

CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in January 2008.

Please copy this book for your own reading only. Refers others to this website. Thank You.

CHAPTER 11.

Formula for Determinantal Coefficients of Circulant Matrices.

There is a closed formula for the circulant determinantal coefficients which will be derived and proved in this chapter. We offer first a proof by Oystein Ore, and then a new proof of our own. Our proof is rather lengthy, but has some advantages over Ore's derivation as will be discussed.

The determinant of $\mathbf{circ}_n(a)$ can be expanded as a homogenous expression of degree n in the variables a_0, a_1, \dots, a_{n-1} . Thus, we define the circulant determinantal coefficient to be $c_n(v_0, v_1, \dots, v_{n-1})$ in the following expansion.

$$\det \mathbf{circ}(a_0, a_1, \dots, a_{n-1}) = \sum_{v_0 \leq v_1 \leq \dots \leq v_{n-1}} c_n(v_0, v_1, \dots, v_{n-1}) a_{v_0} a_{v_1} \cdots a_{v_{n-1}}$$

The coefficient $c_n(v)$ is a function of the multiset of subscripts appearing in the monomial $\Pi a_v := a_{v_0} a_{v_1} a_{v_2} \cdots a_{v_{n-1}}$ which we write more briefly as $\Pi a_{[v]}$. To state the formula for $c_n(v)$, we need to introduce some notation.

11.1 Notation of the Main Theorem Let N be the order of the circulant determinant to be expanded.

We regard the subscripts v_0, v_1, \dots as residues modulo N , and we take the set of residues to be $\{0, 1, 2, \dots, N-1\}$ which we denote by \mathbb{Z}_N .

Given a sequence $v = (v_0, v_1, \dots, v_{n-1})$. Then, $[v] = [v_0, v_1, \dots, v_{n-1}]$, denotes the multiset of the elements of v . The symbol $|v|$ denotes the length of the sequence or of its multiset; in this case, $|v| = n$. For $n \leq N$, \bar{v} is defined to be $(v_0, v_1, \dots, v_{n-1}, 0, \dots, 0)$ which is the sequence v extended by $N - n$ zeroes, so that $|\bar{v}| = N$.

We shall call a sequence v or its multiset $[v]$ a *null multiset* if the sum of its elements is zero (mod N). $\mathcal{P}_0[v]$ denotes the set of partitions of a multiset $[v]$ into null multisets.

For any sequence $w = (w_0, w_1, \dots)$ of arbitrary objects, we let $F(w)$ denote the order of the group of permutations on the subscripts of w which leave w invariant. $F(w)$ equals $a! b! \cdots$ where a, b, \dots are the multiplicities of the elements in $[w]$.

11.2 Statement of the Main Theorem Let \bar{v} be a sequence of N subscripts, and let $c(\bar{v})$ be the coefficient of $\Pi a_{\bar{v}}$ in the expansion of $\det \mathbf{circ}_N(a)$. Let v be the sub-sequence of \bar{v} consisting of its non-zero entries. Then,

$$c(\bar{v}) = (-1)^{|v|} \sum_{[W] \in \mathcal{P}_0[v]} \frac{(-N)^{|W|}}{F(W)} \prod_{[w] \in [W]} \frac{(|w| - 1)!}{F(w)} \quad (1)$$

11.2.1 An Example We illustrate the use of the theorem with an example. Let us compute the coefficient of $a_0^2 a_1^4 a_3 a_7 a_8^2$ in the expansion of the general 10×10 circulant determinant. This is a calculation that would otherwise be practical only by computer.

In the notation of the theorem, we have $N = 10$, and

$$\bar{v} = (0, 0, 1, 1, 1, 1, 3, 7, 8, 8)$$

$$v = (1, 1, 1, 1, 3, 7, 8, 8)$$

The computation of the coefficient is summarized in Table 1 below which shows all partitions in $\mathcal{P}_0[v]$. Partitions consisting of two multisets contribute to N^2 , those of three multisets contribute to N^3 etc., in accordance with formula (1).

Table 1. Computation of $c(v)$.

Part ⁿ	Null Multisets	$\frac{(-1)^{ W }}{F(W)} \times \prod_{[w] \in [W]} \frac{(w - 1)!}{F(w)}$	$N^{ W }$
P_1	[3 7], [1 1 8], [1 1 8]	$-\frac{1}{2!} \times \frac{(2-1)!}{1} \left(\frac{(3-1)!}{2!} \right)^2 = -0.5$	N^3
P_2	[1 1 1 7], [1 3 8 8]	$1 \times \frac{(4-1)!}{3!} \frac{(4-1)!}{2!} = 3$	N^2
P_3	[3 7], [1 1 1 1 8 8]	$1 \times \frac{(2-1)!}{1} \frac{(6-1)!}{4!2!} = 2.5$	N^2
P_4	[1 1 8], [1 1 3 7 8]	$1 \times \frac{(3-1)!}{2!} \frac{(5-1)!}{2!} = 12$	N^2
P_5	[1 1 1 1 3 7 8 8]	$-1 \times \frac{(8-1)!}{4!2!} = -105$	N
Total		$-105N + 17.5N^2 - 0.5N^3$	

$$\therefore c(v) = (-1)^8(-105N + 17.5N^2 - 0.5N^3) = 200$$

(There is an algorithm, illustrated in §5(18), which may be used to check this result.)

11.3 Remarks Concerning Zero Subscripts Formula (1) requires that v contain only the non-zero elements of \bar{v} . The more general version of the theorem in §11.12.1 allows v to contain none, some, or all the zeroes in \bar{v} .

We shall use $c(\bar{v})$ interchangeably with $c(v)$. It turns out that the zero subscripts are in a sense irrelevant.

11.4 The Zero Set Formula. A proof of the main theorem proceeds by first proving a special form called the Zero Set Formula. The main theorem is then deduced by converting the formula from one involving zero sets to one involving multisets. A zero set is defined as follows:

11.5 Definition of Zero Set and Zero Set Partition

For the remainder of this chapter, we shall denote $|v|$ by n .

Let I_n be the set of subscripts appearing in v (in practice, either $I_n = \{0, 1, \dots, n-1\}$ or $I_n = \{1, 2, \dots, n\}$).

