Smith normal form of the n-cycle class sum

P. Graham
https://orcid.org/0009-0007-8493-1505

October 25, 2026

Abstract

We determine the Smith normal form of multiplication by the sum of all n-cycles on the center of $\mathbb{Z}S_n$. For every $n \geq 1$, it has $p(n) - n$ zero entries, where $p(n)$ counts partitions of n, and nonzero factors $d_0 = 1$ and $d_r = a_r r!/\gcd(n, r)$ for $1 \leq r < n$, with $a_r = 2$ when $r \equiv n \pmod 2$ and $a_r = 1$ otherwise. This confirms Stanley's conjectures for odd primes and twice odd primes and gives the n-cycle formula for every positive n. Goupil and Schaeffer gave a formula for long-cycle connection coefficients, and Biane gave an algebraic proof. We determine the two integral coefficient lattices needed to extract its Smith factors, then prove rowwise divisibility. Grinberg's exposition supplies class-sum and representation-theory background used here. Lean proves the image-lattice statement and divisor chain directly from group-ring definitions, including the character formula. The diagonal form and prime cases follow by written arguments.

1 Introduction

Here S_n denotes the symmetric group on n letters. For a partition $\mu \vdash n$, write K_μ for the sum of the permutations of cycle type μ in $\mathbb{Z}S_n$. The elements K_μ form a $\mathbb{Z}$-basis of the center $Z(\mathbb{Z}S_n)$, identifying it with $\mathbb{Z}^{p(n)}$, where $p(n)$ is the number of partitions of n. We consider the matrix M_n defined by

$$K_{(n)} K_\nu = \sum_{\mu \vdash n} M_n[\mu, \nu] K_\mu. \tag{1}$$

Thus the rows record output cycle types and the columns record input cycle types. Write SNF for Smith normal form.

Theorem 1.1. *Let $n \geq 1$, and let $p(n)$ denote the number of partitions of n. Define*

$$d_0 = 1, \qquad d_r = \frac{a_r r!}{\gcd(n, r)} \quad (1 \leq r < n), \qquad a_r = \begin{cases} 2 & r \equiv n \pmod 2, \\ 1 & r \not\equiv n \pmod 2. \end{cases} \tag{2}$$

These are positive integers satisfying $d_r \mid d_{r+1}$ for $0 \leq r < n - 1$. There is a basis

$$b_0, \ldots, b_{n-1}, b'_1, \ldots, b'_{p(n)-n}$$

of $\mathbb{Z}^{p(n)}$ such that

$$M_n \mathbb{Z}^{p(n)} = \bigoplus_{r=0}^{n-1} d_r \mathbb{Z} b_r. \tag{3}$$

Consequently, $\mathrm{SNF}(M_n) = \mathrm{diag}(d_0, \ldots, d_{n-1}, 0, \ldots, 0)$, *with $p(n) - n$ zeros.*

The Smith normal form of an integer matrix A is a diagonal matrix obtained by invertible integral row and column operations, with positive nonzero entries $d_0 \mid d_1 \mid \cdots$ followed by zeros. Equivalently, it describes the embedding of the column lattice of A in its ambient free abelian group up to integral changes of basis.

For example, the nonzero factors for $n = 4$ are $(1, 1, 2, 6)$. Stanley observed that the rank is n before stating his two conjectures [9, paragraph preceding the two specific conjectures]. Conjectures (a) and (b) ask for the odd-prime and twice-odd-prime cases; Stanley also suggested that further data might lead to a conjecture for all n [9, paragraph following conjecture (b)]. Theorem 1.1 gives the n-cycle formula. His broader question also concerns other conjugacy classes and finite groups [9, opening and final paragraphs]. Stanley cites Lindzey's question as his motivation [9, opening paragraph]. Lindzey studies the adjacency matrix of the Cayley graph generated by all n-cycles [5, opening paragraph]. That adjacency operator acts on the full group algebra; here multiplication is restricted to its center.

Goupil and Schaeffer's formula gives the long-cycle connection coefficients [3, equation (4), as identified in Biane]. Biane gives an algebraic proof of that formula [1, opening and equation (2)]; our proof starts with its hook-character expression. Our contribution is to determine the two integral lattices in that rational pairing. The main difficulty is their integral structure: the normalized vectors require an integrality and spanning argument, while the other lattice is determined by a parity invariant. Stanley [7, Lemma 2.1] gives the long-cycle hook values, and Lemma 2.2 gives the dimensions. Grinberg's exposition [4, Definition 3.9.4(c), Theorem 3.9.5 and Corollary 5.17.41] supplies the class-sum and representation-theory background used here. Sagan [6, §4.10] is another reference for the Murnaghan–Nakayama rule. Related Smith-form results are [8, Theorems 5.1–5.2] and [2, Theorem 1.2]. Both concern a different operator on Young's lattice.

