1979

Ordered partitions and codes generated by circulant matrices

R Razen

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

K Wehrhahn

Ordered partitions and codes generated by circulant matrices

Abstract

We consider the set of ordered partitions of n into m parts acted upon by the cyclic permutation (I2 ... m). The resulting family of orbits P(n, m) is shown to have cardinality p(n, m) = (l/n) ∑d│m φ(d) (::.'!~) where φ is Euler's φ-function. P(n, m) is shown to be set-isomorphic to the family of orbits ℓ(n, m) of the set of all m-subsets of an n-set acted upon by the cyclic permutation (12 ... n). This isomorphism yields an efficient method for determining the complete weight enumerator of any code generated by a circulant matrix.

Disciplines

Physical Sciences and Mathematics

Publication Details

Razen, R, Seberry, J and Wehrhahn, K, Ordered partitions and codes generated by circulant matrices, Journal of Combinatorial Theory, Ser. A, 27(3), 1979, 333-341.

Reprinted from JOURNAL OF COMBINATORIAL THEORY, Series A
All Rights Reserved by Academic Press, New York and London

Vol. 27, No. 3, November 1979
Printed in Belgium

Ordered Partitions and Codes Generated by Circulant Matrices

R. RAZEN

Institut für Mathematik, Montanuniversität, Leoben, Austria

JENNIFER SEBERRY

Department of Applied Mathematics, University of Sydney, Sydney N.S.W. 2006, Australia

AND

K. WEHRHAHN

Department of Pure Mathematics, University of Sydney, Sydney N.S.W. 2006, Australia

Communicated by Marshall Hall, Jr.

Received February 23, 1978

We consider the set of ordered partitions of n into m parts acted upon by the cyclic permutation $(12...m)$. The resulting family of orbits $\bar{\mathscr{P}}(n, m)$ is shown to have cardinality $\bar{p}(n, m) = (1/n) \sum_{d|m} \phi(d) \binom{n/d}{m/d}$, where ϕ is Euler's ϕ-function. $\bar{\mathscr{P}}(n, m)$ is shown to be set-isomorphic to the family of orbits $\bar{\mathscr{C}}(n, m)$ of the set of all m-subsets of an n-set acted upon by the cyclic permutation $(12...n)$. This isomorphism yields an efficient method for determining the complete weight enumerator of any code generated by a circulant matrix.

1. INTRODUCTION

An ordered partition (or composition, cf. [2] or m-composition, cf. [1]) of n into m parts is an ordered m-tuple $\alpha = (k_1, k_2, ..., k_m)$, where the k_i are positive integers and $k_1 + k_2 + \cdots + k_m = n$. In this paper we consider the set $\mathscr{P}(n, m)$ of all ordered partitions of n into m parts acted upon by the cyclic permutation

$$\theta = (12 \cdots m).$$

The action of group G generated by θ is defined by

$$\theta\alpha = (k_{1\theta}, k_{2\theta}, ..., k_{m\theta})$$

0097-3165/79/060333-09$02.00/0

and we write $\bar{\mathscr{P}}(n, m)$ for the set of orbits of G under this action. The cardinalities of $\mathscr{P}(n, m)$ and $\bar{\mathscr{P}}(n, m)$ will be denoted by $p(n, m)$ and $\bar{p}(n, m)$, respectively. Writing $\bar{p}_d(n, m)$ for the number of orbits in $\bar{\mathscr{P}}(n, m)$ having exactly d-elements, we derive in Section 3 the identities

$$\bar{p}_m(n, m) = \frac{1}{n} \sum_{d|m} \mu(d) \binom{n/d}{m/d} \tag{1.1}$$

and

$$\bar{p}(n, m) = \frac{1}{n} \sum_{d|m} \phi(d) \binom{n/d}{m/d}, \tag{1.2}$$

where μ is the Möbius function, ϕ is Euler's ϕ-function, and $\binom{n/d}{m/d}$ is defined to be zero unless d is a divisor of both n and m.