(i) For any $S \subset I_n$, we define $v:S = \{v_i \mid i \in S\}$.

(ii) We shall say that S is a zero set on v in the case that $v:S$ is a null multiset.

(iii) Define $\mathcal{P}_0(v)$ to be any partition of I_n such that $v:P$ is a null multiset for every $P \in \mathcal{P}_0(v)$.

11.5.1 Examples

(i) Consider $v = (1, 2, 2, 3, 0, 0)$ with $N = 6$. Then, $S_1 = \{0, 1, 3, 5\}$ and $S_2 = \{0, 2, 3, 4\}$ are two distinct zero sets on v , but the null multisets $v:S_1$ and $v:S_2$ are indistinguishable and therefore equal. Note that if v is a null multiset of n elements, then \mathbb{Z}_n is a zero set.

(ii) Let $v = (2, 3, 5, 6)$, $N = 8$. Then, $P_1(v) = \{\{0, 3\}, \{1, 2\}\}$ and $P_2(v) = \{\{0, 1, 2, 3\}\}$ are all the zero-set partitions. They correspond 1-1 to the multiset partitions, $P_1[v] = [[2, 6], [3, 5]]$ and $P_2[v] = [[2, 3, 5, 6]]$ of v .

(iii) Let $v = (1, 1, 2, 2, 4)$, $N = 5$. There are the three zero-set partitions: $P_1(v) = \{\{0, 4\}, \{1, 2, 3\}\}$, $P_2(v) = \{\{1, 4\}, \{0, 2, 3\}\}$, and $P_3(v) = \{\{0, 1, 2, 3, 4\}\}$, but only two multiset partitions: $P_1[v] = [[1, 4], [1, 2, 2]]$ and $P_3[v] = [[1, 1, 2, 2, 4]]$.

Zero sets allow us to differentiate between like elements of a multiset, and for some mysterious reason drawing such arbitrary distinctions seems necessary to proving the main theorem.

11.6 Ore's Proof of the Zero Set Formula

The Zero Set Formula was first published by Oystein Ore ([Ore]) in 1951. However, Ore's derivation of the formula is telegraphic in the extreme, and requires some interpretation. We provide here an expanded version of Ore's result written using our notation. The general Zero Set Formula allows any number of zeroes in v , the special version proved by Ore assumes v has no zeroes.

11.6.1 Theorem (Special Form of the Zero Set Formula) Let v be the sequence of all non-zero subscripts in \bar{v} , and let $|v| = n$. Then,

$$c_N(\bar{v}) = (-1)^n F(v)^{-1} \sum_{P \in \mathcal{P}_0(v)} (-N)^{|P|} \prod_{S \in P} (|S| - 1)!$$

Proof. (Based on [Ore]).

The eigenvalue formula (Corollary 1.11.2) for the circulant determinant gives

$$\det \mathbf{circ}(a) = \prod_{i \in \mathbb{Z}_N} (a_0 + a_1 \zeta^i + a_2 \zeta^{2i} + \cdots + a_j \zeta^{ij} + \cdots + a_{N-1} \zeta^{i(N-1)}) \quad (2)$$

where $1 = \zeta^0, \zeta, \zeta^2, \dots, \zeta^{N-1}$ are the N^{th} roots of unity.

Pick a sequence of a_i 's, one from each factor of equation (2). Let us suppose that the sequence is $a_0^{N-n} a_{v_1} \cdots a_{v_n}$. (Remember that $v_n = v_0$ if $n = N$.) The coefficient of this particular sequence is

$$\zeta^{1v_1} \cdot \zeta^{2v_2} \cdots \zeta^{n \cdot v_n}$$

(We do not consolidate the powers for reasons that will become plain.)

If $(\bar{t}_0, \bar{t}_1, \dots, \bar{t}_{N-1})$ is a rearrangement of $(\bar{v}_0, \bar{v}_1, \dots, \bar{v}_{N-1})$ (with $N - n$ zeroes in both sequences), then $a_0^{N-n} a_{t_1} a_{t_2} \cdots a_{t_n}$ is algebraically the same as $a_0^{N-n} a_{v_1} a_{v_2} \cdots a_{v_n}$. We collect all such algebraically equal terms and obtain

$$\det \mathbf{circ}_N(a) = \sum_{\{[v] \vdash v \in \mathbb{Z}_N^n\}} \Pi a_v \sum_{\rho \in R(\bar{v})} \zeta^{1\bar{v}_{\rho(0)}} \cdot \zeta^{2\bar{v}_{\rho(1)}} \cdots \zeta^{(N-1)\bar{v}_{\rho(N-1)}} \quad (3)$$

The first summation is over all distinct multisets which can be constructed from arbitrary sequences of N residues modulo N . The second summation is over all distinct rearrangements ρ of the sequence \bar{v} , a set which we denote by $R(\bar{v})$. The term \bar{v}_ρ denotes the rearranged sequence, and $\bar{v}_{\rho(r)}$ is the r^{th} component in the rearranged sequence.

The set $R(\bar{v})$ is defined only to within products by permutations in $F_{\bar{v}}$, the stabilizer subgroup of \bar{v} in the full symmetric group S_N on \bar{v} . Since permutations act on \bar{v} from the left, $R(\bar{v}) = S_N \setminus F_{\bar{v}}$. A coset in R is fully specified by the resulting sequence of values \bar{v}_ρ where ρ is a representative permutation in the coset.

By definition of the circulant determinantal coefficient,

$$\det \mathbf{circ}_N(v) = \sum_{0 < v_1 \leq v_2 \leq \cdots \leq v_n} c_N(v_1, v_2, \dots, v_n) a_0^{N-n} a_{v_1} \cdots a_{v_n} \quad (4)$$

From (4) and (3), we have

$$\begin{aligned} c(v_1, v_2, \dots, v_n) &= \sum_{\rho \in R(\bar{v})} \zeta^{1\bar{v}_{\rho(1)}} \cdot \zeta^{2\bar{v}_{\rho(2)}} \cdots \zeta^{(N-1)\bar{v}_{\rho(N-1)}} \\ &= \sum_{\tau \in R(\bar{v})} \zeta^{\tau(1)\bar{v}_1} \cdot \zeta^{\tau(2)\bar{v}_2} \cdots \zeta^{\tau(N-1)\bar{v}_{(N-1)}} \\ &= \sum_{\tau \in R(\bar{v})} \zeta^{\tau(1)v_1} \cdot \zeta^{\tau(2)v_2} \cdots \zeta^{\tau(n)v_n} \end{aligned} \quad (5)$$

In the second summation, we reordered the powers of ζ , sorting them left to right by the subscript on \bar{v} , and we then set $\tau = \rho^{-1}$. In the last summation, we omitted all zero values of \bar{v} , leaving only the non-zero elements v_1, v_2, \dots, v_n .

