PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 58, July 1976

GENERALIZED VANDERMONDE DETERMINANTS AND ROOTS OF UNITY OF PRIME ORDER

R. J. EVANS AND I. M. ISAACS[1]

ABSTRACT. Easy proofs are given for two theorems of O. H. Mitchell about a type of generalized Vandermonde determinant. One of these results is then used to prove that if $|F(\varepsilon):F| = n$ where F is a field of characteristic zero and ε is a root of unity of prime order, then every set of n powers of ε forms an F-basis for $F(\varepsilon)$.

1. **Introduction and notation.** Let $\mathbf{a} = (a_1, \ldots, a_n)$ be an n-tuple of distinct nonnegative integers and let $V_{\mathbf{a}}(X_1, \ldots, X_n)$ be the polynomial obtained by computing the determinant of the matrix with (i,j) entry equal to $X_i^{a_j}$ where the X_i are indeterminates. We fix the "standard" n-tuple $\mathbf{s} = (0, 1, \ldots, n-1)$ so that

$$V_{\mathbf{s}}(X_1, \ldots, X_n) = \prod_{1 \leqslant i < j \leqslant n} (X_j - X_i)$$

is the Vandermonde determinant.

Note that $V_{\mathbf{a}}$ is divisible by $V_{\mathbf{s}}$ in the polynomial ring $\mathbf{Z}[X_1, \ldots, X_n]$. We write $P_{\mathbf{a}} = V_{\mathbf{a}}/V_{\mathbf{s}}$. Observe that $P_{\mathbf{a}}$ is a homogeneous polynomial since both $V_{\mathbf{a}}$ and $V_{\mathbf{s}}$ are.

Under the hypothesis that $0 \leqslant a_1 < a_2 < \cdots < a_n$, O. H. Mitchell [1] proved the striking result that all of the coefficients of $P_{\mathbf{a}}$ are nonnegative. (Contrast this with the fact that for $n > 1$, only half of the nonzero coefficients of $V_{\mathbf{a}}$ are positive.)

Under the same hypothesis, Mitchell proved that $P_{\mathbf{a}}$ has exactly $V_{\mathbf{s}}(a_1, a_2, \ldots, a_n)/V_{\mathbf{s}}(0, 1, \ldots, n-1)$ "terms", i.e. the sum of the coefficients of $P_{\mathbf{a}}$ is $V_{\mathbf{s}}(\mathbf{a})/V_{\mathbf{s}}(\mathbf{s})$.

In §2 of this paper we give simple new proofs of Mitchell's theorems and in §3 we use information about $V_{\mathbf{a}}$ to prove the following result.

THEOREM 1. *Let F be a field of characteristic zero and let $|F(\varepsilon):F| = n$ where ε is a pth root of unity for some prime p. Then every set of n distinct powers of ε is a basis for $F(\varepsilon)$ over F.*

2. **Mitchell's theorems.**

LEMMA 2. *Let $\mathbf{a} = (a_1, \ldots, a_n)$ with $0 = a_1 < a_2 < \cdots < a_n$ and let $\mathfrak{B}(\mathbf{a})$*

Received by the editors September 2, 1975.
AMS (MOS) subject classifications (1970). Primary 12A35, 15A15.
Key words and phrases. Vandermonde determinant, roots of unity.
[1] The second author's work was partially supported by NSF Grant GP42457X.

denote the following set of $(n-1)$*-tuples*: $\{(b_1,\ldots,b_{n-1}) | a_i \leqslant b_i < a_{i+1}\}$. *Then*

$$V_{\mathbf{a}}(1,X_2,\ldots,X_n) = \prod_{i=2}^{n}(X_i-1)\sum_{\mathbf{b}\in\mathcal{B}(\mathbf{a})} V_{\mathbf{b}}(X_2,\ldots,X_n).$$

PROOF. Since $a_1 = 0$, we have that $V_{\mathbf{a}}(1,X_2,\ldots,X_n)$ is the determinant of a matrix with all entries in the first row and column equal to 1. Subtract the first row from each of the others and expand by minors on the first column. It follows that

$$V_{\mathbf{a}}(1,X_2,\ldots,X_n) = \det(X_i^{a_j}-1)$$

where the row and column indices i and j run from 2 to n. Next, factor $X_i - 1$ from the ith row. This yields

$$V_{\mathbf{a}}(1,X_2,\ldots,X_n) = \prod_{i=2}^{n}(X_i-1)\cdot\Delta$$

where Δ is the $(n-1)\times(n-1)$ determinant with (i,j) entry equal to $\sum_{\nu=0}^{a_j-1} X_i^{\nu}$ for $2 \leqslant i,j \leqslant n$.

