PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 92, Number 1, September 1984

SHORTER NOTES

The purpose of this department is to publish very short papers of unusually elegant and polished character, for which there is no other outlet.

ON A RESULT OF S. DELSARTE

GREGORY CONSTANTINE[1] AND RAVI S. KULKARNI[2]

ABSTRACT. For an isomorphism type of a finite abelian p-group X it is shown that the matrix $(p^{\langle s(D),s(Y)\rangle})$ is nonsingular; $D, Y \in \{S | S \leqslant X$ and $S \neq X\}$, the set of all proper isomorphism type of subgroups of X. Here $s(Y)$ denotes the signature of Y. This completes the proof of a result of S. Delsarte which gives *explicit* formulas for the number of automorphisms of X, the number of subgroups of X isomorphic to Y (and the number of homomorphisms from Y into X) in terms of signatures.

1. Preliminaries. In [**1**], S. Delsarte generalizes the classical Möbius function in number theory and uses it to establish *explicit* formulas for the number of automorphisms of a (finite) abelian group x, and the number of subgroups of x of a given isomorphism type. These formulas are given in terms of signatures of the groups.

Since a finite abelian group decomposes canonically into its p-primary parts it suffices to prove the result for abelian p-groups only. Establishing the nonsingularity of a certain coefficient matrix $(p^{\langle s(D),s(Y)\rangle})$ is a crucial step in Delsarte's proof [**1**, p. 607]. A reference is given in [**1**] to account for the claim on nonsingularity; we have, however, not been successful in completing the proof based on this reference. The purpose of this note is to prove that the aforementioned coefficient matrix $(p^{\langle s(D),s(Y)\rangle})$ is indeed nonsingular (positive definite, in fact).

Let x be a (finite) abelian p-group. By X we denote the isomorphism type of x. Also, $y \leqslant x$ means y is a subgroup of x and $Y \leqslant X$ means that X admits a subgroup of isomorphism type Y.

Assume $x \cong Z_p m_1 \oplus \cdots \oplus Z_p m_k$; $m_i \geqslant 1$. Let $x_1 = \{g \in x$: order of g divides $p\}$. Then $x_1 \leqslant x$. Let $|x_1| = p^{r_1}$ ($r_1 = k$, in fact). Repeat this process in x/x_1, i.e., look at $(x/x_1)_1$ and denote its order by p^{r_2}. Continuing this process we associate a sequence of nonnegative integers (ending in 0's) $(r_1, r_2, r_3, \ldots, 0, 0, \ldots)$ which satisfies $r_1 \geqslant r_2 \geqslant r_3 \geqslant \cdots$ and which we call the *signature* of x. Observe that, in fact, $r_n = |\{i: m_i \geqslant n\}|$. Conversely, a given signature $r_1 \geqslant r_2 \geqslant r_3 \geqslant \cdots$ determines uniquely the isomorphism type of an abelian p-group as $(Z_p)^{r_1 - r_2} \oplus (Z_p^2)^{r_2 - r_3} \oplus \cdots \oplus (Z_p^l)^{r_l - 0}$, where $r_n = 0$ for $n \geqslant l+1$. ($(Z_p^2)^{r_2 - r_3}$ means $Z_p^2 \oplus \cdots \oplus Z_p^2$, a direct sum of $r_2 - r_3$ factors.) Denote by $s(X)$ the signature of X. (For example, if

Received by the editors July 29, 1983.

1980 *Mathematics Subject Classification*. Primary 05A15; Secondary 20B25.

Key words and phrases. Signature of a finite abelian p-group, Möbius inversion, generating function.

[1] This research has been supported by a summer research fellowship grant from Indiana University (1983).

[2] Supported by an NSF grant MCS 83-01614.

$X = Z_p \oplus Z_p^2 \oplus Z_p^2 \oplus Z_p^3$, then $s(X) = (4,3,1,0,\ldots)$; conversely, $(4,3,1,0,\ldots)$ leads uniquely to $(Z_p)^{4-3} \oplus (Z_p^2)^{3-1} \oplus (Z_p^3)^{1-0} = Z_p \oplus Z_p^2 \oplus Z_p^2 \oplus Z_p^3 = X$.)

Let $D \leqslant X$. Assume $s(X) = (r_1,\ldots,r_k,0\ldots)$ and $s(D) = (i_1,\ldots,i_k,0\ldots)$; then $i_1 \leqslant r_1,\ldots,i_k \leqslant r_k$. In fact, for *any* sequence of nonincreasing nonnegative integers ending in zeros $(i_1,\ldots,i_k,0\ldots)$ and satisfying $i_1 \leqslant r_1,\ldots,i_k \leqslant r_k,\ldots$ there exists a subgroup $D \leqslant X$ with signature $(i_1,\ldots,i_k,0\ldots)$.