To see how to proceed, suppose initially that v_1, v_2, \dots, v_n are distinct. Then, cosets of $F_{\bar{v}}$ correspond to maps $I_n = \{1, 2, \dots, n\} \rightarrow \mathbb{Z}_N$. Applying this to formula (5), we see that the sequence $(\zeta^{\tau(1)}, \zeta^{\tau(2)}, \dots, \zeta^{\tau(n)})$ can be any sequence of n distinct N^{th} roots of unity. Thus we see that in this case, the formula for the coefficients assumes a highly symmetric form:

$$c(v_1, v_2, \dots, v_n) = \sum_{\substack{\zeta_i^{N=1} \\ \zeta_i \text{ distinct}}} \zeta_1^{v_1} \cdot \zeta_2^{v_2} \cdot \dots \cdot \zeta_n^{v_n} \quad (6)$$

To see a general pattern, consider how formula (6) develops for low n .

$$c(v_1) = \sum_i (\zeta^i)^{v_1} \quad (7a)$$

$$c(v_1, v_2) = \sum_{i \neq j} (\zeta^i)^{v_1} (\zeta^j)^{v_2} = c(v_1)c(v_2) - c(v_1 + v_2) \quad (7b)$$

$$c(v_1, v_2, v_3) = c(v_1)c(v_2)c(v_3) - c(v_1)c(v_2+v_3) - c(v_2)c(v_1+v_3) - c(v_3)c(v_1+v_2) + 2c(v_1+v_2+v_3) \quad (7c)$$

It is clear that at least when v_1, v_2, \dots, v_n are distinct that the coefficient $c(v)$ can be reduced to a series of products of power sums over N^{th} roots of unity.

We now suppose that v_1, v_2, \dots, v_n contains duplicates. Suppose $v_1 = v_2$, then formula (6) becomes

$$c(v_1, v_1, v_3, \dots, v_n) = \sum_{\substack{\zeta_i^{N=1} \\ \zeta_i \text{ distinct} \\ \zeta_1 \prec \zeta_2}} \zeta_1^{v_1} \cdot \zeta_2^{v_1} \cdot \zeta_3^{v_3} \cdot \dots \cdot \zeta_n^{v_n}$$

where “ \prec ” denotes any well-ordering of the N^{th} roots of unity. In the simplest case, $n = 2$, $v = (a, a)$, we have

$$c(a, a) = \sum_{0 \leq i < j < N} (\zeta^i)^a (\zeta^j)^a$$

There is a decomposition along the lines of (7b) for $c(a, a)$; it is

$$c(a, a) = \frac{1}{2} (c(a)^2 - c(2a)) \quad (7d)$$

This is essentially the decomposition of (7b) but divided by $|F_v| = F(v) = 2!$.

The general method of decomposing $c(v_1, v_2, \dots, v_n)$ appears to be:

- (i) Take the leading term to be $c(v_1)c(v_2) \cdot \dots \cdot c(v_n)$. We regard this product as a sum over an n -dimensional cube situated at $(0, 0, \dots, 0)$, the i^{th} side lying along a coordinate which is graduated by the N roots of unity raised to the power of v_i . Each point inside the cube has the value of the product of the coordinate values.
- (ii) We remove all diagonal lines, planes, and hyperplanes from the cube by subtracting $c(v_1)c(v_2 + \dots + v_n)$, $c(v_1)c(v_2)c(v_3 + \dots + v_n)$ etc. with proper adjustments for intersections.
- (iii) If x occurs in v with multiplicity k . Then, we regard $c(x)^k$ as a sum over Δ , a k -dimensional simplex in the k -dimensional cube. The simplex Δ is such that permutations of the coordinates applied to Δ tessellate the cube (minus the removed hyperplanes). Thus, when $k = 2$, the simplex is a triangle, and is $1/2$ the area of the square without its diagonal; when $k = 3$, the simplex is a tetrahedron and is $1/6^{\text{th}}$ the volume of the cube without its main diagonals and diagonal planes, etc.

According to Ore, the general result of this process was found by Faà di Bruno ([FB]) and is described as follows.

Let α denote any root of an arbitrary polynomial, $q(x)$, say, of degree N . Define a symmetric function

$$s_{v_1, v_2, \dots, v_n}(\alpha) := \sum \alpha_1^{v_1} \alpha_2^{v_2} \cdots \alpha_n^{v_n} \quad (8)$$

where the sum is extended over all possible sets of distinct $\alpha_1, \alpha_2, \dots, \alpha_n$ taken from the roots of q . In the event that two or more v_i 's are the same, then it is to be understood that their roots be taken in one combination only. As in equations (7a) -(7d), $s_{v_1, v_2, \dots, v_n}(\alpha)$ can be expressed in terms of $s_t(\alpha)$ where t is an integer; in other words, in terms of sums of the t^{th} powers of the roots of q .

Consider a partition of the set $I_n = \{1, 2, \dots, n\}$; let us say it is $\mathcal{P} = \{P_1, P_2, \dots, P_m\}$. We let $p_i = |P_i|$. Thus, $p_1 + p_2 + \cdots + p_m$ is a partition of n .

This partition of I_n implies a multiset partition of the multiset $[v]$.

$$[v] = [v:P_1] + [v:P_2] + \cdots + [v:P_m]$$

We now fix the integers p_1, p_2, \dots, p_m and we define

$$A(p) := \sum_{\mathcal{P}} s_{\sigma_1}(\alpha) s_{\sigma_2}(\alpha) \cdots s_{\sigma_m}(\alpha)$$

where the sum extends over all partitions \mathcal{P} of I_n into subsets of sizes p_1, p_2, \dots, p_m , and if we suppose $\mathcal{P} = \{P_1, P_2, \dots, P_m\}$, then $\sigma_i := \sum v:P_i$, is the sum of all elements in the subsequence $v:P_i$.

