

On the sums of permanents generated by certain Vandermonde matrices

By B. GYIRES (Debrecen)

Summary. It is well-known that the calculation of permanents is generally a more complicated problem than that of determinants. In this paper we deal with the following problem: Let V be the unitary Vandermonde matrix generated by the n th ($n \geq 2$) roots of unity, and let U be the Vandermonde matrix generated by the elements $1, \dots, p-1$, where p is an odd prime number. Our aim is to calculate certain sums of permanents of matrices, which are included in the Cauchy—Binet expansion of VV^* , and of $(\text{Det } U)^{p-2} U \text{adj } U^*$, respectively.

1. Introduction and the results

Let $n \geq 2$ be an integer. Let the $n \times n$ matrix $A = (a_{jk})$ with complex entries be given. Denote by A^* the conjugate transpose of A . Let M be the $n \times n$ matrix with all its entries ones. E is the unit matrix.

The permanent of A , denoted by $\text{Per } A$, is defined as follows:

$$\text{Per } A = \sum_{(i_1, \dots, i_n)} a_{1i_1} \dots a_{ni_n},$$

where $(i_1, \dots, i_n)$ runs over the full symmetric group.

Let β_j , $1 \leq j \leq n$, be non-negative integers satisfying the equality $\beta_1 + \dots + \beta_n = n$. Then $C_{\beta_1 \dots \beta_n}(A)$ denotes the $n \times n$ matrix, which contains certain columns of A , namely the j th column of A appears β_j times in $C_{\beta_1 \dots \beta_n}(A)$.

Let $1, \omega_1, \dots, \omega_{n-1}$ be the n th roots of unity different from one another. Let p be an odd prime number. Let the matrices

$$V = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_1 & \omega_2 & \dots & \omega_{n-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \omega_1^{n-1} & \omega_2^{n-1} & \dots & \omega_{n-1}^{n-1} \end{pmatrix},$$

$$U = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 3 & \dots & p-1 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & 2^{p-2} & 3^{p-2} & \dots & (p-1)^{p-2} \end{pmatrix}$$

of Vandermonde type be given, and let

$$(1.1) \quad U^{-1} = (\text{Det } U)^{p-2} \text{adj } U^*.$$

It is known that

$$(1.2) \quad VV^* = E, UU^{-1} \equiv E \pmod{p}.$$

Let $\beta_1 = k$, and let

$$A_k(n) = \sum \frac{1}{\beta_2! \dots \beta_n!} |\text{Per } C_{k\beta_2 \dots \beta_n}(V)|^2,$$

$$B_k = \sum \frac{1}{\beta_2! \dots \beta_{p-1}!} \text{Per } C_{k\beta_2 \dots \beta_{p-1}}(U) \cdot \text{Per } C_{k\beta_2 \dots \beta_{p-1}}(U^{-1*}),$$

where the summation is extended over all non-negative integers β_j , $2 \leq j \leq n$, and $2 \leq j \leq p-1$, satisfying the equalities $\beta_2 + \dots + \beta_n = n - k$, and $\beta_2 + \dots + \beta_{p-1} = p - 1 - k$, respectively.

The aim of the present paper is to prove the following two Theorems:

Theorem 1.1. For $0 \leq k \leq n$ the identity

$$(1.3) \quad A_k(n) = \frac{(-1)^{n-k} n!}{n^n (n-k)!} \sum_{j=0}^{n-k} \binom{n-k}{j} (n-j)! (-n)^j$$

holds.

Theorem 1.2. For $0 \leq k \leq p-1$ the congruence

$$(1.4) \quad B_k \equiv (-1)^{p-k} \sum_{j=0}^{p-1-k} (-1)^j (p-1)^j [j! (p-1-k-j)!]^{p-2} (p-1-j)! \pmod{p}$$

holds.

Using theorems of the papers [1] and [3] both Theorems can be generalized. For the proofs we need a Lemma.

