigma t^{-(n-1)}$ are all distinct, each contributing 1 to per (C). These along with the three permutations $t^0 = 1$, t^i, t^j show that

$$\text{per}\,(C) \geqq n+3. \tag{3.11}$$

Since (3.11) is true for each $C\in\mathfrak{C}(n,\,3)$, the conclusion (3.8) of the theorem is proved.

In case n equals a prime p, inequality (3.11) can be proved by use of theorem 3.2. For by this theorem per $(C) \equiv 3 \pmod p$, while by [2] per $(C) \geqq 6$. Hence per $(C) \geqq p+3$.

Theorem 3.3 can be generalized to a larger class of matrices in the following way. Let $\mathfrak{D}(n;\,k)$ denote the class of all $n\times n$ matrices A which are expressible in the form

$$A = Q^{i_1} + Q^{i_2} + \ldots + Q^{i_k},$$
$$0 \leqq i_1 < \ldots < i_k \leqq n-1,$$

for some permutation matrix Q of order n. We then have

THEOREM 3.4. *For* k $\geqq$ 3,

$$\lim_{n\to\infty} \min_{A\in\mathfrak{D}(n;\,k)} \text{per}\,(A) = \infty. \tag{3.12}$$

PROOF. Again we need only prove (3.12) for the case $k=3$. Thus let A be in $\mathfrak{D}(n;\,3)$. Without loss of generality we may assume that

$$A = I + Q^i + Q^j, \qquad 1 \leqq i < j \leqq n-1.$$

There exists a permutation matrix R such that

$$RQR' = P_{n_1} \dotplus P_{n_2} \dotplus \ldots \dotplus P_{n_r}$$

where P_{n_s} is the full cycle permutation matrix of order $n_s \geqq 1$. Since the permanent of A is not changed if we permute its rows and columns, we may assume that

$$Q = P_{n_1} \dotplus P_{n_2} \dotplus \ldots \dotplus P_{n_r}.$$

Then

$$\text{per}\,(I + Q^i + Q^j) = \prod_{s=1}^{r} \text{per}\,(I + P_{n_s}^i + P_{n_s}^j). \tag{3.13}$$

If $n_s=1$, then per $(I+P_{n_s}^i+P_{n_s}^j)=3$. If $n_s>1$, then either $P_{n_s}^i$ and $P_{n_s}^j$ are disjoint permutation matrices or are identical. If they are identical, then

$$\text{per } (I+P_{n_s}^i+P_{n_s}^j) \geqq 2^{n_s}+1 \geqq n_s+3.$$

Otherwise we may apply (3.11) to obtain

$$\text{per } (I+P_{n_s}^i+P_{n_s}^j) \geqq n_s+3.$$

By applying these results to (3.13) we are able to conclude that

$$\begin{aligned} \text{per } (I+Q^i+Q^j) &\geqq n_1+\ldots+n_r+3 \\ &=n+3. \end{aligned}$$

From this the theorem follows.

4. References

[1] R. A. Brualdi and M. Newman, Inequalities for permanents and permanental minors, Proc. Camb. Phil. Soc. **61**, (1965).

[2] M. Hall, Jr., Distinct representatives of subsets. Bull. Amer. Math. Soc. **54**, 922–926 (1948).

[3] M. Marcus and M. Newman, Inequalities for the permanent function. Ann. Math. **75**, 47–62 (1962).

[4] H. J. Ryser, Combinatorial Mathematics. Carus Math. Monograph, No. 14 (Wiley & Sons, New York, N.Y., 1962).

(Paper 69B3–147)