Then, Faà di Bruno's formula gives

$$s_{v_1, v_2, \dots, v_n}(\alpha) = \frac{1}{F(v)} \sum_p (-1)^{r+m} (p_1 - 1)(p_2 - 1) \cdots (p_m - 1) A(p)$$

where the sum is over all partitions of $n = p_1 + p_2 + \cdots + p_m$.

We now take the roots α to be the N^{th} roots of unity. Then,

$$s_t = \begin{cases} N & \text{if } t \equiv 0 \pmod{N} \\ 0 & \text{otherwise} \end{cases}$$

Thus, we need only consider zero set partitions of I_n , and each set in such a partition contributes exactly a factor of N to $A(p)$, giving the formula of the theorem. \square

11.7 Criticism of the Ore Proof. Ore found the correct formula for the circulant determinantal coefficient, after many before him failed. However, his proof leaves much, indeed too much, to the imagination of the reader. Strictly speaking, Ore proved the formula only in the case of distinct v_1, v_2, \dots, v_n , leaving it entirely to the reader to determine how to proceed in the more general, and indeed, the more difficult case.

Secondly, the proof depends critically on a theorem of Faà di Bruno, a theorem which appeared in a book published in 1881 which is now almost unobtainable outside of Germany. Ordinarily, this would present no difficulties since conventionally a theorem of such critical importance to a proof would be quoted in full. However, Ore did not quote the theorem at all, and as a result, short of visiting a German reference library, and obtaining a translation of the entire book (since no page numbers are given in the reference), it is impossible to verify whether the Faà di Bruno theorem is being correctly used, especially in the case where v_1, v_2, \dots, v_n are not all distinct.

11.11 Zero Set Formula

We now derive alternate formulæ for the determinantal coefficient.

11.11.1 **Theorem** Let $v \in Z_0^n$, and suppose v has m non-zero entries. Then,

$$c_N(\bar{v}) = (-1)^n \binom{N-m}{N-n}^{-1} F(v)^{-1} \sum_{P \in \mathcal{P}_0(v)} (-N)^{|P|} \prod_{S \in P} (|S| - 1)! \quad (13)$$

Proof. Let $s = N - m =$ the number of zeroes in \bar{v} , and let \hat{v} denote v stripped of all its zeroes. From Lemma 12,

$$\begin{aligned} C(D_n, v) &= \frac{F(\bar{v})}{(N-n)!} c(\bar{v}) \\ &= \frac{F(\hat{v}) s!}{(N-n)!} c(\bar{v}) \\ &= \frac{F(v) s!}{(s - (N-n))! (N-n)!} c(\bar{v}) \\ &= F(v) \binom{s}{N-n} c(\bar{v}) \end{aligned}$$

Finally, by Proposition 11.10.4, we can substitute $H_n(v; N)$ for $C(D_n, v)$. \square

11.12 **Multiset Formula** The need to compute zero sets in the formula (13) is undesirable because it is rather prone to error. Not only must one find all the null multiset partitions for v , one must then find all the zero sets representing a given multiset partition. In the theorem which follows, we derive a formula for the coefficient directly in terms of null multiset partitions and thereby entirely eliminate the need to calculate zero sets.

Recall that $\mathcal{P}_0[v]$ denotes the set of all partitions of $[v]$ into null multisets. Note that a partition is a multiset of multisets. For example, $[[2, 4], [2, 4]] \in \mathcal{P}_0[2, 2, 4, 4]$ for $N = 6$.

11.12.1 **Theorem** Let $v \in Z_0^n$, and suppose v has m non-zero entries. Then,

$$c_N(\bar{v}) = (-1)^n \binom{N-m}{N-n}^{-1} \sum_{[U] \in \mathcal{P}_0[v]} \frac{(-N)^{|U|}}{F(U)} \prod_{[u] \in [U]} \frac{(|u| - 1)!}{F(u)} \quad (14)$$

where $F(U) = a! b! \cdots f!$ where a, b, \dots, f are the multiplicities of the multisets in U .

Proof. We define a function $J_n([v]; x)$ by

$$J_n([v]; x) := (-1)^n \sum_{[U] \in \mathcal{P}_0[v]} \frac{(-x)^{|U|}}{F(U)} \prod_{[u] \in [U]} \frac{(|u| - 1)!}{F(u)}$$

By Theorem 11.11.1,

$$c(\bar{v}) = \binom{N-m}{N-n}^{-1} F(v)^{-1} H_n(v; N)$$

By Theorem 11.11.1, we need only show that $F(v)^{-1} H_n(v; N) = J_n([v]; N)$.

We make the natural correspondence between zero sets on v and null multisets, namely, we map the zero set S to the multiset $v : S$. We call this map α . The map α also induces a map from $\mathcal{P}_0(v)$ to $\mathcal{P}_0[v]$ in the obvious way, and we call this map α as well. The cardinality of a partition is not changed by α , and neither is the cardinality of each set appearing in the partition. That is, $|\alpha(S)| = |v : S| = |S|$, and the partition $\{S_1, S_2, \dots, S_r\}$ of $\mathcal{P}_0(v)$ corresponds to the partition $[v : S_1, v : S_2, \dots, v : S_r]$ of $\mathcal{P}_0[v]$, both of

which have cardinality r . Hence, the only adjustment to the zero set formula will be the number of zero sets mapped to a single null multiset.

Let $M \in \mathcal{P}_0[v]$. We need to find $|\alpha^{-1}M|$. Let $M = [[m_1], [m_2], \dots, [m_r]]$ where each m_i is a subsequence of v . There exists $S = \{S_1, S_2, \dots, S_r\} \in \alpha^{-1}M$. For instance, one such can be constructed by setting S_i to the set of subscripts appearing in m_i for each i . We take S to be this partition.

