Journal of Algebraic Combinatorics, 20, 55–60, 2004

The Number of Terms in the Permanent and the Determinant of a Generic Circulant Matrix

HUGH THOMAS hthomas@fields.utoronto.ca
Fields Institute, 222 College Street, Toronto ON, M5T 3J1, Canada

Received September 10, 2002; Revised June 26, 2003; Accepted August 5, 2003

Abstract. Let $A = (a_{ij})$ be the generic $n \times n$ circulant matrix given by $a_{ij} = x_{i+j}$, with subscripts on x interpreted mod n. Define $d(n)$ (resp. $p(n)$) to be the number of terms in the determinant (resp. permanent) of A. The function $p(n)$ is well-known and has several combinatorial interpretations. The function $d(n)$, on the other hand, has not been studied previously. We show that when n is a prime power, $d(n) = p(n)$.

Keywords: generic circulant matrix, determinant, permanent

1. Introduction

A square matrix is said to be a circulant matrix if its rows are successive cyclic permutations of the first row. Thus, the matrix $A = (a_{ij})$ with $a_{ij} = x_{i+j}$, subscripts on x being interpreted mod n, is a generic circulant matrix.

If we expand det(A), we obtain a polynomial in the x_i. We define $d(n)$ to be the number of terms in this polynomial after like terms have been combined. Similarly, we define $p(n)$ to be the number of terms in per(A), the permanent of A.

The function $p(n)$ was studied in Brualdi and Newman [1], where it was pointed out that the main result of Hall [3] shows that $p(n)$ coincides with the number of solutions to

$$\begin{aligned} y_1 + 2y_2 + \cdots + ny_n &\equiv 0 \,(\mathrm{mod}\, n) \\ y_1 + \cdots + y_n &= n \end{aligned} \tag{1}$$

in non-negative integers. Using this formulation, they showed by a generating function argument that

$$p(n) = \frac{1}{n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \binom{2d-1}{d}. \tag{2}$$

Setting $w_i = \sum_{j=i+1}^{n} y_j$, and rewriting (1) in terms of the w_i, we see that $p(n)$ is the number of non-increasing $(n-1)$-tuples $(w_1, \ldots, w_{n-1})$ with $n \geq w_1 \geq \cdots \geq w_{n-1} \geq 0$, such that $\sum_i w_i \equiv 0 \pmod{n}$. If we let L be the $(n-1)$-dimensional lattice consisting of $(n-1)$-tuples of integers whose sum is divisible by n, then this expression for $p(n)$ amounts to the number of points from L lying in the simplex with vertices $(0, 0, \ldots, 0)$, $(n, 0, 0, \ldots, 0)$, $(n, n, 0, \ldots, 0)$, $\ldots$, $(n, n, \ldots, n)$.

There is another combinatorial interpretation for $p(n)$, as follows. Consider all possible necklaces consisting of n white beads and n black beads, where two necklaces are considered

Table 1. Values of $d(n)$ and $p(n)$ for small n.

n	$d(n)$	$p(n)$	n	$d(n)$	$p(n)$
1	1	1	7	246	246
2	2	2	8	810	810
3	4	4	9	2704	2704
4	10	10	10	7492	9252
5	26	26	11	32066	32066
6	68	80	12	86500	112720

equivalent if they differ by a cyclic permutation. A straightforward Pólya counting argument shows that the number of such necklaces is given by the right-hand side of (2), and thus that the number of necklaces equals the number of terms in per(A), though no explicit bijection is known.

The other function we consider here, $d(n)$, the number of terms in the expansion of the determinant of a generic circulant matrix, does not have any known combinatorial interpretation. One motivation for its investigation is the consideration that interesting sequences are known to arise as the number of terms in the expansion of $n \times n$ generic matrices of other types. Clearly, the expansion of the determinant of a completely generic matrix, where the matrix entries consist of n^2 different indeterminates, has $n!$ terms. The same is true for the expansion of a generic Vandermonde matrix. Somewhat less trivially, if we consider matrices with generic entries in the diagonal, subdiagonal, and superdiagonal, and zeros elsewhere, we find that the number of terms in the expansion of the determinant is the n-th Fibonacci number, as it is easily seen to satisfy the Fibonacci recursion and initial conditions.

Previously, little was known about $d(n)$. Some initial results appear in Lehmer [4]. It is clear that $d(n) \leq p(n)$ since every term which appears in the determinant also appears in the permanent. However, some terms from the permanent could be absent from the determinant due to cancellation. In this paper we establish the following theorem:

Theorem *If n is a prime power*, $d(n) = p(n)$.

The above table of values for $d(n)$ and $p(n)$ suggests that the converse may also be true. This is still open.

