

# On the Matrix-Element Expansion of a Circulant Determinant

Jerome Malenfant  
(Dated: April 22, 2015)

The determinant of an  $N \times N$  circulant matrix  $M = \text{CIRC}[x_0, x_1, \dots, x_{N-1}]$  can be expanded in the form  $\det M = \sum C_{a_0 a_1 \dots a_{N-1}} x_{a_0} x_{a_1} \dots x_{a_{N-1}}$ . By using the generating function of a restricted, mod- $N$  partition function, we derive a formula for the coefficients in this expansion as finite sums over products of binomial coefficients with integer variables.

Keywords: circulant matrix, circulant determinant  
MSC2010: 15B05, 15A15

## I. INTRODUCTION

A circulant matrix is a matrix of the form

$$\begin{pmatrix} x_0 & x_{N-1} & \cdots & x_2 & x_1 \\ x_1 & x_0 & \cdots & x_3 & x_2 \\ x_2 & x_1 & \cdots & x_4 & x_3 \\ \vdots & \vdots & & \vdots & \vdots \\ x_{N-2} & x_{N-3} & \cdots & x_0 & x_{N-1} \\ x_{N-1} & x_{N-2} & \cdots & x_1 & x_0 \end{pmatrix} \equiv \text{CIRC}[x_0, x_1, \dots, x_{N-1}]$$

where successive columns are circular permutations of the first column. (An alternative definition used by some authors is to take successive *rows* as circular permutations of the first row.) It is a particular form of a Toeplitz matrix, a matrix whose elements are constant along the diagonals. The  $N$  eigenvalues of the  $N \times N$  circulant matrix above are

$$x_0 + \omega^p x_1 + \omega^{2p} x_2 + \cdots + \omega^{p(N-1)} x_{N-1}, \quad p = 0, \dots, N-1 \quad (1)$$

where  $\omega = e^{2\pi i/N}$  is an  $N$ th root of unity. The determinant of the matrix is therefore the product of these eigenvalues:

$$\begin{vmatrix} x_0 & x_{N-1} & \cdots & x_2 & x_1 \\ x_1 & x_0 & \cdots & x_3 & x_2 \\ x_2 & x_1 & \cdots & x_4 & x_3 \\ \vdots & \vdots & & \vdots & \vdots \\ x_{N-2} & x_{N-3} & \cdots & x_0 & x_{N-1} \\ x_{N-1} & x_{N-2} & \cdots & x_1 & x_0 \end{vmatrix} \equiv \det[x_0, x_1, \dots, x_{N-1}] = \prod_{p=0}^{N-1} \left( x_0 + \omega^p x_1 + \cdots + \omega^{(N-1)p} x_{N-1} \right). \quad (2)$$

Some examples of these determinants for small values of  $N$  are:

$$\det[A, B, C] = A^3 + B^3 + C^3 - 3ABC;$$

$$\det[A, B, C, D] = A^4 - B^4 + C^4 - D^4 - 2A^2C^2 + 2B^2D^2 - 4A^2BD + 4AB^2C - 4BC^2D + 4ACD^2;$$

$$\begin{aligned} \det[A, B, C, D, E] = & A^5 + B^5 + C^5 + D^5 + E^5 \\ & -5A^3BE - 5A^3CD - 5AB^3C - 5B^3DE - 5AC^3E \\ & -5BC^3D - 5ABD^3 - 5CD^3E - 5ADE^3 - 5BCE^3 \\ & +5A^2B^2D + 5A^2BC^2 + 5A^2CE^2 + 5A^2D^2E + 5AB^2E^2 \\ & +5AC^2D^2 + 5B^2C^2E + 5B^2CD^2 + 5BD^2E^2 + 5C^2DE^2 \\ & -5ABCDE. \end{aligned}$$

The product on the right in eq.(2), when expanded out, contains  $N^N$  terms. There are considerably fewer terms in these examples, and show some apparent patterns in the coefficients. There appears then to be considerable cancelations occurring in the expansion of eq. (2), as there must be, since all the complex terms cancel. This suggests that there is a simpler way to calculate these determinants. In addition, expression (2) has the disadvantage of using a complex number,  $\omega$ , to find integer coefficients.

This work was initiated then by the desire to derive an explicit formula for the coefficients in the expansion of the determinant, and to see if the apparent patterns in the coefficients for small  $N$  appear in the general case as well.

Near the completion of these results I discovered the monograph on circulant matrices by Wyn-jones [1], where chapters 10 and 11 are devoted to the same problem that inspired this effort, that of finding a formula for the coefficients. The formula in ref. [1], which was first stated in a 1951 article by Ore [2], bears some similarities to the one derived in this article; both formulas involve sums over the partitions of sets of integers, for example. But there are significant differences between the two, and Wyn-jones' proof uses a completely different method than the one presented here. In addition, it is likely that one formula is more efficient than the other for some coefficients and less efficient for others. So it seems reasonable to present this alternative one as well. Some of the other results in this article were proved in ref. [1], but again the proofs here are by different methods.

## II. PRELIMINARY RESULTS: SYMMETRIES OF THE $C_{[a]}$ COEFFICIENTS

As shown in the examples in Section I, the determinants can be expanded as sums over products of the matrix elements:

$$\det [x_0, x_1, \dots, x_{N-1}] = \sum_{0 \leq a_0 \leq \dots \leq a_{N-1} \leq N-1} C_{a_0 \dots a_{N-1}} x_{a_0} \dots x_{a_{N-1}}. \quad (3a)$$

The sum can also be written in the form

$$\det [x_0, x_1, \dots, x_{N-1}] = \sum_{0 \leq M_0, \dots, M_{N-1} \leq N} C_{M_0 \dots M_{N-1}}^* x_0^{M_0} \dots x_{N-1}^{M_{N-1}}, \quad (3b)$$

where  $C_{M_0 \dots M_{N-1}}^* = C_{a_0 \dots a_{N-1}}$ ,  $M_0 + \dots + M_{N-1} = N$ , and  $M_m$  is the multiplicity of  $m$ , the number of times the integer  $m$  occurs in the index set  $[a_0, \dots, a_{N-1}]$ . Let  $\mathcal{S}_{[a_0, \dots, a_{N-1}]}$  be the set of permutations of the index set  $[a_0, \dots, a_{N-1}] : \sigma[a_0, \dots, a_{N-1}] \rightarrow [\sigma_0, \dots, \sigma_{N-1}]$ . From eq.(2), the coefficients in eq.(3a) are

$$C_{a_0 \dots a_{N-1}} = \sum_{\sigma \in \mathcal{S}_{[a_0, \dots, a_{N-1}]}} \omega^{\sigma_1 + 2\sigma_2 + \dots + (N-1)\sigma_{N-1}} \quad (4)$$

where the sum is over all elements of  $\mathcal{S}_{[a_0, \dots, a_{N-1}]}$ . One could of course use this expression to calculate these coefficients, but it is not very convenient, involving as it does a sum over a large number of complex numbers.

We will use the notations  $[a] \equiv [a_0, \dots, a_{N-1}]$ , ( $a_0 \leq a_1 \leq \dots \leq a_{N-1}$ ), and  $[\sigma] \equiv [\sigma_1, \dots, \sigma_{N-1}]$ , where  $\sigma$  is an arbitrary permutation of  $[a]$ . Let  $\Omega_{[a]}^{(k)}$  be the subset of  $\mathcal{S}_{[a]}$  defined by

$$\Omega_{[a]}^{(k)} = \{ \sigma \in \mathcal{S}_{[a]} \mid \sigma_1 + 2\sigma_2 + \dots + (N-1)\sigma_{N-1} \equiv k \pmod{N} \}$$

and let  $A_{[a]}^{(k)}$  be the number of elements in  $\Omega_{[a]}^{(k)}$ , which we will denote as  $\#\Omega_{[a]}^{(k)}$ . More generally, if  $S$  is a finite set, then  $\#S$  is the number of elements in  $S$ . The elements of  $\Omega_{[a]}^{(k)}$  will be referred to as “ $k$ -mod permutations” (of  $[a]$ ). Since  $\omega^{mN+k} = \omega^k$ , the sum in eq.(4) reduces to the form

$$C_{[a]} = A_{[a]}^{(0)} + A_{[a]}^{(1)}\omega + A_{[a]}^{(2)}\omega^2 + \dots + A_{[a]}^{(N-1)}\omega^{N-1} \quad (5)$$

with

$$A_{[a]}^{(0)} + A_{[a]}^{(1)} + \dots + A_{[a]}^{(N-1)} = \frac{N!}{M_0! \dots M_{N-1}!}. \quad (6)$$

When all the  $a$ 's are equal, ( $a_0 = a_1 = \dots = a_{N-1} = a$ ;  $M_a = N$ ),  $\mathcal{S}_{[a \dots a]}$  has just one element, so there is only one term in the sum in eq.(4). The corresponding coefficient is

$$C_{a \dots a} = e^{2\pi i a(1+2+\dots+N-1)/N} = e^{\pi i a(N-1)} = (-1)^{a(N-1)}.$$

In the rest of this article we will consider coefficients with more than one multiplicity.

We have  $\omega^N = 1$ ; more generally,  $(\omega^d)^N = 1$  for any integer  $d$ . If  $d \neq 0 \pmod{N}$ , the set  $\{\omega^d, \omega^{2d}, \dots, \omega^{(N-1)d}, \omega^{Nd} = 1\}$  consists of the zeros of the polynomial  $z^N - 1$ :

$$z^N - 1 = (z - \omega^d)(z - \omega^{2d}) \dots (z - \omega^{(N-1)d})(z - 1).$$

Expanding on the right, we have

$$z^N - 1 = z^N - (\omega^d + \omega^{2d} + \dots + \omega^{(N-1)d} + 1)z^{N-1} + \dots,$$

and since the coefficient of  $z^{N-1}$  on the left is zero we get the identity,

$$\sum_{q=1}^{N-1} \omega^{qd} = -1 + N\delta_{d,0}^N, \quad (7)$$

where the mod- $N$  Kronecker delta is defined as

$$\delta_{d,0}^N = \begin{cases} 1 & \text{if } d \equiv 0 \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

**Theorem 1**

$C_{[a]} = 0$  if  $a_0 + a_1 + \dots + a_{N-1} \not\equiv 0 \pmod{N}$ .

(This is Proposition (10.4.3) in ref.[1].)

**Proof:** Let  $[a]$  be such that

$$a_0 + a_1 + \dots + a_{N-1} \equiv X \pmod{N}, \quad X \neq 0,$$

and therefore, for any permutation  $[\sigma]$  of  $[a]$ ,

$$\sigma_0 + \sigma_1 + \dots + \sigma_{N-1} \equiv X \pmod{N}.$$

We can assume  $X$  to be positive; (if not, we can make the replacement  $X \rightarrow X' = N - |X|$ ). If we add the second equation repeatedly to the condition

$$\sigma_1 + 2\sigma_2 + \dots + (N-1)\sigma_{N-1} \equiv k \pmod{N},$$

for permutations in  $\Omega_{[a]}^{(k)}$ , we get

$$\begin{aligned} \sigma_0 + 2\sigma_1 + \dots + (N-1)\sigma_{N-2} &\equiv (k+X) \pmod{N}, \\ \sigma_{N-1} + 2\sigma_0 + \dots + (N-1)\sigma_{N-3} &\equiv (k+2X) \pmod{N}, \\ &\vdots \\ \sigma_2 + 2\sigma_3 + \dots + (N-1)\sigma_1 &\equiv (k+N-X) \pmod{N}. \end{aligned}$$

There is therefore, for each  $k$ , a sequence of one-to-one, onto mappings:

$$\Omega_{[a]}^{(k)} \rightarrow \Omega_{[a]}^{(k+X)} \rightarrow \Omega_{[a]}^{(k+2X)} \rightarrow \dots \rightarrow \Omega_{[a]}^{(k+N-X)} \rightarrow \Omega_{[a]}^{(k)}$$

induced by circular permutations of  $\sigma_0, \dots, \sigma_{N-1}$ . Accordingly,

$$A_{[a]}^{(k)} = A_{[a]}^{(k+X)} = A_{[a]}^{(k+2X)} = \dots = A_{[a]}^{(k+N-X)}, \quad \text{for } k = 0, 1, \dots, X-1.$$

If  $X = 1$ , or if  $X$  and  $N$  are relatively prime, then  $A_{[a]}^{(0)} = A_{[a]}^{(1)} = \dots = A_{[a]}^{(N-1)}$ , and the summation in eq.(5) for  $C_{[a]}$  equals zero as a result of the identity (7). If on the other hand  $\gcd(X, N) > 1$ , then  $MX \equiv 0 \pmod{N}$  for some  $M < N$ , and we have instead  $X$  sets of equalities:

$$\begin{aligned} A_{[a]}^{(0)} &= A_{[a]}^{(X)} = \dots = A_{[a]}^{((M-1)X)}, \\ A_{[a]}^{(1)} &= A_{[a]}^{(1+X)} = \dots = A_{[a]}^{(1+(M-1)X)}, \\ &\vdots \\ A_{[a]}^{(X-1)} &= A_{[a]}^{(2X-1)} = \dots = A_{[a]}^{(N-1)}. \end{aligned}$$

In this case, eq.(5) becomes

$$C_{[a]} = (A_{[a]}^{(0)} + A_{[a]}^{(1)}\omega + \dots + A_{[a]}^{(X-1)}\omega^{X-1})(1 + \omega^X + \omega^{2X} + \dots + \omega^{(M-1)X}).$$

But since  $\omega^X = e^{2\pi i X/N} = (e^{2\pi i/M})^x$  for some integer  $x \neq 0 \pmod{N}$ , the sum  $1 + \omega^X + \omega^{2X} + \dots + \omega^{(M-1)X}$  equals zero as a result of the identity corresponding to eq. (7) with the substitutions  $N \rightarrow M$  and  $\omega \rightarrow \omega_M = e^{2\pi i/M}$ .  $\triangle$

A number of corollaries follow from Theorem 1.

**Corollary 1** For even  $N$ ,  $C_{0123\dots N-1} = 0$ .

**Corollary 2** For odd  $N$ ,  $C_{a_0\dots a_{N-1}} = 0$  if the multiplicities are 2, 1,  $\dots$ , 1, 0.

**Corollary 3**  $C_{a\dots ab\dots b} = 0$  if the multiplicities  $M_a$  and  $M_b$  are relatively prime to  $N$ .

The proofs are straightforward and we omit them.

As noted, if  $[a_0, \dots, a_{N-1}]$  satisfies the condition,

$$a_0 + a_1 + \dots + a_{N-1} \equiv 0 \pmod{N}, \quad (8a)$$

then any permutation  $[\sigma]$  of  $[a]$  also satisfies it. Expressed in terms of the set of multiplicities,  $[M] = [M_0, M_1, \dots, M_{N-1}]$ ,  $0 \leq M_0, M_1, \dots, M_{N-1} \leq N$ , this condition becomes

$$0 \cdot M_0 + 1 \cdot M_1 + \dots + (N-1) \cdot M_{N-1} \equiv 0 \pmod{N}, \quad (8b)$$

subject to the restriction

$$M_0 + M_1 + \dots + M_{N-1} = N. \quad (8c)$$

Since we are only interested in non-zero coefficients, unless otherwise stated we will assume that all  $[a]$ 's and  $[\sigma]$ 's satisfy (8a), and all  $[M]$ 's satisfy (8b,c).

We define  $P$  to be the circular permutation operator,  $P(\sigma_q) = \sigma_{q+1}$ :

$$P[\sigma] = P[\sigma_0, \sigma_1, \dots, \sigma_{N-2}, \sigma_{N-1}] = [\sigma_1, \sigma_2, \dots, \sigma_{N-2}, \sigma_{N-1}, \sigma_0]. \quad (9)$$

Let  $\{\sigma\} = \{\sigma_0, \dots, \sigma_{N-1}\}$  denote the equivalence class under  $P$  of a  $k$ -mod permutation  $[\sigma]$ :

$$\{\sigma\} = \text{distinct elements of the set } \{ [\sigma], P[\sigma], \dots, P^{N-1}[\sigma] \}.$$

If  $[a]$ , with multiplicities  $M_0, M_1, \dots, M_{N-1}$ , is such that  $\gcd(M_0, M_1, \dots, M_{N-1}) = 1$ , each equivalence class of the permutations of  $[a]$  has  $N$  elements and each  $A_{[a]}^{(k)}$  is  $N$  times the total number of such equivalence classes. Therefore  $C_{[a]} \equiv 0 \pmod{N}$ . On the other hand, if the multiplicities have a common divisor  $d$  and if a permutation in  $\Omega_{[a]}^{(k)}$  takes the form  $[a_p a_q a_r \dots a_s \ a_p \dots a_s \ a_p a_q a_r \dots a_s]$  where the sequence  $a_p a_q a_r \dots a_s$  is repeated  $d$  times, then the equivalence class containing this permutation has only  $N/d$  distinct elements. So, from eq.(5), we have

**Proposition 1** *If  $\gcd(M_0, M_1, \dots, M_{N-1}) = d$ , then  $C_{a_0 \dots a_{N-1}} \equiv 0 \pmod{N/d}$ .*

For an integer  $n$  and a permutation  $[\sigma_0, \dots, \sigma_{N-1}]$  we define the operations

$$\begin{aligned} n + [\sigma_0, \dots, \sigma_{N-1}] &\equiv [n + \sigma_0, \dots, n + \sigma_{N-1}], \\ n \times [\sigma_0, \dots, \sigma_{N-1}] &\equiv [n\sigma_0, \dots, n\sigma_{N-1}], \end{aligned}$$

where addition and multiplication is modulo  $N$ . Further, we define  $|\sigma|$  to be the permutation  $[\sigma']$  of  $[\sigma_0, \sigma_1, \dots, \sigma_{N-1}]$  that puts it into ascending order:  $\sigma'_0 \leq \sigma'_1 \leq \dots \leq \sigma'_{N-1}$ .

**Proposition 2**

$$(A) \ C_{a_0 \dots a_{N-1}} = (-1)^{n(N-1)} C_{|n+[a_0, \dots, a_{N-1}]|}.$$

$$(B) \ C_{a_0 \dots a_{N-1}} = C_{|n \times [a_0 \dots a_{N-1}]|} \text{ for } n \text{ and } N \text{ relatively prime.}$$

(This is Proposition 10.5.5 in ref [1].)

**Proof:**

(A) Condition (8a) is invariant under the transformation  $\sigma_k \rightarrow (n + \sigma_k) \pmod{N}$  for  $n = 1, \dots, N-1$ , while  $\sigma_1 + 2\sigma_2 + \dots + (N-1)\sigma_{N-1}$  changes by

$$\Delta(\sigma_1 + 2\sigma_2 + \dots + (N-1)\sigma_{N-1}) = n \frac{(N-1)N}{2}.$$

This transformation will then give a factor of  $e^{2\pi i \Delta/N}$  to each term on the right side of eq.(4), so

$$C_{|n+a_0, \dots, n+a_{N-1}|} = (-1)^{n(N-1)} C_{a_0 \dots a_{N-1}}.$$

(B) The set  $\{1, \omega^n, \omega^{2n}, \dots, \omega^{(N-1)n}\}$  contains the same elements, up to order, as the set  $\{1, \omega, \omega^2, \dots, \omega^{N-1}\}$  when  $N$  and  $n$  are coprime. We can therefore make the replacement  $\omega \rightarrow \omega^n$  in all the terms and factors in the product on the right in eq.(2), since this amounts to just a re-ordering of the factors. Eq.(4) then becomes

$$C_{[a]} = \sum_{\sigma \in \mathcal{S}_{[a_0, \dots, a_{N-1}]}} (\omega^n)^{\sigma_1 + 2\sigma_2 + \dots + (N-1)\sigma_{N-1}} = \sum_{\sigma \in \mathcal{S}_{[a_0, \dots, a_{N-1}]}} \omega^{n\sigma_1 + 2n\sigma_2 + \dots + (N-1)n\sigma_{N-1}} = C_{[(n \times [a])].} \quad \triangle$$

In section IV below, we will use the two symmetry operations above to classify the coefficients, (or, equivalently, their multiplicative index sets), into “additive multiplets”, in which the coefficients are related by the additive symmetry, and into “super-multiplets”, in which they are related by the additive symmetry, the multiplicative symmetry, or a combination of both. We will use the notation  $\{C_{[a]}\}$  or  $\{C_{[M]}^*\}$  to represent the additive multiplet containing  $C_{[a]}$ , and  $(C_{[a]})$  or  $(C_{[M]}^*)$  to represent the corresponding super-multiplet. As a result of Proposition 2, coefficients in an additive multiplet or in a super-multiplet are equal, up to sign, and have the same multiplicities, up to order. The number of super-multiplets is thus equal to the number of coefficients that need to be calculated to solve for the determinant.

As pointed out by Wyn-jones, condition (8a) is a necessary but not sufficient condition for a coefficient to be non-zero; he gives two examples,  $C_{001335}$  and  $C_{0000111368}$ , which are zero despite satisfying (8a). A sufficient (but not necessary) criteria for “condition-(8)” coefficients to be zero is given in Section IIID, as a corollary to Theorem 3.

Wyn-jones did prove that, for  $N$  a prime number, condition (8a) is a sufficient condition for  $C_{[a]}$  to be non-zero. An alternate proof of this is given as a corollary of Theorem 2 below.

The Möbius function [3]  $\mu(n)$  is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n \text{ has one or more repeated prime factors;} \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct prime factors.} \end{cases}$$

Then

### Theorem 2

$$C_{[a]} = \sum_{d|N} \mu\left(\frac{N}{d}\right) A_{[a]}^{(d)}$$

where, in the sum over the divisors of  $N$ ,  $A_{[a]}^{(N)}$  is to be identified with  $A_{[a]}^{(0)}$ .

**Proof:** We define the mapping  $n \cdot [\sigma] \rightarrow [\sigma']$ , where  $n$  is an integer that is coprime to  $N$ , by  $\sigma_q \rightarrow \sigma'_q = \sigma_{nq \bmod N}$ , (or just  $\sigma_{nq}$ , with mod  $N$  multiplication understood). Under this map,

$$\sum_{q=0}^{N-1} q\sigma_q \rightarrow \sum_{q=0}^{N-1} q\sigma_{nq} = \sum_{q'=0}^{N-1} (n^{-1}q')\sigma_{q'} = n^{-1} \sum_{q'=0}^{N-1} q'\sigma_{q'}$$

where  $n^{-1}$  is the multiplicative inverse of  $n$ .  $[\sigma']$  is therefore an element of  $\Omega_{[a]}^{(n^{-1}k)}$  and  $n$  induces a mapping:

$$\Omega_{[a]}^{(k)} \xrightarrow{n} \Omega_{[a]}^{(n^{-1}k)}.$$

If  $n$  is coprime to  $N$  then so is  $n^{-1}$ , which induces the inverse map:

$$\Omega_{[a]}^{(k)} \xrightarrow{n^{-1}} \Omega_{[a]}^{(n^{-1}k)}.$$

This is therefore a one-to-one onto mapping between  $\Omega_{[a]}^{(k)}$  and  $\Omega_{[a]}^{(nk)}$ . These two sets have the same number of elements then, and  $A_{[a]}^{(k)} = A_{[a]}^{(nk)}$  for all  $n$  coprime to  $N$ . In particular,  $A_{[a]}^{(1)} = A_{[a]}^{(n)}$  for all  $n$  coprime to  $N$  and, if  $N$

is a prime number,  $A_{[a]}^{(1)} = A_{[a]}^{(2)} = \dots = A_{[a]}^{(N-1)}$ .

Let  $\{d_0, d_1, \dots, d_K\}$  be the set of divisors of  $N$ :  $1 = d_0 < d_1 < \dots < d_K = N$ . With the replacement  $A_{[a]}^{(0)} \rightarrow A_{[a]}^{(N)}$ , we separate the sum in eq.(5) in the manner below:

$$C_{[a]} = A_{[a]}^{(N)} + \sum_{\gcd(N,q)=1}^{N-1} A_{[a]}^{(q)} \omega^q + \sum_{\gcd(N,q)=d_1}^{N-d_1} A_{[a]}^{(q)} \omega^q + \dots + \sum_{\gcd(N,q)=d_{K-1}}^{N-d_{K-1}} A_{[a]}^{(q)} \omega^q.$$

In the sum corresponding to  $\gcd(N, q) = d_p$ , the summation variable  $q$  equals  $kd_p$  for some  $k$  coprime to  $N$ . By the relation above,  $A_{[a]}^{(kd_p)} = A_{[a]}^{(d_p)}$  for this sum. The  $A$  coefficients can therefore be brought outside:

$$C_{[a]} = A_{[a]}^{(N)} + \sum_{p=0}^{K-1} A_{[a]}^{(d_p)} \sum_{\gcd(N,k)=1}^{N/d_p-1} \omega^{kd_p} = \sum_{p=0}^{K-1} A_{[a]}^{(d_p)} \sum_{\gcd(N,k)=1}^{N/d_p-1} \omega^{kd_p}.$$

The result then follows by noting that the sum over  $k$

$$\sum_{\gcd(N,k)=1}^{N/d_p-1} \omega^{kd_p}$$

is the Möbius function  $\mu(N/d_p)[3]$ .  $\triangle$

The coefficient  $C_{[a]}$  can thus be expressed as a sum of integers, without the use of complex numbers. This expression is not very useful in calculating  $C_{[a]}$  since it still leaves us with the need to count the number of elements in the  $\Omega_{[a]}^{(k)}$  sets, although for fewer of these sets than appear in eq.(5).