The defining difference between zero sets and null multisets is that order matters in zero sets but not in null multisets. Hence, we can find all zero sets for a given multiset by acting upon one member of $\alpha^{-1}M$, S say, with permutations on the subscripts of v .

Let G be the stabilizer group of v ; specifically, define

$$G := \{\gamma : \mathbb{Z}_n \rightarrow \mathbb{Z}_n \mid v = v_\gamma\}$$

Then, $|G| = F(v)$.

Every permutation $\gamma \in G$, maps M to itself, but maps S to a possibly different partition, γS of $\mathcal{P}_0(v)$, where $\gamma S := \{\gamma S_1, \gamma S_2, \dots, \gamma S_r\}$. However, not all $(\gamma S)_{\gamma \in G}$ will be distinct; there will be duplications whenever $\gamma S = S$. Denote the set of such permutations by R . Clearly, the number of distinct elements in $|\alpha^{-1}M| = G/R = |G|/|R|$.

R is that subgroup of G in which each element maps every S_i onto some S_j . To compute $|R|$ we shall factor it into those permutations which permute elements within the S_i 's, and those which permute the S_i 's among themselves. To this end, define

$$Q := \{\gamma \in G \mid \gamma S_i = S_i, \forall i = 1, 2, \dots, r\}$$

We know $|Q|$, it is

$$|Q| = \prod_{i=1}^r F(v : S_i) = \prod_{i=1}^r F(m_i)$$

One easily sees that $Q \triangleleft R$. So we can define $R^* = R/Q$. Members of R^* represent permutations of (S_1, S_2, \dots, S_r) . Their number is

$$\begin{aligned} |R^*| &= F(v : S_1, v : S_2, \dots, v : S_r) = F([m_1], [m_2], \dots, [m_r]) \\ \therefore |R| &= |R^*| \cdot |Q| = F([m_1], [m_2], \dots, [m_r]) \prod_{i=1}^r F(m_i) = F(M) \prod_{m \in M} F(m) \\ \therefore |\alpha^{-1}M| &= |G/R| = \frac{F(v)}{F(M) \prod_{m \in M} F(m)} \end{aligned}$$

which is the number of zero set partitions per null multiset partition.

We now apply this to $F(v)^{-1}H_n(v; N)$.

$$\begin{aligned} \frac{(-1)^n}{F(v)} H_n(v; N) &= \frac{1}{F(v)} \sum_{T \in \mathcal{P}_0(v)} (-N)^{|T|} \prod_{S \in T} (|S| - 1)! \\ &= \sum_{T \in \mathcal{P}_0(v)} (-N)^{|T|} \frac{1}{F(v)} \prod_{S \in T} (|S| - 1)! \\ &= \sum_{[U] \in \mathcal{P}_0[v]} (-N)^{|U|} \frac{1}{F(v)} \frac{F(v)}{F(U) \prod_{u \in [U]} F(u)} \prod_{[u] \in [U]} (|u| - 1)! \\ &= \sum_{[U] \in \mathcal{P}_0[v]} \frac{(-N)^{|U|}}{F(U)} \prod_{[u] \in [U]} \frac{(|u| - 1)!}{F(u)} \\ &= (-1)^n J_n([v]; N) \quad \square \end{aligned}$$

We note that the theorem holds for arbitrary $v \in \mathbb{Z}_N^n$ provided we interpret an empty sum as zero, since clearly there are no partitions of v into null multisets if v itself is not a null multiset.

11.13 Power Formula.

The monomials Πa_v would most commonly be expressed as a product of powers of the variables a_0, a_1, \dots, a_{N-1} . Thus, $\Pi a_v = a_0^{k_0} a_1^{k_1} \dots a_{N-1}^{k_{N-1}}$ where k_i is the multiplicity of v_i in $[v]$. It is quite straightforward to express the determinantal coefficients in terms of the powers k_0, k_1, \dots, k_{N-1} .

$$\det \mathbf{circ}_N(a) = (-1)^N \sum_{\substack{k \in \mathbb{N}^N \\ \Sigma k = N}} a_0^{k_0} a_1^{k_1} \dots a_{N-1}^{k_{N-1}} \sum_{\substack{[T] \subset \Delta \\ \Sigma T = k}} \frac{(-N)^{|T|}}{F(T)} \prod_{t \in T} \frac{1}{\Sigma t} \binom{\Sigma t}{t}$$

where $\Delta := [t \in \mathbb{Z}^N \mid t \neq 0 \text{ and } \sum it_i \equiv 0 \pmod{N}]$, and $\binom{s}{t}$ with $s = \Sigma t$ is the multinomial coefficient of the first kind.

The restriction $\sum T = k$ means that the sum of vectors in T must equal the vector k . The condition $\sum k_i = N$ states the degree is N . The condition $[T] \subset \Delta$ means that T is the equivalent of a null multiset partition.

11.14 Application to Permutations

According to Proposition 10.5.3, if $c(v)$ is non-zero, then there exists a permutation, τ , on \mathbb{Z}_N whose multiset of translations equals $[v]$. When $N = p$, prime, the theorem gives a precise criterion for when $c(v)$ is non-zero.

11.14.2 Proposition Let p be an odd prime, and let $v \in Z_0^p$. If v consists of only a single residue of multiplicity p , then $c_p(v) = 1$. Otherwise, $F(v) \not\equiv 0 \pmod{p}$, and

$$c_p(v) \equiv -p F(v)^{-1} \pmod{p^2}$$

Proof. The requirement that $v \in Z_0^p$ means that the vector v is of full length. Suppose first that v contains only one distinct residue, r , say, then $c(v)$ is the coefficient of the term a_r^p which one can easily see is 1 for odd order circulants.

Now suppose that v contains at least two distinct residues. By the Zero Set Formula of Proposition 27,

$$c(v) = \frac{(-1)^p}{F(v)} \sum_{W \in \mathcal{P}_0(v)} (-p)^{|W|} \prod_{S \in W} (|S| - 1)!$$

Consider first the denominator, $F(v)$. It equals a product of factorials, $a!b! \dots$ where a, b, \dots are multiplicities of elements in v . Since v contains at least two distinct elements, no multiplicity can equal or exceed p . Hence, $p \nmid F(v)$, and so $F(v)$ has an inverse in \mathbb{Z}_{p^2} and the formula can be evaluated modulo p^2 by taking the inverse residue. The p term is derived from single set partitions, but there is only one such, namely $W = \{\{\mathbb{Z}_p\}\}$.

$$\therefore c(v) \equiv -F(v)^{-1} (-p)(p-1)! \equiv -p F(v)^{-1} \pmod{p^2}$$

The last congruence follows by Wilson's Theorem. \square

Ore also derived the above result from the Zero Set Formula.