The initial reason for our interest in the set $\bar{\mathscr{P}}(n, m)$ is due to the fundamental relationship between $\bar{\mathscr{P}}(n, m)$ and the set of all m-subsets of a given n-set. Write S for the set of integers $\{1, 2,..., n\}$ and $\mathscr{C}(n, m)$ for the set of all m-subsets of S. Let H be the cyclic group generated by the permutation

$$\psi = (12 \cdots n).$$

For $I = \{\alpha_1, \alpha_2, ..., \alpha_m\}$, any element of $\mathscr{C}(n, m)$, we define the action of H on $\mathscr{C}(n, m)$ by

$$\psi I = \{\alpha_1\psi, \alpha_2\psi, ..., \alpha_m\psi\}, \tag{1.3}$$

i.e.,

$$\alpha_i\psi = \alpha_i + 1 \qquad (\text{modulo } n).$$

The set $\bar{\mathscr{C}}(n, m)$ of orbits of H is shown in Section 2 to be set-isomorphic to $\bar{\mathscr{P}}(n, m)$, and the properties of the isomorphism are studied in some detail.

The isomorphism between $\bar{\mathscr{C}}(n, m)$ and $\bar{\mathscr{P}}(n, m)$ yields an efficient method for determining the complete weight enumerator of any code generated by the row vectors of a circulant matrix or a matrix of the form $[IW]$, where I is the $n \times n$ identity matrix and W is an $n \times n$ circulant matrix. This application is discussed in Section 4.

2. The Relationship between Ordered Partitions and m-Sets

The purpose of this section is to establish the fundamental relationship between the two sets $\bar{\mathscr{P}}(n, m)$ and $\bar{\mathscr{C}}(n, m)$. We will denote the cardinalities of $\mathscr{C}(n, m)$ and $\bar{\mathscr{C}}(n, m)$ by $c(n, m)$ and $\bar{c}(n, m)$, respectively. The number of orbits in $\bar{\mathscr{C}}(n, m)$ with d elements will be denoted by $\bar{c}_d(n, m)$.

Each m-subset of S has a natural ordering. Let $l = \{\alpha_1, \alpha_2, ..., \alpha_m\}$, where $\alpha_1 < \alpha_2 < \cdots < \alpha_m$. Associated with l we have the ordered partition of n into m parts

$$\alpha(l) = (d_1, d_2, ..., d_m) \tag{2.1}$$

defined by

$$\begin{aligned} d_i &= \alpha_{i+1} - \alpha_i \qquad \text{for} \quad i = 1, ..., m-1, \\ d_m &= n - \alpha_m + \alpha_1 . \end{aligned}$$

Also, with each ordered partition $\alpha = (k_1, k_2, ..., k_m)$ we associate the m-set

$$l(\alpha) = \{1, 1 + k_1, ..., 1 + k_1 + k_2 + \cdots + k_{m-1}\}. \tag{2.2}$$

We prove next that (2.1) and (2.2) yield a bijection between the sets $\mathscr{P}(n, m)$ and $\mathscr{C}(n, m)$.

LEMMA 2.1. *The ordered partitions associated with a class in $\mathscr{C}(n, m)$ are contained in a class in $\mathscr{P}(n, m)$.*

Proof. Let $l = \{\alpha_1, \alpha_2, ..., \alpha_m\}$, where $\alpha_1 < \alpha_2 < \cdots < \alpha_m \leqslant n$, and let $\alpha(l) = (d_1, d_2, ..., d_m)$ be defined by (2.1). Then

$$\psi^k l = \{\alpha_1 + k, \alpha_2 + k, ..., \alpha_m + k\},$$

where the elements are reduced modulo n. In natural order

$$\psi^k l = \{\alpha_t + k, \alpha_{t+1} + k, ..., \alpha_m + k, \alpha_1 + k, ..., \alpha_{t-1} + k\},$$

for some integer t. Hence the ordered partition associated with $\psi^k l$ is

$$\alpha(\psi^k l) = (d_t, ..., d_{m-1}, \alpha_1 - \alpha_m, d_1, ..., d_{t-2}, n - \alpha_{t-1} - k + \alpha_t + k).$$

But

$$\alpha_1 - \alpha_m \equiv d_m \qquad (\text{mod } n)$$

and

$$n - \alpha_{t-1} - k + \alpha_t + k \equiv d_{t-1} \qquad (\text{mod } n),$$

and so

$$\alpha(\psi^k l) = \theta^{t-1}\alpha(l), \tag{2.3}$$

which proves the assertion of the lemma.

LEMMA 2.2. *The m-sets associated with a class in $\mathscr{P}(n, m)$ are contained in a class in $\mathscr{C}(n, m)$. In particular*

$$l(\theta^i \alpha) = \psi^{b_i} l(\alpha) \tag{2.4}$$

for $i = 0, 1, \ldots, m-1$, *where* $b_i = k_{i+1} + k_{i+2} + \cdots + k_m$.