Using this theorem though we can prove that  $C_{[a]}$  is non-zero when  $N$  is prime, provided of course that the index set  $[a]$  satisfies condition (8a). Changing back to the previous notation  $A_{[a]}^{(0)}$ , we have

**Corollary 4** For  $N$  prime,

$$C_{[a]} = \frac{N}{N-1} \left( A_{[a]}^{(0)} - \frac{(N-1)!}{M_0! \dots M_{N-1}!} \right) \neq 0.$$

**Proof:** The divisors of  $N$  consist of just 1 and  $N$ , so from Theorem 2

$$C_{[a]} = A_{[a]}^{(0)} - A_{[a]}^{(1)}.$$

We also have in this case that

$$\frac{N!}{M_0! \dots M_{N-1}!} = A_{[a]}^{(0)} + A_{[a]}^{(1)} + \dots + A_{[a]}^{(N-1)} = A_{[a]}^{(0)} + (N-1)A_{[a]}^{(1)}$$

from the proof of Theorem 2 and from eq.(6). The first equality follows from these relations. To show that  $C_{[a]} \neq 0$ ,  $C_{a \dots a} = (-1)^{(N-1)a} \neq 0$ , so we need consider just the cases where all the multiplicities are less than  $N$ . For these,  $A_{[a]}^{(0)} \propto N$ , so  $A_{[a]}^{(0)} = NB_{[a]}$  for some integer  $B_{[a]}$ . If  $C_{[a]} = 0$ , then

$$B_{[a]} = \frac{(N-1)!}{N M_0! \dots M_{N-1}!}.$$

$N$  must therefore divide  $(N-1)!$ . But this is a contradiction since  $N$  is prime and all the factors in  $(N-1)!$  are less than  $N$ .  $\triangle$

Corollary 5 in Section IIIB below, also a corollary to Theorem 3, extends the criteria for  $C_{[a]} \neq 0$ , i.e.,  $N$  being a prime number, to  $N$  not dividing  $\frac{(N-M_0-1)!}{M_1!}$ .

### III. DERIVATION OF A FORMULA FOR $C_{a_0 \dots a_{N-1}}$

#### A. Definitions and statement of the theorem

We will denote the set of partitions of the integer  $p$  by  $\mathcal{P}_p$ , with a particular partition consisting of  $j$  parts denoted by  $Z = (z_1, \dots, z_j)$  or, equivalently, by the set of multiplicities  $[k_1, \dots, k_p]$ :

$$\begin{aligned} p &= z_1 + \dots + z_j \\ &= k_1 + 2k_2 + \dots + pk_p; \quad k_1 + \dots + k_p = j. \end{aligned}$$

The set of partitions of a set of not-necessarily-distinct integers  $\{a, b, \dots, c\}$  will be denoted by  $\mathcal{P}\{ab \dots c\}$ . For a particular partition  $\Theta \in \mathcal{P}\{ab \dots c\}$ ,  $\Theta = (\theta_1) \dots (\theta_j)$ , where each  $\theta_k$  is a subset of  $\{a, b, \dots, c\}$ . We will express these subsets, for example, as  $\theta = abc$ , in contexts where there should be no confusion. As an illustration, the set of partitions of the set  $\{a, a, b, c\}$ , where  $a \neq b \neq c$ , is

$$\begin{aligned} \mathcal{P}\{aabc\} &= \left\{ (aabc), (aab)(c), (aac)(b), (abc)(a), (aa)(bc), (ab)(ac), \right. \\ &\quad \left. (aa)(b)(c), (ab)(a)(c), (ac)(a)(b), (bc)(a)(a), (a)(a)(b)(c) \right\}. \end{aligned}$$

For a partition  $\Theta$  and for any subset  $\theta$  of  $\{a, b, \dots, c\}$ ,  $\kappa_\theta$  will denote the multiplicity of  $\theta$  in the partition; for  $\theta \in \Theta$ ,  $m_a^{(\theta)}$  will denote the multiplicity of the element  $a$  in  $\theta$ . Finally, the sum of the elements of  $\theta$  will be denoted as the trace of  $\theta$ ,  $\text{Tr}(\theta)$ :

$$\text{Tr}(\theta) = \sum_{a \in \theta} a.$$

The map given by  $z_k = \#\theta_k$  sends the set partition  $\Theta = (\theta_1) \dots (\theta_j)$  to the integer partition  $Z = (z_1, \dots, z_j)$ . Two partitions  $\Theta$  and  $\Theta'$  in  $\mathcal{P}\{ab \dots c\}$  are equivalent iff they map to the same partition  $Z$ . In this case, each  $\theta_k$  and  $\theta'_k$  have the same number,  $z_k$ , of elements. The  $\Theta$  equivalence classes can then be labeled by the partition  $Z$ , and each  $\Theta \in \{Z\}$  for some  $Z$ .

We will also use the multinomial coefficient  $(p; k_1, \dots, k_p)^*$ , defined as [4]

$$(p; k_1, k_2, \dots, k_p)^* = \frac{p!}{1^{k_1} k_1! 2^{k_2} k_2! \dots p^{k_p} k_p!}, \quad p = k_1 + 2k_2 + \dots + pk_p,$$

and the Heaviside step function  $H[n]$ :

$$H[n] = \begin{cases} 1 & \text{if } n \geq 0, \\ 0 & \text{if } n < 0. \end{cases}$$

For convenience, we will write the coefficient  $C_{a_0 \dots a_{N-1}}$  as  $C_{0 \dots 0 1 \dots 1 A_1 \dots A_p A_{p+1}}$  with the 0's and 1's separated off, with  $A_1 = a_{M_0+M_1}$ ,  $A_{p+1} = a_{N-1}$ , and  $p = N - M_0 - M_1 - 1 \geq 0$ . The  $A$  indices lie between 2 and  $N - 1$ , with multiplicities  $M_2, M_3, \dots, M_{N-1}$ .

With these definitions, Theorem 3 is the statement below.

#### Theorem 3

*The coefficients with multiplicities  $0 \leq M_0, M_1, \dots, M_{N-1} \leq N - 1$  in the expansion (3a) are given by*

$$\begin{aligned}
C_{0 \dots 0 1 \dots 1 A_1 \dots A_p A_{p+1}} &= \delta_{0, M_1+2M_2+\dots+(N-1)M_{N-1}}^N (-1)^{N-M_0-1} N \\
&\times \left\{ \frac{(N-M_0-1)!}{M_1! M_2! \dots M_{N-1}!} + \frac{1}{M_{A_{p+1}}} \sum_{\Theta \in \mathcal{P}\{A_1 \dots A_p\}} \prod_{\theta} \frac{1}{\kappa_{\theta}!} \prod_{k=1}^j \frac{(z_k-1)!}{m_2^{(\theta_k)}! \dots m_{N-1}^{(\theta_k)}!} \right. \\
&\times \sum_{\mu=1}^j (-N)^{\mu} \sum_{\lambda_1, \dots, \lambda_j=0,1} \delta_{\mu, \lambda_1+\dots+\lambda_j} H \left[ M_1 - \sum_{t=1}^j \lambda_t X(\theta_t) \right] \\
&\times \left. \binom{N-M_0-1-\sum_{t=1}^j \lambda_t (X(\theta_t) + z_t)}{M_1 - \sum_{t=1}^j \lambda_t X(\theta_t)} \prod_{s=1}^j \binom{X(\theta_s) + z_s - 1}{z_s - 1}^{\lambda_s} \right\}
\end{aligned}$$

where  $j$  is the number of parts in the partition  $\Theta$ ,  $z_s = \#\theta_s$  is the number of elements in the part  $\theta_s$ , and

$$X(\theta_s) \equiv -\text{Tr}(\theta_s) \pmod{N}$$

such that  $0 \leq X(\theta_s) \leq N-1$ .

For each partition, the sum over the  $\lambda$ 's has  $2^j - 1$  terms. However, the presence of the step function in the expression means that, for a term to be non-zero, it must satisfy the condition

$$M_1 - \sum_{t=1}^j \lambda_t X(\theta_t) \geq 0.$$

As a consequence, for many coefficients, many if not most of the terms in the sum over the  $\lambda$ 's are zero.

As an example, and as a comparison to the method used in [1], we will calculate the coefficient  $C_{0011113788}$  using this theorem. In this case, the  $\kappa$ ,  $m$  and the  $M_{k>1}$  multiplicities all equal 1 except for  $M_{A_{p+1}}$ . We have then

$$\begin{aligned}
C_{0011113788} &= -10 \left\{ \frac{7!}{4!1!1!2!} + \frac{1}{2} \sum_{\Theta \in \mathcal{P}\{378\}} (z_1-1)! \dots (z_j-1)! \sum_{\mu=1}^j (-10)^{\mu} \sum_{\lambda_1, \dots, \lambda_j=0,1} \delta_{\mu, \lambda_1+\dots+\lambda_j} \right. \\
&\times H \left[ 4 - \sum_{t=1}^j \lambda_t X(\theta_t) \right] \binom{7 - \sum_{t=1}^j \lambda_t (X(\theta_t) + z_t)}{4 - \sum_{t=1}^j \lambda_t X(\theta_t)} \prod_{s=1}^j \binom{X(\theta_s) + z_s - 1}{z_s - 1}^{\lambda_s} \left. \right\}.
\end{aligned}$$

The partitions of the set  $\{3, 7, 8\}$  and the values of  $(z_1, \dots, z_j)$  and  $(\lambda_1, \dots, \lambda_j)$  for the non-zero terms are:

$$(378) : \quad z_1 = 3; \quad X(378) = 2; \quad \lambda_1 = 1;$$

$$(37)(8) : \quad (z_1, z_2) = (2, 1); \quad X(37) = 0, \quad X(8) = 2; \quad (\lambda_1, \lambda_2) = (1, 0), (0, 1), (1, 1);$$

$$(38)(7) : \quad (z_1, z_2) = (2, 1); \quad X(38) = 9, \quad X(7) = 3; \quad (\lambda_1, \lambda_2) = (0, 1);$$

$$(3)(7)(8) : \quad (z_1, z_2, z_3) = (1, 1, 1); \quad X(3) = 7, \quad X(7) = 3, \quad X(8) = 2; \quad (\lambda_1, \lambda_2, \lambda_3) = (0, 1, 0), (0, 0, 1).$$

Then

$$\begin{aligned}
C_{0011113788} &= -10 \left\{ 105 - 5 \left[ 2 \binom{2}{2} \binom{4}{2} + \binom{5}{4} \binom{1}{1} + \binom{4}{2} \binom{2}{0} + \binom{3}{1} \binom{3}{0} \right. \right. \\
&\quad \left. \left. + \binom{3}{1} \binom{3}{0} + \binom{4}{2} \binom{2}{0} \right] + (-10) \binom{2}{2} \binom{1}{1} \binom{2}{0} \right\} \\
&= -10 \{ 105 - 175 + 50 \} = 200,
\end{aligned}$$

in agreement with the value obtained in ref. [1].

By way of comparison, the method used by Wyn-jones involves partitions of the partial index set  $\{1, 1, 1, 1, 3, 7, 8, 8\}$  that are made up entirely of “null multisets”; i.e. (in my notation) subsets  $\theta$  of  $\{1, 1, 1, 1, 3, 7, 8, 8\}$  such that  $\text{Tr}(\theta) \equiv 0 \pmod{N}$ . Such a partition consisting of  $j$  subsets contributes to the  $N^j$  term in the expansion, unlike the calculation above, where each partition can contribute to several  $N^j$  terms. Although  $\mathcal{P}(11113788)$  contains many more partitions than  $\mathcal{P}(378)$ , (4,140 compared to 5), the calculation of this coefficient in ref. [1] involves only the 5 partitions,

$$(37)(118)(118), (1117)(1388), (37)(111188), (118)(11378), (11113788).$$

### B. Proof of Theorem 3

We will assume in the following that the indices of all coefficients considered satisfy conditions (8) and will omit writing out explicitly the mod- $N$  Kronecker delta  $\delta_{0, M_1 + \dots + (N-1)M_{N-1}}^N$  in the formulas for the coefficient.

Consider first the case  $M_A = 1$  and the coefficient  $C_{0\dots 01\dots 1A}$ . In this case we have  $M_0 + M_1 + 1 = N$  and  $0 \cdot M_0 + 1 \cdot M_1 + A \cdot 1 \equiv 0$ , so  $A = N - M_1$ .

With the freedom we have from the circular-permutation symmetry we can choose, when counting the number of elements in each set  $\Omega_{0\dots 01\dots 1(N-M_1)}^{(k)}$ , to consider only permutations of  $[0 \dots 01 \dots 1(N - M_1)]$  for which

$$\begin{aligned} \sigma_0 &= A = N - M_1, \\ \sigma_{p_1} &= \sigma_{p_2} = \dots = \sigma_{p_{M_1}} = 1, \quad 1 \leq p_1 < p_2 < \dots < p_{M_1} \leq N - 1, \\ \text{all other } \sigma_q &= 0. \end{aligned}$$

The number of elements in  $\Omega_{0\dots 01\dots 1(N-M_1)}^{(k)}$  is  $N$  times the number of such permutations that satisfy the condition

$$k \equiv 0 \cdot \sigma_0 + 1 \cdot \sigma_1 + \dots + (N - 1) \cdot \sigma_{N-1} \equiv p_1 + p_2 + \dots + p_{M_1}.$$

$A_{0\dots 01\dots 1(N-M_1)}^{(k)}$  therefore equals  $N$  times the number of partitions (mod  $N$ ) of  $k$  into exactly  $M_1$  distinct parts less than or equal to  $N - 1$ . We define  $Q(n; X, b)$  to be the restricted, mod- $N$  partition function

$$Q(n; X, b) = \#\{ (p_1, p_2, \dots, p_X) \mid p_1 + \dots + p_X \equiv n \pmod{N}; 1 \leq p_1 < \dots < p_X \leq b < N \};$$

i.e., the number of partitions mod  $N$  of  $n$  into  $X$ , distinct parts, with each part less than or equal to  $b$ . For  $n = k$ ,  $X = M_1$ , and  $b = N - 1$ , each such partition corresponds to a circular-permutation equivalence class  $\{N - M_1, \sigma_1, \dots, \sigma_{N-1}\}$ .  $C_{0\dots 01\dots 1(N-M_1)}$  is then, from eq.(5)

$$C_{0\dots 01\dots 1(N-M_1)} = \sum_{k=0}^{N-1} A_{0\dots 01\dots 1(N-M_1)}^{(k)} \omega^k = N \cdot \sum_{k=0}^{N-1} Q(k; M_1, N - 1) \omega^k.$$

By inspection, it can be seen that the partition function  $Q(n; X, N - 1)$  has the generating function

$$\sum_{X=0}^{N-1} \sum_{n=0}^{N-1} Q(n; X, N - 1) y^X \omega^n = \prod_{q=1}^{N-1} (1 + y\omega^q) = 1 + \dots + y^s (\omega^{p_1 + \dots + p_s} + \dots) + \dots.$$

Now referring back to eq.(2), the product over  $q$  in the equation above is, except for the missing  $q = 0$  factor, the determinant of an  $N \times N$  circulant matrix with elements  $1, k, 0, \dots, 0$ . Using this fact and evaluating the determinant, we find

$$\prod_{q=1}^{N-1} (1 + y\omega^q) = \frac{1}{1 + y} \begin{vmatrix} 1 & 0 & 0 & \dots & 0 & y \\ y & 1 & 0 & \dots & 0 & 0 \\ 0 & y & 1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & y & 1 & 0 \\ 0 & 0 & 0 & \dots & y & 1 \end{vmatrix}_{N \times N} = \sum_{m=0}^{N-1} (-y)^m.$$

Then

$$\sum_{n=0}^{N-1} Q(n; X, N-1) \omega^n = (-1)^X.$$

and our result for this coefficient is

$$C_{0 \dots 0 1 \dots 1 (N-M_1)} = (-1)^{M_1} N.$$

Next we consider the coefficient  $C_{0 \dots 0 1 \dots 1 A_1 A_2 \dots A_p A_{p+1}}$ , with  $p = N - M_0 - M_1 - 1$ . For given sets  $\{p_1, \dots, p_{M_1}\}$  and  $\{q_1, \dots, q_p\}$  of, respectively,  $M_1$  and  $p$  distinct integers between 1 and  $N-1$ , we assign the permutation sending  $[0 \dots 0 1 \dots 1 A_1 \dots A_{p+1}]$  to  $[\sigma_0 \dots \sigma_{N-1}]$  as follows:

$$\begin{aligned} \sigma_0 &= A_{p+1}; \\ \sigma_{p_1} &= \dots = \sigma_{p_{M_1}} = 1, \quad 1 \leq p_1 < \dots < p_{M_1} \leq N-1; \\ \sigma_{q_1} &= A_1, \quad \sigma_{q_2} = A_2, \quad \dots, \quad \sigma_{q_p} = A_p; \quad 1 \leq q_1, q_2, \dots, q_p \leq N-1, \quad q_i \neq q_j \text{ for all } i \neq j. \end{aligned}$$

The requirement that a particular permutation be an element of  $\Omega_{0 \dots 0 1 \dots 1 A_1 \dots A_{p+1}}^{(k)}$  is now

$$p_1 + \dots + p_{M_1} \equiv k - A_1 q_1 - A_2 q_2 - \dots - A_p q_p.$$

For the above set of distinct integers  $\{q_j\}$ ,  $1 \leq q_1, \dots, q_p \leq N-1$ , we define  $Q(n; X, b \mid q_1, \dots, q_p)$  to be the mod- $N$  restricted partition function,

$$\begin{aligned} Q(n; X, b \mid q_1, \dots, q_p) \\ = \# \left\{ (p_1, \dots, p_X) \mid p_1 + \dots + p_X \equiv n \pmod{N}; \quad 1 \leq p_1 < \dots < p_X \leq b; \quad p_i \neq q_j \text{ for all } i \text{ and } j \right\}. \end{aligned}$$

As before,  $Q$  is the number of partitions mod  $N$  of  $n$  into  $X$ , distinct parts less than or equal to  $b$ , but now with the additional restrictions that none of the parts are equal to any  $q_j$ . The set of all permutations in  $\Omega_{0 \dots 0 1 \dots 1 A_1 \dots A_{p+1}}^{(k)}$  is then the sum of  $N \cdot Q(k - A_1 q_1 - \dots - A_p q_p; M_1, N-1 \mid q_1, \dots, q_p)$  over all allowed values of the  $q$ 's, divided by the factorials of the multiplicities to avoid overcounting:

$$A_{0 \dots 0 1 \dots 1 A_1 \dots A_{p+1}}^{(k)} = \frac{N}{M_2! \dots M_{N-1}!} \sum_{1 \leq q_1, \dots, q_p \leq N-1} Q(k - A_1 q_1 - \dots - A_p q_p; M_1, N-1 \mid q_1, \dots, q_p) \Bigg|_{q_i \neq q_j}.$$

I.e. the sum is over all lattice points  $(q_1, \dots, q_p)$ ,  $q_i \in [1, N-1]$  such that no coordinates are equal. In the following, we will omit explicitly writing out the limits of the summation over the  $q$  variables, with the understanding that the limits will, unless otherwise indicated, always be from 1 to  $N-1$ .

[Note: As pointed out in a previous section, in the case where the multiplicities of an index set all have a common factor  $d$ , there are some equivalence classes that have only  $N/d$  distinct elements. The expression above is however valid in those cases as well; see Appendix B for a discussion of this issue. ]

Therefore, again using eq.(5),

$$\begin{aligned} C_{0 \dots 0 1 \dots 1 A_1 \dots A_{p+1}} &= \frac{N}{M_2! \dots M_{N-1}!} \sum_{k=0}^{N-1} \omega^k \sum_{q_i \neq q_j} Q(k - A_1 q_1 - \dots - A_p q_p; M_1, N-1 \mid q_1, \dots, q_p) \\ &= \frac{N}{M_2! \dots M_{N-1}!} \sum_{q_i \neq q_j} \omega^{A_1 q_1 + \dots + A_p q_p} \sum_{k'=0}^{N-1} \omega^{k'} Q(k'; M_1, N-1 \mid q_1, \dots, q_p) \end{aligned} \quad (10a)$$

where we've changed the summation index to  $k' = k - A_1 q_1 - \dots - A_p q_p$ ; since  $Q$  uses modular arithmetic, this does not change the limits of the sum over  $k$ .

The generating function for this restricted partition function can be obtained by omitting the factors  $(1 + y\omega^{q_j})$  for  $j = 1, \dots, p$  in the product in the previous section for  $Q(n; X, b)$ 's generating function or, equivalently, by dividing that product by these factors:

$$\sum_{X=0}^{N-1} y^X \sum_{n=0}^{N-1} Q(n; X, N-1 \mid q_1, \dots, q_p) \omega^n = \sum_{m=0}^{N-1} (-y)^m \frac{1}{(1 + y\omega^{q_1}) \cdots (1 + y\omega^{q_p})}.$$

### Lemma 1

Let  $\omega = e^{2\pi i/N}$  and let  $\{q_1, \dots, q_p \mid 1 \leq q_i \leq N-1\}$  be a set of  $p$  distinct integers. Then

$$\sum_{m=0}^{N-1} (-y)^m \prod_{s=1}^p \frac{1}{1 + y\omega^{q_s}} = \sum_{m=0}^{N-1-p} (-y)^m \sum_{0 \leq \kappa_1, \dots, \kappa_p \leq m} \omega^{\kappa_1 q_1 + \kappa_2 q_2 + \cdots + \kappa_p q_p} H[m - (\kappa_1 + \cdots + \kappa_p)].$$

For the proof of this lemma, and that of Lemma 2 below, see Appendices C and D, respectively.

Lemma 1 allows us to write eq.(10a) as,

$$C_{0 \dots 0 1 \dots 1 A_1 \dots A_{p+1}} = \frac{(-1)^{M_1} N}{M_2! \cdots M_{N-1}!} \sum_{q_i \neq q_l} \sum_{0 \leq \kappa_1, \dots, \kappa_p \leq M_1} \omega^{(\kappa_1 + A_1)q_1 + \cdots + (\kappa_p + A_p)q_p} H[M_1 - (\kappa_1 + \cdots + \kappa_p)]. \quad (10b)$$

We plan to use eq.(7) to perform the summations over the  $q$  variables in eq.(10b). This is complicated by the fact that the sum in (7) is over the complete range of  $q$ , from 1 to  $N-1$ , but each  $q$ -sum above, while having this range, is restricted by the condition that  $q_i \neq q_l$  for all  $i \neq l$ . We will therefore express the restricted,  $p$ -dimensional sum in eq.(10b) by a sum over unrestricted, lower-dimensional  $q$ -sums. An elementary example of this is

$$\sum_{x < y} h(x, y) = \frac{1}{2} \left\{ \sum_{x, y} h(x, y) - \sum_x h(x, x) \right\}$$

for a symmetric function  $h(x, y)$ . Lemma 2 below generalizes this example to higher dimensions.

We first define the  $p$ -dimensional vector  $\mathbf{q}_Z$ : For each part  $z_k$  of a partition  $Z$  of  $p$ , with  $j$  parts, the  $p$ -dimensional vector  $\mathbf{u}_k$  has components

$$u_k^i = \begin{cases} 1 & \text{if } z_1 + \cdots + z_k \leq i < z_1 + \cdots + z_{k+1}; \\ 0 & \text{otherwise.} \end{cases}$$

Then for variables  $(q_1, q_2, \dots, q_j)$ ,  $\mathbf{q}_Z$  is defined as

$$\mathbf{q}_Z = q_1 \mathbf{u}_1 + \cdots + q_j \mathbf{u}_j = (q_1, \dots, q_1, q_2, \dots, q_2, \dots, q_j, \dots, q_j).$$

$$\begin{array}{ccccccc} \longleftrightarrow & & \longleftrightarrow & & & & \longleftrightarrow \\ & z_1 & & z_2 & & \cdots & & z_j \end{array}$$

$\mathbf{q}_Z$  thus lies on a  $j$ -dimensional sublattice determined by the partition  $Z$ .