Let

$$(1.5) \quad C = (a_{jk}), \quad D = (b_{jk})$$

be $(n+1) \times (n+1)$ upper triangular matrices with entries

$$(1.6) \quad \begin{cases} a_{j\alpha} = 0, & 0 \leq \alpha \leq j-1; \\ a_{jj+s} = \frac{1}{s!}; & 0 \leq s \leq n-j, \end{cases}$$

$$(1.7) \quad \begin{cases} b_{j\alpha} = 0, & 0 \leq \alpha \leq j-1, \\ b_{jj+s} = \frac{(-1)^s}{s!}, & 0 \leq s \leq n-j, \end{cases}$$

respectively.

Lemma 1.1. D is the inverse of C , i.e.

$$CD = E.$$

PROOF. Let $CD = (c_{jk})$. Since C and D are upper triangular matrices,

$$(1.8) \quad c_{jk} = 0, \quad 0 \leq k < j \leq n.$$

If $j \leq k$, then

$$c_{jk} = \sum_{s=0}^{k-j} a_{jj+s} b_{j+s,k} = \sum_{s=0}^{k-j} \frac{(-1)^{k-j-s}}{s!(k-j-s)!}$$

by (1.6) and (1.7). Thus

$$(1.9) \quad c_{jj} = 1, \quad 0 \leq j \leq n.$$

If $j < k$, we have

$$(1.10) \quad c_{jk} = \frac{(-1)^{k-j}}{(k-j)!} \sum_{s=0}^{k-j} (-1)^s \binom{k-j}{s} = 0$$

by the well-known combinatorial identity.

Formulas (1.8), (1.9) and (1.10) give us the statement of the Lemma.

The proofs of Theorems 1.1 and 1.2 can be found in sections 2 and 3, respectively.

2. The proof of Theorem 1.1.

For the purpose of Theorem 1.1 let $A^{(n)}(x, y)$ be the $n \times n$ matrix with entries y , except the main diagonal, in which the entries are x . It is obvious that

$$(2.1) \quad A^{(n)}(x, y) = yM + (x - y)E.$$

Using the variables $z = x - y$ and y instead of x and y the eigenvalues of the matrix (2.1) are the following:

$$\lambda_0 = z + ny, \quad \lambda_k = z, \quad 1 \leq k \leq n-1.$$

It is known that the spectral representation

$$(2.2) \quad A^{(n)}(x, y) = V \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & (0) \\ & (0) & \ddots & \\ & & & \lambda_{n-1} \end{pmatrix} V^*$$

holds. Using representation (2.1)

$$(2.3) \quad \text{Per } A^{(n)}(x, y) = \sum_{k=0}^n \binom{n}{k} k! y^k z^{n-k}.$$

Applying the Cauchy—Binet expansion formula ([2], Theorem 1.3) we obtain by (2.2) that

$$\text{Per } A^{(n)}(x, y) = \sum \frac{\lambda_0^{\beta_0} \lambda_1^{n-\beta_0}}{\beta_1! \dots \beta_n!} |\text{Per } C_{\beta_1 \beta_2 \dots \beta_n}(V)|^2,$$

where the summation is extended over all non-negative integers β_j , $1 \leq j \leq n$, satisfying the equality $\beta_1 + \dots + \beta_n = n$. It is obvious that

$$(2.4) \quad \text{Per } A^{(n)}(x, y) = \sum_{k=0}^n \frac{1}{k!} (z + ny)^k z^{n-k} A'_k(n).$$

By (2.3) and (2.4) the identity

$$\sum_{k=0}^n \binom{n}{k} k! y^k z^{n-k} = \sum_{k=0}^n \frac{A_k(n)}{k!} \sum_{v=0}^k \binom{k}{v} z^{n-k+v} n^{k-v} y^{k-v}$$

holds in y and in z . After a rearrangement this identity has the form

$$\sum_{k=0}^n n^k y^k z^{n-k} \sum_{v=k}^n \binom{v}{k} \frac{A_v(n)}{v!} = \sum_{k=0}^n \binom{n}{k} k! y^k z^{n-k}.$$

If $z=1$, we get the polynomial identity

$$\sum_{k=0}^n \left[n^k \sum_{v=k}^n \binom{v}{k} \frac{A_v(n)}{v!} \right] y^k = \sum_{k=0}^n \binom{n}{k} k! y^k.$$