11.14.3 Corollary For p prime, there exists a permutation $\tau \in S_p$ such that $[\tau] = [v]$ iff v is a null multiset \pmod{p} .

Proof. This is immediate from Proposition 10.5.3 and the proposition when p is odd. The corollary also holds for $p = 2$ because then the determinant is $a_0^2 - a_1^2$. \square

This corollary proves a special case of a conjecture of E.T. Parker [Guy]. The full conjecture, if true, would imply that the primality condition in Corollary 11.14.3 is unnecessary.

11.15 Application to Cyclotomic Norms.

We shall apply Proposition 11.14.2 to estimate the congruence class of the determinant modulo p^2 .

11.15.1 **Proposition** Let p be an odd prime, and let $A = \text{CIRC}_p(a)$ where $a \in \mathbb{Z}^p$. Then,

$$\det A \equiv (A^p)_{0,0} \equiv p^{-1} \text{tr} A^p \pmod{p^2}$$

Proof. Proposition 11.14.2 provides a formula for the determinantal coefficient modulo p^2 unless the monomial is a p^{th} power when the coefficient equals 1. Hence,

$$\det A = \sum_{\Sigma[v] \equiv 0 \pmod{p}} c(v) \prod a_v \equiv -p S(a) + \sum_{j=0}^{p-1} a_j^p \pmod{p^2} \quad (15)$$

$$\text{where } S(a) := \sum \left\{ \frac{a_1^{i_1} a_2^{i_2} \cdots a_p^{i_p}}{i_1! i_2! \cdots i_p!} \mid \Sigma i_j = p, \Sigma j i_j \equiv 0 \pmod{p}, i_k < p, \forall k \right\}$$

We can express $S(a)$ in terms of A^p . We proceed by expanding A in terms of the standard circulant basis $\{I, U, U^2, \dots, U^{p-1}\}$. Then, by the multinomial theorem,

$$A^p = \left(\sum_{k=0}^{p-1} a_k U^k \right)^p = \sum_{m=0}^{p-1} U^m \sum_{\substack{\Sigma i_j = p \\ \Sigma j i_j \equiv m \pmod{p}}} \frac{m!}{i_1! i_2! \cdots i_m!} a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m}$$

Now, the coefficient of $U^0 = I$ term in the above expansion equals the $(0, 0)^{\text{th}}$ entry in A^p . Therefore,

$$\begin{aligned} \therefore (A^p)_{0,0} &= \sum_{\substack{\Sigma i_j = p \\ \Sigma j i_j \equiv 0 \pmod{p}}} \frac{p!}{i_1! i_2! \cdots i_m!} a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m} \\ &= p! S(a) + \sum_{j=0}^{p-1} a_j^p \\ &\equiv -p S(a) + \sum_{j=0}^{p-1} a_j^p \pmod{p^2} && \text{by Wilson's Theorem} \\ &\equiv \det A \pmod{p^2} && \text{from (15)} \end{aligned}$$

This proves the first congruence in the proposition. The second follows because A^p is a circulant, and so its trace is just p times the top left element. \square

11.15.2 **Corollary** Let $A = \text{CIRC}(a_0, a_1, \dots, a_{p-1}) \in \text{CIRC}_p(\mathbb{Z})$ with eigenvalues $\mu_0, \mu_1, \dots, \mu_{p-1}$, then the cyclotomic norm of μ_1 in $\mathbb{Z}(\zeta_p)$ is

$$\mathcal{N}(\mu_1) \equiv \frac{(A^p)_{0,0}}{\mu_0} \pmod{p^2} \quad \square$$

If $p \mid \mu_0$ then the fraction on the right must of course be evaluated before taking of residues.

11.15.3 **Corollary** Let $\xi \in \mathbb{Z}(\zeta_p)$. Then,

$$\mathcal{N}(1 + p\xi) \equiv 1 - p \ell_p(\xi) \pmod{p^2}$$

(See §7.2.6 for the definition of the ℓ_p homomorphism.)

Proof. Let $\xi \in \mathbb{Z}(\zeta_p)$, and let $c \in \lambda_1^{-1}(\xi)$. Following Corollary 11.15.2 we estimate the scalar term in $(1 + pc)^p = 1 + p^2(c + \dots) \equiv 1 \pmod{p^2}$. Hence,

$$\mathcal{N}(1 + p\xi) \equiv (1 + p\lambda_0(c))^{-1} \equiv 1 - p\ell_p \pmod{p^2} \quad \square$$

11.16.1 Application to Combinatorics I.

Let $n \leq N$ but otherwise unrestricted, and we let $v = 0 \in \mathbb{Z}^n$. The coefficient of this subscript vector is 1, and the multiset partitions of v correspond to unordered partitions of the integer n . These are all solutions to

$$\sum_{i=1}^n ik_i = n \quad \text{with } k_i \in \mathbb{N}$$

Each ik_i term represents the multiset $[[0, \dots, 0], [0, \dots, 0], [0, \dots, 0]]$ which is k_i multisets of i zeroes each. The order of the stabilizer group for each $u = [0, \dots, 0]$ is $F(u) = i!$, and the order of the stabilizer group for a partition is $F(U) = k_1!k_2! \dots k_n!$. Entering this into the Multiset Formula (see equation (14) in §11.12.1), and multiplying throughout by $\binom{N}{n}$, we get

$$\begin{aligned} \binom{N}{n} &= (-1)^n \sum_{\{k_i \vdash \Sigma ik_i = n\}} \frac{(-N)^{\Sigma k_i}}{k_1!k_2! \dots k_n!} \prod_{i=1}^n \left(\frac{(i-1)!}{i!} \right)^{k_i} \\ &= (-1)^n \sum_{\{k_i \vdash \Sigma ik_i = n\}} \frac{(-N)^{\Sigma k_i}}{k_1!k_2! \dots k_n!} \left(\prod_{i=1}^n i^{-1} \right) \left(\prod_{i=1}^n i^{1-k_i} \right) \end{aligned}$$