### Lemma 2

Let  $h(q_1, \dots, q_p) = h(\mathbf{q})$  be a completely symmetric function of the variables  $q_1, \dots, q_p$ . Then

$$\sum_{1 \leq q_1 < \cdots < q_p \leq M} h(\mathbf{q}) = \frac{1}{p!} \sum_{Z \in \mathcal{P}_p} (-1)^{p+j} (p; k_1, k_2, \dots, k_p)^* \sum_{1 \leq q_1, \dots, q_j \leq M} h(\mathbf{q}_Z).$$

The function  $f(q_1, \dots, q_p)$  that appears in eq.(10b) above,

$$f(q_1, \dots, q_p) = \omega^{A_1 q_1 + \dots + A_p q_p} \sum_{0 \leq \kappa_1, \dots, \kappa_p \leq M_1} \omega^{\kappa_1 q_1 + \dots + \kappa_p q_p} H[M_1 - (\kappa_1 + \dots + \kappa_p)],$$

is however not a symmetric function on account of the factor in front. To correct this we divide the sum over  $q_1, \dots, q_p$  in eq.(10b) into  $p!$  subregions:

$$\sum_{q_i \neq q_l} f(q_1, \dots, q_p) = \left\{ \sum_{q_1 < q_2 < \dots < q_p} + \sum_{q_2 < q_1 < \dots < q_p} + \dots + \sum_{q_p < \dots < q_1} \right\} f(q_1, \dots, q_p),$$

where the sums inside the brackets correspond to the  $p!$  orderings of  $(q_1, \dots, q_p)$ . Relabeling the summation indices, this is

$$\sum_{q_i \neq q_l} f(q_1, \dots, q_p) = \sum_{q_1 < \dots < q_p} \{ f(q_1, \dots, q_p) + \dots + f(q_p, \dots, q_1) \} = p! \sum_{q_1 < \dots < q_p} f_S(q_1, \dots, q_p)$$

where  $f_S(q_1, \dots, q_p)$  is the symmetrized function,

$$f_S(q_1, \dots, q_p) = \frac{1}{p!} \sum_{\sigma \in \mathcal{S}_p} f(q_{\sigma(1)}, \dots, q_{\sigma(p)}).$$

Now, for  $\sigma \in \mathcal{S}_p$ , define the  $p \times p$  matrix

$$(\mathcal{O}(\sigma))_{ik} = \delta_{\sigma(i), k}.$$

Then

$$f_S(\mathbf{q}_Z) = \frac{1}{p!} \sum_{\sigma \in \mathcal{S}_p} \omega^{\mathbf{A} \cdot \mathcal{O}(\sigma) \mathbf{q}_Z} \sum_{0 \leq \kappa_1, \dots, \kappa_p \leq M_1} \omega^{(\kappa_1 + \dots + \kappa_{z_1}) q_1 + \dots + (\kappa_{p-z_j} + \dots + \kappa_p) q_j} H[M_1 - (\kappa_1 + \dots + \kappa_p)]$$

where  $\mathbf{A} = (A_1, A_2, \dots, A_p)$ . Now defining  $X_s^{(\sigma)}$  as the integer in  $[0, N-1]$  such that

$$\begin{aligned} X_s^{(\sigma)} &\equiv -(\mathbf{A} \cdot \mathcal{O}(\sigma) \mathbf{u}_s) \bmod N \\ &\equiv -(A_{\sigma(d_s+1)} + \dots + A_{\sigma(d_s+z_s)}) \bmod N, \quad \text{with } d_s = z_1 + \dots + z_{s-1}, \end{aligned}$$

we have, applying Lemma 2,

$$\begin{aligned} \sum_{q_i \neq q_l} f(q_1, \dots, q_p) &= \sum_{Z \in \mathcal{P}_p} (-1)^{p+j} \frac{(p; k_1, k_2, \dots, k_p)^*}{p!} \sum_{q_1, \dots, q_j} \sum_{\sigma \in \mathcal{S}_p} \omega^{-(q_1 X_1^{(\sigma)} + \dots + q_j X_j^{(\sigma)})} \\ &\quad \times \sum_{0 \leq \kappa_1, \dots, \kappa_p \leq M_1} \omega^{(\kappa_1 + \dots + \kappa_{z_1}) q_1 + \dots + (\kappa_{p-z_j} + \dots + \kappa_p) q_j} H[M_1 - (\kappa_1 + \dots + \kappa_p)]. \end{aligned}$$

The  $p$  sums over the  $\kappa$  variables can be reduced to  $j$  sums over  $\alpha$  variables, defined as

$$\begin{aligned} \alpha_1 &= \kappa_1 + \dots + \kappa_{z_1}, \\ &\vdots \\ \alpha_k &= \kappa_{z_1 + \dots + z_{k-1} + 1} + \dots + \kappa_{z_1 + \dots + z_k}, \\ &\vdots \\ \alpha_j &= \kappa_{p-z_j} + \dots + \kappa_p; \\ \alpha_1 + \dots + \alpha_j &= \kappa_1 + \dots + \kappa_p. \end{aligned}$$

Then

$$\begin{aligned} &\sum_{0 \leq \kappa_1, \dots, \kappa_p \leq M_1} \omega^{(\kappa_1 + \dots + \kappa_{z_1}) q_1 + \dots + (\kappa_{p-z_j} + \dots + \kappa_p) q_j} H[M_1 - (\kappa_1 + \dots + \kappa_p)] \\ &= \sum_{0 \leq \alpha_1, \dots, \alpha_j \leq M_1} \omega^{\alpha_1 q_1 + \dots + \alpha_j q_j} H[M_1 - (\alpha_1 + \dots + \alpha_j)] \prod_{s=1}^j \binom{\alpha_s + z_s - 1}{z_s - 1}, \end{aligned}$$

where the multiplicative factor  $\binom{\alpha_s + z_s - 1}{z_s - 1}$  is the number of compositions of  $\alpha_s$  consisting of  $z_s$  or fewer parts.

Making this substitution, we can finally use eq.(7) to evaluate the sums over the  $q$ 's:

$$\begin{aligned} \sum_{q_i \neq q_j} f(q_1, \dots, q_p) &= (-1)^p \sum_{\sigma \in S_p} \sum_{Z \in \mathcal{P}_p} \frac{(p; k_1, k_2, \dots, k_p)^*}{p!} \sum_{0 \leq \alpha_1, \dots, \alpha_j \leq M_1} H[ M_1 - (\alpha_1 + \dots + \alpha_j) ] \\ &\quad \times \prod_{s=1}^j \binom{\alpha_s + z_s - 1}{z_s - 1} \prod_{s=1}^j (1 - N \delta_{\alpha_s, X_s^{(\sigma)}}). \end{aligned}$$

We expand the product  $\prod_{s=1}^j (1 - N \delta_{\alpha_s, X_s^{(\sigma)}})$  in powers of  $(-N)$  as

$$\prod_{s=1}^j (1 - N \delta_{\alpha_s, X_s^{(\sigma)}}) = \sum_{\lambda_1, \dots, \lambda_j = 0, 1} (-N)^{\lambda_1 + \dots + \lambda_j} (\delta_{\alpha_1, X_1^{(\sigma)}})^{\lambda_1} \dots (\delta_{\alpha_j, X_j^{(\sigma)}})^{\lambda_j}$$

and get, after rearranging the order of some of the sums,

$$\begin{aligned} \sum_{q_i \neq q_j} f(q_1, \dots, q_p) &= (-1)^p \sum_{\sigma \in S_p} \sum_{Z \in \mathcal{P}_p} \frac{(p; k_1, k_2, \dots, k_p)^*}{p!} \sum_{\lambda_1, \dots, \lambda_j = 0, 1} (-N)^{\lambda_1 + \dots + \lambda_j} \\ &\quad \times \sum_{0 \leq \alpha_1, \dots, \alpha_j \leq M_1} H[ M_1 - (\alpha_1 + \dots + \alpha_j) ] \prod_{s=1}^j \binom{\alpha_s + z_s - 1}{z_s - 1} \prod_{s=1}^j (\delta_{\alpha_s, X_s^{(\sigma)}})^{\lambda_s}. \end{aligned}$$

Now if, for fixed  $(\lambda_1, \dots, \lambda_j)$ , a particular  $\lambda_t$  is equal to 1, then that term will contain a factor of  $\delta_{\alpha_t, X_t^{(\sigma)}}$ , and we can replace the  $\alpha_t$  in the binomial coefficient by  $X_t^{(\sigma)}$ . The above equation can therefore be written as

$$\begin{aligned} \sum_{q_i \neq q_j} f(q_1, \dots, q_p) &= (-1)^p \sum_{\sigma \in S_p} \sum_{Z \in \mathcal{P}_p} \frac{(p; k_1, k_2, \dots, k_p)^*}{p!} \sum_{\lambda_1, \dots, \lambda_j = 0, 1} (-N)^{\lambda_1 + \dots + \lambda_j} \\ &\quad \times \sum_{0 \leq \alpha_1, \dots, \alpha_j \leq M_1} H[M_1 - (\alpha_1 + \dots + \alpha_j)] \\ &\quad \times \prod_{s=1}^j \left[ \binom{\alpha_s + z_s - 1}{z_s - 1}^{1 - \lambda_s} \binom{X_s^{(\sigma)} + z_s - 1}{z_s - 1}^{\lambda_s} (\delta_{\alpha_s, X_s^{(\sigma)}})^{\lambda_s} \right]. \end{aligned}$$

Again take  $(\lambda_1, \dots, \lambda_j)$  as fixed and assume that a particular  $\lambda_t$  is equal to 1. The summand in the sum over the corresponding  $\alpha_t$  is then  $H[M - (\alpha_1 + \dots + \alpha_j)] \delta_{\alpha_t, X_t^{(\sigma)}}$  times factors independent of  $\alpha_t$ . We can thus replace  $\alpha_t$  in the step function by  $X_t^{(\sigma)}$ . The sum over  $\alpha_t$  is from 0 to  $M_1$ , and the sum over  $\delta_{\alpha_t, X_t^{(\sigma)}}$  will be zero if  $X_t^{(\sigma)} > M_1$ . But, with the above replacement, the step function is also zero in this case. So the ‘‘zero condition’’ is enforced by  $H$  and we can simply make the replacement:  $\sum_{\alpha_t} H[M - (\alpha_1 + \dots + \alpha_j)] \delta_{\alpha_t, X_t^{(\sigma)}} \rightarrow H[M - (\alpha_1 + \dots + \alpha_j)]|_{\alpha_t = X_t^{(\sigma)}}$ .

After performing the summations over all the  $\alpha_s$ 's for which  $\lambda_s = 1$ , we are left with the sums over the  $\alpha$ 's for which  $\lambda_s = 0$ . For  $\lambda_t = 0$ ,

$$\begin{aligned} \sum_{\alpha_t=0}^{M_1} \binom{\alpha_t + z_t - 1}{z_t - 1} H \left[ M_1 - \alpha_t - \sum_{q=1}^{j'} (1 - \lambda_q) \alpha_q - \sum_{q=1}^j \lambda_q X_q^{(\sigma)} \right] &= \sum_{\alpha_t=0}^{M'_1} \binom{\alpha_t + z_t - 1}{z_t - 1} \\ &= \binom{M'_1 + (1 - \lambda_t) z_t}{(1 - \lambda_t) z_t} H[M'_1], \end{aligned}$$

where the prime on the first sum over  $q$  means that the sum is over all  $q \neq t$ , and where

$$M'_1 = M_1 - \sum_{q=1}^{j'} (1 - \lambda_q) \alpha_q - \sum_{q=1}^j \lambda_q X_q^{(\sigma)}.$$

Summing again for  $\lambda_s = 0$ , with  $M_1'' = M_1' - \alpha_s$ , we have

$$\begin{aligned} & \sum_{\alpha_s=0}^{M_1} \binom{\alpha_s + z_s - 1}{z_s - 1} \binom{M_1'' - \alpha_s + (1 - \lambda_t)z_t}{(1 - \lambda_t)z_t} H[M_1'' - \alpha_s] \\ &= \sum_{\alpha_s=0}^{M_1''} \binom{\alpha_s + z_s - 1}{z_s - 1} \binom{M_1'' - \alpha_s + (1 - \lambda_t)z_t}{(1 - \lambda_t)z_t} \\ &= \binom{M_1'' + (1 - \lambda_t)z_t + (1 - \lambda_s)z_s}{(1 - \lambda_t)z_t + (1 - \lambda_s)z_s} H[M_1''], \end{aligned}$$

using the identity

$$\sum_{m=0}^n \binom{m}{l} \binom{n-m}{k-l} = \binom{n+1}{k+1}, \quad 0 \leq l \leq k \leq n.$$

Continuing, the effect of summing over these  $\alpha_t$ 's is to remove a  $(-\alpha)$  from the step function and the binomial coefficient, and to add  $(1 - \lambda_t)z_t$  to both the upper and lower elements of the binomial coefficient. So, after summing over all  $\alpha$  variables, we are left with the factor

$$H \left[ M_1 - \sum_{t=1}^j \lambda_t X_t^{(\sigma)} \right] \binom{M_1 + \sum_{t=1}^j (1 - \lambda_t)z_t - \sum_{t=1}^j \lambda_t X_t^{(\sigma)}}{\sum_{t=1}^j (1 - \lambda_t)z_t} \prod_{s=1}^j \binom{X_s^{(\sigma)} + z_s - 1}{z_s - 1}^{\lambda_s}.$$

Putting this into the equation above for the sum over  $f$  and then that into (10b), and then making the replacement  $\sum (1 - \lambda_t)z_t = p - \sum \lambda_t z_t$ , we arrive at

$$\begin{aligned} C_{0 \dots 0 1 \dots 1 A_1 \dots A_p A_{p+1}} &= \frac{(-1)^{N-M_0-1} N}{M_2! \dots M_{N-1}!} \sum_{\sigma \in S_p} \sum_{Z \in \mathcal{P}_p} \frac{(p; k_1, k_2, \dots, k_p)^*}{p!} \sum_{\lambda_1, \dots, \lambda_j=0,1} (-N)^{\lambda_1 + \dots + \lambda_j} \\ &\quad \times H \left[ M_1 - \sum_{t=1}^j \lambda_t X_t^{(\sigma)} \right] \binom{N - M_0 - 1 - \sum_{s=1}^j \lambda_s (X_s^{(\sigma)} + z_s)}{M_1 - \sum \lambda_s X_s^{(\sigma)}} \prod_{s=1}^j \binom{X_s^{(\sigma)} + z_s - 1}{z_s - 1}^{\lambda_s}. \end{aligned}$$

For the terms for which  $\lambda_1 = \dots = \lambda_j = 0$ , the sum over  $Z \in \mathcal{P}_p$ , and then trivially the sum over  $\sigma \in S_p$ , can be done using the identity

$$\sum_{Z \in \mathcal{P}_p} (p; k_1, k_2, \dots, k_p)^* \equiv \sum_{j=0}^p \sum_{k_1, \dots, k_p} \delta_{k_1+2k_2+\dots+pk_p, p} \delta_{k_1+k_2+\dots+k_p, j} (p; k_1, k_2, \dots, k_p)^* = p!;$$

(this is eq.(E4) in Appendix E). Then

$$\begin{aligned} C_{0 \dots 0 1 \dots 1 A_1 \dots A_p A_{p+1}} &= \frac{(-1)^{N-M_0-1} N}{M_2! \dots M_{N-1}!} \left\{ \frac{(N - M_0 - 1)!}{M_1!} + \sum_{Z \in \mathcal{P}_p} \sum_{\sigma \in S_p} \frac{(p; k_1, k_2, \dots, k_p)^*}{p!} \right. \\ &\quad \times \sum_{\mu=1}^j (-N)^\mu \sum_{\lambda_1, \dots, \lambda_j=0,1} \delta_{\mu, \lambda_1 + \dots + \lambda_j} H \left[ M_1 - \sum_{t=1}^j \lambda_t X_t^{(\sigma)} \right] \\ &\quad \left. \times \binom{N - M_0 - 1 - \sum_{s=1}^j \lambda_s (X_s^{(\sigma)} + z_s)}{M_1 - \sum \lambda_s X_s^{(\sigma)}} \prod_{s=1}^j \binom{X_s^{(\sigma)} + z_s - 1}{z_s - 1}^{\lambda_s} \right\}. \end{aligned} \quad (10c)$$

We now note that in the sum over  $S_p$ , the set of  $X_s^{(\sigma)}$ 's is invariant for all  $\sigma$  that map a partition onto itself,  $\sigma(\Theta) = \Theta$ , since in this case  $\sigma$  either just reorders the elements in each  $\theta \in \Theta$  or interchanges the order of the  $\theta$ 's,

and neither of these operations change the set  $\{X_s^{(\sigma)}|_{s=1,\dots,j}\}$ . The sum over  $S_p$  and  $\mathcal{P}_p$  can then be replaced by a sum over the set of partitions of the index set  $\{12\dots p\}$  by multiplying each term by  $z_1!z_2!\dots z_j! k_1!k_2!\dots k_p!$ :

$$\begin{aligned} \sum_{Z \in \mathcal{P}_p} \sum_{\sigma \in S_p} &\rightarrow \sum_{\Theta \in \mathcal{P}\{12\dots p\}} ; \\ \frac{(p; k_1, k_2, \dots, k_p)^*}{p!} &\rightarrow \frac{(p; k_1, k_2, \dots, k_p)^*}{(p; z_1, \dots, z_j)} \times k_1! \dots k_p! = \frac{z_1! \dots z_j!}{1^{k_1} 2^{k_2} \dots p^{k_p}} = (z_1 - 1)! \dots (z_j - 1)!. \end{aligned}$$

With this substitution,

$$X_s^{(\sigma)} \rightarrow X(\theta_s) \equiv - \left( \sum_{q=n_1^{(s)}}^{n_{z_s}^{(s)}} A_q \right) \pmod{N}, \text{ for } \theta_s = \{n_1^{(s)}, \dots, n_{z_s}^{(s)}\},$$

and we get

$$\begin{aligned} C_{0\dots 0 1\dots 1 A_1 \dots A_p A_{p+1}} &= \frac{(-1)^{N-M_0-1} N}{M_2! \dots M_{N-1}!} \left\{ \frac{(N-M_0-1)!}{M_1!} + \sum_{\Theta \in \mathcal{P}\{12\dots p\}} (z_1 - 1)! \dots (z_j - 1)! \right. \\ &\times \sum_{\mu=1}^j (-N)^\mu \sum_{\lambda_1, \dots, \lambda_j=0,1} \delta_{\mu, \lambda_1 + \dots + \lambda_j} H \left[ M_1 - \sum_{t=1}^j \lambda_t X(\theta_t) \right] \\ &\times \left( \frac{N - M_0 - 1 - \sum_{t=1}^j \lambda_t (X(\theta_t) + z_t)}{M_1 - \sum_{t=1}^j \lambda_t X(\theta_t)} \right) \prod_{s=1}^j \binom{X(\theta_s) + z_s - 1}{z_s - 1}^{\lambda_s} \left. \right\}. \quad (10d) \end{aligned}$$

Expression (10d) above is an alternative expression for the coefficient to that stated in the theorem. The final expression is derived from (10d) by the replacement of the sum over  $\mathcal{P}\{12\dots p\}$  by a sum over  $\mathcal{P}\{A_1 \dots A_p\}$ , (which is a smaller set when the coefficients  $A_1, \dots, A_p$  are not all distinct), and then noting that if, for example,  $A_1 = A_2$ , a partition of the form  $(A_1 \dots)(A_2 \dots) \dots (\dots)$  will contribute the same to the sum as the partition obtained by interchanging 1 and 2. So, replacing the sum over  $\mathcal{P}\{12\dots p\}$  by a sum over the smaller set  $\mathcal{P}\{A_1 \dots A_p\}$  requires that the sum be multiplied by a factor of 2, or, more generally, by the factor  $M_{A_1}! \dots M_{A_p}!$ . However, for partitions of the form  $(A_1 A_2 \dots) \dots (\dots)$  or of the form  $(A_1 B \dots C)(A_2 B \dots C) \dots (\dots)$ , interchanging the indices 1 and 2 does not generate additional partitions if  $A_1 = A_2$ . To correct for this overcounting, the sum then needs to be divided by the factorials of the  $\kappa_\theta$  and the  $m_a^{(\theta)}$  multiplicities.  $\triangle$

**Corollary 5** *If  $a_0 + a_1 + \dots + a_{N-1} \equiv 0 \pmod{N}$ , then  $C_{[a]} = 0$  only if  $N$  divides  $\frac{(N-M_0-1)!}{M_1!}$*

The proof follows by noting that every term inside the brackets in expression (10d) is an integer, and that all terms other than the first one are proportional to  $N$ .

### C. Coefficients of the form $C_{0\dots 0 1\dots 1 a\dots ab}$

In the special case where  $A_1 = A_2 = \dots = A_p = a$  the expression for the coefficients simplifies considerably. In this case, in eq.(10c),  $X_s^{(\sigma)} \rightarrow X_{z_s}^{(\sigma)} \equiv (-az_s) \pmod{N}$ , independent of the permutation  $\sigma$ . The sum over  $\mathcal{S}_p$  can then be done and, after some manipulation, so can the sum over  $\mathcal{P}_p$ .

Summing over the permutations we have, for  $M_b = 0, 1$ ,

$$C_{0\dots 01\dots 1a\dots ab} = \frac{(-1)^{N-M_0-1}N}{M_a!M_b!} \left\{ \frac{(N-M_0-1)!}{M_1!} + \sum_{Z \in \mathcal{P}_p} (p; k_1, k_2, \dots, k_p)^* \right. \\ \times \sum_{\mu=1}^j (-N)^\mu \sum_{\lambda_1, \dots, \lambda_j=0,1} \delta_{\mu, \lambda_1 + \dots + \lambda_j} H \left[ M_1 - \sum_{t=1}^j \lambda_t X_{z_t} \right] \\ \times \left. \left( \begin{matrix} N-M_0-1 - \sum_{t=1}^j \lambda_t (X_{z_t} + z_t) \\ M_1 - \sum_{t=1}^j \lambda_t X_{z_t} \end{matrix} \right) \prod_{s=1}^j \binom{X_{z_s} + z_s - 1}{z_s - 1}^{\lambda_s} \right\}.$$

We now replace the sum over  $(\lambda_1, \dots, \lambda_j)$  by a sum over  $(\beta_1, \dots, \beta_p)$ , which we define as follows: Let the part  $z_n$  have multiplicity  $k (= k_{z_n})$ . Then, (after a possible relabeling of the parts),  $z_n = z_{n+1} = \dots = z_{n+k-1}$ . For fixed  $(\lambda_1, \dots, \lambda_j)$ , let  $\beta$  equal the number of non-zero  $\lambda$ 's in the subset  $(\lambda_n, \dots, \lambda_{n+k-1})$ ; i.e.,  $\beta = \sum_{t=n}^{n+k-1} \lambda_t$ .  $\beta_{z_n}$  is thus defined for each unique part  $z_n$ . This definition can be extended to all integers  $q \in [1, \dots, p]$  by setting  $\beta_q = 0$  if  $k_q = 0$ .

For  $q \in [1, \dots, p]$ ,  $q$  and  $X_q$  will each appear  $\beta_q$  times in the sums over  $t$ , and the binomial coefficient  $\binom{X_q + q - 1}{q - 1}$  will occur  $\beta_q$  times in the product over  $s$ . For a given  $(\beta_1, \dots, \beta_p)$ , there are  $\binom{k_1}{\beta_1} \dots \binom{k_p}{\beta_p}$  different  $(\lambda_1, \dots, \lambda_j)$ 's that correspond to it. Replacing the sums over  $(\lambda_1, \dots, \lambda_j)$  in the above expression by sums over  $(\beta_1, \dots, \beta_p)$ ,

$$\sum_{t=1}^j \lambda_t z_t, \quad \sum_{t=1}^j \lambda_t X_{z_t} \rightarrow \sum_{t=1}^p t \beta_t, \quad \sum_{t=1}^p \beta_t X_t,$$

and including this factor gives us

$$C_{0\dots 01\dots 1a\dots ab} = (-1)^{N-M_0-1} \frac{N}{M_a!M_b!} \left\{ \frac{(N-M_0-1)!}{M_1!} + \sum_{j=0}^p \sum_{k_1, \dots, k_p} (p; k_1, k_2, \dots, k_p)^* \right. \\ \times \sum_{\mu=1}^j (-N)^\mu \sum_{\beta_1, \dots, \beta_p} \delta_{\mu, \beta_1 + \dots + \beta_p} \binom{k_1}{\beta_1} \dots \binom{k_p}{\beta_p} H \left[ M_1 - \sum_{t=1}^p \beta_t X_t \right] \\ \times \left. \left( \begin{matrix} N-M_0-1 - \sum_{t=1}^p \beta_t (X_t + t) \\ M_1 - \sum_{t=1}^p \beta_t X_t \end{matrix} \right) \prod_{s=1}^p \binom{X_s + s - 1}{s - 1}^{\beta_s} \right\}.$$

We now interchange the sums over the  $k$ 's and the  $\beta$ 's and perform the sum over the  $k$ 's by using the lemma below:

**Lemma 3** For  $p \geq \beta_1 + 2\beta_2 + \dots + p\beta_p$ ,

$$\sum_{j=0}^p \sum_{k_1, \dots, k_p} \binom{k_1}{\beta_1} \dots \binom{k_p}{\beta_p} (p; k_1, k_2, \dots, k_p)^* = \frac{p!}{1^{\beta_1} \beta_1! 2^{\beta_2} \beta_2! \dots p^{\beta_p} \beta_p!}.$$

(For the proof, see Appendix E.) Then our result is

$$\begin{aligned}
\left. \begin{array}{l} C_{0\dots 01\dots 1 a\dots ab} \\ C_{0\dots 01\dots 1 ba\dots a} \end{array} \right\} &= (-1)^{N-M_0-1} \frac{N}{M_a + M_b} \binom{M_a + M_b}{M_a} \left\{ \binom{N - M_0 - 1}{M_1} \right. \\
&+ \sum_{\mu=1}^p (-N)^\mu \sum_{0 \leq \beta_1, \dots, \beta_p \leq \mu} \delta_{\mu, \beta_1 + \dots + \beta_p} H \left[ M_1 - \sum_{t=1}^p \beta_t X_t \right] \\
&\times \binom{N - M_0 - 1 - \sum_{t=1}^p \beta_t (X_t + t)}{M_1 - \sum_{t=1}^p \beta_t X_t} \prod_{s=1}^p \frac{1}{s^{\beta_s} \beta_s!} \binom{X_s + s - 1}{s - 1}^{\beta_s} \left. \right\}; \\
X_s &\equiv -sa \pmod{N} \text{ such that } 0 \leq X_s \leq N - 1; \\
p &= N - M_0 - M_1 - 1.
\end{aligned} \tag{10e}$$

for  $M_b = 0$  or 1.

As indicated, this expression is valid for  $b < a$  as well as for  $b \geq a$ . The reason is that, in the proof of Theorem 3, in summing over the equivalence classes we have the freedom to “hide” any particular index in the  $\sigma_0$  position, where it’s value has no effect, (other than on the requirement that it and the other indices satisfy condition (8a)). We can therefore sum over equivalence classes of the form  $[b, \sigma_1, \dots, \sigma_{N-1}]$  for  $b$  either less than or greater than  $a$ .