The image-lattice theorem and divisor chain are checked in Lean from these definitions; this paper has not yet been reviewed by experts. The proofs, the Lean formalization and the text were produced by AI models (from OpenAI and Anthropic), working under the author's direction.

The proof proceeds as follows. The hook-character formula expresses M_n as a rational pairing. After shifting the character-generating variable, its coefficient matrix vanishes beyond the anti-diagonal. We prove that the normalized coefficient vectors span $\mathbb{Z}^n$, then construct a triangular basis for the other integral coefficient lattice. Divisibility in each row reduces the pairing to a diagonal matrix times a unimodular matrix. A left inverse then extends the resulting vectors to a basis of the full class-sum lattice, giving the Smith form.

2 The character formula and a change of basis

The character formula takes a particularly useful form in shifted polynomial coordinates. Fix $n \geq 1$ and put $N = n - 1$. For $\mu \vdash n$, let $\ell(\mu)$ be its number of parts and $m_j(\mu)$ the multiplicity of j. Set

$$z_\mu = \prod_{j \geq 1} j^{m_j(\mu)} m_j(\mu)!, \qquad \epsilon_\mu = (-1)^{\ell(\mu)-1}.$$

The number z_μ is the order of the centralizer of a permutation of type μ. Write $\chi_k = \chi^{(n-k,1^k)}$ for the hook character, where $0 \leq k \leq N$. The hook characters are the characters of the exterior powers of the standard representation, so

$$\sum_{k=0}^{N} \chi_k(\mu) q^k = \frac{\prod_{j=1}^{\ell(\mu)} (1 - (-q)^{\mu_j})}{1 + q}. \tag{4}$$

Indeed, the characteristic polynomial on the permutation representation is the product of the characteristic polynomials of its cycles. Removing its one-dimensional trivial summand divides the exterior-power generating function by $1+q$.

For Frobenius's formula and the hook restriction used below, see Biane [1, equations (1)–(2) and the intervening hook restriction].

Proposition 2.1. *For $\mu, \nu \vdash n$,*

$$M_n[\mu,\nu] = \frac{1}{z_\nu}\sum_{k=0}^{N}(-1)^k k!(N-k)!\chi_k(\mu)\chi_k(\nu). \tag{5}$$

Proof. Frobenius's class-multiplication formula gives

$$M_n[\mu,\nu] = \frac{|K_{(n)}|\,|K_\nu|}{n!}\sum_{\lambda\vdash n}\frac{\chi^\lambda((n))\chi^\lambda(\nu)\chi^\lambda(\mu)}{\chi^\lambda(1)}.$$

All symmetric-group characters here are real, and every conjugacy class is closed under inversion. By the Murnaghan–Nakayama rule, only hooks contribute: $\chi_k((n)) = (-1)^k$. Their dimensions are $\binom{N}{k}$, while $|K_{(n)}| = N!$ and $|K_\nu| = n!/z_\nu$. Substitution gives (5). □

To relate the normalization to the factorization literature, let $c_{\mu\nu}^{(n)}$ count the factorizations of a fixed n-cycle as a product of permutations of types μ and ν. Biane's formula [1, equation (2)], identified there with equation (4) of Goupil and Schaeffer [3], gives

$$c_{\mu\nu}^{(n)} = \frac{n}{z_\mu z_\nu}\sum_{k=0}^{N}(-1)^k k!(N-k)!\chi_k(\mu)\chi_k(\nu).$$

Thus $M_n[\mu,\nu] = (z_\mu/n)c_{\mu\nu}^{(n)}$. The multiplier depends on the row and can be nonintegral, so the integral lattices must also be determined. The character expression supplies the entries, while the lattice arguments below determine their integral invariant factors.