The proof of the theorem uses the theory of symmetric functions. In this section, we review the necessary definitions and results. For more detail on symmetric functions, see Stanley [5].

2. Background on symmetric functions

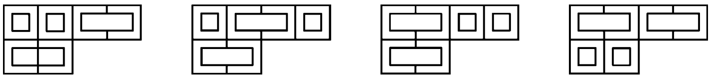
Symmetric functions are power series (in our case, over $\mathbb{Q}$) in an infinite number of variables $z_1, z_2, \ldots,$ such that for any $(b_1, \ldots, b_k) \in \mathbb{N}^k$ the coefficient of $z_{i_1}^{b_1} \ldots z_{i_k}^{b_k}$ does not depend on the choice of distinct natural numbers $i_1, \ldots, i_k$.

We write $\lambda \vdash q$ to signify that λ is a partition of q. The symmetric functions of degree q form a vector space whose dimension is the number of partitions of q. There are several standard bases for them. We shall need two here: $\{m_\lambda \mid \lambda \vdash q\}$ and $\{p_\lambda \mid \lambda \vdash q\}$. For $\lambda = (\lambda_1, \ldots, \lambda_k)$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$, m_λ is the power series in which $z_{i_1}^{\lambda_1} \ldots z_{i_k}^{\lambda_k}$ occurs with coefficient one for every distinct sequence of natural numbers $i_1, \ldots, i_k$ and no other terms occur. The symmetric function p_i is defined to be $z_1^i + z_2^i + \ldots$, and the symmetric function p_λ is defined to be $p_{\lambda_1} \ldots p_{\lambda_k}$.

As we remarked, $\{p_\lambda \mid \lambda \vdash q\}$ and $\{m_\lambda \mid \lambda \vdash q\}$ form bases for the symmetric functions of degree q. We will need to convert from the m_λ basis to the p_λ basis, which we shall do using a result of Eğecioğlu and Remmel [2], for which we must introduce some notation.

For $\lambda \vdash q$, let $k(\lambda)$ denote the number of parts of λ. If $\lambda = \langle 1^{l_1} 2^{l_2} \ldots q^{l_q} \rangle$, let $\lambda! = 1!^{l_1} 2!^{l_2} \ldots q!^{l_q}$, and let $z_\lambda = l_1! \ldots l_q! 1^{l_1} 2^{l_2} \ldots q^{l_q}$.

The Ferrers diagram of λ consists of a left-justified column of rows of boxes of lengths $\lambda_1, \lambda_2, \ldots, \lambda_k$. For μ another partition of q, a filling of λ by μ is a way to cover the Ferrers diagram of λ in a non-overlapping manner by "bricks" consisting of horizontal sequences of boxes of length $\mu_1, \mu_2, \ldots$. The weight of a filling is the product over all rows of the length of the final brick in each row. In deciding whether two fillings are the same, bricks of the same size are considered to be indistinguishable. Thus, the four fillings of $\lambda = (4, 2)$ by $\mu = (2, 2, 1, 1)$, having weights respectively 4, 2, 2, and 2, are:



Let $w(\lambda, \mu)$ be the sum over all distinct fillings of λ by μ of the weight of the filling. Then the result we shall need from [2] is that:

$$m_\mu = \sum_{\lambda \vdash q} \frac{(-1)^{k(\mu)-k(\lambda)} w(\lambda, \mu)}{z_\lambda} p_\lambda.$$

Proof of theorem

First, let us consider what terms occur in per(A). Let $b = (b_1, \ldots, b_n)$ be an n-tuple of natural numbers summing to n. Let x^b denote $x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$. We are interested in whether x^b appears in per(A) with non-zero coefficient. Suppose it does. Then there is some permutation σ of $\{1, \ldots, n\}$ such that $\prod_i x_{i-\sigma(i)} = x^b$. Since $\sum_i (i - \sigma(i)) = 0$, it follows that $\sum_i i b_i \equiv 0 \pmod{n}$. By the result of [3] mentioned above, this necessary condition for x^b to occur in per(A) is also sufficient.

Now we proceed to consider det(A). Let ξ be a primitive n-th root of unity. A is diagonalizable, and its eigenvalues are $c_1, \ldots, c_n$, where $c_i = \sum_j \xi^{ij} x_j$. Thus, $\det(A) = \prod c_i$.