#### D. Coefficients of the form $C_{0\dots 01\dots 1 A_1 A_2 A_3}$

As previously noted, the two coefficients  $C_{001335}$  and  $C_{0000111368}$ , corresponding to  $N = 6$  and 10 respectively, are zero despite satisfying condition (8a). Generalizing, we consider coefficients of the form  $C_{0\dots 01\dots 1 A_1 A_2 A_3}$ , with  $M_0, M_1 \geq 1$  and  $2 \leq A_1 \leq A_2 \leq A_3 \leq N - 1$ ; i.e., coefficients with non-zero  $M_0$  and  $M_1$  that contain 3 and only 3 indices greater than 1. We are interested in the question of when coefficients of this form equal zero even if they satisfy conditions (8). From (8b,c) we have

$$\begin{aligned}
M_1 + A_1 + A_2 + A_3 &\equiv 0 \pmod{N}, \\
M_0 + M_1 + 3 &= N,
\end{aligned}$$

and from eq.(10d),

$$\begin{aligned}
C_{0\dots 01\dots 1 A_1 A_2 A_3} &\propto \left\{ (M_1 + 2)(M_1 + 1) - NH [ M_1 - X(A_1 A_2) ] (X(A_1 A_2) + 1) \right. \\
&\quad \left. - N ( H [ M_1 - X(A_1) ] ( M_1 + 1 - X(A_1) ) + (A_1 \rightarrow A_2) ) + N^2 H [ M_1 - X(A_1) - X(A_2) ] \right\}.
\end{aligned} \tag{11}$$

For  $C_{0\dots 01\dots 1 A_1 A_2 A_3}$  to be zero,  $N$  must divide  $(M_1 + 2)(M_1 + 1)$  for  $M_1 \leq N - 4$ . If  $N$  divides  $(M_1 + 2)(M_1 + 1)$ , then it also divides  $(M_0 + 2)(M_0 + 1)$ :

$$\frac{(M_1 + 2)(M_1 + 1)}{N} = \frac{(N - M_0 - 1)(N - M_0 - 2)}{N} = N - 2M_0 - 3 + \frac{(M_0 + 2)(M_0 + 1)}{N}.$$

The  $X$  functions in eq.(11) are:

$$\begin{aligned}
X(A_{1,2}) &= N - A_{1,2}, \\
X(A_1 A_2) &\equiv -(A_1 + A_2) \equiv M_1 + A_3 = \begin{cases} M_1 + A_3 & \text{if } A_3 < N - M_1; \\ M_1 + A_3 - N & \text{if } A_3 \geq N - M_1. \end{cases}
\end{aligned}$$

If  $A_3$  (and therefore  $A_1$  and  $A_2$ ) is less than  $N - M_1$ , all of the Heaviside step functions in eq.(11) are zero and the coefficient is therefore non-zero. So we will assume that  $A_3 \geq N - M_1$ . That leaves only 4 possibilities:

- (1)  $N - M_1 \leq A_3$  and  $A_1 \leq A_2 < N - M_1$ ;
- (2)  $N - M_1 \leq A_2 \leq A_3$ ,  $A_1 < N - M_1$ , and  $A_1 + A_2 < 2N - M_1$ ;
- (3)  $N - M_1 \leq A_1 \leq A_2 \leq A_3$  and  $A_1 + A_2 < 2N - M_1$ ;
- (4)  $N - M_1 \leq A_1 \leq A_2 \leq A_3$  and  $A_1 + A_2 \geq 2N - M_1$ .

Now let  $\psi$  be the symmetry operator defined as multiplication of an index set  $[a]$  by  $(N - 1)$  followed by addition of 1. Under this operator,

$$M_0 \rightarrow M'_0 = M_1, \quad M_1 \rightarrow M'_1 = M_0, \quad A_1 \rightarrow A'_1 = N - A_3 + 1, \quad A_2 \rightarrow A'_2 = N - A_2 + 1, \quad A_3 \rightarrow A'_3 = N - A_1 + 1.$$

Thus, if  $N - M_1 \leq A_1 \leq A_2 \leq A_3$ , then  $A'_1 \leq A'_2 \leq A'_3 < N - M'_1$ . From the discussion above and from Proposition 2, in this case,

$$C_{0\dots 01\dots 1A_1A_2A_3} = (-1)^{N-1} C_{\psi*[0\dots 01\dots 1A_1A_2A_3]} \neq 0,$$

and we need to consider only cases (1) and (2). Setting the right side of eq.(11) to zero in these two cases gives us the corollary to Theorem 3:

**Corollary 6** For  $N = M_0 + M_1 + 3$  with  $M_0, M_1 \geq 1$ , the coefficient  $C_{0\dots 01\dots 1A_1A_2A_3}$  satisfies conditions (8) but is zero if  $N$  divides  $(M_1 + 2)(M_1 + 1)$  and either

$$\begin{aligned} &A_1 \leq A_2 < N - M_1, \quad A_1 + A_2 = N + 1 - \frac{(M_1 + 2)(M_1 + 1)}{N}, \quad \text{and } A_3 = M_0 + 2 + \frac{(M_1 + 2)(M_1 + 1)}{N}, \\ \text{or} & \\ &N - M_1 \leq A_2 \leq A_3, \quad A_2 + A_3 = N + 1 + \frac{(M_0 + 2)(M_0 + 1)}{N}, \quad \text{and } A_1 = M_0 + 2 - \frac{(M_0 + 2)(M_0 + 1)}{N}. \end{aligned}$$

By Proposition 2, all coefficients that are related to these zero coefficients by an additive- and/or a multiplicative-symmetry operator also equal zero.

For integers  $a$  and  $q$ ,  $N$  in the corollary has the form  $N = q(q + 1)/a$ , with values 6, 10, 12, 14, 15, 18,  $\dots$ , corresponding to sequence A139799 in OEIS [5].

As an example, we take  $N = 6$ . In this case  $N$  divides  $(M_1 + 2)(M_1 + 1) = 6, 12, 30, 42, \dots$ , but only the first two integers satisfy the condition  $N \geq M_1 + 4$ . From the corollary,

$$\begin{aligned} C_{001245}, C_{011235} & (= -C_{\psi*[001245]}), \\ C_{001335}, C_{011244} & (= -C_{\psi*[001335]}) \end{aligned}$$

are zero coefficients. Including all the coefficients generated from these by the Proposition-2 symmetries, there are a total of 12 zero coefficients.

As a second example,  $N = 10$ .  $N$  divides  $(M_1 + 2)(M_1 + 1) = 20, 30$ , and the corollary gives us the zero coefficients

$$\begin{aligned} C_{0000111377}, C_{0001111448} & (= -C_{\psi*[0000111377]}), \\ C_{0000111368}, C_{0001111358} & (= -C_{\psi*[0000111368]}), \\ C_{0000111458}, C_{0001111367} & (= -C_{\psi*[0000111458]}). \end{aligned}$$

Including the Proposition-2-operator-generated coefficients, there are 120 zero coefficients of this form.

#### IV. ADDITIONAL RESULTS: MULTIPLET STRUCTURE

Having a formula to calculate any coefficient in the expansion (3a/b), it is of interest to determine how many calculations one needs to perform to solve for the complete determinant. The number of solutions to eq.(8b,c) is given by the expression [5, 6],

$$F(N) = \frac{1}{2N} \sum_{d|N} \phi\left(\frac{N}{d}\right) \binom{2d}{d} = (\text{A003239})_{N+1} \text{ in OEIS.} \quad (12)$$

where  $\phi$  is the Euler totient function [7]. Then, except for coefficients that equal zero as a result of satisfying the criteria of Corollary 6 and any other ‘‘accidental zeros’’, eq. (12) gives the number of terms in the expansions (3a/b).

As discussed above following Proposition 2, coefficients can be grouped into additive multiplets, related by the additive symmetry, and into super-multiplets, related by the additive symmetry and/or the multiplicative symmetry. For example, for  $N = 5$ , the coefficients can be formed into the table:

$$\begin{aligned} 5 &: \{C_{50000}^*\}_5 \\ 311 &: \{C_{31001}^*\}_5, \{C_{30110}^*\}_5 \\ 221 &: \{C_{12002}^*\}_5, \{C_{10220}^*\}_5 \\ 11111 &: \{C_{11111}^*\}_1. \end{aligned}$$

The set of coefficients consist of six additive multiplets  $\{C_{[M]}^*\}_n$ , (where  $n$  is the number of elements), and four super-multiplets. (In this example there is only one super-multiplet for each of the allowed partitions of 5, but that is not generally the case; see the table for the  $N = 8$  coefficients in Appendix G.)

The nonnegative integers less than  $N$  form a group under addition modulo  $N$ , which we will denote as  $(\mathbf{Z}/N\mathbf{Z})^+$ . The group  $(\mathbf{Z}/N\mathbf{Z})^+$  is of order  $N$ , and is a cyclic group, so all its subgroups are cyclic. The set of integers less than and relatively prime to  $N$  is the multiplicative group of integers modulo  $N$ , denoted as  $(\mathbf{Z}/N\mathbf{Z})^\times$ . This group has order  $\phi(N)$ . The direct product of these two groups,

$$H_N \equiv (\mathbf{Z}/N\mathbf{Z})^+ \times (\mathbf{Z}/N\mathbf{Z})^\times,$$

is thus of order  $N\phi(N)$ .

If the index set  $[M]$  is such that  $a * [M] = [M]$  for all elements  $a$  in a group, we say that  $[M]$  is invariant under the action of that group. To find the numbers of additive multiplets and of super-multiplets, we will need to count the number of index sets that are invariant under the various subgroups of  $(\mathbf{Z}/N\mathbf{Z})^+$  and of  $H_N$ , respectively.

### A. The number of additive multiplets

From eq.(3b) the determinants are expressible in the form

$$\det [x_0, x_1, \dots, x_{N-1}] = \sum_{0 \leq M_0, \dots, M_{N-1} \leq N} C_{M_0 \dots M_{N-1}}^* x_0^{M_0} \dots x_{N-1}^{M_{N-1}}.$$

For a given coefficient  $C_{M_0 \dots M_{N-1}}^*$ , the elements of the  $n$ -element additive multiplet  $\{C_{M_0 M_1 \dots M_{N-1}}^*\}_n$  are obtained by circularly permuting the index set  $[M_0 M_1 \dots M_{N-1}]$ :

$$\{C_{M_0 M_1 \dots M_{N-1}}^*\}_n = \left\{ C_{M_0 M_1 \dots M_{N-1}}^*, C_{P[M_0 M_1 \dots M_{N-1}]}^*, C_{P^2[M_0 M_1 \dots M_{N-1}]}^*, \dots, C_{P^{n-1}[M_0 M_1 \dots M_{N-1}]}^* \right\}$$

where  $P$  is the circular permutation operator defined in eq.(9). We define the symbol  $[\{C_{M_0 M_1 \dots M_{N-1}}^*\}_n]$  as equal to the value of the coefficient that labels the additive multiplet:

$$[\{C_{M_0 M_1 \dots M_{N-1}}^*\}_n] = C_{M_0 M_1 \dots M_{N-1}}^*. \quad (13)$$

Then, as a sum over these multiplets, the above expansion can be written as

$$\det [x_0, x_1, \dots, x_{N-1}] = \sum_{\text{Multiplets}} [\{C_{M_0 M_1 \dots M_{N-1}}^*\}_n] \left[ x_0^{M_0} x_1^{M_1} \dots x_{N-1}^{M_{N-1}} + (-1)^{N-1} x_1^{M_0} x_2^{M_1} \dots x_0^{M_{N-1}} \right. \\ \left. + \dots + (-1)^{(N-1)(n-1)} x_{n-1}^{M_0} x_n^{M_1} \dots x_{n-2}^{M_{N-1}} \right]. \quad (14)$$

**Proposition 3** For a given  $N$ , the number  $g_N(n)$  of  $n$ -element additive multiplets  $\{C_{[M]}^*\}_n$  is

$$g_N(n) = \frac{1 + (-1)^{N-n}}{4n^2} \sum_{d|n} (-1)^{n+d} \mu\left(\frac{n}{d}\right) \binom{2d}{d}$$

**Proof:**

Operating on an index set  $[M]$ , the additive group  $(\mathbf{Z}/N\mathbf{Z})^+$  generates a set with  $N$  not-necessarily-distinct elements:

$$(\mathbf{Z}/N\mathbf{Z})^+ * [M] = \{ P^{-a}[M] \mid 0 \leq a \leq N-1 \}.$$

Let  $\{M\}_n = \{ [M], P[M], P^2[M], \dots, P^{n-1}[M] \}$  be an  $n$ -element additive multiplet. Then  $n$  divides  $N$  and, for  $d = N/n$ , each element in the multiplet is invariant under the action of any element of the subgroup  $S_d^+ \subseteq \mathbf{Z}/N\mathbf{Z}^+$ . One of the index sets in  $\{M\}$ , which, without loss of generality we can take to be the ‘‘labeling’’ set  $[M]$ , must then have the form

$$[M_0, M_1, \dots, M_{N-1}] = [M_0, M_1, \dots, M_{n-1}, M_0, M_1, \dots, M_{n-1}, \dots, M_0, M_1, \dots, M_{n-1}],$$

in which the subset  $\{M_0, M_1, \dots, M_{n-1}\}$  is sequentially repeated  $d$  times. We have then:

$$\begin{aligned} \sum_{q=0}^{N-1} M_q &= (N/n) \sum_{q=0}^{n-1} M_q, \\ \sum_{q=0}^{N-1} qM_q &= \sum_{q=0}^{n-1} M_q [ q + (q+n) + (q+2n) + \dots + (q+n(N/n-1)) ] \\ &= \sum_{q=0}^{n-1} M_q \left[ q \frac{N}{n} + n \frac{(N/n-1)(N/n)}{2} \right] \\ &= \frac{N}{n} \sum_{q=0}^{n-1} qM_q + \frac{N}{n} \frac{N-n}{2} \sum_{q=0}^{n-1} M_q. \end{aligned}$$

Conditions (8b,c) then require that

$$\sum_{q=0}^{n-1} M_q = n, \tag{15a}$$

and

$$\sum_{q=0}^{n-1} qM_q + \frac{(N-n)n}{2} \equiv 0 \pmod{n}. \tag{15b}$$

The second of these equations can only be satisfied if  $N-n$  is even. (If  $N-n$  is odd,  $n$  must then be even in order that the right side to be an integer. But then  $N$  is odd, which contradicts the requirement that  $n$  divide  $N$ .) In this case then,

$$\sum_{q=0}^{n-1} qM_q \equiv 0 \pmod{n}, \quad N-n \text{ even}. \tag{15c}$$

From eq.(12), the number of solutions  $[M_0, M_1, \dots, M_{N-1}]$  that satisfy both eqs.(8a,b) and (15a,c) is therefore

$$F_N(n) = \frac{1 + (-1)^{N-n}}{4n} \sum_{d|n} \phi\left(\frac{n}{d}\right) \binom{2d}{d},$$

and  $n$ -member multiplets  $\{M\}_n$  and  $\{C_{[M]}^*\}_n$  exist only if  $n$  is a same-parity divisor of  $N$ .

The number of solutions  $F_N(n)$  is a sum over all coefficients that lie in  $d$ -element multiplets for all  $d$  that divides  $n$  and is of the same parity as  $n$  and  $N$ . Let  $l(d)$  denote the total number of coefficients  $C_{[M]}$  for which  $d$  is the smallest integer such that  $P^d[M] = [M]$ . Then the number of  $n$ -element additive multiplets,  $g_N(n)$ , is  $l(n)/n$ , and

$$F_N(n) = \sum_{d|n} \frac{1 + (-1)^{n-d}}{2} l(d) \equiv \sum_{d|n} l(d),$$

where the notation  $d||n$  means that the sum is over all same-parity divisors of  $n$ . It is straightforward to show that

$$l(n) = \sum_{d||n} F_N(d) \mu\left(\frac{n}{d}\right),$$

by considering separately the  $n$  odd and the  $n$  even cases and using Möbius inversion. Then

$$g_N(n) = \frac{1 + (-1)^{N-n}}{4n^2} \sum_{d||n} \sum_{q|d} \frac{n}{d} \mu\left(\frac{n}{d}\right) \phi\left(\frac{d}{q}\right) \binom{2q}{q}.$$

It remains to prove the identity

$$\sum_{d||n} \sum_{q|d} \frac{n}{d} \mu\left(\frac{n}{d}\right) \phi\left(\frac{d}{q}\right) f(q) = \sum_{b|n} (-1)^{n+b} \mu\left(\frac{n}{b}\right) f(b) \quad (16)$$

where  $f(q)$  is an arbitrary function of  $q$ . In evaluating the right-hand side of this equation, we express  $n$  as  $n = 2^k m$ , where  $m$  is an odd integer and  $k \geq 0$ . The divisors of  $n$  are of the form  $b = 2^l a$ , where  $a$  divides  $m$  and is therefore odd, and  $l \leq k$ . Then

$$\text{RHS} = \sum_{b|n} (-1)^{n+b} \mu\left(\frac{n}{b}\right) f(b) = \sum_{a|m} \mu\left(\frac{m}{a}\right) \begin{cases} f(a), & k=0; \\ f(2a) + f(a), & k=1; \\ f(2^k a) - f(2^{k-1} a), & k \geq 2. \end{cases} \quad (17)$$

We now consider the expression on the left side of eq.(16), and first take  $n$  to be odd, ( $k=0$ ). Then all of its divisors are also odd, and we can make the replacement  $d||n \rightarrow d|n$ . For a given divisor  $b$ , we set  $d = bc$ ,  $c \leq n/b$ , and isolate the  $q = b$  term in the sum over  $q$ :

$$\begin{aligned} \text{LHS}_{n \text{ odd}} &= \sum_{d|n} \sum_{q|d} \frac{n}{d} \mu\left(\frac{n}{d}\right) \phi\left(\frac{d}{q}\right) f(q) = \cdots + f(b) \sum_{c|(n/b)} \frac{n/b}{c} \mu\left(\frac{n/b}{c}\right) \phi(c) + \cdots \\ &= \cdots + f(b) \mu\left(\frac{n}{b}\right) + \cdots = \cdots + \sum_{a=b|m=n} \mu\left(\frac{m}{a}\right) f(a) + \cdots, \end{aligned}$$

where we've used the identity

$$\sum_{c|m} \frac{m}{c} \mu\left(\frac{m}{c}\right) \phi(c) = \mu(m),$$

which follows from Möbius inversion of

$$\phi(m) = m \sum_{d|m} \frac{\mu(d)}{d}. \quad (18)$$

Eq.(16) is therefore valid for  $n$  odd.

For even  $n$ , we again set  $n = 2^k m$ , with  $k \geq 1$  and  $m$  odd. Its same-parity divisors are  $d = 2^l a$ , with  $a|m$  and  $1 \leq l \leq k$ . Setting  $q = 2^s p$ , with  $0 \leq s \leq l$  and  $p$  an odd integer that divides  $a$ , the left-hand side of (16) is

$$\text{LHS}_{n \text{ even}} = \sum_{a|m} \sum_{l=1}^k \sum_{p|a} \sum_{s=0}^l \frac{2^{k-l} m}{a} \mu\left(\frac{2^{k-l} m}{a}\right) \phi\left(\frac{2^{l-s} a}{p}\right) f(2^s p).$$

But since  $\mu(2^K m) = 0$  for any  $K > 1$ , the only non-zero terms in the sum over  $d||n$  are those for which  $l = k$ ,  $k-1 > 0$ ;

$$\text{LHS}_{n \text{ even}} = \sum_{a|m} \sum_{p|a} \left[ \sum_{s=0}^{k-1} \frac{m}{a} \mu\left(\frac{m}{a}\right) \phi\left(\frac{2^{k-s} a}{p}\right) f(2^s p) + (1 - \delta_{1,k}) \sum_{s=0}^{k-1} \frac{2m}{a} \mu\left(\frac{2m}{a}\right) \phi\left(\frac{2^{k-1-s} a}{p}\right) f(2^s p) \right].$$

The two identities

$$\mu(2x) = -\mu(x), \quad \phi(2^K x) = 2^{K-1}\phi(x) \quad \text{for } K > 0,$$

where  $x$  is in both cases an odd positive integer, can be used to take the Möbius and Euler functions outside the parentheses:

$$\text{LHS}_{n \text{ even}} = \sum_{a|m} \frac{m}{a} \mu\left(\frac{m}{a}\right) \sum_{p|a} \phi\left(\frac{a}{p}\right) \left[ f(2^k p) + \sum_{s=0}^{k-1} 2^{k-s-1} f(2^s p) - (1 - \delta_{1,k}) \left( 2f(2^{k-1} p) + \sum_{s=0}^{k-2} 2^{k-s-1} f(2^s p) \right) \right].$$

The two sums from  $s = 0$  to  $k - 2$  cancel and we have

$$\text{LHS}_{n \text{ even}} = \sum_{a|m} \frac{m}{a} \mu\left(\frac{m}{a}\right) \sum_{p|a} \phi\left(\frac{a}{p}\right) [ f(2^k p) + (2\delta_{1,k} - 1)f(2^{k-1} p) ].$$

Now applying the ‘‘odd- $n$ ’’ result,

$$\sum_{d|n} \sum_{q|d} \frac{n}{d} \mu\left(\frac{n}{d}\right) \phi\left(\frac{d}{q}\right) f(q) = \sum_{b|n} \mu\left(\frac{n}{b}\right) f(b),$$

to the last expression, it becomes

$$\text{LHS}_{n \text{ even}} = \sum_{a|m} \mu\left(\frac{m}{a}\right) [f(2^k a) + (2\delta_{1,k} - 1)f(2^{k-1} a)],$$

in agreement with the 2nd and 3rd lines in eq.(17).  $\triangle$

Note that the expression

$$\frac{1}{2n^2} \sum_{d|n} (-1)^{n+d} \mu\left(\frac{n}{d}\right) \binom{2d}{d}$$

corresponds to the sequence A131868 in OEIS. So  $g_N(n) = (\text{A131868})_{n||N}$ , and the total number of additive multiplets,  $n_{AM}$ , is

$$\sum_{n||N} g_N(n) = \sum_{n||N} (\text{A131868})_n.$$

## B. The number of super-multiplets

To find the number of super-multiplets, we consider the direct product:

$$H_N = (\mathbf{Z}/N\mathbf{Z})^+ \times (\mathbf{Z}/N\mathbf{Z})^\times.$$

We will denote an element of  $H_N$  either with boldface,  $\mathbf{a}$ , or as the pair  $(a, b)$ . Group multiplication of two elements of  $H_N$  is defined by

$$(a, b) \cdot (c, d) = (a + c, bd); \quad a, c \in (\mathbf{Z}/N\mathbf{Z})^+, \quad b, d \in (\mathbf{Z}/N\mathbf{Z})^\times.$$

In this formalism, the symmetry operations in Proposition 2 are expressed as the action of an element  $(a, b)$  on an index set  $[M]$ , which we will denote as  $(a, b) * [M]$ :

$$(a, b) * [M] = [M_{N-a}, M_{b^{-1}-a}, M_{2b^{-1}-a}, \dots, M_{(N-1)b^{-1}-a}].$$

In particular, if  $b = 1$ ,

$$(a, 1) * [M] = P^{-a}[M].$$

A direct-product group  $G_1 \times G_2$  is cyclic iff  $G_1$  and  $G_2$  are both cyclic and have orders that are relatively prime to each other. By Gauss' Theorem,  $(\mathbf{Z}/N\mathbf{Z})^\times$  is a cyclic group iff  $N$  is of the form 2, 4,  $p^n$  or  $2p^n$  where  $p$  is an odd prime and  $n \geq 1$  [8]. Consequently  $H_N$  is cyclic only for the case where  $N$  is a prime number.

We will denote an order- $d$  subgroup of  $(\mathbf{Z}/N\mathbf{Z})^+$  as  $S_d^+$ ; since  $(\mathbf{Z}/N\mathbf{Z})^+$  is a cyclic group, all its subgroups are cyclic, and each  $d$  corresponds to only one subgroup. Likewise, we will denote order- $d$  subgroups of  $(\mathbf{Z}/N\mathbf{Z})^\times$  as  $S_{d;\alpha}^\times$ , and those of  $H_N$  as  $S_{d;\alpha}$ , where the  $\alpha$  indices are used to distinguish same- $d$  subgroups from one another.

Operating on an index set  $[M]$ ,  $H_N$  generates a set with  $N\phi(N)$  elements:

$$H_N * [M] = \{ (a, b) * [M] \mid 0 \leq a \leq N-1; 1 \leq b \leq N-1, \gcd(b, N) = 1 \}.$$

If  $[M]$  is a member of an  $m$ -element super-multiplet, then  $[M]$  is invariant under the action of an order- $(N\phi(N)/m)$  subgroup of  $H_N$ . If  $[M]$  is invariant under the action of all elements of a subgroup  $S_{d;\alpha}$ , then  $\mathbf{c}_k * [M] = \mathbf{c}_j * [M]$  for all elements  $\mathbf{c}_a, \mathbf{c}_b$  of a coset  $\{\mathbf{c}_k\}$  of  $S_{d;\alpha}$ . If the elements of the set  $\{ [M], \mathbf{c}_1 * [M], \dots, \mathbf{c}_{m-1} * [M] \}$  are all distinct, where  $m = N\phi(N)/d$  and  $\mathbf{c}_k$  is any element of the coset  $\{\mathbf{c}_k\}$ , then this set is an  $m$ -element super-multiplet.

For  $S_{d;\alpha} \subseteq H_N$  we define  $K(S_{d;\alpha})$  to be the number of index sets  $[M]$  that are invariant under  $S_{d;\alpha}$  and in addition satisfy eqs.(8b,c):

$$K(S_{d;\alpha}) = \# \left\{ [M] \mid S_{d;\alpha} * [M] = [M], S_{d;\alpha} \subseteq H_N; \sum_k k M_k \equiv 0 \pmod{N}; \sum_k M_k = N \right\}.$$

If  $[M]$  is invariant under the action of the subgroup  $S_{d;\alpha}$ , it is also invariant under all subgroups of  $S_{d;\alpha}$ . It may also be invariant under larger subgroups of  $H_N$  that contain  $S_{d;\alpha}$ ; i.e., it may have a higher degree of symmetry than that required to be invariant under just  $S_{d;\alpha}$ .  $K(S_{d;\alpha})$  therefore counts these higher-symmetry sets as well. We define  $L(S_{q;\beta})$  as the number of index sets satisfying (8b,c) for which  $S_{q;\beta}$  is the largest subgroup that they are invariant under. Then

$$K(S_{d;\alpha}) = \sum_{S_{q;\beta} \supseteq S_{d;\alpha}} L(S_{q;\beta}).$$

Let

$$n = \frac{N\phi(N)}{q}.$$

Then  $L(S_q)/n$  is the number of  $n$ -element super-multiplets, and the total number,  $n_{SM}$ , is

$$n_{SM} = \sum_{S_q \subseteq H_N} \frac{qL(S_q)}{N\phi(N)}. \quad (19)$$

We can formally solve this equation by expressing the previous equation in matrix form:

$$\mathbf{K} = \mathbf{A}\mathbf{L}, \quad \mathbf{L} = \mathbf{A}^{-1}\mathbf{K},$$

$$n_{SM} = \frac{1}{N\phi(N)} \mathbf{q} \cdot \mathbf{L}$$

where the elements of the matrix  $\mathbf{A}$  are either 1 or 0 depending on whether or not a particular subgroup  $S_{q;\beta}$  contains the subgroup  $S_{d;\alpha}$  or not, and the rest of the notation should be clear from the context.