Identifying the coefficients we have

$$(2.5) \quad \sum_{v=k}^n \frac{A_v(n)}{(v-k)!} = c_k, \quad 0 \leq k \leq n,$$

where

$$(2.6) \quad c_k = \frac{n! k!}{(n-k)! n^k}, \quad 0 \leq k \leq n.$$

Let v and u be the column vectors with components $A_k(n)$ and c_k , $0 \leq k \leq n$, respectively. Then (2.5) may be written in the form of a linear equation system $Cv=u$ with matrix defined by the first formula of (1.5). From Lemma 1.1 we have $v=Du$, where D is defined by the second formula of (1.5). Thus we obtain

$$(2.7) \quad A_k(n) = \sum_{j=0}^{n-k} \frac{(-1)^j}{j!} c_{k+j}, \quad 0 \leq k \leq n.$$

Substituting (2.6) into (2.7) we get that

$$A_k(n) = \frac{n!}{n^k (n-k)!} \sum_{j=0}^{n-k} \binom{n-k}{j} (k+j)! \left(-\frac{1}{n}\right)^j,$$

and after a short calculation the solution (1.3).

From the first formula of (1.2) we have

$$\sum_{k=0}^n \frac{1}{k!} A_k(n) = 1,$$

and from here we obtain subsequent consequence using (1.3).

Corollary 2.1. *The combinatorial identity*

$$\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} \sum_{j=0}^{n-k} \binom{n-k}{j} (n-j)! (-n)^j = n^n$$

holds.

In the case of $k=n-1$ we get from (1.3) that $A_{n-1}(n)=0$, i.e.

$$C_{n-1\beta_2\ldots\beta_n}(V) = 0 \quad \text{for} \quad \beta_2 + \ldots + \beta_n = 1.$$

This result can be obtained directly by

$$\sum_{j=0}^{n-1} \omega_j^k = 0, \quad 1 \leq k \leq n-1.$$

3. The proof of Theorem 1.2.

In the sequel the following elementary congruences will be applied several times. Let the prime number p be given. Then

$$(3.1) \quad \begin{aligned} (p-1)! &\equiv -1 \pmod{p}, \\ k^{p-1} &\equiv 1 \pmod{p} \quad \text{if and only if} \quad k \not\equiv 0 \pmod{p}, \\ k! &\not\equiv 0 \pmod{p} \quad \text{if and only if} \quad 1 \leq k \leq p-1. \end{aligned}$$

As in section 2 let p be an odd prime number. Since

$$(3.2) \quad \text{Det } U = \prod_{k=1}^{p-2} k! \equiv \prod_{k=2}^{p-1} (p-k)^{k-1} \not\equiv 0 \pmod{p},$$

we have

$$\begin{aligned} \text{Per } C_{\beta_1 \ldots \beta_{p-1}}(U^{-1*}) &= (\text{Det } U)^{(p-1)(p-2)} \text{Per } C_{\beta_1 \ldots \beta_{p-1}}(\text{adj } U) \equiv \\ &\equiv \text{Per } C_{\beta_1 \ldots \beta_{p-1}}(\text{adj } U) \pmod{p} \end{aligned}$$

by (3.2), and thus we get for $0 \leq k \leq p-1$ that

$$B_k \equiv \sum \frac{1}{\beta_2! \ldots \beta_{p-1}!} \text{Per } C_{k\beta_2 \ldots \beta_{p-1}}(U) \text{Per } C_{k\beta_2 \ldots \beta_{p-1}}(\text{adj } U) \pmod{p},$$

where the summation is extended over all non-negative integers β_j , $2 \leq j \leq p-1$, satisfying the equation $\beta_2 + \ldots + \beta_{p-1} = p-1-k$.

Let x and y be arbitrary integers, and let $z=x-y$. Using the polynomial

$$f(\omega) = x + y(\omega + \ldots + \omega^{p-2}) = z + y(1 + \omega + \ldots + \omega^{p-2}),$$

it is obvious that

$$f(1) = f(\omega_0) = z + (p-1)y = \lambda_0,$$

$$f(k) \equiv f(\omega_{k-1}) = z = \lambda_{k-1} \pmod{p}, \quad 2 \leq k \leq p-1.$$