Again, let $b = (b_1, \ldots, b_n)$ be an n-tuple of integers summing to n. Let $q = b_1 + 2b_2 + \cdots + nb_n$. Let $\mu = \langle 1^{b_1} 2^{b_2} \ldots n^{b_n} \rangle$, so $\mu \vdash q$. Then $[x^b] \det(A)$, the coefficient of x^b in $\det(A)$, is given by

$$[x^b] \det(A) = \sum_{\substack{f:\{1,\ldots,n\} \to \{1,\ldots,n\} \\ |f^{-1}(i)| = b_i}} \xi^{\sum_{i=1}^n i f(i)}.$$

We observe that this also equals $m_\mu(\xi^1, \xi^2, \ldots, \xi^n, 0, 0, \ldots)$. (A symmetric function is a power series, so it is not generally legitimate to substitute in values for the indeterminates, but since m_μ is homogeneous and all but finitely many of the values being substituted are zero, it is allowed in this case.)

Now we use the result of [2] mentioned above, which shows that:

$$[x^b]\det(A) = \sum_{\lambda \vdash q} \frac{(-1)^{k(\mu)-k(\lambda)} w(\lambda, \mu) p_\lambda(\xi^1, \xi^2, \ldots, \xi^n, 0, 0, \ldots)}{z_\lambda}. \tag{3}$$

What can we say about $p_\lambda(\xi^1, \xi^2, \ldots, \xi^n, 0, 0, \ldots)$? Firstly, $p_i(\xi^1, \xi^2, \ldots, \xi^n, 0, 0, \ldots) = n$ if $n \mid i$ and 0 otherwise. Thus, $p_\lambda(\xi^1, \xi^2, \ldots, \xi^n, 0, 0, \ldots) = n^{k(\lambda)}$ if all the parts of λ are multiples of n, and 0 otherwise.

(From this we could deduce that if $[x^b]\det(A)$ is non-zero, $q = b_1 + 2b_2 + \cdots + nb_n$ must be a multiple of n. Of course, we already know this, by the argument given when discussing per(A).)

To establish our result, we must now show that if q is a multiple of n and n is a prime power, then the sum in (3) is non-zero. So assume that $n = p^r$, p a prime. Let $v : \mathbb{Q}^\times \to \mathbb{Z}$ denote the usual valuation with respect to p.

For λ any partition of q, divide the fillings of λ by μ into equivalence classes where two fillings are equivalent if one can be obtained from the other by rearranging the bricks within each row, and by swapping the sets of bricks filling pairs of rows of equal length.

We wish to show that the contribution to (3) from the partition $\langle q \rangle$ (all of whose fillings form a single equivalence class) has a smaller valuation than the sum of weights of the fillings in any equivalence class of fillings of any other partition. Once this is established, it follows that the sum (3) is non-zero.

Fix $\lambda = (\lambda_1, \lambda_2, \ldots) = \langle 1^{l_1} 2^{l_2} \ldots q^{l_q} \rangle$, with all the λ_i divisible by n, and fix an equivalence class $\mathcal{F}$ of fillings of λ by μ. Write k for $k(\lambda)$. Consider first a subclass of fillings $\mathcal{G}$, those which can be obtained from some fixed $F \in \mathcal{F}$ by rearranging the bricks in each row, but without interchanging rows. Let the j-th row of the filling F of λ contain r_j bricks. Let e_{ij} be the number of these bricks having length i. The number of rearrangements of this row with ending in a brick of length i is $\binom{r_j - 1}{e_{1j}, \ldots, e_{ij} - 1, \ldots, e_{nj}}$.

Thus, the total weight of all the rearrangements of this row is:

$$\begin{aligned}\sum_{i=1}^{n} \binom{r_j - 1}{e_{1j}, \ldots, e_{ij} - 1, \ldots, e_{nj}} i &= \sum_{i=1}^{n} \frac{1}{r_j} \binom{r_j}{e_{1j}, \ldots, e_{ij}, \ldots, e_{nj}} i e_{ij} \\ &= \frac{1}{r_j} \binom{r_j}{e_{1j}, \ldots, e_{nj}} \lambda_j.\end{aligned}$$

It follows that the total weight of all the fillings in $\mathcal{G}$ is:

$$\prod_{j=1}^{k} \frac{1}{r_j} \binom{r_j}{e_{1j}, \ldots, e_{nj}} \lambda_j.$$

Consider the l_i parts of λ of length i. The equivalence class $\mathcal{F}$ determines a partition $\gamma(\mathcal{F}, i)$ of l_i, where the parts of $\gamma(\mathcal{F}, i)$ are the sizes of the sets of rows of length i which are filled with an indistinguishable set of bricks. The sum of all the weights over all the fillings in $\mathcal{F}$ is:

$$\prod_{i=1}^{q} \frac{l_i!}{\gamma(F, i)!} \prod_{j=1}^{k} \frac{1}{r_j} \binom{r_j}{e_{1j}, \dots, e_{nj}} \lambda_j.$$