Because of the more complicated structure of the multiplicative group, calculating the number of super-multiplets is more involved than for the additive multiplets. Expression (19) however simplifies in the cases where  $N = p$  or  $2p$ , where  $p$  is an odd prime number. In Appendix A, we calculate the number of super-multiplets for these two cases.

Our results are:

$$n_{SM}(N = p) = \frac{1}{p(p-1)} \left\{ \frac{1}{2p} \binom{2p}{p} + \frac{p^2-1}{p} + p \sum_{m|(p-1)}^{m < p-1} \phi\left(\frac{p-1}{m}\right) \binom{2m}{m} \right\}; \quad (20a)$$

$$n_{SM}(N = 2p) = \frac{1}{2p(p-1)} \left\{ \frac{1}{4p} \binom{4p}{2p} + \frac{4p^2+1}{4p} \binom{2p}{p} + \frac{2(p^2-1)}{p} \right. \\ \left. + p \sum_{m|(p-1)}^{m < (p-1)/2} \phi\left(\frac{p-1}{m}\right) \left[ \left( \frac{p+4m+1}{2m+1} - \frac{1-(-1)^{\frac{p-1}{m}}}{4} \right) \binom{4m}{2m} + \frac{1-(-1)^{\frac{p-1}{m}}}{4} \binom{2m}{m} \right] \right\}. \quad (20b)$$

Using eq.(12) and another series expression in OEIS,

$$\frac{1}{2} \sum_{m|n} \phi\left(\frac{n}{m}\right) \binom{2m}{m} = (\text{A081875})_n,$$

expression (20a) becomes

$$n_{SM}(N = p) = \frac{1}{p(p-1)} \left\{ (\text{A003239})_{p+1} + 2p(\text{A081875})_{p-1} + p-1 - p \binom{2p-2}{p-1} \right\}.$$

## V. CONCLUSION

The expression for  $C_{a_0 \dots a_{N-1}}$  in Theorem 3 constitutes in principle a complete solution to the problem of calculating the determinant of an arbitrary circulant matrix. This expression has some similarities to that of Wyn-jones, as well as some significant differences, but the proofs of the two expressions are along completely different lines.

However, Wyn-jones's method does require that one find all of the null subsets/multisets contained in a generally much larger set than the set of partitions employed in Theorem 3. And since, in applying Theorem 3, one deals only with partitions of sets that do not include any  $a = 1$  indices, it may be that it is more efficient than the method of Wyn-jones for coefficients with  $M_1 \gg 1$ .

In many cases, the number of terms in the expression for a particular coefficient can be decreased by using one or both of the symmetry operations in Proposition 2 to equate the coefficient (up to a sign) to another coefficient. This can often be done in one of two ways: By either making the new multiplicities  $M'_0$  and/or  $M'_1$  as large as possible, thereby making the set of partitions to be summed over smaller, or by setting  $M'_1$  to 0, making the constraint  $M_1 - \sum \lambda_s X(\theta_s) \geq 0$  more restrictive.

To illustrate this second method, let  $C_{a_0 \dots a_{N-1}}$  be such that the integer  $n$  is not in the index set. Then if we add  $(N+1-n)$  to  $[a_0, \dots, a_{N-1}]$ , the resulting index set will not contain 1, so  $M'_1 = 0$ . We can always do this except for the index set  $[0, 1, 2, \dots, N-1]$ .

Consider the previous example,  $C_{0011113788}$ . The missing indices are  $n = 2, 4, 5, 6, 9$ , so  $N+1-n = 9, 7, 6, 5, 2$ , and

$$C_{0011113788} = -C_{0000267799} = -C_{0455778888} = +C_{3446677779} = -C_{2335566668} = +C_{0022333359}.$$

Of these,  $C_{0000267799}$  is the easiest to compute as there are only two partitions, (677)(29) and (677)(2)(9), that contribute to the sum.

This method of setting  $M_1$  to zero has some similarity to Wyn-jones' method, in its reliance on the null subsets/multisets. The contributing partitions of the set  $\{267799\}$  would be in that case the trivial partition, (267799), and the partition (677)(299).

For  $C_{0011113788}$ , the number of non-zero terms in the sum can actually be reduced further by instead multiplying the index set by  $(N - 1)$  and then adding 1. This has the effect of interchanging  $M_0$  and  $M_1$ :

$$[0011113788]^{\times 9} \rightarrow [0022379999]^{+1} \rightarrow [0000113348]$$

In this case the only contribution to the sum comes from the trivial partition (334), with  $X(334) = 0$ . All other partitions correspond to values of  $X(\theta)$  that are greater than  $M'_1 = 2$  and therefore do not contribute.

### Appendix A: Derivation of equations (20)

We will use the notation

$$\langle g|g^d = 1 \rangle \equiv \{ 1, g, g^2, \dots, g^{d-1} \},$$

or the short-hand notation  $\langle g|g^d \rangle$ , to denote a general order- $d$  cyclic group generated by  $g$ .

Throughout this section,  $p$  will denote a prime number greater than 2.

**Proposition 4** For  $N = p$  or  $N = 2p$ ,

$$n_{SM} = \frac{1}{N\phi(N)} \sum_{S_d \subseteq H_N} \phi(d) K(S_d).$$

The proof of this proposition uses the following lemma:

**Lemma 4 :** Let  $f$  and  $g$  be mappings from the set of subgroups  $\{S_d\}$  of a cyclic group  $G$  into the set of nonnegative integers  $\mathbf{Z}$  such that

$$f(S_d) = \sum_{S_q \supseteq S_d} g(S_q).$$

Then

$$g(S_q) = \sum_{S_d \supseteq S_q} \mu\left(\frac{d}{q}\right) f(S_d).$$

In both equations, the sums on the right are over all subgroups that contain the subgroup on the left.

**Proof of Lemma 4:** Let  $G$  be of order  $k$ . Since  $G$  is cyclic, for each integer  $d$  that divides  $k$  there is one and only one subgroup of order  $d$  in  $G$ . Then we can make the replacements  $f(S_d) \rightarrow f(d)$ ,  $g(S_q) \rightarrow g(q)$ , where  $f(d)$ ,  $g(d)$  are defined for all integers that divide  $k$ . Then the condition in the lemma becomes

$$f(d)_{d|k} = \sum_{d|q|k} g(q)$$

where the sum is over all  $q$  that divides  $k$  and is divisible by  $d$ . For a given  $d$  and  $q$  that divide  $k$  let

$$n = \frac{k}{q}, \quad m = \frac{k}{d}$$

and

$$\bar{f}(m) \equiv f\left(\frac{k}{m}\right), \quad \bar{g}(n) \equiv g\left(\frac{k}{n}\right).$$

Then the sum above becomes

$$\bar{f}(m) = \sum_{n|m} \bar{g}(n), \quad \text{for } m|k.$$

Now let  $\widehat{f}(s)$  and  $\widehat{g}(s)$  be extensions of  $\bar{f}(s)$  and  $\bar{g}(s)$  to the full domain of the nonnegative integers which preserve this relation but which are otherwise arbitrary:

$$\left. \begin{aligned} \widehat{f}(s) &= \bar{f}(s) \\ \widehat{g}(s) &= \bar{g}(s) \end{aligned} \right\} \text{ for } s|k;$$

$$\widehat{f}(s) = \sum_{a|s} \widehat{g}(a) \text{ for all } s \in \mathbf{Z}.$$

By Möbius inversion,

$$\widehat{g}(s) = \sum_{a|s} \mu(s/a) \widehat{f}(a).$$

Setting  $s = n = k/q$  and  $a = m = k/d$  we get

$$g(q) = \sum_{q|d} \mu(d/q) f(d)$$

and

$$g(S_q) = \sum_{S_d \supseteq S_q} \mu(d/q) f(S_d).$$

△

**Proof of Proposition 4** Let  $D = N\phi(N)$ .

If  $N$  is a prime number then  $H_N$  is cyclic and from Lemma 4 we have

$$L(S_q) = \sum_{S_d \supseteq S_q} \mu\left(\frac{d}{q}\right) K(S_d) = \sum_{q|d|D} \mu\left(\frac{d}{q}\right) K(S_d),$$

so

$$\begin{aligned} n_{SM} &= \sum_{q|D} \frac{q}{D} \sum_{q|d|D} \mu\left(\frac{d}{q}\right) K(S_d) \\ &= \sum_{d|D} K(S_d) \sum_{q|d} \frac{q}{D} \mu\left(\frac{d}{q}\right) \\ &= \frac{1}{D} \sum_{d|D} K(S_d) \phi(d), \end{aligned}$$

where the last line follows from the eq. (18) identity. Since each divider  $d$  corresponds to one and only one subgroup  $S_d$ , this sum is equal to the sum in the proposition.

Now let  $N$  be equal to twice an odd prime number. In this case  $H_N$  is not cyclic. We consider the element  $(1, b) \in H_N$ , where  $b$  is any element of  $(\mathbf{Z}/N\mathbf{Z})^\times$ , and let  $[M]$  be an index set that is invariant under  $(1, b)$ . We have

$$[M_0, M_1, M_2, \dots, M_{N-1}] = (1, b) * [M] = [M_{N-1}, M_{b^{-1}-1}, M_{2b^{-1}-1}, \dots, M_{(N-1)b^{-1}-1}],$$

and so  $M_0 = M_{N-1}$  and  $M_k = M_{kb^{-1}-1}$  for all  $k = 1, \dots, N-1$ .  $b$  is an odd integer, so if  $k$  is even,  $(kb^{-1}-1)$  is odd, and vice versa. Each index with an even subscript is thus equal to an index with an odd subscript, and we can write the sums in  $(8b, c)$  as sums over just the even indices:

$$\begin{aligned} N &= \sum_{k=0}^{N-1} M_k = 2 \sum_{q=0}^{(N-2)/2} M_{2q}, \\ \sum_{k=0}^{N-1} kM_k &= \sum_{q=0}^{(N-2)/2} (2q + 2qb^{-1} - 1)M_{2q} = 2(1 + b^{-1}) \sum_{q=0}^{(N-2)/2} qM_{2q} - \frac{N}{2}. \end{aligned}$$

Since by assumption  $N$  is twice an odd prime,  $\sum kM_k$  is an odd integer and is not congruent to 0 mod  $N$ . Thus, index sets that are invariant under any subgroup  $S_d$  that contains an element  $(1, b)$  for any  $b \in (\mathbf{Z}/N\mathbf{Z})^\times$ , (which of course includes the full group  $H_N$ ), do not satisfy condition (8b) and, as a consequence,  $K(S_d) = 0$  for such a subgroup. Then

$$\sum_{S_d \subseteq H_N} \phi(d) K(S_d) = \sum_{S_d \subseteq \hat{H}_N} \phi(d) K(S_d)$$

where the proper subgroup

$$\hat{H}_N = \{0, 2, 4, \dots, N-2\} \times \{1, 3, 5, \dots, N/2-2, N/2+2, \dots, N-1\} \subset H_N$$

is cyclic. The proof then follows as above for the  $N$  equal to a prime number case.  $\triangle$ .

If  $[M]$  is invariant under a cyclic subgroup  $S_d$  of  $H_N$ , then the conditions  $\mathbf{a} * [M] = [M]$  for all  $\mathbf{a} \in S_d$  can be replaced by the single equation  $\mathbf{g} * [M] = [M]$ , where  $\mathbf{g}$  is a generator of  $S_d$ . The product subgroup  $S_N^+ \times S_1^\times$  is cyclic, with generator  $(1, 1)$ , since it can be identified with the cyclic group  $S_N^+ = (\mathbf{Z}/N\mathbf{Z})^+$ . Its generator, expressed as a permutation on  $[M]$ , is

$$(1, 1)* = (0123 \cdots (N-1))$$

The only solution to  $(1, 1) * [M] = [M]$  and to  $N = \sum_q M_q$ , (eq.(8c)), is  $[M] = [111 \cdots 1]$ . This solution however satisfies conditions (8b) only for odd  $N$ . Consequently,

$$K(S_N^+ \times S_1^\times) = \begin{cases} 1 & \text{for odd } N, \\ 0 & \text{for even } N. \end{cases} \quad (\text{A1})$$

In addition, since all index sets are invariant under the identity subgroup  $S_1 = S_1^+ \times S_1^\times = \{(0, 1)\}$ ,

$$K(S_1) = \frac{1}{2N} \sum_{d|N} \phi\left(\frac{N}{d}\right) \binom{2d}{d}. \quad (\text{A2})$$

We will use the lemma below to calculate  $n_{SM}(N)$  for  $N = p$  and  $N = 2p$ :

**Lemma 5** *If  $[M]$  is invariant under the action of the group element  $(a, b)$ ,  $b \neq 1$ , then  $P^c[M]$  is invariant under the action of  $(a + (1 - b^{-1})c, b)$*

Proof: Acting on the multiplicity index set  $[M] = [M_0, M_1, \dots, M_{N-1}]$ , the circular permutation operator  $P^c$  permutes it to

$$P^c[M] = [M_{N-c}, M_{1-c}, \dots, M_{N-1-c}]$$

Then

$$\begin{aligned} (a + (1 - b^{-1})c, b) * (P^c[M]) &= (a + (1 - b^{-1})c, b) * [M_{N-c}, M_{1-c}, \dots, M_{N-1-c}] \\ &= [M_{(N-c)b^{-1}-a-c+b^{-1}c}, M_{(1-c)b^{-1}-a-c+b^{-1}c}, \dots, M_{(N-1-c)b^{-1}-a-c+b^{-1}c}] \\ &= [M_{-a-c}, M_{b^{-1}-a-c}, \dots, M_{(N-1)b^{-1}-a-c}] \\ &= P^c(a, b) * [M] = P^c[M] \quad \triangle \end{aligned}$$

a.  $N = p$

For  $N = p$ , we have, from Proposition 4,

$$\begin{aligned} n_{SM}(p) &= \frac{1}{p(p-1)} \sum_{S_k \subseteq H_p} \phi(k) K(S_k), \\ H_p &= \{0, 1, 2, \dots, p-1\} \times \{1, 2, \dots, p-1\}. \end{aligned}$$

$H_p$  is cyclic. All of its subgroups are therefore cyclic and are equal to the direct product of a subgroup of  $(\mathbf{Z}/p\mathbf{Z})^+$  and of  $(\mathbf{Z}/p\mathbf{Z})^\times$ . The subgroups of  $(\mathbf{Z}/p\mathbf{Z})^+$  are  $S_1^+ = \{0\}$  and  $S_p^+ = \{0, 1, 2, \dots, p-1\}$ , with generators 0 and 1, respectively. The subgroups of  $H_p$  are then of the form

$$S_1^+ \times S_d^\times = \{0\} \times S_d^\times = \langle (0, g) | (0, g)^d \rangle,$$

and

$$S_p^+ \times S_d^\times = \{0, 1, 2, \dots, p-1\} \times S_d^\times = \langle (1, g) | (1, g)^{pd} \rangle,$$

where  $d$  divides  $(p-1)$  and  $g$  is a generator of  $S_d^\times \subseteq (\mathbf{Z}/p\mathbf{Z})^\times$ . Then

$$n_{SM}(p) = \frac{1}{p(p-1)} \left\{ K(S_1^+ \times S_1^\times) + (p-1)K(S_p^+ \times S_1^\times) + \sum_{d|(p-1)}^{d>1} \phi(d)[K(S_1^+ \times S_d^\times) + (p-1)K(S_p^+ \times S_d^\times)] \right\}, \quad (\text{A3})$$

where we've used the relation  $\phi(pd) = \phi(p)\phi(d) = (p-1)\phi(d)$ . The  $d=1$  functions,  $K(S_1^+ \times S_1^\times)$  and  $K(S_p^+ \times S_1^\times)$ , are given by eqs.(A2) and (A1), respectively, and we have

$$K(S_1^+ \times S_1^\times) + (p-1)K(S_p^+ \times S_1^\times) = \frac{1}{2p} \binom{2p}{p} + \frac{p^2-1}{p}. \quad (\text{A4})$$

For  $d > 1$ , we show that

$$K(S_p^+ \times S_d^\times) = K(S_1^+ \times S_d^\times) = \binom{\frac{2(p-1)}{d}}{\frac{p-1}{d}}.$$

To prove the first identity, we set  $(a, b) = (0, g)$  and  $(a + (1-b^{-1})c, b) = (1, g)$  in Lemma 5 above. Then  $c = g(g-1)^{-1}$ . For each  $[M]$  that satisfies  $(0, g) * [M] = [M]$ , there is a circular permutation  $[M'] = P^{g(g-1)^{-1}}[M]$  that satisfies  $(1, g) * [M'] = [M']$ , and vice versa. The number of solutions to both eqs.(8b,c) and to  $(1, g) * [M] = [M]$  is therefore the same as the number of solutions to (8b,c) and  $(0, g) * [M] = [M]$ , and so  $K(S_p^+ \times S_d^\times) = K(S_1^+ \times S_d^\times)$ .

[Note that this argument fails for  $d=1$  since in this case  $g=1$ .]

To prove the second identity, we identify  $S_1^+ \times S_d^\times$  with  $S_d^\times$  and set  $m = (p-1)/d$ .  $S_d^\times$  has  $(m-1)$  cosets that we denote as  $\{c_1\}, \dots, \{c_{m-1}\}$ , with  $c_k \in \{c_k\} \subset [1, 2, \dots, (p-1)]$ . Multiplication mod  $p$  by  $g$  induces a cyclic permutation  $g^*$  on  $[012 \dots (p-1)]$ :

$$g^* = (0)(1g \dots g^{d-1})(c_1(gc_1) \dots (g^{d-1}c_1)) \dots (c_{m-1}(gc_{m-1}) \dots (g^{d-1}c_{m-1})).$$

Then  $[M]$  is invariant under  $g^*$  if and only if

$$\begin{aligned} M_1 &= M_g = \dots = M_{g^{d-1}}, \\ M_{c_1} &= M_{gc_1} = \dots = M_{g^{d-1}c_1}, \\ &\vdots \\ M_{c_{m-1}} &= M_{gc_{m-1}} = \dots = M_{g^{d-1}c_{m-1}}. \end{aligned} \quad (\text{A5})$$

Therefore,

$$\begin{aligned} \sum_{q=0}^{N-1} M_q &= M_0 + d(M_1 + M_{c_1} + \dots + M_{c_{m-1}}), \\ \text{and} \\ \sum_{q=0}^{N-1} qM_q &= (M_1 + c_1M_{c_1} + \dots + c_{m-1}M_{c_{m-1}})(1 + g + \dots + g^{d-1}). \end{aligned}$$

We have

$$1 + g + \dots + g^{d-1} = \frac{g^d - 1}{g - 1} = \frac{kp}{g - 1}$$

for some integer  $k$ , where the last equality follows from  $g^d \equiv 1 \pmod{p}$ .  $(g-1)$  then divides  $kp$ ; since  $p$  is prime, it must divide  $k$ . Therefore, for  $d > 1$ ,  $1 + g + \dots + g^{d-1} \equiv 0 \pmod{p}$  and condition (8b) is satisfied for any index set  $[M]$  that satisfies equations (A5).

Condition (8c) and the first equation above require that

$$M_1 + M_{c_1} + \dots + M_{c_{m-1}} = \frac{N - M_0}{d} = m - \frac{M_0 - 1}{d},$$

so we must have that

$$M_0 = 1 + d\alpha \geq 1, \quad M_1 + M_{c_1} + \dots + M_{c_{m-1}} = m - \alpha \geq 0,$$

for some integer  $\alpha \in [0, m]$ ; ( $M_0 = 0$  is excluded since  $d > 1$ ). For a given value of  $\alpha$ , the set  $\{M_1 + 1, \dots, M_{c_{m-1}} + 1\}$  is a composition of  $(2m - \alpha)$ . The number of compositions of an integer  $n$  into  $k$  parts is  $\binom{n-1}{k-1}$ , so the number of solutions to the set of equations in (A5) which also satisfy (8c) is

$$K(S_1^+ \times S_d^\times) = \sum_{\alpha=0}^m \binom{2m - \alpha - 1}{m - 1} = \sum_{\beta=m-1}^{2m-1} \binom{\beta}{m-1} = \binom{2m}{m}. \quad (\text{A6})$$

Putting equations (A4) and (A6) into (A3), we get eq.(20a).

$$b. \quad N = 2p$$

In this case,

$$n_{SM}(2p) = \frac{1}{2p(p-1)} \sum_{S_k \subseteq \widehat{H}_{2p}} \phi(k) K(S_k),$$

$$\widehat{H}_{2p} = \{0, 2, 4, \dots, 2p-2\} \times \{1, 3, 5, \dots, p-2, p+2, \dots, 2p-1\}.$$

$\widehat{H}_{2p}$  is cyclic and its subgroups are of the form

$$\begin{aligned} S_1^+ \times S_d^\times &= \{0\} \times S_d^\times = \langle (0, g) | (0, g)^p \rangle, \\ S_p^+ \times S_d^\times &= \{0, 2, 4, \dots, 2p-2\} \times S_d^\times = \langle (2, g) | (2, g)^{pd} \rangle, \end{aligned}$$

where  $S_d^\times = \{1, g, \dots, g^{d-1}\} \subseteq (\mathbf{Z}/(2p)\mathbf{Z})^\times$  is a  $d$ -element cyclic subgroup generated by the odd integer  $g$ . As indicated above,  $S_1^+ \times S_d^\times$  and  $S_p^+ \times S_d^\times$  are both cyclic, with generators  $(0, g)$  and  $(2, g)$ , respectively. Then

$$n_{SM}(2p) = \frac{1}{2p(p-1)} \left\{ K(S_1^+ \times S_1^\times) + (p-1)K(S_p^+ \times S_1^\times) + \sum_{d|p-1}^{d>1} \phi(d) [K(S_1^+ \times S_d^\times) + (p-1)K(S_p^+ \times S_d^\times)] \right\}. \quad (\text{A7})$$

For  $d = 1$  we have

$$K(S_1^+ \times S_1^\times) = \frac{1}{4p} \sum_{q=1,2,p,2p} \phi\left(\frac{2p}{q}\right) \binom{2q}{q} = \frac{2(p-1)}{p} + \frac{1}{4p} \left[ \binom{2p}{p} + \binom{4p}{2p} \right]$$

The cyclic subgroup  $S_p^+ \times S_1^\times$  has the generator  $(2, 1)$ . As a permutation on  $[M]$ ,

$$(2, 1)* = (024 \dots 2p-2)(135 \dots 2p-1).$$

The only solutions to  $(2, 1) * [M] = [M]$  which satisfy (8b, c) are  $[M] = [2020 \dots 20]$  and  $[0202 \dots 02]$ , and so  $K(S_p^+ \times S_1^\times) = 2$ .