To compute Δ, subtract column $j-1$ from column j for $j = n, n-1, \ldots, 3$. The (i,j) entry of what results is $\sum_{\nu=a_{j-1}}^{a_j-1} X_i^{\nu}$ where i and j still run between 2 and n. Expansion by linearity on the columns now yields

$$\Delta = \sum_{\mathbf{b}\in\mathcal{B}(\mathbf{a})} V_{\mathbf{b}}(X_2,\ldots,X_n)$$

and the proof is complete. □

LEMMA 3. *Let* $\mathbf{a} = (a_1,a_2,\ldots,a_n)$ *with* $0 = a_1 < a_2 < \cdots < a_n$ *and let* $\mathcal{B}(\mathbf{a})$ *be as in Lemma* 2. *Then*

$$P_{\mathbf{a}}(1,X_2,\ldots,X_n) = \sum_{\mathbf{b}\in\mathcal{B}(\mathbf{a})} P_{\mathbf{b}}(X_2,\ldots,X_n).$$

PROOF. Since $\mathcal{B}(\mathbf{s})$ contains only the standard $(n-1)$-tuple $(0,1,\ldots,n-2)$, the result follows upon application of Lemma 2 to both the numerator and denominator of $V_{\mathbf{a}}/V_{\mathbf{s}} = P_{\mathbf{a}}$. □

THEOREM 4 (MITCHELL). *Let* $\mathbf{a} = (a_1,\ldots,a_n)$ *with* $0 \leqslant a_1 < \cdots < a_n$. *Then all of the coefficients of* $P_{\mathbf{a}}$ *are nonnegative.*

PROOF. We may factor out $(X_1X_2\cdots X_n)^{a_1}$ from $P_{\mathbf{a}}$ and it is thus no loss to assume that $a_1 = 0$. If $\mathbf{b} = (b_1,b_2,\ldots,b_{n-1}) \in \mathcal{B}(\mathbf{a})$, then $0 \leqslant b_1 < b_2 < \cdots < b_{n-1}$ and so all coefficients of $P_{\mathbf{b}}(X_2,\ldots,X_n)$ are nonnegative, by induction on n. By Lemma 3, therefore, the coefficients of $P_{\mathbf{a}}(1,X_2,\ldots,X_n)$ (viewed as a polynomial in $n-1$ indeterminates) are all nonnegative. Since $P_{\mathbf{a}}(X_1,\ldots,X_n)$ is homogeneous, the result follows. □

THEOREM 5 (MITCHELL). *Let* $\mathbf{a} = (a_1,\ldots,a_n)$. *Then the sum of the coefficients of* $P_{\mathbf{a}}$ *equals* $V_{\mathbf{s}}(a_1,\ldots,a_n)/V_{\mathbf{s}}(0,1,\ldots,n-1)$.

PROOF. We have

$$P_{\mathbf{a}}(1, X, X^2, \ldots, X^{n-1}) V_{\mathbf{s}}(1, X, X^2, \ldots, X^{n-1}) = V_{\mathbf{a}}(1, X, X^2, \ldots, X^{n-1}) = V_{\mathbf{s}}(X^{a_1}, X^{a_2}, \ldots, X^{a_n}) \tag{1}$$

where the last equality follows since the two polynomials are determinants of transposed matrices.