Proof. By definition

$$\psi^{b_i} l(\alpha) = \{1 + b_i, 1 + b_i + k_1, \ldots, 1 + b_i + k_1 + \cdots + k_{m-1}\}.$$

Since

$$1 + b_i + k_1 + \cdots + k_i \equiv 1 \pmod{n}$$

we have in natural order

$$\begin{aligned}\psi^{b_i} l(\alpha) &= \{1, 1 + k_{i+1}, \ldots, 1 + k_{i+1} + \cdots + k_{m-1}, 1 + k_{i+1} + \cdots + k_m, \\ &\quad 1 + k_{i+1} + \cdots + k_m + k_1, \ldots, 1 + k_{i+1} + \cdots + k_m + k_1 + \cdots \\ &\quad + k_{i+1}\} \\ &= l(\theta^i \alpha).\end{aligned}$$

THEOREM 2.1. *Define* $f\colon \mathscr{P}(n, m) \to \mathscr{C}(n, m)$ *by*

$$f[\alpha] = [l(\alpha)] \tag{2.5}$$

and define

$$g\colon \mathscr{C}(n, m) \to \mathscr{P}(n, m)$$

by

$$g[\alpha] = [\alpha(l)], \tag{2.6}$$

where the representative l contains 1.

Then f and g are well defined and $f \circ g = 1$, $g \circ f = 1$.

Proof. f is well defined by Lemma 2.2 and g is well defined by Lemma 2.1; hence it suffices to prove that f and g are mutual inverses.

Let $l = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and write $[l]$ for the corresponding class in $\mathscr{C}(n, m)$. Then for $\alpha(l) = (d_1, d_2, \ldots, d_m)$ defined by (2.1) we have that

$$l(\alpha(l)) = \psi^{1-\alpha_1} l;$$

hence $[l(\alpha(l))] = [l]$ and so $f \circ g = 1$.

On the other hand, let $\alpha = (k_1, k_2, \ldots, k_m)$. Then by (2.2)

$$l(\alpha) = \{1, 1 + k_1, \ldots, 1 + k_1 + \cdots + k_{m-1}\}$$

and by (2.1)

$$\alpha(l(\alpha)) = (d_1, d_2, \ldots, d_m),$$

where

$$d_1 = 1 + k_1 - 1 = k_1, \quad d_2 = 1 + k_1 + k_2 - 1 - k_1 = k_2, \ldots, d_{m-1} = k_{m-1}$$

and

$$d_m = n - (1 + k_1 + \cdots + k_{m-1}) + 1 = k_m.$$

Hence

$$\alpha(l(\alpha)) = \alpha,$$

and so $[\alpha(l(\alpha))] = [\alpha]$, which proves that $g \circ f = 1$. This completes the proof of the theorem.

An immediate consequence of Theorem 2.1 is

$$\bar{p}(n, m) = \bar{c}(n, m). \tag{2.7}$$

The next theorem shows that the bijection f preserves, in a sense, the class size.

THEOREM 2.2. *Let f be the mapping defined by Eq.* (2.5) *and suppose k is a divisor of m. If $[\alpha] \in \bar{\mathscr{P}}(n, m)$ is a class containing m/k elements then the class $f[\alpha]$ contains n/k elements.*

Proof. Suppose $[\alpha]$ contains m/k elements. Then

$$\alpha = (k_1, \ldots, k_d, k_1, \ldots, k_d, \ldots, k_1, \ldots, k_d),$$

where $d = m/k$ and each d-tuple $(k_1, \ldots, k_d)$ is an ordered partition of n/k into m/k parts whose class in $\bar{\mathscr{P}}(n/k, m/k)$ contains exactly m/k elements. Write $h = n/k$. Then

$$l(\alpha) = \{1, 1 + k_1, \ldots, 1 + k_1 + \cdots + k_{d-1}, 1 + h, 1 + h + k_1, \ldots, \\ 1 + (k-1)h + k_1 + \cdots + k_{d-1}\}.$$

Hence $\psi^h l(\alpha) = l(\alpha)$, from which it follows that

$$f[\alpha] = [l(\alpha)] \text{ contains } h = n/k \text{ distinct elements.}$$

COROLLARY. *The following identity holds for $k \mid (m, n)$,*

$$\bar{c}_{n/k}(n, m) = \bar{p}_{m/k}(n, m).$$

To each m-subset l of S there corresponds the $(n - m)$-subset $S - l$. This correspondence defines a natural bijection between $\mathscr{C}(n, m)$ and $\mathscr{C}(n, n - m)$. Moreover since

$$S - \psi l = \psi S - \psi l = \psi(S - l)$$

the mapping

$$t: \mathscr{C}(n, m) \to \mathscr{C}(n, n - m), \tag{2.8}$$

defined by

$$t[l] = [S - l],$$

is well defined and is a bijection.