The identity  $K(S_p^+ \times S_d^\times) = K(S_1^+ \times S_d^\times)$  for  $d > 1$  follows by a similar argument as that in the previous section, using Lemma 5, with  $c = 2g(g-1)^{-1}$ . It remains then to calculate  $K(S_1^+ \times S_d^\times)$  for  $d > 1$ , which we do in essentially the same fashion as was done for the  $N = p$  case. We identify  $S_1^+ \times S_d^\times$  with  $S_d^\times$  and consider the permutation  $(0, g)* = g*$  acting on  $[012 \dots N-1]$ :

$$g* = (0)(1g \cdots g^{d-1})(c_1 g \cdot c_1 \cdots g^{d-1} \cdot c_1) \cdots (c_{m-1} g \cdot c_{m-1} \cdots g^{d-1} \cdot c_{m-1}) \\ (2 \ 2g \cdots 2g^{d-1})(2c_1 \ 2gc_1 \cdots 2g^{d-1}c_1) \cdots (2c_{m-1} \ 2gc_{m-1} \cdots 2g^{d-1}c_{m-1})(p).$$

Again the  $c_k$ 's label the cosets of  $S_d^\times$  and  $m$  is defined as  $(p-1)/d$ . If  $[M]$  is invariant under  $S_d^\times$  then  $g*[M] = [M]$ , and conditions (8b,c) become

$$2p = \sum_q M_q = M_0 + M_p + d(M_1 + M_{c_1} + \cdots + M_{c_{m-1}} + M_2 + M_{2c_1} + \cdots + M_{2c_{m-1}}) \quad (\text{A8a})$$

or

$$M_1 + M_{c_1} + \cdots + M_{c_{m-1}} + M_2 + M_{2c_1} + \cdots + M_{2c_{m-1}} = \frac{2p - M_0 - M_p}{d} = 2m - \frac{M_0 + M_p - 2}{d}, \quad (\text{A8b})$$

and

$$0 \equiv \sum_q qM_q = pM_p + (1 + g + \cdots + g^{d-1})(M_1 + c_1M_{c_1} + \cdots + c_{m-1}M_{c_{m-1}} \\ + 2M_2 + 2c_1M_{2c_1} + \cdots + 2c_{m-1}M_{2c_{m-1}}). \quad (\text{A8c})$$

Since  $g^d \equiv 1 \pmod{2p}$ ,  $g^d = q(2p) + 1$  for some integer  $q$ . Then, for  $d > 1$ ,

$$\text{Tr}(S_d^\times) = 1 + g + \cdots + g^{d-1} = \frac{g^d - 1}{g - 1} = \frac{2qp}{g - 1}.$$

The trace of  $S_d^\times$  is a sum of  $d$  odd integers, which is odd or even depending on where  $d$  is odd or even. Since  $p$  is odd, the parity of the integer  $2q/(g-1)$  is the same as the parity of  $d$ . As a result,

$$\text{Tr}(S_d^\times) \equiv \begin{cases} 0 \pmod{2p} & \text{if } d \text{ is even;} \\ p \pmod{2p} & \text{if } d > 1 \text{ is odd.} \end{cases}$$

We consider the cases  $d$  equal to an even integer and  $d$  equal to an odd integer greater than 1 separately:

(I)  $d = 2k$ . Eq. (A8c) then requires that  $M_p$  is even. From (A8a/b)  $M_0$  must also be even. Setting  $M_0 = 2m_0$ ,  $M_p = 2m_p$ , we have from (A8b)

$$M_1 + M_{c_1} + \cdots + M_{c_{m-1}} + M_2 + M_{2c_1} + \cdots + M_{2c_{m-1}} = 2m - \alpha$$

where  $\alpha$  is an integer less than or equal to  $2m$  defined as

$$\alpha = \frac{M_0 + M_p - 2}{d} = \frac{m_0 + m_p - 1}{k};$$

$$\text{or } m_0 + m_p = k\alpha + 1, \geq 0.$$

The set  $\{M_1+1, M_{c_1}+1, \dots, M_{2c_{m-1}}+1\}$  is then a composition of  $(4m-\alpha)$ . For each  $\alpha$  there are  $(k\alpha+2)$  combinations of  $M_0$  and  $M_p$  such that  $M_0/2 + M_p/2 = k\alpha + 1$ . For  $k > 1$ ,  $\alpha$  can take on values from 0 to  $2m$ , while for  $k = 1$  the range of  $\alpha$  extends downwards to -1. The total number of solutions  $\{M_0, M_1, \dots, M_{2c_{m-1}}\}$  is then

$$K(S_1^+ \times S_d^\times)|_{d \text{ even}} = \sum_{\alpha=0}^{2m} (k\alpha + 2) \binom{4m - \alpha - 1}{2m - 1} + \delta_{d,2} \binom{4m}{2m - 1} \\ = \begin{cases} \binom{2p}{p}, & d = 2, \\ 2p \binom{4m}{2m} - (p-1) \binom{4m+1}{2m+1}, & d > 2. \end{cases}$$

(II)  $d = 2k + 1$ ,  $k > 0$ . In this case,

$$\sum qM_q \equiv p(M_p + M_1 + c_1M_{c_1} + \cdots + c_{m-1}M_{c_{m-1}}) \pmod{2p},$$

and condition (8b) requires that the sum  $M_p + M_1 + c_1M_{c_1} + \cdots + c_{m-1}M_{c_{m-1}}$  is even. But since all the  $c_k$ 's are odd integers, this condition becomes

$$M_p + M_1 + M_{c_1} + \cdots + M_{c_{m-1}} = 2n_1 \tag{A9a}$$

for some nonnegative integer  $n_1$ . Then from (A8a)

$$\begin{aligned} 2p &= M_0 + M_p + d(2n_1 - M_p + M_2 + M_{2c_1} + \cdots + M_{2c_{m-1}}) \\ &= M_0 + 2dn_1 - (d-1)M_p + d(M_2 + M_{2c_1} + \cdots + M_{2c_{m-1}}) \end{aligned}$$

so that the sum  $M_0 + M_2 + \cdots + M_{2c_{m-1}}$  is also even:

$$M_0 + M_2 + \cdots + M_{2c_{m-1}} = 2n_2, \quad n_2 \geq 0. \tag{A9b}$$

We define  $Z_1$  and  $Z_2$  as

$$Z_1 = 2n_1 - M_p, \quad Z_2 = 2n_2 - M_0.$$

Then

$$2p = M_0 + M_p + d(Z_1 + Z_2), \tag{A9c}$$

and we re-express (A9a,b,c) as

$$M_1 + M_{c_1} + \cdots + M_{c_{m-1}} = Z_1, \tag{A10a}$$

$$M_2 + M_{2c_1} + \cdots + M_{2c_{m-1}} = Z_2, \tag{A10b}$$

$$M_0 + M_p = 2p - d(Z_1 + Z_2), \tag{A10c}$$

which formally decouples the three sets of indices. The first two equations require that  $0 \leq Z_1, Z_2 \leq 2m$ . The third equation requires that  $0 \leq Z_1 + Z_2 \leq 2m$ , and that  $Z_1 + Z_2$  has the same parity as  $M_0 + M_p$ . Equations (A9) however have the additional requirement that the pairs  $(Z_1, M_p)$  and  $(Z_2, M_0)$  individually have the same parity, so we must impose this by hand on the solutions to equations (A10). (If one set has the same parity, then so does the other.)

For a given  $(Z_1, Z_2)$ , the number of solutions to (A10c) without this restriction is

$$\binom{2p + 1 - d(Z_1 + Z_2)}{1} \equiv W.$$

If  $Z_1 + Z_2$  is odd, then  $W$  is even and there are  $W/2$  compositions  $(M_0, M_p)$  in which  $M_p$  is even, and  $W/2$  compositions in which it is odd. So to count only the compositions in which  $Z_1$  and  $M_p$  have the same parity, we divide  $W$  by 2:  $W \rightarrow W/2$ , for  $Z_1 + Z_2$  odd.

If on the other hand  $Z_1 + Z_2$  is even, then  $W$  is odd, and there are  $(W \pm 1)/2$  such compositions for  $Z_1$  even/odd, respectively.

So, to impose the requirement that  $(Z_1, M_p)$ , (or equivalently  $(Z_2, M_0)$ ), have the same parity we make the replacement

$$W \rightarrow \frac{1}{2} \left[ W + \frac{(-1)^{Z_1} + (-1)^{Z_2}}{2} \right].$$

The number of solutions to (A10) with this requirement is then

$$K(S_1^+ \times S_d^\times)|_{d \text{ odd}, > 1} = \sum_{Z_1=0}^{2m} \sum_{Z_2=0}^{2m-Z_1} \frac{1}{2} \left[ 2p + 1 - d(Z_1 + Z_2) + \frac{(-1)^{Z_1} + (-1)^{Z_2}}{2} \right] \binom{Z_1 + m - 1}{m - 1} \binom{Z_2 + m - 1}{m - 1}.$$

From the  $(Z_1, Z_2)$  symmetry of the summand we can replace  $( (-1)^{Z_1} + (-1)^{Z_2} )/2$  by  $(-1)^{Z_1}$ . Evaluating this expression we get

$$K(S_1^+ \times S_d^\times)|_{d \text{ odd}, >1} = \frac{4p-1}{2} \binom{4m}{2m} - (p-1) \binom{4m+1}{2m+1} + \sum_{Z_1=0}^{2m} \frac{(-1)^{Z_1}}{2} \binom{Z_1+m-1}{m-1} \binom{3m-Z_1}{m}.$$

To evaluate the remaining sum we use the following lemma:

**Lemma 6**

$$\sum_{k=0}^X \binom{k}{m-1} \binom{X-k}{m} (-1)^k = (-1)^{m-1} \binom{\lceil X/2 \rceil}{m}$$

where  $\lceil \cdot \rceil$  denotes the ceiling function. To prove this identity we write it in the form

$$(A) \quad \sum_{k=0}^{2n} \binom{k}{m-1} \binom{2n-k}{m} (-1)^k = (-1)^{m-1} \binom{n}{m},$$

$$(B) \quad \sum_{k=0}^{2n+1} \binom{k}{m-1} \binom{2n+1-k}{m} (-1)^k = (-1)^{m-1} \binom{n+1}{m}.$$

These two identities can be proven by using the identity

$$\frac{x^m}{(1-x)^{m+1}} = \sum_{q=0}^{\infty} \binom{q}{m} x^q$$

and expressing the product

$$\frac{(-x)^{m-1}}{(1+x)^m} \frac{x^m}{(1-x)^{m+1}}$$

first as the product of two sums,

$$\frac{(-x)^{m-1}}{(1+x)^m} \frac{x^m}{(1-x)^{m+1}} = \left( \sum_{k=0}^{\infty} \binom{k}{m-1} (-1)^k x^k \right) \left( \sum_{q=0}^{\infty} \binom{q}{m} x^q \right), \quad (A11)$$

then as a single sum,

$$\frac{(-x)^{m-1}}{(1+x)^m} \frac{x^m}{(1-x)^{m+1}} = \frac{(-1)^{m-1} x^{2m-1} (1+x)}{(1-x^2)^{m+1}} = (-1)^{m-1} \sum_{p=0}^{\infty} \binom{p}{m} (x^{2p-1} + x^{2p}), \quad (A12)$$

and then equating the even-exponent and the odd-exponent terms on the right-hand side of (A11) to those on the right-hand side of (A12).

Now setting  $k = Z_1 + m - 1$  and  $X = 4m - 1$  we have from this lemma

$$\sum_{Z_1=0}^{2m} \binom{Z_1+m-1}{m-1} \binom{3m-Z_1}{m} (-1)^{Z_1+m-1} = (-1)^{m-1} \binom{2m}{m}.$$

And so

$$K(S_1^+ \times S_d^\times)|_{d \text{ odd}, >1} = \frac{4p-1}{2} \binom{4m}{2m} - (p-1) \binom{4m+1}{2m+1} + \frac{1}{2} \binom{2m}{m}.$$

Putting all these results together, we get eq.(20b).

## Appendix B

We have, from the discussion in the proof of Theorem 3, that

$$A_{0\dots 0 1\dots 1 A_1\dots A_{p+1}}^{(k)} \propto \sum_{q_1, \dots, q_p} Q(k - A_1 q_1 - \dots - A_p q_p; M_1, N - 1 \mid q_1, \dots, q_p) \Bigg|_{q_i \neq q_l}. \quad (\text{B1})$$

To determine the relation between this partition function and  $A_{0\dots 0 1\dots 1 A_1\dots A_p}^{(k)}$ , we first consider the case where all multiplicities  $M_0, M_1, \dots, M_{N-1}$  have no common factor. Then, as discussed earlier, all the cyclic-permutation equivalence classes  $\{\sigma_0 = A_{p+1}, \sigma_1, \dots, \sigma_{M-1}\}$  have  $N$  elements. The coefficient  $A_{0\dots 0 1\dots 1 A_1\dots A_{p+1}}^{(k)}$  is then proportional to  $N$  times a sum of  $Q$  over all possible  $q$ 's divided, to avoid overcounting, by the factorials of the multiplicities:

$$A_{0\dots 0 1\dots 1 A_1\dots A_{p+1}}^{(k)} \propto \frac{N M_{A_{p+1}}}{M_2! \dots M_{N-1}!} \sum_{q_1, \dots, q_p} Q(k - A_1 q_1 - \dots - A_p q_p; M_1, N - 1 \mid q_1, \dots, q_p) \Bigg|_{q_i \neq q_l}.$$

(The factor of  $M_{A_{p+1}}$  occurs in the numerator because the multiplicity of  $A_{p+1}$  within the indices  $\{A_1, \dots, A_p\}$  is only  $M_{A_{p+1}} - 1$ .)

Now consider a particular permutation  $[\sigma] = [A_{p+1}, \sigma_1, \dots, \sigma_{N-1}]$  corresponding to a particular set  $\{q_1, \dots, q_p\}$  and a particular partition  $(p_1, \dots, p_{M_1})$ .  $[\sigma]$  contains, in addition to the  $A_{p+1}$  at the 0 position, an additional  $(M_{A_{p+1}} - 1)$   $A_{p+1}$ 's at various  $q_j$  positions. The equivalence class containing this  $[\sigma]$ , i.e.,  $\{\sigma\}$ , also contains (among others) all permutations of the form  $[\sigma'] = [\sigma'_0 = \sigma_{q_j} = A_{p+1}, \sigma'_1, \dots, \sigma'_0 = A_{p+1}, \dots, \sigma'_{N-1}]$ , obtained by cycling the  $A_{p+1}$  at the  $q_j$  position to the 0 position, (and the  $A_{p+1}$  at the 0 position to somewhere else). These permutations will also be counted in the sum over the  $q$ 's, under a different set of  $q$ 's and  $p$ 's. Since there are  $(M_{A_{p+1}} - 1)$  such  $q$ 's, each equivalence class will be counted  $M_{A_{p+1}}$  times in the sum above. We must therefore divide  $N$  by an additional  $M_{A_{p+1}}$  to get the number of *distinct* permutations:

$$A_{0\dots 0 1\dots 1 A_1\dots A_{p+1}}^{(k)} = \frac{N}{M_2! \dots M_{N-1}!} \sum_{q_1, \dots, q_p} Q(k - A_1 q_1 - \dots - A_p q_p; M_1, N - 1 \mid q_1, \dots, q_p) \Bigg|_{q_i \neq q_l}.$$

For example, consider the index set [0011255] and the two equivalence classes below that appear in the sum over  $q_1, q_2$ :

$$\begin{aligned} \{5001125\}: \quad & \{p_1, p_2\} = \{3, 4\}; \quad \{q_1, q_2\} = \{5, 6\}; \\ \{5500112\}: \quad & \{p_1, p_2\} = \{4, 5\}; \quad \{q_1, q_2\} = \{1, 6\}. \end{aligned}$$

Each of the permutations [5001125] and [5500112] are in both of these equivalence classes, so we must divide by 2.

Now let the multiplicities have a common factor  $d$ :  $\gcd(M_0, M_1, M_2, \dots, M_{N-1}) = d$ . Then there will be some equivalence classes of the form  $\{A_{p+1}x \dots y A_{p+1}x \dots y \dots A_{p+1}x \dots y\}$  for which  $\sigma_j = \sigma_{j+N/d}$ , so that the ‘‘phrase’’  $A_{p+1}x \dots y$  is repeated  $d$  times. These classes have only  $N/d$  distinct elements. The sum in (B1) will then consist of two sums, one over the  $N$ -element classes and one over the  $(N/d)$ -element classes, which we will express in short-hand notation as

$$A_{0\dots 0 1\dots 1 A_1\dots A_{p+1}}^{(k)} = \frac{M_{A_{p+1}}}{M_2! \dots M_{N-1}!} \left\{ \frac{N}{M_{A_{p+1}}} \sum_I Q + \frac{N/d}{X} \sum_{II} Q \right\}$$

where division by some factor  $X$  is needed to correct for overcounting due to the duplication of equivalence classes in the sum. The index  $A_{p+1}$  occurs  $M_{A_{p+1}}$  times in the entire index set  $[A_{p+1}x \dots y A_{p+1}x \dots y \dots A_{p+1}x \dots y]$ , and  $M_{A_{p+1}}/d$  times in the phrase  $A_{p+1}x \dots y$ ;  $M_{A_{p+1}}/d$  is thus the factor  $X$  by which each distinct equivalence class is overcounted:  $(N/d)/(M_{A_{p+1}}/d) = N/M_{A_{p+1}}$ .

As an example of this situation, we consider [001122333333], with  $N = 12$ ,  $M_0 = M_1 = M_2 = 2$ ,  $M_3 = 6$ ,  $d = 2$ , and the equivalence classes:

$$\begin{aligned} \{303312\ 303312\} &: \{p_1, p_2\} = \{4, 10\}; \{q_1, q_2, q_3, q_4, q_5, q_6, q_7\} = \{2, 3, 5, 6, 8, 9, 11\}; \\ \{331230\ 331230\} &: \{p_1, p_2\} = \{2, 8\}; \{q_1, q_2, q_3, q_4, q_5, q_6, q_7\} = \{1, 3, 4, 6, 7, 9, 10\}; \\ \{312303\ 312303\} &: \{p_1, p_2\} = \{1, 7\}; \{q_1, q_2, q_3, q_4, q_5, q_6, q_7\} = \{2, 3, 5, 6, 8, 9, 11\}. \end{aligned}$$

Each equivalence class has  $N/d = 6$  distinct elements, and each class is overcounted by a factor of  $3 = M_3/d$ . The overall correction factor is then  $6/3 = N/M_3$ . (Although classes 1 and 3 have the same  $q$  values, their  $p$  values are different and will therefore be counted separately by the partition function.)

Since the correction factor is the same as for the first sum, we can use the same multiplying factor for both without any further need to consider them separately:

### Appendix C: Proof of Lemma 1

For a given set  $\{\kappa_1, \dots, \kappa_p\}$  let

$$\beta_j = \kappa_1 + \dots + \kappa_j, \quad 1 \leq j \leq p.$$

Then  $\kappa_1 = \beta_1$  and  $\kappa_j = \beta_j - \beta_{j-1}$  for  $j \geq 2$ . In the sums over the  $\kappa$ 's in the statement of the lemma, the restriction that  $\kappa_1 + \dots + \kappa_p \leq m$  requires that each  $\beta_j \leq m$ . And, since each  $\kappa_j$  has the range  $[0, m]$ , each  $\beta_{j-1}$  has the range  $[0, \beta_j]$ . We therefore have

$$\begin{aligned} \sum_{0 \leq \kappa_1, \dots, \kappa_p \leq m} \omega^{\kappa_1 q_1 + \kappa_2 q_2 + \dots + \kappa_p q_p} H[m - (\kappa_1 + \dots + \kappa_p)] \\ = \sum_{\beta_p=0}^m \sum_{\beta_{p-1}=0}^{\beta_p} \dots \sum_{\beta_2=0}^{\beta_3} \sum_{\beta_1=0}^{\beta_2} \omega^{(\beta_p - \beta_{p-1})q_p} \dots \omega^{(\beta_2 - \beta_1)q_2} \omega^{\beta_1 q_1}, \end{aligned}$$

and the statement of Lemma I is equivalent to

$$\sum_{m=0}^{N-1} (-y)^m \prod_{s=1}^p \frac{1}{1 + y\omega^{q_s}} = \sum_{m=0}^{N-1-p} (-y)^m \sum_{\beta_p=0}^m \sum_{\beta_{p-1}=0}^{\beta_p} \dots \sum_{\beta_2=0}^{\beta_3} \sum_{\beta_1=0}^{\beta_2} \omega^{(\beta_p - \beta_{p-1})q_p} \dots \omega^{(\beta_2 - \beta_1)q_2} \omega^{\beta_1 q_1}.$$

The proof of Lemma I, by induction on  $p$ , is more direct when stated in this form.

To prove the lemma we first set  $p$  equal to 1 on the right side, multiply that expression by  $(1 + y\omega^q)$ , and expand:

$$(1 + y\omega^q) \sum_{m=0}^{N-2} (-y)^m \sum_{\beta=0}^m \omega^{\beta q} = \sum_{m=0}^{N-2} (-y)^m \sum_{\beta=0}^m \omega^{\beta q} - \sum_{m=0}^{N-2} (-y)^{m+1} \sum_{\beta=0}^m \omega^{(\beta+1)q}. \quad (\text{C1})$$

The first sum on the right in eq.(C1) is

$$\sum_{m=0}^{N-2} (-y)^m + \sum_{m=1}^{N-2} (-y)^m \sum_{\beta=1}^m \omega^{\beta q}, \quad (\text{C2})$$

while the 2nd sum, after relabeling  $\beta$  and then  $m$ , is

$$- \sum_{m=1}^{N-1} (-y)^m \sum_{\beta=1}^m \omega^{\beta q}. \quad (\text{C3})$$

The 2nd sum in expression (C2) will therefore cancel with all but the  $m = N - 1$  term in (C3), and we have

$$(1 + y\omega^q) \sum_{m=0}^{N-2} (-y)^m \sum_{\beta=0}^m \omega^{\beta q} = \sum_{m=0}^{N-2} (-y)^m - (-y)^{N-1} \sum_{\beta=1}^{N-1} \omega^{\beta q} = \sum_{m=0}^{N-1} (-y)^m \quad (\text{C4})$$

where we've used eq.(7) to evaluate the sum over  $\beta$  as equal to -1. The lemma is therefore valid for  $p = 1$ .

We now assume the lemma is valid for the product of  $(p - 1)$  factors,  $\prod_{s=1}^{p-1} (1 + y\omega^{q_s})^{-1}$ , and express the product of  $p$  factors as the difference of two  $(p - 1)$  products:

$$\begin{aligned} & \sum_{m=0}^{N-1} (-y)^m \prod_{s=1}^p \frac{1}{1 + y\omega^{q_s}} \\ &= \frac{-1}{y(\omega^{q_2} - \omega^{q_3})} \sum_{m=0}^{N-1} (-y)^m \frac{1}{1 + y\omega^{q_1}} \left\{ \frac{1}{1 + y\omega^{q_2}} - \frac{1}{1 + y\omega^{q_3}} \right\} \prod_{s=4}^p \frac{1}{1 + y\omega^{q_s}} \\ &= \frac{1}{\omega^{q_2} - \omega^{q_3}} \sum_{m=1}^{N-p} (-y)^{m-1} \left\{ \sum_{\beta_p=0}^m \dots \sum_{\beta_2=0}^{\beta_4} \sum_{\beta_1=0}^{\beta_2} \omega^{(\beta_p - \beta_{p-1})q_p} \dots \omega^{(\beta_4 - \beta_2)q_4} \omega^{(\beta_2 - \beta_1)q_2} \omega^{\beta_1 q_1} \right. \\ & \quad \left. - \sum_{\beta_p=0}^m \dots \sum_{\beta_3=0}^{\beta_4} \sum_{\beta_1=0}^{\beta_3} \omega^{(\beta_p - \beta_{p-1})q_p} \dots \omega^{(\beta_4 - \beta_3)q_4} \omega^{(\beta_3 - \beta_1)q_3} \omega^{\beta_1 q_1} \right\}. \end{aligned}$$

In the first term inside the brackets we make the replacement  $\beta_2 \rightarrow \beta_3$  and factor out the  $q_p, \dots, q_4$  sums, so we have

$$\begin{aligned} & \frac{1}{\omega^{q_2} - \omega^{q_3}} \left\{ \sum_{\beta_p=0}^m \dots \sum_{\beta_2=0}^{\beta_4} \sum_{\beta_1=0}^{\beta_2} \omega^{(\beta_p - \beta_{p-1})q_p} \dots \omega^{(\beta_4 - \beta_2)q_4} \omega^{(\beta_2 - \beta_1)q_2} \omega^{\beta_1 q_1} \right\} \\ & \quad - \sum_{\beta_p=0}^m \dots \sum_{\beta_3=0}^{\beta_4} \sum_{\beta_1=0}^{\beta_3} \omega^{(\beta_p - \beta_{p-1})q_p} \dots \omega^{(\beta_4 - \beta_3)q_4} \omega^{(\beta_3 - \beta_1)q_3} \omega^{\beta_1 q_1} \left\} \\ &= \sum_{\beta_p=0}^m \dots \sum_{\beta_3=0}^{\beta_4} \omega^{(\beta_p - \beta_{p-1})q_p} \dots \omega^{(\beta_4 - \beta_3)q_4} \sum_{\beta_1=0}^{\beta_3} \frac{\omega^{(\beta_3 - \beta_1)q_2} - \omega^{(\beta_3 - \beta_1)q_3}}{\omega^{q_2} - \omega^{q_3}} \omega^{\beta_1 q_1}. \end{aligned}$$

The validity of the lemma for  $p$  factors then follows from the identity

$$\frac{a^n - b^n}{a - b} = \sum_{p=0}^{n-1} a^{n-1-p} b^p,$$

and a relabeling of the summation indices.  $\triangle$

## Appendix D: Proof of Lemma 2

To remind ourselves, for a partition  $Z = (z_1, z_2, \dots, z_j)$  of  $p$ , the vector  $\mathbf{q}_Z$  is defined as

$$\begin{array}{ccccccc} \mathbf{q}_Z & = & (q_1, \dots, q_1, q_2, \dots, q_2, & \dots & \dots & , q_j, \dots, q_j). \\ & & \longleftrightarrow & & \longleftrightarrow & & \longleftrightarrow \\ & & z_1 & & z_2 & & \dots & & z_j \end{array}$$

and the statement of the lemma is that

$$\sum_{1 \leq q_1 < \dots < q_p \leq M} h(\mathbf{q}) = \frac{1}{p!} \sum_{Z \in \mathcal{P}_p} (-1)^{p+j} (p; k_1, k_2, \dots, k_p)^* \sum_{1 \leq q_1, \dots, q_j \leq M} h(\mathbf{q}_Z)$$

where  $h$  is a completely symmetric function of its arguments.

This proof is also by induction. We separate off the  $j = p$  term in the sum and write the lemma in the form

$$\sum_{q_1, \dots, q_p} h(q_1, \dots, q_p) = p! \sum_{q_1 < \dots < q_p} h(q_1, \dots, q_p) + \sum_{j=1}^{p-1} \sum_{k_1, \dots, k_p} (-1)^{p+j-1} (p; k_1, k_2, \dots, k_p)^* \sum_{q_1, \dots, q_j} h(\mathbf{q}_Z) \quad (\text{D1})$$

with  $j = k_1 + \dots + k_p$ , and the summation limits  $1 \leq q_n \leq M$  and  $0 \leq k_n \leq p$  for all  $q_n$  and  $k_n$  understood.