Brackets denote coefficient extraction. Introduce polynomials

$$H_\mu(y) = \prod_{j=1}^{\ell(\mu)}((1+y)^{\mu_j}-1), \qquad \eta_\mu(i) = [y^{i+1}]H_\mu(y), \quad 0\le i\le N,$$

$$\Phi_\mu(y) = \frac{H_\mu(y)}{z_\mu}, \qquad e_s = s!\,\gcd(n,s+1), \quad 0\le s\le N.$$

The order of H_μ is $\ell(\mu)$, and its lowest coefficient is $\prod_j \mu_j$. For $0\le i,s\le N$, define

$$Q(i,s) = \begin{cases}(-1)^{i+s}\dfrac{(N-i)!(N-s)!}{(N-i-s)!}, & i+s\le N,\\ 0, & i+s>N.\end{cases} \tag{6}$$

Lemma 2.2. *For $0\le i,s\le N$,*

$$\sum_{k=0}^{N}(-1)^k k!(N-k)![x^k](x-1)^i\,[x^k](x-1)^s = Q(i,s).$$

Consequently,

$$M_n[\mu,\nu] = \frac{\epsilon_\mu\epsilon_\nu}{z_\nu}\sum_{i,s=0}^{N}\eta_\mu(i)Q(i,s)\eta_\nu(s). \tag{7}$$

The coefficient identity follows by repeated use of Pascal's identity; the calculation is in Appendix A.

3 The normalized coefficient lattice

This section proves that the normalized coefficient vectors span the full integer lattice. Define the rational vector $\alpha(\nu)$ by

$$\alpha(\nu)_s = \epsilon_\nu e_s[y^{s+1}]\Phi_\nu = \frac{\epsilon_\nu e_s \eta_\nu(s)}{z_\nu}.$$

In the proof, v_p denotes the p-adic valuation; the product formula for Φ_μ extends its definition to arbitrary multisets.

Lemma 3.1. *The vectors $\alpha(\nu)$, for $\nu \vdash n$, belong to $\mathbb{Z}^n$ and span $\mathbb{Z}^n$ over $\mathbb{Z}$.*

Proof. We first prove integrality. Allow μ to be any multiset of positive integers, including the empty multiset, and put

$$\phi_j(y) = \frac{(1+y)^j - 1}{j}, \qquad \Phi_\mu = \prod_{j\geq 1} \frac{\phi_j^{m_j(\mu)}}{m_j(\mu)!}, \qquad I_t(\mu) = t![y^t]\Phi_\mu.$$

For the empty multiset, $\Phi_\varnothing = 1$. Removing one part j is denoted by $\mu - j$. Since $\phi_j' = (1+y)^{j-1}$,

$$\Phi_\mu' = \sum_{j:m_j(\mu)>0} (1+y)^{j-1}\Phi_{\mu-j}. \tag{8}$$

Induction on the sum of the parts proves $I_t(\mu) \in \mathbb{Z}$ for every $t \geq 0$. The constant coefficient is immediate; for $t \geq 1$, (8) expresses $I_t(\mu)$ as a sum of

$$\binom{j-1}{i} \frac{(t-1)!}{(t-1-i)!} I_{t-1-i}(\mu - j), \qquad 0 \leq i \leq \min(j-1, t-1),$$

each an integer by induction.

When the sum of the parts is n, the identity $jm_j(\mu)\Phi_\mu = ((1+y)^j - 1)\Phi_{\mu-j}$ yields

$$n\Phi_\mu = \sum_{j:m_j(\mu)>0} ((1+y)^j - 1)\Phi_{\mu-j}. \tag{9}$$

For $t \geq 1$, multiply the coefficient of y^t by $(t-1)!$. The right side is a sum of

$$\binom{j}{i} \frac{(t-1)!}{(t-i)!} I_{t-i}(\mu - j), \qquad 1 \leq i \leq \min(j, t),$$

so $nI_t(\mu)/t$ is an integer. Bézout's identity for n and t then shows that $\gcd(n,t)I_t(\mu)/t$ is an integer. Setting $t = s+1$ proves the required integrality.

For spanning, fix a length $\ell = s+1$. The vectors from partitions of this length vanish in coordinates below s, and their sth coordinates, up to sign, are

$$\frac{(\ell-1)!\gcd(n,\ell)}{\prod_j m_j(\nu)!}. \tag{10}$$

We show that the gcd of these integers is one. If $\ell = n$, the partition 1^n gives one. Suppose $\ell < n$, fix a prime p, and write $v = v_p(\gcd(n,\ell))$. If $v = 0$, the partition $(n-\ell+1, 1^{\ell-1})$ gives $\gcd(n,\ell)$, prime to p. If $v > 0$, put $q = p^v$ and $A = (n-\ell)/q + 1 \geq 2$. The partition $(A^q, 1^{\ell-q})$ gives