For a direct sum $X \oplus Y$ we have $s(X \oplus Y) = s(X) + s(Y)$ with usual (componentwise) addition of sequences. We shall also denote by $\langle s(X), s(Y)\rangle$ the usual inner product of two sequences, i.e., if $s(X) = (r_1, r_2,\ldots)$ and $s(Y) = (s_1, s_2,\ldots)$ then $\langle s(X), s(Y)\rangle = \sum_{i=1}^{\infty} r_i s_i$.

We can now state Delsarte's result.

THEOREM (S. DELSARTE). *For finite abelian p-groups x and y with signatures* $s(x) = (r_1,\ldots,r_k,0\ldots)$ *and* $s(y) = (s_1,\ldots,s_l,0\ldots)$ *satisfying* $r_1 \leqslant s_1,\ldots,r_k \leqslant s_k$ *we have*

(i) *the number of automorphisms of x equals* $F_x(p^{r_1},\ldots,p^{r_k})$,

(ii) *the number of subgroups of y isomorphic to x equals*

$$F_x(p^{s_1},\ldots,p^{s_k})/F_x(p^{r_1},\ldots,p^{r_k})$$

where

$$F_x(z_1,\ldots,z_k) = z_1^{r_2} z_2^{r_3} \cdots z_{k-1}^{r_k}\left[\prod_{i_1=r_2}^{r_1-1}\left(z_1 - p^{i_1}\right)\right] \times\left[\prod_{i_2=r_3}^{r_2-1}\left(z_2 - p^{i_2}\right)\right]\cdots\left[\prod_{i_k=0}^{r_k-1}\left(z_k - p^{i_k}\right)\right],$$

(iii) *the number of homomorphisms from x into y equals* $(p^{\langle s(x),s(y)\rangle})$.

The proof is contained in [1], the original work of S. Delsarte. It can also be found in [3], rewritten in the more contemporary notation on Möbius inversion.

For a complete proof it is necessary to establish the following Lemma. Let X be (an isomorphism type of) a finite abelian p-group. Let $\mathscr{S} = \{S\colon S \leqslant X \text{ and } S \neq X\}$. Order $\mathscr{S}$ in some way. Let C be the symmetric matrix $(p^{\langle s(D),s(Y)\rangle})$, where D and Y run over $\mathscr{S}$; the numbering of rows and columns in C comes from the order of $\mathscr{S}$.

LEMMA. *C is nonsingular.*

2. Proof of the Lemma. Let the signature of X be $(r_1, r_2,\ldots,r_k,0\ldots)$. The rows and columns of C are labeled by the (isomorphism types of) proper subgroups of X; think, instead, of its rows and columns being labeled by the corresponding signature sequences. A *block* of C is a set of signatures $(s, s_2,\ldots,s_k,0\ldots)$ with $s_2,\ldots,s_k$ fixed and s varying, $s_2 \leqslant s \leqslant r_1$. The block $(s, s_2,\ldots,s_k,0\ldots)$ is said to be larger or of the same magnitude as the block $(l, l_2,\ldots,l_k,0\ldots)$ if $l_2 \geqslant s_2$. Arrange the rows and columns of C by blocks in their order of magnitude (larger to smaller—blocks of the same magnitude can be arranged among themselves in any order).

Now write $C = (C_{ij})$ as a partitioned matrix with $C_{ij} = (p^{\langle s(D),s(Y)\rangle})$, with $s(D)$ running through block i and $s(Y)$ running through block j.

Let block 1 be $(s, s_2, \ldots, s_k, 0\ldots)$, $s_2 \leqslant s \leqslant r_1$, and let block 2 be $(l, l_2, \ldots, l_k, 0\ldots)$, $l_2 \leqslant l \leqslant r_1$ (with $l_2 \geqslant s_2$). The signatures in blocks 1 and 2 (written as columns and truncated at the kth entry for simplicity) are, respectively,

$$\begin{pmatrix} s_2 & s_2+1 & s_2+2 & \cdots & r_1 \\ s_2 & s_2 & s_2 & \cdots & s_2 \\ s_3 & s_3 & s_3 & \cdots & s_3 \\ s_4 & s_4 & s_4 & \cdots & s_4 \\ \vdots & \vdots & \vdots & \cdots & \vdots \end{pmatrix} \text{ and } \begin{pmatrix} l_2 & l_2+1 & l_2+2 & \cdots & r_1 \\ l_2 & l_2 & l_2 & \cdots & l_2 \\ l_3 & l_3 & l_3 & \cdots & l_3 \\ l_4 & l_4 & l_4 & \cdots & l_4 \\ \vdots & \vdots & \vdots & \cdots & \vdots \end{pmatrix}.$$

Let $\alpha = \sum_{i=2}^{r_1} s_i^2$, $\gamma = \sum_{i=2}^{r_1} l_i^2$ and $\beta = \sum_{i=2}^{r_1} s_i l_i$.