Cancelling $n!$ with $\prod i^{-1}$,

$$\begin{aligned} \frac{N!}{(N-n)!} &= (-1)^n \sum_{\{k_i \vdash \Sigma ik_i = n\}} (-N)^r \prod_{i=1}^n \frac{i^{1-k_i}}{k_i!} \quad \text{where } r = \sum_{i=1}^n k_i \\ &= (-1)^n \sum_{r=0}^n (-N)^r \sum_{\substack{\Sigma ik_i = n \\ \Sigma k_i = r}} \prod_{i=1}^n \frac{i^{1-k_i}}{k_i!} \end{aligned}$$

Both sides of the equation are manifestly polynomials in N with coefficients constant with respect to N . Since the equation holds for general N , and the left has integral coefficients, so must the right.

The Stirling numbers of the first kind, $S_N^{(m)}$, are defined by (see [AbS]),

$$x(x-1) \dots (x-n+1) = \sum_{m=0}^n S_n^{(m)} x^m$$

which gives:

$$11.16.2 \quad \textbf{Proposition} \quad S_n^{(m)} = (-1)^{n+r} \sum_{\substack{\Sigma ik_i = n \\ \Sigma k_i = r}} \prod_{i=1}^n \frac{i^{1-k_i}}{k_i!}. \quad \square$$

11.16.3 Application to Combinatorics II.

In this section, we shall take all subscript vectors v to be of full length, so that $v = \bar{v}$.

It was shown in §5.2.14 that if $N = mn$ then

$$\Delta_N(a_0, 0, \dots, 0, a_m, 0, \dots, 0, a_{2m}, 0, \dots, 0, a_{N-n}, 0, \dots, 0) = \Delta_n(a_0, a_m, a_{2m}, \dots, a_{N-m})^m \quad (16)$$

Since this holds for arbitrary $a_0, a_m, a_{2m}, \dots, a_{m(n-1)}$, we can deduce relationships between the coefficients using the multinomial theorem which, in our notation, is

$$\left(\sum_{i \in \mathbb{Z}_n} x_i \right)^m = \sum_{v \in \mathbb{Z}_n^m} \frac{m!}{F(v)} \prod x_v$$

In the present case, from equation (16), the x_i 's are terms of the form $c_n(u)\Pi a_{mu}$. All terms in $\det \mathbf{circ}_N$ in equation (16) are of the form $c(mv)\Pi a_{mv}$, and can arise from the multinomial expansion only from products of the form

$$c(u_0)\Pi a_{mu_0} c(u_1)\Pi a_{mu_1} \cdots c(u_{m-1})\Pi a_{mu_{m-1}}$$

where $[u_0] \cup [u_1] \cup \cdots \cup [u_{m-1}] = v$. Hence,

$$c_{mn}(mv) = \sum_{U \in \mathcal{P}_0^n(v)} \frac{m!}{F(U)} \prod_{u \in U} c_n(u) \quad (17)$$

where $\mathcal{P}_0^n(v)$ is all partitions of v into m null multisets modulo n each of length n . That is, $U \in \mathcal{P}_0^n(v) \Rightarrow |U| = m$ and $u \in U \Rightarrow |u| = n$.

We illustrate formula (17) with one example. Let $N = 8$, $n = 4$, $m = 2$. $v = [0 \ 1 \ 1 \ 1 \ 1 \ 2 \ 3 \ 3]$, $2v = [0 \ 2 \ 2 \ 2 \ 2 \ 4 \ 6 \ 6]$.

$$\begin{aligned} c_8[0 \ 2 \ 2 \ 2 \ 2 \ 4 \ 6 \ 6] &= 2c_4[1 \ 1 \ 1 \ 1]c_4[0 \ 2 \ 3 \ 3] + 2c_4[0 \ 1 \ 1 \ 2]c_4[1 \ 1 \ 3 \ 3] \\ &= 2(-1)(4) + 2(4)(2) \quad \text{from section 1.11} \\ &= 16 \end{aligned}$$

This relationship leads to the following combinatorial statement.

11.16.4 Proposition If $c_{mn}(mv) \neq 0$, then v can be split into m sequences of n numbers whose sums are each divisible by n .

Proof. If the left side of equation (17) is non-zero, the sum on the right must have a non-empty range. Hence there must be a partition of the required form. \square

11.17 The EGZ Theorem.

The above Proposition 11.16.4 deduces a combinatorial result concerning a multiset v given that its circulant determinantal coefficient is non-zero. This is reminiscent of Proposition 10.5.3.

We believe that in both examples that the non-zero coefficient condition can be replaced by the weaker condition that v be a null multiset. We can prove this assertion in the case of Proposition 11.16.4 using a theorem of Erdős, Ginzburg, and Ziv. First we restate Proposition 11.16.4 with a weaker condition.

11.17.1 First Assertion Pick any mn whole numbers, with or without repetitions, whose sum is divisible by mn . Then, the mn numbers can be partitioned into m parts of n numbers each whose sum is divisible by n .

Here is an equivalent and more intuitive form:

Fill a rectangular table of m rows and n columns with arbitrary whole numbers so that their average is also a whole number. Then, the numbers can be rearranged so that the average of each row is a whole number.

In fact we shall prove a slightly different statement which implies the above whereby the requirement of divisibility by mn is weakened to divisibility by only n .

11.17.2 Second Assertion Pick any mn whole numbers, with or without repetitions, whose sum is divisible by n . Then, the numbers can be partitioned so that each part contains n numbers whose sum is divisible by n .

11.17.3 **Definition** We shall say that a multiset of integers is n -null if the sum of its elements is divisible by n . We shall say that it is an **exact n -null** multiset if it is n -null and contains exactly n elements.

We now state our third assertion, namely, the EGZ Theorem.

11.17.3 **The EGZ Theorem** Every multiset of $2n - 1$ whole numbers contains an exact n -null sub-multiset.

We defer the proof until we have shown that the three assertions are equivalent, and that the theorem need only be proved for n prime.