$$\binom{\ell-1}{q-1} \frac{\gcd(n,\ell)}{q}.$$

The second factor is prime to p. In $\binom{\ell-1}{q-1} = \prod_{i=1}^{q-1}(\ell-i)/i$, the valuations of numerator and denominator agree term by term, because $v_p(i) < v \le v_p(\ell)$. Thus the first factor is also prime to p. No prime divides every number in (10). Bézout therefore gives a combination f_s of the length-$s+1$ vectors with coordinate one at s and zero below it. The vectors $f_0, \dots, f_N$ form a unitriangular integral matrix, hence a basis of $\mathbb{Z}^n$. □

4 The integral coefficient lattice

This section gives a triangular basis for the unnormalized coefficient lattice. Let U be the $\mathbb{Z}$-span of the vectors η_μ in $\mathbb{Z}^n$. Extend the notation (2) by setting $a_0 = n$, so that $d_r = a_r r!/\gcd(n,r)$ also holds at $r = 0$, using $\gcd(n,0) = n$.

Lemma 4.1. *The lattice U has a basis $u_0, \dots, u_N$ such that $u_r(i) = 0$ for $i < r$ and $u_r(r) = a_r$. Each u_r is an integral combination of the η_μ with $\ell(\mu) = r+1$.*

Proof. Take $u_0 = \eta_{(n)}$. When $N > 0$, take $u_N = \eta_{1^n}$. For $1 \le r < N$, the two partitions

$$(n-r, 1^r), \qquad (n-r-1, 2, 1^{r-1})$$

have length $r+1$ and leading coefficients $n-r$ and $2(n-r-1)$. Their gcd is $\gcd(n-r, 2) = a_r$, so Bézout gives the desired u_r. This constructs independent vectors with the asserted leading terms.

We prove that they span. Identify $v \in \mathbb{Z}^n$ with $\sum_{i=0}^N v(i)y^i$. Every $v \in U$ satisfies $n \mid v(0)$. It also satisfies

$$T_N(v) \equiv v \pmod 2, \qquad T_m(f) = (1+y)^m f\big(y/(1+y)\big). \tag{11}$$

Indeed, $T_{a+b}(fg) = T_a(f)T_b(g)$ and

$$T_m((1+y)^m - 1) = (1+2y)^m - (1+y)^m \equiv (1+y)^m - 1 \pmod 2.$$

Consequently $T_n(H_\mu) \equiv H_\mu \pmod 2$. Since $T_n(H_\mu) = yT_N(H_\mu/y)$, cancellation of y proves (11) on the generators and hence on U.

Suppose $v(i) = 0$ for $i < r$. At $r = 0$ we have $a_0 \mid v(0)$. For $1 \le r < N$, comparing coefficients of y^{r+1} in (11) gives $(N-r)v(r) \equiv 0 \pmod 2$. When $r \equiv n \pmod 2$, the factor $N-r$ is odd, so $a_r = 2$ divides $v(r)$. In all other cases, including $r = N$, $a_r = 1$. Subtracting $(v(r)/a_r)u_r$, successively for $r = 0, \dots, N$, therefore expresses every element of U in the constructed basis. □

5 Divisibility of the pairing

This section proves the divisibility needed for each row of the pairing. For a partition μ and $0 \le s \le N$, put

$$\Gamma(\mu, s) = \frac{1}{e_s} \sum_{i=0}^{N} \eta_\mu(i) Q(i,s).$$

Lemma 5.1. *If $\ell(\mu) = r+1$, then $\Gamma(\mu, s) \in d_r\mathbb{Z}$ for every s.*

Proof. Rewrite (6) as

$$Q(i,s) = (-1)^{i+s} s!(N-s)! \binom{N-i}{s}.$$

Thus, for the integer $X_s = \sum_i (-1)^i \binom{N-i}{s} \eta_\mu(i)$,

$$\Gamma(\mu, s) = (-1)^s \frac{(N-s)!}{\gcd(n, s+1)} X_s. \tag{12}$$

Terms vanish unless $r \le i \le N - s$. If $s > N - r$ the assertion follows at once. If $s = N - r$, then $X_s = (-1)^r \prod_j \mu_j$ and

$$\Gamma(\mu, N-r) = \pm \frac{r!}{\gcd(n, r)} \prod_j \mu_j.$$

The product is divisible by a_r: for $r = 0$ it equals n; for $a_r = 2$ and $r \ge 1$, $r+1$ odd parts would have sum of parity $r+1$, contrary to $n \equiv r \pmod 2$.