Writing $\delta(\mathcal{F})$ for the partition of k which is the sum of the $\gamma(\mathcal{F}, i)$ for all i, the contribution to (3) from all these fillings is:

$$\frac{(-1)^{k(\mu)-k} n^k}{\delta(\mathcal{F})!} \prod_{j=1}^{k} \frac{(r_j - 1)!}{e_{1j}! \dots e_{nj}!} \tag{4}$$

Now let us consider (4) in the case where $\lambda = \langle q \rangle$. Here, we obtain

$$\frac{(-1)^{k(\mu)-1} n!}{b_1! \dots b_n!}. \tag{5}$$

We wish to show that (4) evaluated for any other equivalence class has a greater valuation with respect to p than does (5). This is equivalent to showing that, for any $\lambda \neq \langle q \rangle$, and any equivalence class of fillings $\mathcal{F}$, that the following expression has a positive valuation:

$$\begin{aligned} &\frac{n^k}{\delta(\mathcal{F})!} \left(\prod_{j=1}^{k} \frac{(r_j - 1)!}{e_{1j}! \dots e_{nj}!} \right) \frac{b_1! \dots b_n!}{n!} \\ &= \left(\frac{1}{\delta(\mathcal{F})!} \prod_{i=1}^{n} \binom{b_i}{e_{i1}, \dots, e_{ik}} \right) \left(\frac{n^{k-1}}{(n-1) \dots (n-k+1) \binom{n-k}{r_1-1, \dots, r_k-1}} \right). \end{aligned} \tag{6}$$

We have written (6) as a product of two terms. We will show that the first term is an integer, and therefore has non-negative valuation, and that the second term has positive valuation, which will complete the proof.

For the first term, observe that if we rewrite the partition $b_i = e_{i1} + \dots + e_{ik}$ as $\langle 1^{c_{i1}} \dots n^{c_{in}} \rangle$, then $c_{i1}! \dots c_{in}!$ divides $\binom{b_i}{e_{i1}, \dots, e_{ik}}$ because

$$\frac{1}{c_{i1}! \dots c_{in}!} \binom{b_i}{e_{i1}, \dots, e_{ik}}$$

counts the number of ways of dividing b_i objects into subsets of certain sizes, where we don't distinguish the different subsets of the same size. The first term of (6) is now disposed of by remarking that

$$\delta(\mathcal{F})! | \prod_{i=1}^{n} c_{i1}! \dots c_{in}!$$

since each term in $\delta(\mathcal{F})!$ implies the existence of at least one equal term among the product of factorials on the right hand side.

For the second term, we need the following simple lemma:

Lemma *If $m < p^s$,*
(i)

$$v\left(\binom{m}{d}\right) < s,$$

(ii)

$$v\left(\binom{m}{d_1,\ldots,d_k}\right) < (k-1)s.$$

Proof:

$$v\left(\binom{m}{d}\right) = \left(\left\lfloor\frac{m}{p}\right\rfloor - \left\lfloor\frac{d}{p}\right\rfloor - \left\lfloor\frac{(m-d)}{p}\right\rfloor\right) + \cdots$$
$$+ \left(\left\lfloor\frac{m}{p^{s-1}}\right\rfloor - \left\lfloor\frac{d}{p^{s-1}}\right\rfloor - \left\lfloor\frac{(m-d)}{p^{s-1}}\right\rfloor\right) \le 1 + \cdots + 1 = s-1.$$

The second part follows immediately from repeated application of the first part, which completes the proof of the lemma. □

Now, we know that

$$v(n^{k-1}) = (k-1)r,$$
$$v\left(\binom{n-k}{r_1-1,\ldots,r_k-1}\right) \le (k-1)(r-1),$$
$$v((n-1)\ldots(n-k+1)) = v((k-1)!) = \lfloor k/p\rfloor + \cdots < \frac{k-1}{p-1} \le k-1,$$

and the desired result follows.

Acknowledgments

I would like to thank Graham Denham for a useful suggestions and Jim Propp for asking the question and for helpful comments on a previous draft.

References

1. R. Brualdi and M. Newman, “An enumeration problem for a congruence equation,” *J. Res. Nat. Bur. Standards Sect. B* **74B** (1970), 37–40.
2. Ö. Eğecioğlu and J. Remmel, “Brick tabloids and the connection matrices between bases of symmetric functions,” *Discrete Appl. Math.* **34** (1991), 107–120.
3. M. Hall, Jr., “A combinatorial problem on abelian groups,” *Proc. Amer. Math. Soc.* **3** (1952), 584–587.
4. D. Lehmer, “Some properties of circulants,” *J. Number Theory* **5** (1973), 43–54.
5. R. Stanley, *Enumerative Combinatorics*, Volume 2 Cambridge University Press, Cambridge, 1999.