Now if u and v are distinct nonnegative integers, then the polynomial $(X^u - X^v)/(X - 1)$ takes on the value $u - v$ when $X = 1$. Since

$$V_{\mathbf{s}}(X^{b_1}, \ldots, X^{b_n}) = \prod_{i<j} (X^{b_j} - X^{b_i}),$$

it follows for any n-tuple of distinct nonnegative integers $(b_1, b_2, \ldots, b_n)$, that the polynomial

$$V_{\mathbf{s}}(X^{b_1}, \ldots, X^{b_n})/(X - 1)^{\binom{n}{2}}$$

takes on the value $V_{\mathbf{s}}(b_1, \ldots, b_n)$ when $X = 1$. Thus dividing both sides of (1) by

$$(X - 1)^{\binom{n}{2}}$$

and setting $X = 1$, we obtain

$$P_{\mathbf{a}}(1, \ldots, 1) = V_{\mathbf{s}}(a_1, \ldots, a_n)/V_{\mathbf{s}}(0, 1, \ldots, n - 1)$$

and the result follows. □

3. **Powers of ε.**

THEOREM 6. *Let p be a prime and let ε be a pth root of unity in some field of characteristic zero. Suppose $a_1, \ldots, a_n \in \mathbf{Z}$ are pairwise incongruent* (mod p) *and suppose the same for $b_1, \ldots, b_n \in \mathbf{Z}$. Then* $\det(\varepsilon^{a_i b_j}) \neq 0$.

PROOF. We may assume without loss that all $a_i \geqslant 0$ and we let $\mathbf{a} = (a_1, \ldots, a_n)$. We need to show that $V_{\mathbf{a}}(\varepsilon^{b_1}, \ldots, \varepsilon^{b_n}) \neq 0$. Since the ε^{b_i} are distinct, we have that $V_{\mathbf{s}}(\varepsilon^{b_1}, \ldots, \varepsilon^{b_n}) \neq 0$ and thus it suffices to show that $P_{\mathbf{a}}(\varepsilon^{b_1}, \ldots, \varepsilon^{b_n}) \neq 0$.

Now if $f \in \mathbf{Z}[X]$ with $f(\varepsilon) = 0$, then f is divisible by $X^{p-1} + \cdots + X + 1$ in $\mathbf{Z}[X]$ and thus $f(1) \equiv 0 \pmod{p}$. If $P_{\mathbf{a}}(\varepsilon^{b_1}, \ldots, \varepsilon^{b_n}) = 0$, it follows that $P_{\mathbf{a}}(1, 1, \ldots, 1) \equiv 0 \pmod{p}$ and thus by Theorem 5, $0 \equiv V_{\mathbf{s}}(a_1, \ldots, a_n) = \prod_{i<j} (a_j - a_i) \pmod{p}$. This contradicts the hypothesis on the a_i and completes the proof. □

We now prove the theorem stated in §1.

PROOF OF THEOREM 1. We may assume that $n > 1$ and thus ε is a primitive pth root of unity. Let $\varepsilon^{a_1}, \ldots, \varepsilon^{a_n}$ be distinct and assume that

$$\sum \alpha_i \varepsilon^{a_i} = 0 \quad (\alpha_i \in F). \tag{2}$$

Let $G = \mathrm{Gal}\,(F(\varepsilon)/F)$. Then ε has n distinct images $\varepsilon^{b_1}, \varepsilon^{b_2}, \ldots, \varepsilon^{b_n}$ under G. Application of the elements of G to (2) yields that $\sum_{i=1}^{n} \alpha_i \varepsilon^{a_i b_j} = 0$ for all j. Since $\det(\varepsilon^{a_i b_j}) \neq 0$ by Theorem 6, we conclude that all $\alpha_i = 0$. The result now follows. □

COROLLARY 7. *Let F have characteristic zero and let p be a prime. Suppose $f \in F[X]$ is irreducible of degree n and divides $X^p - 1$. Then all $n + 1$ coefficients of f are nonzero.*

PROOF. Otherwise, f provides a nontrivial dependence relation on n powers of ϵ, contradicting Theorem 1. □

We close with the remark that Corollary 7 does not remain true if the hypothesis that F has characteristic zero is dropped. For instance, over $GF(2)$, the polynomial $X^3 + X + 1$ is irreducible and divides $X^7 - 1$. It follows that Theorem 6 and Theorem 1 are also false for general fields.

REFERENCES

1. O. H. Mitchell, *Note on determinants of powers*, Amer. J. Math. **4** (1881), 341–344.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT SAN DIEGO, LA JOLLA, CALIFORNIA 92037

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706