Incorporating the results of Theorem 2.1 we have the commutative diagram

$$\begin{array}{ccc} \mathscr{C}(n, m) & \xrightarrow{t} & \mathscr{C}(n, n - m) \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle g} \\ \mathscr{P}(n, m) & \xrightarrow[g \circ t \circ f]{} & \mathscr{P}(n, n - m) \end{array} \tag{2.9}$$

where $g \circ t \circ f$: $[\alpha] \to [\alpha(S - l(\alpha))]$.

Since f, t, and g are bijections we can conclude that $g \circ t \circ f$ is also. Suppose next that $[l]$ is a class in $\mathscr{C}(n, m)$ with n/k elements; then if $h = n/k$ we have

$$\psi^h l = l$$

and consequently

$$S - l = S - \psi^h l = \psi^h(S - l).$$

This shows that classes with n/k elements in $\mathscr{C}(n, m)$ are in one-one correspondence with classes having n/k elements in $\mathscr{C}(n, n - m)$.

Hence we have the following theorem.

THEOREM 2.3. *The mapping $g \circ t \circ f$ defined in* (2.9) *is a bijection between $\mathscr{P}(n, m)$ and $\mathscr{P}(n, n - m)$ which maps classes containing m/k elements to classes containing $(n - m)/k$ elements.*

COROLLARY. (1) $\bar{c}(n, m) = \bar{c}(n, n - m)$,

(2) $\bar{p}(n, m) = \bar{p}(n, n - m)$,

(3) $\bar{p}_{m/k}(n, m) = \bar{p}_{(n-m)/k}(n, n - m)$.

3. The Cardinality of $\mathscr{P}(n, m)$

In this section we derive (1.1) and (1.2). Since $p(n, m)$ can be interpreted as the number of ways of inserting $m - 1$ commas into $n - 1$ places [2] we have

$$p(n, m) = \binom{n-1}{m-1} = \frac{m}{n}\binom{n}{m}. \tag{3.1}$$

Also, the cardinality of each orbit is a divisor of m. Hence we immediately have the equations

$$\frac{m}{n}\binom{n}{m} = p(n, m) = \sum_{d \mid m} d\bar{p}_d(n, m) \tag{3.2}$$

and

$$\bar{p}(n, m) = \sum_{d \mid m} \bar{p}_d(n, m). \tag{3.3}$$

Perhaps the most elegant way to obtain (1.1) is to observe that $p((n/m)k, k)$ is defined for all positive integers k, if we let $p((n/m)k, k) = 0$ whenever $(n/m)k$ is not an integer; i.e., we define $\binom{nk/m}{k} = 0$ if nk/m is not an integer. Moreover, $\bar{p}_d(n, m)$ is defined for all positive integers d, being equal to 0 whenever d is not a divisor of (n, m), the greatest common divisor of n and m. With these observations, we may invert (3.2) to obtain

$$m\bar{p}_m(n, m) = \sum_{d \mid m} \mu(d)\, p\left(\frac{n}{m} \cdot \frac{m}{d}, \frac{m}{d}\right). \tag{3.4}$$

Equation (1.1) is a trivial consequence of (3.1) and (3.4).

To obtain (1.2) we recall that G, the cyclic group of order m, acts on the set $\mathscr{P}(n, m)$ of all ordered partitions of n into m parts. Let $\lambda(g)$ denote the number of elements of $\mathscr{P}(n, m)$ fixed by the permutation $g \in G$. If $g = e$, the identity element, then

$$\lambda(g) = \binom{n-1}{m-1}$$

since e fixes every ordered partition. If g consists of d-cycles then g fixes only those ordered partitions which are repeated copies of ordered partitions of n/d into m/d parts. For example, (1, 3, 2, 1, 3, 2, 1, 3, 2) is fixed by (147)(258)(369) $= (123456789)^3$. But the number of permutations of G consisting of d-cycles is $\phi(d)$. Hence by Burnside's lemma

$$\bar{p}(n, m) = \frac{1}{m}\sum_{d \mid m} \phi(d)\binom{n/d - 1}{m/d - 1} = \frac{1}{n}\sum_{d \mid m} \phi(d)\binom{n/d}{m/d}.$$