The theorem statement cannot be strengthened by reducing the size of the given multiset. For instance, the multiset consisting of $n - 1$ zeroes and $n - 1$ ones has no sub-multiset of the required form.

It is clear that the EGZ Theorem implies the Second Assertion since we can use EGZ to successively remove exact n -null sub-multisets from the mn elements of the second assertion until only n elements are left. Contrariwise, the Second Assertion with $m = 2$ implies the Second Assertion. Hence, the second and third assertions are equivalent.

In fact, the second and first assertions are also equivalent. To see this we note that both assertions depend only on the congruence class mod n of the multiset members -- we can add any multiple of n to any element without affecting the conditions or conclusions of either assertion.

Suppose that $[v]$ is a multiset satisfying the conditions of the Second Assertion. Then, $\sum[v] \equiv sn \pmod{mn}$ for some integer s . By the foregoing we can subtract sn from any element of v giving an mn -null multiset v' which satisfies the conditions of the First Assertion. Hence, if the First Assertion holds, then so does the Second.

11.17.4 **Definition** We shall call n a **fine** number if the Second Assertion (and therefore, each of the three assertions) holds for modulus n and for all m .

11.17.5 **Proposition** If n is divisible by only fine primes then n is fine.

Proof. The proposition is trivially true for $n = 1$. Assume inductively that it is true for all $n' < n$.

Let v satisfies the conditions of the Second Assersion, and suppose that n is divisible only by fine primes. If n is prime, we are done. So assume that $n = pn_1$ where p is prime and therefore fine. Considering v arranged into a rectangle V of mn_1 rows by p columns, it follows that v can be rearranged within the rectangle V so that each row is p -null. Let the row sums be $s = (s_0, s_1, \dots, s_{mn_1-1})$, and let r be the sequence s divided throughout by p . Then, $\sum r$ is divisible by n_1 . Arrange r into a rectangle R of m rows by n_1 columns. Since n_1 is divisible by only fine primes, by induction hypothesis, n_1 is fine. Hence, r can be rearranged within R so that each row in R is n_1 -null. Now replace each r_i by s_i in the rectangle R . We obtain a rectangle whose every row sum is divisible by $pn_1 = n$. But, each s_i is a sum of a row in the rectangle V . Replace each s_i by its corresponding row in V . We obtain a rectangle of m rows and n columns containing the multiset v whose every row sum is divisible by n as required. \square

11.17.6 **Corollary** The three assertions hold iff every prime is fine. \square

We are now ready to prove the EGZ Theorem. In the propositions which follow, if $X, Y \subset \mathbb{Z}_n$, then $X + Y$ is to mean the set of all sums of pairs from X and Y ; that is, $\{x + y \mid x \in X, y \in Y\} \subset \mathbb{Z}_n$.

11.17.7 **The Cauchy-Davenport Lemma**

If p is a prime, and A, B are two nonempty subsets of \mathbb{Z}_p , then $|A + B| \geq \min\{p, |A| + |B| - 1\}$.

Proof. [AD]

We do an induction on $|B|$. It is trivial for $|B| = 1$. So we assume it holds for every A' and B' with $|B'| < |B|$.

We can assume we have A and B with $|A| < p, 2 \leq |B| < p$.

Suppose first that $A \cap B$ is a nonempty proper subset of B . In this case, one can apply the induction hypothesis to $A' = A \cup B$ and $B' = A \cap B$ and obtain the desired result because $A' + B' \subset A + B$ and $|A'| + |B'| = |A| + |B|$. Hence,

$$|A + B| \geq |A' + B'| \geq \min\{p, |A'| + |B'| - 1\} = \min\{p, |A| + |B| - 1\}$$

In case $A \cap B$ is not a nonempty, proper subset of B we shall show that there is a $c \in \mathbb{Z}_p$ such that $(B+c) \cap A$ is a nonempty proper subset of $(B+c)$ and hence the result follows as before because $|(B+c) + A| = |B + A|$.

Suppose for a contradiction that such an element c does not exist. Then all translates of B in \mathbb{Z}_p are either entirely in A or disjoint from it. So, if $b_1 + c \in A$ for some $b_1 \in B$, then $b + c \in A$ for every $b \in B$. For any $b_1 \in B$, $a \in A$ set $c = a - b_1$. Trivially, $b_1 + c \in A$. Therefore, $b_2 + c = a + b_2 - b_1 \in A$ for all $b_2 \in B$. But $a \in A$ is arbitrary, so $A + d \subset A$ where $d = b_2 - b_1$. Since $|B| \geq 2$, we can pick $b_2 \neq b_1$; that is, we can guarantee $d \neq 0$. So given $a \in A$, then A also contains $\{a, a + d, a + 2d, a + 3d, \dots\} = \mathbb{Z}_p$ because p is prime. This contradicts our assumption that $|A| < p$. \square

11.17.3 The EGZ Theorem Every multiset of $2n - 1$ whole numbers contains an exact n -null sub-multiset.

Proof. [AD]

By Proposition 11.17.5 and its corollary, we need only prove the theorem for $n = p$, prime.

Let the multiset be $[a]$ where a is the sequence $(a_1, a_2, \dots, a_{2p-1})$. Relabel so that the sequence is sorted in ascending order, $a_1 \leq a_2 \leq \dots < a_{2p-1}$. If $a_i = a_{i+p-1}$ for some $i \leq p-1$, then a_i would have multiplicity of p (in \mathbb{Z}_p) and the desired result follows. So we can assume that this is not case. Define $A_i = \{a_i, a_{i+p-1}\}$, for $1 \leq i \leq p-1$. By repeated application of the Cauchy-Davenport Lemma, we conclude that $|A_1 + A_2 + \dots + A_{p-1}| = p$, and hence every element of \mathbb{Z}_p is a sum of precisely $p-1$ of the first $2p-2$ elements of the sequence a . In particular, $-a_{2p-1}$ is such a sum, supplying the required p -null submultiset. \square

There are several other proofs of this celebrated theorem; the above proof using the Cauchy-Davenport Lemma seems to be the simplest and most direct. See for example [AD] and [Pan]; these two papers also suggest various generalizations.