For  $p = 1$  the equality is trivial. For  $p = 2$ , this expression reduces to

$$\sum_{q_1, q_2} h(q_1, q_2) = 2 \sum_{q_1 < q_2} h(q_1, q_2) + \sum_{q_1} h(q_1, q_1), \quad (\text{D2})$$

which is clearly valid. We now assume that the lemma is valid for summation over the  $(p-1)$ -dimensional lattice and show that it is then valid for the  $p$ -dimensional one. For clarity in the notation, we will denote a partition of  $(p-1)$  by  $Y = (y_1, y_2, \dots, y_j)$ , with multiplicities  $[l_1, \dots, l_{p-1}, l_p = 0]$ . We then have for the summation over  $p$  dimensions,

$$\begin{aligned} \sum_{q_1, \dots, q_p} h(q_1, \dots, q_p) &= \sum_{q_p} \sum_{q_1, \dots, q_{p-1}} h(q_1, \dots, q_{p-1}, q_p) \\ &= \sum_{q_p} \left\{ (p-1)! \sum_{q_1 < \dots < q_{p-1}} h(q_1, \dots, q_{p-1}, q_p) \right. \\ &\quad \left. + \sum_{j=1}^{p-2} \sum_{l_1, \dots, l_{p-1}} (-1)^{p+j} (p-1; l_1, l_2, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j} h(\mathbf{q}_Y, q_p) \right\} \end{aligned} \quad (\text{D3})$$

by the induction assumption. We now separate the sum over  $q_p$  applied to the first term inside the brackets into sums over the  $p$  regions

$$(q_p < q_1 < q_2 < \dots < q_{p-1}) \quad (q_1 < q_p < q_2 < \dots < q_{p-1}) \quad \dots \quad (q_1 < q_2 < \dots < q_{p-1} < q_p)$$

and the  $(p-1)$  boundaries

$$(q_p = q_1 < q_2 < \dots < q_{p-1}) \quad \dots \quad (q_1 < q_2 < \dots < q_{p-1} = q_p).$$

By the symmetry of the function  $h$ , the  $p$ -dimensional sum over each subregion is the same, and we can write (making the change  $p \rightarrow j+1, q_p \rightarrow q_{j+1}$  in the last sum),

$$\begin{aligned} \sum_{q_1, \dots, q_p} h(q_1, \dots, q_p) &= p! \sum_{q_1 < \dots < q_{p-1} < q_p} h(q_1, \dots, q_p) \\ &\quad + (p-1)! \sum_{q_1 < \dots < q_{p-1}} \{h(q_1, \dots, q_{p-1}, q_1) + h(q_1, \dots, q_{p-1}, q_2) + \dots + h(q_1, \dots, q_{p-1}, q_{p-1})\} \\ &\quad + \sum_{j=1}^{p-2} \sum_{l_1, \dots, l_{p-1}} (-1)^{p+j} (p-1; l_1, l_2, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j, q_{j+1}} h(\mathbf{q}_Y, q_{j+1}). \end{aligned} \quad (\text{D4})$$

Now although the functions  $h(q_1, q_2, \dots, q_{p-1}, q_1), \dots, h(q_1, q_2, \dots, q_{p-1}, q_{p-1})$  in the second term are not completely symmetric functions on the  $(p-1)$ -dimensional lattice, the sum of these functions *is* symmetric, and we can apply the lemma in its  $(p-1)$  form to it:

$$\begin{aligned} &(p-1)! \sum_{q_1 < \dots < q_{p-1}} \{h(q_1, \dots, q_{p-1}, q_1) + h(q_1, \dots, q_{p-1}, q_2) + \dots + h(q_1, \dots, q_{p-1}, q_{p-1})\} \\ &= \sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, l_2, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j} \{h(\mathbf{q}_Y, q_{(1)}) + h(\mathbf{q}_Y, q_{(2)}) + \dots + h(\mathbf{q}_Y, q_{(p-1)})\}. \end{aligned}$$

The notation  $q_{(k)}$  here means, for a partition  $Y$ ,  $q_{(k)}$  is equal to the value of the  $k$ -th coordinate in the associated lattice point  $\mathbf{q}_Y$ . E.g., for  $Y = (3, 2, 2)$  and for  $k = 2$ , we have

$$\begin{array}{ccccccc} h(q_1, q_1, q_1, q_2, q_2, q_3, q_3, q_{(2)}) & = & h(q_1, q_1, q_1, q_2, q_2, q_3, q_3, q_1) \\ \uparrow & & & & & & \uparrow \end{array}$$

Therefore,

$$\begin{aligned}
\sum_{q_1, \dots, q_p} h(q_1, \dots, q_p) &= p! \sum_{q_1 < \dots < q_p} h(q_1, \dots, q_p) \\
&+ \sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, l_2, \dots, l_{p-1}, 0)^* \\
&\quad \times \sum_{q_1, \dots, q_j} \{h(\mathbf{q}_Y, q_{(1)}) + h(\mathbf{q}_Y, q_{(2)}) + \dots + h(\mathbf{q}_Y, q_{(p-1)})\} \\
&+ \sum_{j=1}^{p-2} \sum_{l_1, \dots, l_{p-1}} (-1)^{p+j} (p-1; l_1, l_2, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_{j+1}} h(\mathbf{q}_Y, q_{j+1}).
\end{aligned} \tag{D5}$$

The term on the left and the 1st term on the right are in the ‘‘correct’’ form for the proposition. The 2nd and 3rd terms on the right contain sums over the partitions of  $(p-1)$  that, to complete the proof, we want to express as sums over the partitions of  $p$ . Given a partition  $(y_1, \dots, y_j)$  of  $(p-1)$ , there are two ways a partition of  $p$  can be generated from it: one can add 1 to an individual part,  $y_m \rightarrow (y_m + 1)$ , or one can add a 1 to the total sum  $y_1 + \dots + y_j \rightarrow y_1 + \dots + y_j + 1$ . As shown below, the 2nd term converts to a sum over the partitions of  $p$  by this first process, and the 3rd term by the second process.

We consider the 2nd term first:

$$\sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j} \sum_{s=1}^{p-1} h(\mathbf{q}_Y, q_{(s)}).$$

For a partition  $Y = (y_1, \dots, y_j)$  and for a particular  $q_{(s)}$  such that

$$y_1 + \dots + y_{d-1} < s \leq y_1 + \dots + y_{d-1} + y_d \tag{D6}$$

for some  $d$ , the lattice point  $(\mathbf{q}_Y, q_{(s)})$  is equivalent to the partition  $Z \equiv Z_{y_d} = (y_1, \dots, y_d + 1, \dots, y_j)$  of  $p$ , since  $h(\mathbf{q}_Y, q_{(s)}) = h(q_1, \dots, q_1, q_2, \dots, q_2, \dots, q_j, \dots, q_j, q_d)$ , and, by the symmetry of  $h$ , we can move the  $q_d$  in the final position to a position among the other  $q_d$ 's, so there are  $(y_d + 1)$   $q_d$ 's. In terms of multiplicities, if

$$Y = [l_1, \dots, l_{y_d}, l_{y_d+1}, \dots, l_{p-1}, 0],$$

then

$$Z_{y_d} = [l_1, \dots, l_{y_d} - 1, l_{y_d+1} + 1, \dots, l_{p-1}, 0].$$

In the sum over  $s$ , the number of  $s$ 's that satisfy condition (D6) above is  $y_d l_{y_d}$ , so the partition  $Z_{y_d}$  will appear  $y_d l_{y_d}$  times in this sum, and we have,

$$\begin{aligned}
&\sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j} \sum_{s=1}^{p-1} h(\mathbf{q}_Y, q_{(s)}) \\
&= \sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{n=1}^{p-1} n l_n \sum_{q_1, \dots, q_j} h(\mathbf{q}_{Z_n})
\end{aligned} \tag{D7}$$

where the partition  $Z_n$  has multiplicities  $[k_1, \dots, k_p]$  given by  $k_m = l_m - \delta_{n,m}$ ,  $k_{m+1} = l_{m+1} + \delta_{n,m}$  for  $m = 1, \dots, p-1$ . We now multiply and divide on the right by the corresponding multinomial coefficient  $(p; k_1, \dots, k_p)_n^*$ :

$$\begin{aligned}
&\sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j} \sum_{s=1}^{p-1} h(\mathbf{q}_Y, q_{(s)}) \\
&= \sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} \sum_{n=1}^{p-1} \frac{(p-1; l_1, \dots, l_{p-1}, 0)^*}{(p; k_1, \dots, k_p)_n^*} (p; k_1, \dots, k_p)_n^* n l_n \sum_{q_1, \dots, q_j} h(\mathbf{q}_{X_n}).
\end{aligned} \tag{D8}$$

Since

$$\frac{(p-1; l_1, \dots, l_{p-1}, 0)^*}{(p; k_1, \dots, k_p)_n^*} = \frac{1}{p} \frac{n^{l_n-1} (l_n-1)! (n+1)^{l_{n+1}+1} (l_{n+1}+1)!}{n^{l_n} l_n! (n+1)^{l_{n+1}} l_{n+1}!} = \frac{1}{p} \frac{(n+1)(l_{n+1}+1)}{n l_n} \tag{D9}$$

we have

$$\begin{aligned}
& \sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j} \sum_{s=1}^{p-1} h(\mathbf{q}_Y, q_{(s)}) \\
&= \sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} \sum_{n=1}^{p-1} \frac{(n+1)k_{n+1}}{p} (p; k_1, \dots, k_p)_n^* \sum_{q_1, \dots, q_j} h(\mathbf{q}_{X_n}). \tag{D10}
\end{aligned}$$

In this equation, for a given partition  $Y$ , we sum over all partitions  $Z_n$ . We now interchange the sums and, for a given partition  $Z$ , we sum over the corresponding  $Y$  partitions. This amounts to dropping the subscripts ‘ $n$ ’ and replacing the sums over the  $l$ ’s by sums over  $k$ ’s. So, making the replacement  $n' = n + 1$  and then dropping the prime,

$$\begin{aligned}
& \sum_{j=1}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p-1+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_j} \sum_{s=1}^{p-1} h(\mathbf{q}_Y, q_{(s)}) \\
&= \sum_{j=1}^{p-1} \sum_{k_1, \dots, k_p} (-1)^{p-1+j} \sum_{n=2}^p \frac{nk_n}{p} (p; k_1, \dots, k_p)^* \sum_{q_1, \dots, q_j} h(\mathbf{q}_Z) \\
&= \sum_{j=1}^{p-1} \sum_{k_1, \dots, k_p} (-1)^{p-1+j} \frac{p-k_1}{p} (p; k_1, \dots, k_p)^* \sum_{q_1, \dots, q_j} h(\mathbf{q}_Z) \tag{D11}
\end{aligned}$$

where we’ve used  $k_1 + 2k_2 + \dots + pk_p = p$  in the last line.

Turning now to the 3rd term,

$$\sum_{j=1}^{p-2} \sum_{l_1, \dots, l_{p-1}} (-1)^{p+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_{j+1}} h(\mathbf{q}_Y, q_{j+1}),$$

the lattice point  $(\mathbf{q}_Y, q_{j+1})$  is equal to the lattice point  $\mathbf{q}_Z$  for the partition  $Z = (y_1, \dots, y_j, 1) = [l_1+1, l_2, \dots, l_{p-1}, 0] \in \mathcal{P}(p)$  with  $j+1$  parts. Setting  $j' = j+1$ , we can express this term as a sum over the partitions of  $p$  from  $j' = 2$  to  $p-1$ :

$$\begin{aligned}
& \sum_{j=1}^{p-2} \sum_{l_1, \dots, l_{p-1}} (-1)^{p+j} (p-1; l_1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_{j+1}} h(\mathbf{q}_Y, q_{j+1}) \\
&= \sum_{j'=2}^{p-1} \sum_{l_1, \dots, l_{p-1}} (-1)^{p+j'-1} \frac{(p-1; l_1, \dots, l_{p-1}, 0)^*}{(p; l_1+1, \dots, l_{p-1}, 0)^*} (p; l_1+1, \dots, l_{p-1}, 0)^* \sum_{q_1, \dots, q_{j'}} h(\mathbf{q}_Z) \\
&= \sum_{j'=2}^{p-1} \sum_{k_1, \dots, k_{p-1}} (-1)^{p+j'-1} \frac{k_1}{p} (p; k_1, \dots, k_{p-1}, 0)^* \sum_{q_1, \dots, q_{j'}} h(\mathbf{q}_Z) \tag{D12}
\end{aligned}$$

using

$$\frac{(p-1; l_1, l_2, \dots, l_{p-1})^*}{(p; l_1+1, \dots, l_{p-1}, 0)^*} = \frac{1}{p} \frac{1^{l_1+1}(l_1+1)! 2^{l_2} l_2! \dots (p-1)^{l_{p-1}} l_{p-1}!}{1^{l_1} l_1! 2^{l_2} l_2! \dots (p-1)^{l_{p-1}} l_{p-1}!} = \frac{l_1+1}{p} = \frac{k_1}{p}.$$

But since  $k_1 = 0$  if  $j' = 1$ , (corresponding to the partition  $p = p$  and  $k_p = 1$ ), the summation lower limit can be extended to  $j' = 1$  and a ‘sum’ over  $k_p$  added, along with the replacement  $(p; k_1, \dots, k_{p-1}, 0)^* \rightarrow (p; k_1, \dots, k_{p-1}, k_p)^*$ .

Putting (D11) and (D12) into (D5), the  $k_1/p$  terms cancel and we get

$$\sum_{q_1, \dots, q_p} h(q_1, \dots, q_p) = p! \sum_{q_1 < \dots < q_p} h(q_1, \dots, q_p) + \sum_{j=1}^{p-1} \sum_{k_1, \dots, k_p} (-1)^{p+j-1} (p; k_1, \dots, k_p)^* \sum_{q_1, \dots, q_j} h(\mathbf{q}_Z). \quad \triangle$$

### Appendix E: Proof of Lemma 3

The multinomial coefficient  $(p; k_1, \dots, k_p)^*$  has the generating function [4]

$$j! \sum_{p=j}^{\infty} \frac{t^p}{p!} \sum_{k_1, \dots, k_p} (p; k_1, k_2, \dots, k_p)^* x_1^{k_1} x_2^{k_2} \cdots x_p^{k_p} = \left( \sum_{i=1}^{\infty} \frac{x_i}{i} t^i \right)^j \quad (\text{E1})$$

where the sums over the  $k$ 's are subject to the two constraints

$$\begin{aligned} k_1 + k_2 + \cdots + k_p &= j, \\ k_1 + 2k_2 + \cdots + pk_p &= p. \end{aligned}$$

Dividing both sides by  $j!$ , summing over  $j$ , and interchanging the  $j$  and the  $p$  summations on the left, this becomes

$$\sum_{p=0}^{\infty} \frac{t^p}{p!} \sum_{j=0}^p \sum_{k_1, \dots, k_p} (p; k_1, k_2, \dots, k_p)^* x_1^{k_1} x_2^{k_2} \cdots x_p^{k_p} = \sum_{j=0}^{\infty} \frac{1}{j!} \left( \sum_{i=1}^{\infty} \frac{x_i}{i} t^i \right)^j = \exp \left( \sum_{i=1}^{\infty} \frac{x_i}{i} t^i \right). \quad (\text{E2})$$

Now setting all  $x_i$  to 1, we get

$$\sum_{p=0}^{\infty} \frac{t^p}{p!} \sum_{j=0}^p \sum_{k_1, \dots, k_p} (p; k_1, k_2, \dots, k_p)^* = \exp \left( \sum_{i=1}^{\infty} \frac{t^i}{i} \right) = \exp(-\ln(1-t)) = \frac{1}{1-t} = \sum_{n=0}^{\infty} t^n. \quad (\text{E3})$$

Comparing the two,

$$\sum_{j=0}^p \sum_{k_1, \dots, k_p} (p; k_1, k_2, \dots, k_p)^* = p!. \quad (\text{E4})$$

Now, for a set on nonnegative integers,  $\{\beta_1, \dots, \beta_q \mid \beta_i \geq 0\}$ , we apply the differential operator

$$\frac{\partial^{\beta_1 + \beta_2 + \cdots + \beta_q}}{\partial^{\beta_1} x_1 \cdots \partial^{\beta_q} x_q}$$

to both sides of (E2) and again set all  $x_i$  equal to 1. On the right we get

$$\frac{\partial^{\beta_1 + \beta_2 + \cdots + \beta_q}}{\partial^{\beta_1} x_1 \cdots \partial^{\beta_q} x_q} \exp \left( \sum_{i=1}^{\infty} \frac{x_i}{i} t^i \right) \Big|_{x_i=1} = \frac{t^{\beta_1 + 2\beta_2 + \cdots + q\beta_q}}{1^{\beta_1} \cdots q^{\beta_q}} \sum_{n=0}^{\infty} t^n = \frac{1}{1^{\beta_1} \cdots q^{\beta_q}} \sum_{n=n_0}^{\infty} t^n, \quad (\text{E5})$$

$$\text{with } n_0 = \beta_1 + 2\beta_2 + \cdots + q\beta_q,$$

and on the left,

$$\begin{aligned} & \frac{\partial^{\beta_1 + \beta_2 + \cdots + \beta_q}}{\partial^{\beta_1} x_1 \cdots \partial^{\beta_q} x_q} \sum_{p=0}^{\infty} \frac{t^p}{p!} \sum_{j=0}^p \sum_{k_1, \dots, k_p} (p; k_1, k_2, \dots, k_p)^* x_1^{k_1} x_2^{k_2} \cdots x_p^{k_p} \Big|_{x_i=1} \\ &= \sum_{p=n_0}^{\infty} \frac{t^p}{p!} \sum_{j=0}^p \sum_{k_1, \dots, k_p} (p; k_1, k_2, \dots, k_p)^* k_1(k_1-1) \cdots (k_1-\beta_1+1) \\ & \quad \times k_2(k_2-1) \cdots (k_2-\beta_2+1) \cdots k_q(k_q-1) \cdots (k_q-\beta_q+1) \\ &= \sum_{p=n_0}^{\infty} \frac{t^p}{p!} \sum_{j=0}^p \sum_{k_1, \dots, k_p} \beta_1! \binom{k_1}{\beta_1} \cdots \beta_q! \binom{k_q}{\beta_q} (p; k_1, k_2, \dots, k_p)^*. \end{aligned} \quad (\text{E6})$$

Therefore

$$\sum_{j=0}^p \sum_{k_1, \dots, k_p} \binom{k_1}{\beta_1} \cdots \binom{k_p}{\beta_p} (p; k_1, k_2, \dots, k_p)^* = \frac{p!}{1^{\beta_1} \beta_1! 2^{\beta_2} \beta_2! \cdots p^{\beta_p} \beta_p!} \quad (\text{E7})$$

for  $p \geq \beta_1 + 2\beta_2 + \cdots + p\beta_p$ .  $\triangle$

### Appendix F: Sample calculations

As examples, we will use Theorem 3 to calculate the  $N = 7$  coefficient  $C_{0123456}$  and the  $N = 8$  coefficient  $C_{00224466}$ .

#### 1. $C_{0123456}$

Since the  $A_k$ 's are all distinct in this example, the set of partitions of the set  $\{A_1, A_2, A_3, A_4\}$ , i.e.,  $\mathcal{P}\{A_1 A_2 A_3 A_4\}$ , and the set of partitions of the set of indices of the  $A_k$ 's,  $\mathcal{P}\{1234\}$ , have the same number of elements. We will therefore use  $\mathcal{P}\{1234\}$  and the somewhat simpler expression, (10d), to find  $C_{0123456}$ :

$$C_{0123456} = -7 \times \left\{ 5! + \sum_{\Theta \in \mathcal{P}\{1234\}} \prod_{k=1}^j (z_k - 1)! \sum_{\mu=1}^j (-N)^\mu \sum_{\lambda_1, \dots, \lambda_j=0,1} \delta_{\mu, \lambda_1 + \dots + \lambda_j} H \left[ 1 - \sum_{t=1}^j \lambda_t X(\theta_t) \right] \right. \\ \left. \times \left( \begin{array}{c} 5 - \sum_{t=1}^j \lambda_t (X(\theta_t) + z_t) \\ 1 - \sum_{t=1}^j \lambda_t X(\theta_t) \end{array} \right) \prod_{s=1}^j \left( \begin{array}{c} X(\theta_s) + z_s - 1 \\ z_s - 1 \end{array} \right)^{\lambda_s} \right\}.$$

$$\mathcal{P}\{1234\} = \left\{ (1234), (123)(4), (124)(3), (134)(2), (234)(1), (12)(34), (13)(24), (14)(23), \right. \\ \left. (12)(3)(4), (13)(2)(4), (14)(2)(3), (23)(1)(4), (24)(1)(3), (34)(1)(2), (1)(2)(3)(4) \right\}.$$

The value of, for example,  $X(\theta = 1234)$  is  $X(1234) \equiv -(A_1 + A_2 + A_3 + A_4) \pmod{7} \equiv -(2 + 3 + 4 + 5) = 0$ . The rest of the  $X(\theta)$ 's are:

$$\begin{aligned} X(123) &= 5, & X(124) &= 4, & X(134) &= 3, & X(234) &= 2, \\ X(12) &= 2, & X(34) &= 5, & X(13) &= 1, & X(24) &= 6, & X(14) &= 0, & X(23) &= 0, \\ X(1) &= 5, & X(2) &= 4, & X(3) &= 3, & X(4) &= 2. \end{aligned}$$

The subset of  $\mathcal{P}\{1234\}$  of partitions that correspond to non-zero terms, for which  $1 - \sum \lambda_t X(\theta_t) \geq 0$  for at least some values of the  $\lambda_t$ 's, is then:

$$\left\{ (1234), (13)(24), (14)(23), (13)(2)(4), (14)(2)(3), (23)(1)(4) \right\}.$$

So

$$\begin{aligned}
C_{0123456} = & -7 \left\{ 5! + (-7)^{\lambda_1} 3! \binom{5-4\lambda_1}{1} \binom{3}{3}^{\lambda_1} \right\}_{\Theta=(1234)}^{\lambda_1=1} \\
& + (-7)^{\lambda_1+\lambda_2} 1!1! \binom{5-3\lambda_1-8\lambda_2}{1-\lambda_1-6\lambda_2} \binom{2}{1}^{\lambda_1} \binom{7}{1}^{\lambda_2} \Big|_{\Theta=(13)(24)}^{(\lambda_1,\lambda_2)=(1,0)} \\
& + (-7)^{\lambda_1+\lambda_2} 1!1! \binom{5-2\lambda_1-2\lambda_2}{1-0\lambda_1-0\lambda_2} \binom{1}{1}^{\lambda_1} \binom{1}{1}^{\lambda_2} \Big|_{\Theta=(14)(23)}^{(\lambda_1,\lambda_2)=(1,0),(0,1),(1,1)} \\
& + (-7)^{\lambda_1+\lambda_2+\lambda_3} 1!0!0! \binom{5-3\lambda_1-5\lambda_2-3\lambda_3}{1-\lambda_1-4\lambda_2-2\lambda_3} \binom{2}{1}^{\lambda_1} \binom{4}{0}^{\lambda_2} \binom{2}{0}^{\lambda_3} \Big|_{\Theta=(13)(2)(4)}^{(\lambda_1,\lambda_2,\lambda_3)=(1,0,0)} \\
& + (-7)^{\lambda_1+\lambda_2+\lambda_3} 1!0!0! \binom{5-2\lambda_1-5\lambda_2-4\lambda_3}{1-0\lambda_1-4\lambda_2-3\lambda_3} \binom{1}{1}^{\lambda_1} \binom{4}{0}^{\lambda_2} \binom{3}{0}^{\lambda_3} \Big|_{\Theta=(14)(2)(3)}^{(\lambda_1,\lambda_2,\lambda_3)=(1,0,0)} \\
& + (-7)^{\lambda_1+\lambda_2+\lambda_3} 1!0!0! \binom{5-2\lambda_1-6\lambda_2-3\lambda_3}{1-0\lambda_1-5\lambda_2-2\lambda_3} \binom{1}{1}^{\lambda_1} \binom{5}{0}^{\lambda_2} \binom{2}{0}^{\lambda_3} \Big|_{\Theta=(23)(1)(4)}^{(\lambda_1,\lambda_2,\lambda_3)=(1,0)} \Big\}
\end{aligned}$$

where for clarity we've indicated the particular partition that each term corresponds to and the allowed values of the  $\lambda_t$ 's. We have then

$$\begin{aligned}
C_{0123456} = & -7 \left\{ 5! - 7 \cdot 3! \binom{1}{1} \binom{3}{3} - 7 \binom{2}{0} \binom{2}{1} - 7 \binom{3}{1} \binom{1}{1} - 7 \binom{3}{1} \binom{1}{1} \right. \\
& \left. + (-7)^2 \binom{1}{1} \binom{1}{1} \binom{1}{1} - 7 \binom{2}{0} \binom{2}{1} - 7 \binom{3}{1} \binom{1}{1} - 7 \binom{3}{1} \binom{1}{1} \right\} \\
= & -105.
\end{aligned}$$

## 2. $C_{00224466}$

In this example  $M_1 = 0$  and the non-zero terms are characterized by  $\sum \lambda_t X(\theta_t) = 0$ . So only partitions  $\Theta = (\theta_1) \cdots (\theta_j)$  that contain at least one "null" part  $\theta_k$  such that  $X(\theta_k) = 0$ , will contribute; for a non-null part  $\theta_q$ ,  $\lambda_q$  must equal zero for the term to contribute to the coefficient. When  $M_1 = 0$ , the two binomial coefficients in the formula,

$$\binom{N - M_0 - 1 - \sum \lambda_t (X(\theta_t) + z_t)}{M_1 - \sum \lambda_t X(\theta_t)} \quad \text{and} \quad \binom{X(\theta_s) + z_s - 1}{z_s - 1}^{\lambda_s},$$

can both be replaced by 1. The first binomial coefficient equals 1 since, for non-zero terms, it has zero in its lower entry; in the second coefficient, either  $X(\theta_s) = 0$  or  $\lambda_s = 0$ . So we have

$$C_{00224466} = -8 \left\{ \frac{5!}{2!2!2!} + \frac{1}{2} \sum_{\Theta \in \mathcal{P}\{224466\}} \prod_{\theta} \frac{1}{\kappa_{\theta}!} \prod_{k=1}^j \frac{(z_k - 1)!}{m_2^{(\theta_k)}! m_4^{(\theta_k)}! m_6^{(\theta_k)}!} \right. \\ \left. \times \sum_{\mu=1}^j (-8)^{\mu} \sum_{\lambda_1, \dots, \lambda_j=0,1} \delta_{\mu, \lambda_1 + \dots + \lambda_j} H \left[ - \sum_{t=1}^j \lambda_t X(\theta_t) \right] \right\}.$$