As an example suppose that $n = 24$ and $m = 4$. Then

$$\bar{p}(24, 4) = \frac{1}{24}\left[\phi(1)\binom{24}{4} + \phi(2)\binom{12}{2} + \phi(4)\binom{6}{1}\right]$$
$$= \frac{1}{24}\left[\binom{24}{4} + \binom{12}{2} + 2\binom{6}{1}\right] = 446.$$

The following corollaries may serve as further illustrations.[1]

COROLLARY 1. *If n and m are relatively prime then*

$$\bar{p}(n, m) = \bar{p}_m(n, m) = \frac{1}{n}\binom{n}{m}.$$

COROLLARY 2. *If $(n, m) = q$ is a prime then*

$$\bar{p}(n, m) = \frac{1}{n}\binom{n}{m} + \frac{q-1}{n}\binom{n/q}{m/q}.$$

COROLLARY 3.

$$\begin{aligned}
\bar{p}(n, 3) &= \frac{1}{n}\binom{n}{3} && \text{if } (n, 3) = 1\\
&= \frac{1}{n}\binom{n}{3} + \frac{2}{3} && \text{if } (n, 3) = 3,\\
\bar{p}(n, 4) &= \frac{1}{n}\binom{n}{4} && \text{if } (n, 4) = 1\\
&= \frac{1}{n}\binom{n}{4} + \frac{n}{8} - \frac{1}{4} && \text{if } (n, 4) = 2\\
&= \frac{1}{n}\binom{n}{4} + \frac{n}{8} + \frac{1}{4} && \text{if } (n, 4) = 4.
\end{aligned}$$

4. AN APPLICATION

Let $\mathscr{C}$ be a linear code generated by the row vectors of a matrix $[IW]$, where I is $n \times n$ identity matrix and W is an $n \times n$ circulant matrix with entries in a finite field $GF(q)$. Such codes have the property that they have the same weight enumerators as their duals [4] and hence share many of the

[1] *Added in proof.* The total number of ordered partition classes of n is $\bar{p}(n) = \sum_{m=1}^{n} \bar{p}(n, m) = (1/n) \sum_{d/n} \phi(d) 2^{n/d} - 1$. We are grateful to Professor G. Baron of the Technical University, Vienna, for this observation.

properties of self-dual codes. The design properties of linear codes and their subcodes of constant weight are closely related to their weight enumerators [3]. In general the problem of determining the weight enumerator (WE) of a code, or better still the complete weight enumerator (CWE), involves the determination of the WE or CWE of each of the q^n codewords. If W is circulant and W_i denotes the ith row of W then the linear combination

$$W_{i_1} + W_{i_2} + \cdots + W_{i_m}$$

has the same CWE as

$$W_{i_1+k} + W_{i_2+k} + \cdots + W_{i_m+k}$$

for any integer k, where the subscripts are reduced modulo n. Hence the codewords of $\mathscr{C}$ can be grouped into classes in which elements are "linear shifts" of one another. For given m the family of classes is in obvious correspondence with $\mathscr{C}(n, m)$. Hence the problem of determining the CWE of $\mathscr{C}$ reduces to two problems:

(1) Finding a complete system of coset representatives of $\mathscr{C}(n, m)$ for $m = 1, \ldots, n$.

(2) Determining the CWEs of the linear combinations corresponding to the coset representatives.

The problem of finding a complete system of coset representatives is very easy for $\bar{\mathscr{P}}(n, m)$, where such a system occurs in lexicographical order among the set of all ordered partitions of n into m parts with the first entry at most the integer part of n/m. An ordered partition in this class is a suitable representative provided that it is lexicographically less than any ordered partition in its orbit. An efficient computer algorithm exists to determine the complete system of representatives for $\bar{\mathscr{P}}(n, m)$.

We may note that in the case of binary codes Theorem 2.3 allows us to reduce the calculation time by a further factor of 2.

References

1. M. Abramson, Restricted combinations and compositions, *Fibonacci Quart.* (1976), 439–452.
2. G. E. Andrews, "The Theory of Partitions," Addison–Wesley, Reading, Mass., 1976.
3. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Phillips Res. Repts. Suppl.* **10** (1973).
4. J. Seberry and K. Wehrhahn, A class of codes generated by circulant weighing matrices, *in* "Combinatorics: Proceedings of the International Conference, Canberra, August, 1977," Australian Academy of Science; and Lecture Notes in Mathematics, Vol. 686, Springer-Verlag, Berlin/Heidelberg/New York 686, pp. 282–289, 1978.

Printed by the St. Catherine Press Ltd., Tempelhof 37, Bruges, Belgium