If

$$B(x, y) = U \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & (0) \\ & (0) & \ddots & \\ & & & \lambda_{p-2} \end{pmatrix} U^{-1},$$

we get from Theorem 1 of the paper [1] that

$$B(x, y) \equiv A^{(p-1)}(x, y) \pmod{p},$$

where $A^{(p-1)}(x, y)$ is defined by (2.2). Thus we have

$$(3.3) \quad \text{Per } B(x, y) \equiv \text{Per } A^{(p-1)}(x, y) \pmod{p}.$$

Applying the Cauchy—Binet expansion formula ([2], Theorem 1.3) the congruence

$$\text{Per } B(x, y) \equiv \sum_{k=0}^{p-1} \frac{1}{k!} (z + (p-1)y)^k z^{p-1-k} B_k \pmod{p}$$

holds. Using (2.4) we obtain

$$(3.4) \quad \sum_{k=0}^{p-1} \frac{1}{k!} (B_k - A_k(p-1)) [z + (p-1)y]^k z^{p-1-k} \equiv 0 \pmod{p}$$

by (3.3).

Let $z=1$, and let us substitute the numbers $p, p-1, \dots, 3, 2$ into y . Then we get the homogeneous linear congruence system

$$(3.5) \quad \sum_{k=0}^{p-1} \frac{1}{k!} (B_k - A_k(p-1)) j^k \equiv 0 \pmod{p}$$

for $1 \leq j \leq p-1$ from (3.4).

We assert that the congruence

$$(3.6) \quad \frac{1}{(p-1)!} (B_{p-1} - A_{p-1}(p-1)) \equiv 0 \pmod{p}$$

holds. Namely

$$(3.7) \quad \frac{A_{p-1}(p-1)}{(p-1)!} = (p-1)!.$$

On the other hand the only solution of the linear congruence system

$$U^* \chi \equiv \begin{pmatrix} \text{Det } U \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \chi = (x_k)$$

is

$$x_j \equiv (p-1) \text{Det } U \pmod{p}$$

for $1 \leq k \leq p-1$. Thus

$$(3.8) \quad \frac{B_{p-1}}{(p-1)!} \equiv (p-1)!(p-1)^{p-1} (\text{Det } U)^{p-1} \equiv (p-1)! \pmod{p}.$$

From (3.7) and (3.8) we get our statement (3.6).

Taking (3.6) into account we get that (3.5) can be reduced to the homogeneous linear congruence system

$$\sum_{k=0}^{p-2} \frac{1}{k!} (B_k - A_k(p-1))j^k \equiv 0 \pmod{p}, \quad 1 \leq j \leq p-1,$$

with matrix U , which has only the trivial solution by (3.2). Thus, using also (3.6);

$$(3.9) \quad B_k \equiv A_k(p-1) \equiv (p-1)^{p-1} A_k(p-1) \pmod{p}$$

where for $0 \leq k \leq p-1$

$$(p-1)^{p-1} A_k(p-1) = (-1)^{p-1-k} (p-1)! \sum_{j=0}^{p-1-k} \binom{p-1-k}{j} (p-1-j)! (-p+1)^j$$

is an integer. From here we get the statement (1.4) of Theorem 1.2 by (3.9) using the elementary congruences (3.1).

Substituting $n=p-1$ into Corollary 2.1 we get the following Corollary using congruences (3.1).

Corollary 3.1. *The congruence*

$$\sum_{k=0}^{p-1} (-1)^{p-k} (k!)^{p-2} \sum_{v=0}^{p-1-k} (-1)^v (p-1)^v \cdot [v!(p-1-k-v)!]^{p-2} (p-1-v)! \equiv 1 \pmod{p}$$

holds.

Since $A_{p-2}(p-1)=0$, we have the congruence $B_{p-2} \equiv 0 \pmod{p}$ by (3.9). Moreover $B_{p-1} \equiv 1 \pmod{p}$ from (3.8).

References

- [1] B. GYIRES, On a generalization of Wilson's theorem. *Acta Arithmetica* **6** (1960), 185—191.
- [2] H. MINC, Permanents. *Addison-Wesley Publ. Co.*, 1978.
- [3] J. WELLSTEIN, Lösung der Aufgabe 89. *I. Jber. Deutsche Math. Verein.* **42** (1932), 7—9.

(Received April 10, 1985)