The null subsets of  $\{2,2,4,4,6\}$  are (2446), (224), (44), and (26). The 10 contributing partitions are then:

$$\begin{aligned} (2446)(2) : & \quad (\lambda_1, \lambda_2) = (1, 0) \\ (224)(46) : & \quad (\lambda_1, \lambda_2) = (1, 0) \\ (226)(44) : & \quad (\lambda_1, \lambda_2) = (0, 1) \\ (244)(26) : & \quad (\lambda_1, \lambda_2) = (0, 1) \\ (224)(4)(6) : & \quad (\lambda_1, \lambda_2, \lambda_3) = (1, 0, 0) \\ (44)(26)(2) : & \quad (\lambda_1, \lambda_2, \lambda_3) = (1, 0, 0), (0, 1, 0), (1, 1, 0) \\ (44)(22)(6) : & \quad (\lambda_1, \lambda_2, \lambda_3) = (1, 0, 0) \\ (26)(24)(4) : & \quad (\lambda_1, \lambda_2, \lambda_3) = (1, 0, 0) \\ (44)(2)(2)(6) : & \quad (\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (1, 0, 0, 0) \\ (26)(2)(4)(4) : & \quad (\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (1, 0, 0, 0) \end{aligned}$$

(To simplify the expression below, we will omit the factor  $\prod_{\theta} \frac{1}{\kappa_{\theta}!}$  when all the  $\kappa$ 's equal 0 or 1.) Summing over these partitions, we get

$$\begin{aligned} C_{00224466} = & -8 \left\{ 15 - \frac{8}{2} \left[ \frac{(4-1)!(1-1)!}{1!2!1!1!0!0!} + \frac{(3-1)!(2-1)!}{2!1!0!0!1!1!} + \frac{(3-1)!(2-1)!}{2!0!1!0!2!0!} + \frac{(3-1)!(2-1)!}{1!2!0!1!0!1!} \right. \right. \\ & \left. \left. + \frac{(3-1)!(1-1)!(1-1)!}{2!1!0!0!1!0!0!0!1!} \right] \right. \\ & + 2 \times \frac{(2-1)!(2-1)!(1-1)!}{0!2!0!1!0!1!1!0!0!} + \frac{(2-1)!(2-1)!(1-1)!}{0!2!0!2!0!0!0!0!1!} + \frac{(2-1)!(2-1)!(1-1)!}{1!0!1!1!1!0!0!1!0!} \\ & \left. + \frac{1}{1!2!1!} \frac{(2-1)!(1-1)!(1-1)!(1-1)!}{0!2!0!1!0!0!1!0!0!0!0!1!} + \frac{1}{1!1!2!} \frac{(2-1)!(1-1)!(1-1)!(1-1)!}{1!0!1!1!0!0!0!1!0!0!1!0!} \right] \\ & \left. + \frac{64}{2} \frac{(2-1)!(2-1)!(1-1)!}{0!2!0!1!0!1!1!0!0!} \right\} \\ = & -120 + 96 + 32 + 16 + 32 + 32 + 32 + 8 + 32 + 8 + 16 - 128 = 56. \end{aligned}$$

For this coefficient, the W-J method is actually more efficient. The null subsets of  $\{2,2,4,4,6,6\}$  are (224466), (2266), (2446), (466), (224), (44), and (26). There are then 5 null multisets to be summed over: (224466), (2266)(44), (2446)(26), (224)(466), (26)(26)(44). We have then, using Wyn-jones' formula,

$$\begin{aligned} C_{00224466} = & (-8) \frac{(6-1)!}{2!2!2!} + (-8)^2 \frac{(4-1)!(2-1)!}{2!2!2!} + (-8)^2 \frac{(4-1)!(2-1)!}{2!} + (-8)^2 \frac{(3-1)!(3-1)!}{2!2!} \\ & + (-8)^3 \frac{1}{2!} \frac{(2-1)!(2-1)!(2-1)!}{2!} \\ = & -120 + 48 + 192 + 64 - 128 = 56. \end{aligned}$$

### Appendix G: The coefficients for the $N = 6, 7, 8$ determinants

In this section we give our results for the coefficients  $[ \{ C_{M_0 \dots M_{N-1}}^* \} ]$  for  $N=6, 7, 8$ , using Theorem 3. The results are expressed in the form of a table. In the first column are listed the allowed partitions of  $N$ ; the second and third columns list, respectively, the form of the coefficient  $C_{a_0 \dots a_{N-1}}$  and all the additive multiplets associated with this partition; and the fourth column lists the values of  $[ \{ C_{M_0 \dots M_{N-1}}^* \} ]$ .

The subscript  $n$  on  $\{C_{M_0 \dots M_{N-1}}^*\}_n$  is used to indicate the number of elements in a particular additive multiplet. To simplify the notation however it is understood that if there is no subscript then the multiplet has  $N$  elements.

Our results are:

$N = 6 :$	(12 super – multiplets).		$[ \{C_{M_0 \dots M_5}^*\} ]$
6	$C_{000000}$	$\{C_{600000}^*\}$	1
42	$C_{0000aa}$	$\{C_{400200}^*\}$	-3
411	$C_{0000ab}$	$\left\{ \begin{array}{l} \{C_{410001}^*\} \\ \{C_{401010}^*\} \end{array} \right\}$	$\left\{ \begin{array}{l} -6 \\ -6 \end{array} \right\}$
33	$C_{000aaa}$	$\{C_{303000}^*\}$	2
321	$C_{000aab}$	$\{C_{320010}^*\}, \{C_{301002}^*\}$	6
3111	$C_{000abc}$	$\{C_{311100}^*\}, \{C_{300111}^*\}$	12
222	$C_{00aabb}$	$\left\{ \begin{array}{l} \{C_{222000}^*\} \\ \{C_{202020}^*\}_{n=2} \end{array} \right\}$	$\left\{ \begin{array}{l} -9 \\ 9 \end{array} \right\}$
2211	$C_{00aabc}$	$\left\{ \begin{array}{l} \{C_{210120}^*\} \\ \{C_{210201}^*\} \end{array} \right\}$	$\left\{ \begin{array}{l} -18 \\ 0 \end{array} \right\}$
21111	$C_{00abcd}$	$\{C_{211011}^*\}$	0

$N = 7 :$	(12 super – multiplets)		$[ \{C_{M_0 \dots M_6}^*\} ]$
7	$C_{0000000}$	$\{C_{7000000}^*\}$	1
511	$C_{00000ab}$	$\{C_{5100001}^*\}, \{C_{5010010}^*\}, \{C_{5001100}^*\}$	-7
421	$C_{0000aab}$	$\{C_{4200010}^*\}, \{C_{4021000}^*\}, \{C_{4102000}^*\}, \{C_{4000201}^*\}, \{C_{4000120}^*\}, \{C_{4010002}^*\}$	7
4111	$C_{0000abc}$	$\{C_{4110100}^*\}, \{C_{4001011}^*\}$	14
331	$C_{000aaab}$	$\{C_{3300100}^*\}, \{C_{3130000}^*\}, \{C_{3003010}^*\}$	-7
322	$C_{000aabb}$	$\{C_{3200002}^*\}, \{C_{3020020}^*\}, \{C_{3002200}^*\}$	14
3211	$C_{000aabc}$	$\{C_{3211000}^*\}, \{C_{3020101}^*\}, \{C_{3012001}^*\}, \{C_{3100210}^*\}, \{C_{3101020}^*\}, \{C_{3000112}^*\}$	-21
31111	$C_{000abcd}$	$\{C_{3110011}^*\}, \{C_{3011110}^*\}, \{C_{3101101}^*\}$	7
2221	$C_{00aabb}$	$\{C_{1002022}^*\}, \{C_{1220200}^*\}$	-7
22111	$C_{00aabcd}$	$\left\{ \begin{array}{l} \{C_{1012210}^*\}, \{C_{1201102}^*\}, \{C_{1120021}^*\} \\ \{C_{1102201}^*\}, \{C_{1210012}^*\}, \{C_{1021120}^*\} \end{array} \right\}$	$\left\{ \begin{array}{l} -14 \\ 35 \end{array} \right\}$
1111111	$C_{0abcdef}$	$\{C_{1111111}^*\}_{n=1}$	-105

$N = 8 : (49 \text{ super - multiplets})$			$[ \{ C_{M_0 \dots M_7}^* \} ]$
8	$C_{00000000}$	$\{ C_{80000000}^* \}$	1
62	$C_{000000aa}$	$\{ C_{60002000}^* \}$	-4
611	$C_{000000ab}$	$\left\{ \begin{array}{l} \{ C_{61000001}^* \}, \{ C_{60010100}^* \} \\ \{ C_{60100010}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} -8 \\ -8 \end{array} \right\}$
521	$C_{00000aab}$	$\left\{ \begin{array}{l} \{ C_{52000010}^* \}, \{ C_{50120000}^* \}, \{ C_{50000210}^* \}, \{ C_{50100002}^* \} \\ \{ C_{50201000}^* \}, \{ C_{50001020}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} 8 \\ 8 \end{array} \right\}$
5111	$C_{00000abc}$	$\left\{ \begin{array}{l} \{ C_{51100100}^* \}, \{ C_{50010011}^* \} \\ \{ C_{51011000}^* \}, \{ C_{50001101}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} 16 \\ 16 \end{array} \right\}$
44	$C_{0000aaaa}$	$\left\{ \begin{array}{l} \{ C_{40400000}^* \} \\ \{ C_{40004000}^* \}_{n=4} \end{array} \right\}$	$\left\{ \begin{array}{l} -2 \\ 6 \end{array} \right\}$
431	$C_{0000aaab}$	$\{ C_{43000100}^* \}, \{ C_{40030001}^* \}, \{ C_{41000300}^* \}, \{ C_{40010003}^* \}$	-8
422	$C_{0000aabb}$	$\left\{ \begin{array}{l} \{ C_{42020000}^* \}, \{ C_{40000202}^* \} \\ \{ C_{40200020}^* \} \\ \{ C_{42000002}^* \}, \{ C_{40020200}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} -12 \\ 20 \\ 20 \end{array} \right\}$
4211	$C_{0000aabc}$	$\left\{ \begin{array}{l} \{ C_{42101000}^* \}, \{ C_{40021010}^* \}, \{ C_{40101200}^* \}, \{ C_{40001012}^* \} \\ \{ C_{41210000}^* \}, \{ C_{41010020}^* \}, \{ C_{40200101}^* \}, \{ C_{40000121}^* \} \\ \{ C_{41002001}^* \}, \{ C_{40012100}^* \} \\ \{ C_{40102010}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} -24 \\ -24 \\ 8 \\ 8 \end{array} \right\}$
41111	$C_{0000abcd}$	$\left\{ \begin{array}{l} \{ C_{41100011}^* \}, \{ C_{40110110}^* \} \\ \{ C_{41010101}^* \} \\ \{ C_{41001110}^* \}, \{ C_{40111001}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} 16 \\ 16 \\ -48 \end{array} \right\}$
332	$C_{000aaabb}$	$\left\{ \begin{array}{l} \{ C_{23000003}^* \}, \{ C_{20030300}^* \} \\ \{ C_{20300030}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} 16 \\ -16 \end{array} \right\}$
3311	$C_{000aaabc}$	$\left\{ \begin{array}{l} \{ C_{33110000}^* \}, \{ C_{31030010}^* \}, \{ C_{30100301}^* \}, \{ C_{30000113}^* \} \\ \{ C_{00130310}^* \} \\ \{ C_{01030301}^* \} \\ \{ C_{01300031}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} 32 \\ 32 \\ -32 \\ -32 \end{array} \right\}$
3221	$C_{000aabbc}$	$\left\{ \begin{array}{l} \{ C_{32100020}^* \}, \{ C_{30220010}^* \}, \{ C_{30100220}^* \}, \{ C_{30200012}^* \} \\ \{ C_{32001200}^* \}, \{ C_{30021002}^* \} \\ \{ C_{32002010}^* \}, \{ C_{30122000}^* \}, \{ C_{30002210}^* \}, \{ C_{30102002}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} -16 \\ 48 \\ 16 \end{array} \right\}$
32111	$C_{000aabcd}$	$\left\{ \begin{array}{l} \{ C_{32100101}^* \}, \{ C_{30020111}^* \}, \{ C_{31110200}^* \}, \{ C_{31010012}^* \} \\ \{ C_{32010110}^* \}, \{ C_{31120001}^* \}, \{ C_{31000211}^* \}, \{ C_{30110102}^* \} \\ \{ C_{32011001}^* \}, \{ C_{31021100}^* \}, \{ C_{30011201}^* \}, \{ C_{31001102}^* \} \\ \{ C_{31201001}^* \}, \{ C_{30011120}^* \}, \{ C_{30211100}^* \}, \{ C_{31001021}^* \} \\ \{ C_{31200110}^* \}, \{ C_{30110021}^* \} \\ \{ C_{31102100}^* \}, \{ C_{30012011}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} -32 \\ 32 \\ -32 \\ 32 \\ -32 \\ 32 \end{array} \right\}$
311111	$C_{000abcde}$	$\{ C_{31111010}^* \}, \{ C_{30101111}^* \}$	64
2222	$C_{00aabbcc}$	$\left\{ \begin{array}{l} \{ C_{20022200}^* \} \\ \{ C_{02200022}^* \} \\ \{ C_{20202020}^* \}_{n=2} \end{array} \right\}$	$\left\{ \begin{array}{l} 8 \\ 56 \\ 56 \end{array} \right\}$
22211	$C_{00aabbcd}$	$\left\{ \begin{array}{l} \{ C_{00122210}^* \}, \{ C_{02102012}^* \} \\ \{ C_{01022201}^* \}, \{ C_{02012102}^* \} \\ \{ C_{22120010}^* \}, \{ C_{20100212}^* \} \\ \{ C_{00212120}^* \}, \{ C_{01202021}^* \} \end{array} \right\}$	$\left\{ \begin{array}{l} -48 \\ 16 \\ -80 \\ -16 \end{array} \right\}$
221111	$C_{00abcde}$	$\left\{ \begin{array}{l} \{ C_{22111100}^* \}, \{ C_{21021011}^* \}, \{ C_{21101201}^* \}, \{ C_{20011112}^* \} \\ \{ C_{02110112}^* \} \\ \{ C_{21102011}^* \} \\ \{ C_{21012101}^* \}_{n=4} \end{array} \right\}$	$\left\{ \begin{array}{l} -32 \\ 32 \\ -160 \\ 96 \end{array} \right\}$
2111111	$C_{00abcdef}$	$\{ C_{21110111}^* \}$	-64

To avoid writing out all  $N$  of the circular permutations for the  $N = 7$  and 8 determinants, we will use the short-hand notations “ $+\dots$ ” and “ $\pm\dots$ ” to mean, respectively, “plus all cyclic permutations of the preceding terms” and “plus all alternating-in-sign cyclic permutations of the preceding terms”. Then the determinants are:

$$\begin{aligned}
\det[A, B, C, D, E, F] = & A^6 - B^6 + C^6 - D^6 + E^6 - F^6 \\
& - 3 [ A^4 D^2 - B^4 E^2 + C^4 F^2 - D^4 A^2 + E^4 B^2 - F^4 C^2 ] \\
& - 6 [ A^4 B F - B^4 C A + C^4 D B - D^4 E C + E^4 F D - F^4 A E ] \\
& - 6 [ A^4 C E - B^4 D F + C^4 E A - D^4 F B + E^4 A C - F^4 B D ] \\
& + 2 [ A^3 C^3 - B^3 D^3 + C^3 E^3 - D^3 F^3 + E^3 A^3 - F^3 B^3 ] \\
& + 6 [ A^3 B^2 E - B^3 C^2 F + C^3 D^2 A - D^3 E^2 B + E^3 F^2 C - F^3 A^2 D ] \\
& + 6 [ A^3 C F^2 - B^3 D A^2 + C^3 E B^2 - D^3 F C^2 + E^3 A D^2 - F^3 B E^2 ] \\
& + 12 [ A^3 B C D - B^3 C D E + C^3 D E F - D^3 E F A + E^3 F A B - F^3 A B C ] \\
& + 12 [ A^3 D E F - B^3 E F A + C^3 F A B - D^3 A B C + E^3 B C D - F^3 C D E ] \\
& - 9 [ A^2 B^2 C^2 - B^2 C^2 D^2 + C^2 D^2 E^2 - D^2 E^2 F^2 + E^2 F^2 A^2 - F^2 A^2 B^2 ] \\
& + 9 [ A^2 C^2 E^2 - B^2 D^2 F^2 ] \\
& - 18 [ A^2 B D E^2 - B^2 C E F^2 + C^2 D F A^2 - D^2 E A B^2 + E^2 F B C^2 - F^2 A C D^2 ];
\end{aligned}$$

$$\begin{aligned}
\det[A, B, C, D, E, F, G] = & A^7 + B^7 + C^7 + D^7 + E^7 + F^7 + G^7 \\
& - 7 [ A^5 B G + A^5 C F + A^5 D E + \dots ] \\
& + 7 [ A^4 B^2 F + A^4 C^2 D + A^4 B D^2 + A^4 E^2 G + A^4 E F^2 + A^4 C G^2 + \dots ] \\
& + 14 [ A^4 B C E + A^4 D F G + \dots ] \\
& - 7 [ A^3 B^3 E + A^3 B C^3 + A^3 D^3 F + \dots ] \\
& + 14 [ A^3 B^2 G^2 + A^3 C^2 F^2 + A^3 D^2 E^2 + \dots ] \\
& - 21 [ A^3 B^2 C D + A^3 C^2 E G + A^3 C D^2 G + A^3 B E^2 F + A^3 B D F^2 + A^3 E F G^2 + \dots ] \\
& + 7 [ A^3 B C F G + A^3 C D E F + A^3 B D E G + \dots ] \\
& - 7 [ A^2 B^2 C F^2 + A^2 B^2 D^2 G + \dots ] \\
& - 14 [ A^2 B^2 C E G + A^2 B C^2 E F + A^2 D^2 E F G + \dots ] \\
& + 35 [ A^2 B^2 D E F + A^2 B C^2 D G + A^2 B C D^2 F + \dots ] \\
& - 105 A B C D E F G;
\end{aligned}$$

$$\begin{aligned}
\det[A, B, C, D, E, F, G, H] = & A^8 - B^8 + C^8 - D^8 + E^8 - F^8 + G^8 - H^8 \\
& - 4 [ A^6 E^2 \pm \dots ] \\
& - 8 [ A^6 B H + A^6 D F \pm \dots ] - 8 [ A^6 C G \pm \dots ] \\
& + 8 [ A^5 B^2 G + A^5 C D^2 + A^5 F^2 G + A^5 C H^2 \pm \dots ] + 8 [ A^5 C^2 E + A^5 E G^2 \pm \dots ] \\
& + 16 [ A^5 B C F + A^5 D G H \pm \dots ] + 16 [ A^5 B D E + A^5 E F H \pm \dots ] \\
& - 2 [ A^4 C^4 \pm \dots ] + 6 [ A^4 E^4 - B^4 F^4 + C^4 G^4 - D^4 H^4 ] \\
& - 8 [ A^4 B^3 F + A^4 D^3 H + A^4 B F^3 + A^4 D H^3 \pm \dots ] \\
& - 12 [ A^4 B^2 D^2 + A^4 F^2 H^2 \pm \dots ] + 20 [ A^4 C^2 G^2 \pm \dots ] + 20 [ A^4 B^2 H^2 + A^4 D^2 F^2 \pm \dots ] \\
& - 24 [ A^4 B^2 C E + A^4 D^2 E G + A^4 C E F^2 + A^4 E G H^2 \pm \dots ] \\
& \quad - 24 [ A^4 B C^2 D + A^4 B D G^2 + A^4 C^2 F G + A^4 F G^2 H \pm \dots ] \\
& \quad + 8 [ A^4 B E^2 H + A^4 D E^2 F \pm \dots ] + 8 [ A^4 C E^2 G \pm \dots ] \\
& + 16 [ A^4 B C G H + A^4 C D F G \pm \dots ] + 16 [ A^4 B D F H \pm \dots ] \\
& \quad - 48 [ A^4 B E F G + A^4 C D E H \pm \dots ] \\
& + 16 [ A^3 B^2 C^3 + A^3 D^2 G^3 \pm \dots ] - 16 [ A^3 C^2 E^3 \pm \dots ] \\
& + 32 [ A^3 B^3 C D + A^3 B D^3 G + A^3 C F^3 H + A^3 F G H^3 \pm \dots ] \\
& \quad + 32 [ A^3 C^3 D H \pm \dots ] - 32 [ A^3 C^3 E G \pm \dots ] - 32 [ A^3 B D E^3 \pm \dots ] \\
& - 16 [ A^3 B^2 C G^2 + A^3 C^2 D^2 G + A^3 C F^2 G^2 + A^3 C^2 G H^2 \pm \dots ] \\
& \quad + 48 [ A^3 B^2 E F^2 + A^3 D^2 E H^2 \pm \dots ] \\
& \quad + 16 [ A^3 B^2 E^2 G + A^3 C D^2 E^2 + A^3 E^2 F^2 G + A^3 C E^2 H^2 \pm \dots ] \\
& - 32 [ A^3 B^2 C F H + A^3 D^2 F G H + A^3 B C D F^2 + A^3 B D G H^2 \pm \dots ] \\
& \quad + 32 [ A^3 B^2 D F G + A^3 B C D^2 H + A^3 B F^2 G H + A^3 C D F H^2 \pm \dots ] \\
& \quad - 32 [ A^3 B^2 D E H + A^3 B D^2 E F + A^3 D E F^2 H + A^3 B E F H^2 \pm \dots ] \\
& \quad + 32 [ A^3 B C^2 E H + A^3 D E F G^2 + A^3 C^2 D E F + A^3 B E G^2 H \pm \dots ] \\
& \quad - 32 [ A^3 B C^2 F G + A^3 C D G^2 H \pm \dots ] \\
& \quad + 32 [ A^3 B C E^2 F + A^3 D E^2 G H \pm \dots ] \\
& + 64 [ A^3 B C D E G + A^3 C E F G H \pm \dots ] \\
& + 8 [ A^2 B^2 C^2 F^2 \pm \dots ] + 56 [ A^2 B^2 D^2 E^2 \pm \dots ] + 56 [ A^2 C^2 E^2 G^2 - B^2 D^2 F^2 H^2 ] \\
& - 48 [ A^2 B^2 C^2 D H + A^2 B D^2 F G^2 \pm \dots ] + 16 [ A^2 B^2 C^2 E G + A^2 C D^2 E G^2 \pm \dots ] \\
& \quad - 80 [ A^2 B^2 C D^2 G + A^2 C F^2 G H^2 \pm \dots ] - 16 [ A^2 B C^2 D E^2 + A^2 B D E^2 G^2 \pm \dots ] \\
& - 32 [ A^2 B^2 C D E F + A^2 B D^2 E G H + A^2 B C E F^2 H + A^2 D E F G H^2 \pm \dots ] \\
& \quad + 32 [ A^2 B C E F G^2 \pm \dots ] - 160 [ A^2 B C E^2 G H \pm \dots ] \\
& \quad + 96 [ A^2 B D E^2 F H - B^2 C E F^2 G A + C^2 D F G^2 H B - D^2 E G H^2 A C ] \\
& - 64 [ A^2 B C D F G H \pm \dots ].
\end{aligned}$$

There are various methods that can be used to check these results. One way is to use the identities

$$\begin{aligned}
\det[1, 1, \dots, 1] &= 0, \\
\det[0, 1, \dots, 1] &= (-1)^{N-1} (N-1).
\end{aligned}$$

[The second identity follows directly from eqs.(2) and (7)]. The first identity does not however constitute a check for even  $N$ ; since the coefficients in additive multiplets alternate in sign, it is satisfied automatically. As sums over multiplets, these identities are:

$$\begin{aligned}
& \sum n [ \{ C_{M_0 M_1 \dots M_{N-1}}^* \} ] = 0, \quad (N \text{ odd}), \\
& \sum \frac{n}{N} [ \{ C_{M_0 M_1 \dots M_{N-1}}^* \} ] \sum_{k=0}^{N-1} (-1)^{k(N-1)} \delta_{M_k, 0} = (-1)^{N-1} (N-1).
\end{aligned}$$

Another method, when  $N$  is divisible by some integer  $d$  and when the coefficients for the smaller  $(N/d)$ -dimensional determinant are known, is to use the relation

$$\det[x_0, 0, \dots, 0, x_d, 0, \dots, 0, x_{2d}, 0, \dots, 0, x_{N-d}, 0, \dots, 0] = ( \det[x_0, x_d, x_{2d}, \dots, x_{N-d}] )^d,$$

where the only non-zero matrix elements in the determinant on the left are those of the form  $x_{nd \bmod N}$ . For example, for  $N = 6$  and  $d = 2$ ,

$$\det[A, 0, C, 0, E, 0] = ( \det[A, C, E] )^2 = (A^3 + C^3 + E^3 - 3ACE)^2.$$

Expanding the right side, all coefficients of the form  $C_{M_0 0 M_2 0 M_4 0}^*$  can be read off and compared with the calculated values.

- 
- [1] Wyn-Jones, Alun, *Circulants*, Chapters 10 and 11. [www.circulants.org/circ/circall.pdf](http://www.circulants.org/circ/circall.pdf).  
 [2] Ore, Oyster, "Some Studies on Cyclic Determinants", *Duke Mathematical Journal*, **18**, 1951, pp. 343-354.  
 [3] Wikipedia, *Möbius function*. [http://en.wikipedia.org/wiki/Möbius\\_function](http://en.wikipedia.org/wiki/Möbius_function).  
 [4] Abramowitz and Stegun, *Handbook of Mathematical Functions*, Section 24.1, pg. 823.  
 [5] "The Online Encyclopedia of Integer Sequences", published electronically at <http://oeis.org>, 2010.  
 [6] Brualdi and Newman, "An Enumeration Problem for a Congruence Equation", *J. Res. Nat. Bureau Standards*, B74 (1970), 37-40.  
 [7] Weisstein, Eric W., "Totient Function". <http://mathworld.wolfram.com/TotientFunction.html>.  
 [8] Weisstein, Eric W., "Modulo Multiplication Group." <http://mathworld.wolfram.com/ModuloMultiplicationGroup.html>.