Note that $C_{mn} = V_{nn} D_{mn}$, $1 \leqslant m, n \leqslant 2$, where V_{11} (resp. V_{22}) is a square matrix with $r_1 - s_2 + 1$ (resp. $r_1 - l_2 + 1$) rows and (i, j)th entry $p^{(i-1)(s_2+j-1)}$ (resp. $p^{(i-1)(l_2+j-1)}$), and

$$D_{11} = p^{\alpha}\operatorname{diag}\big(p^{s_2(s_2+i-1)}\big)_{1 \leqslant i \leqslant r_1 - s_2 + 1};$$
$$D_{12} = p^{\beta}\operatorname{diag}\big(p^{s_2(l_2+i-1)}\big)_{1 \leqslant i \leqslant r_1 - l_2 + 1};$$
$$D_{21} = p^{\beta}\operatorname{diag}\big(p^{l_2(s_2+i-1)}\big)_{1 \leqslant i \leqslant r_1 - s_2 + 1};$$
$$D_{22} = p^{\gamma}\operatorname{diag}\big(p^{l_2(l_2+i-1)}\big)_{1 \leqslant i \leqslant r_1 - l_2 + 1}.$$

The significance of this rearrangement is that V_{11} and V_{22} are Vandermonde matrices and hence nonsingular. Since $l_2 \geqslant s_2$ each column of C_{12} appears also as a column of C_{11}. Multiplying the $(l + i)$th column of C_{11} by $p^{\beta - \alpha}$ and subtracting it from the ith column of C_{12} we reduce C_{12} to the zero matrix $(1 \leqslant i \leqslant r_1 - l_2 + 1)$. This process changes C_{22} into

$$\big(p^{\gamma} - p^{2\beta - \alpha}\big)C_{22} = p^{-\alpha}\big(p^{\gamma + \alpha} - p^{2\beta}\big)C_{22} \quad \big(= \tilde{C}_{22}, \text{ say}\big).$$

We thus reduce by column operations the matrix

$$\begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}$$

to

$$\begin{bmatrix} C_{11} & 0 \\ C_{21} & \tilde{C}_{22} \end{bmatrix}.$$

Note that $p^{\gamma+\alpha} - p^{2\beta} > 0$, since $\gamma + \alpha - 2\beta = \sum_{i=2}^{r_1}(l_i - s_i)^2 > 0$; $\gamma + \alpha - 2\beta$ is strictly positive since the two blocks in question are not identical, i.e., $l_i \neq s_i$ for some i, $2 \leqslant i \leqslant r_1$. This shows that $\tilde{C}_{22}$ is also nonsingular.

We now repeat the process to make all $C_{ij} = 0$, for $i < j$. C will be reduced to a lower block-triangular matrix with nonsingular diagonal blocks of Vandermonde type. This proves the nonsingularity of C and completes the proof of S. Delsarte's result.

REMARK. C is, in fact, positive definite. One way to see this is to recall a result of I. Schur [2]. It states that if $A = (a_{ij})$ and $B = (b_{ij})$ are positive semidefinite then

$A \circ B = (a_{ij} b_{ij})$ (componentwise multiplication) is again positive semidefinite. Clearly, the matrix $A = (\langle s(D), s(Y) \rangle)$ is positive semidefinite (it is an inner product matrix). Then $(lnp)^n A^n / n!$ is positive semidefinite by Schur's result. ($A^n = A \circ \cdots \circ A$, n times). So then is our matrix

$$C = \sum_{n=0}^{\infty} \frac{1}{n!} (lnp)^n A^n$$

as a sum of positive semidefinite matrices. Starting with a positive semidefinite matrix, one is, in general, led only to a positive semidefinite matrix by this process. We just established the nonsingularity of C, however, and can now conclude that C is positive definite.

REFERENCES

1. S. Delsarte, *Fonctions de Möbius sur les groupes abeliens finis*, Ann. of Math. (2) 3 (1948), 600–609.

2. I. Schur, *Bemerkungen zur Theorie der beschränkten Bilinearformen suit unendlich vielen Veränderlichen*, J. Reine Angew. Math. **140** (1911), 1–28.

3. G. Constantine, *Topics in combinatorics*, Unpublished Manuscript, Indiana University, 1982.

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47405