It remains to treat $s < N - r$. Put $t = N - s > r$ and $b = \gcd(n, s+1)$. As $b \mid n - (s+1) = t$, we have

$$\frac{t!}{b} = r! R, \qquad R = (r+1)(r+2)\cdots(t-1)\frac{t}{b} \in \mathbb{Z}.$$

It suffices to show $a_r \mid \gcd(n, r) R$. This is immediate if $r = 0$, or $a_r = 1$, or n, r are even. The remaining case has $a_r = 2$ and n, r odd. Then b is odd. If $t > r+1$, R contains the even factor $r+1$; if $t = r+1$, its factor t/b is even. This proves the required divisibility, including integrality. □

6 The Smith normal form

Proof of Theorem 1.1. We apply the three lattice lemmas to compute the image in (3). The symbol $\mathbf{e}_r$ denotes the rth standard coordinate vector, distinct from the scalar e_s. In this proof, Q at the final basis change denotes a new matrix, rather than the pairing $Q(i, s)$. For $0 \le r, s \le N$, define

$$G(r, s) = \frac{1}{e_s} \sum_i u_r(i) Q(i, s).$$

Lemma 5.1 and the length restriction in Lemma 4.1 show that d_r divides every entry of row r. Moreover $G(r, s) = 0$ if $r + s > N$, and

$$G(r, N-r) = \frac{a_r Q(r, N-r)}{e_{N-r}} = (-1)^N \frac{a_r r!}{\gcd(n, n-r)} = (-1)^N d_r.$$

Thus

$$G = \operatorname{diag}(d_0, \ldots, d_N) V, \tag{13}$$

where V is an integral anti-triangular matrix with entries ± 1 on the anti-diagonal. Its determinant is ± 1, so V is unimodular.

Write $\eta_\mu = \sum_r X(\mu, r) u_r$ using Lemma 4.1, and write $u_r = \sum_\mu W(r, \mu) \eta_\mu$ using the construction there. The matrices X and W are integral, and independence of the u_r gives $WX = I_n$. Let $E = \operatorname{diag}(\epsilon_\mu)$ and let α be the matrix whose columns are $\alpha(\nu)$. Equation (7) and the definitions give

$$M_n = E \Gamma \alpha = EXG\alpha.$$

By Lemma 3.1, $\alpha : \mathbb{Z}^{p(n)} \to \mathbb{Z}^n$ is surjective. Since V is unimodular, (13) now yields

$$M_n \mathbb{Z}^{p(n)} = EX \operatorname{diag}(d_0, \ldots, d_N) \mathbb{Z}^n = \bigoplus_{r=0}^{N} d_r \mathbb{Z} b_r, \qquad b_r = EX\mathbf{e}_r.$$

The map WE is a left inverse of EX, because $E^2 = I$. Therefore

$$\mathbb{Z}^{p(n)} = EX\mathbb{Z}^n \oplus \ker(WE).$$

The kernel is a free abelian group, being a subgroup of a finitely generated free abelian group. Choosing its basis extends the b_r to a basis of $\mathbb{Z}^{p(n)}$, proving (3).

For completeness, all d_r are positive integers: $d_0 = 1$, and for $r \geq 1$ the divisor $\gcd(n, r)$ divides $r!$. We also have $d_0 \mid d_1$ whenever the latter occurs. For $1 \leq r < N$,

$$\frac{d_{r+1}}{d_r} = \frac{a_{r+1}}{a_r} \frac{(r+1)\gcd(n, r)}{\gcd(n, r+1)}.$$

Since $\gcd(n, r+1) \mid r+1$, only $a_r = 2$ could cause a denominator. In that case $a_{r+1} = 1$. If n, r are even, $\gcd(n, r)$ is even and $\gcd(n, r+1)$ is odd. If n, r are odd, $r+1$ is even and $\gcd(n, r+1)$ is odd. The ratio is integral in both cases, establishing the divisor chain.

Finally, choose an integral change of basis P carrying b_r to the first n standard basis vectors. Then PM_n maps $\mathbb{Z}^{p(n)}$ onto $\bigoplus_r d_r\mathbb{Z}\mathbf{e}_r$. Lift the basis vectors $d_r\mathbf{e}_r$ of this image to the domain. These lifts, together with a basis of the kernel, form a basis of the domain: the map onto its free image splits. The corresponding unimodular column change Q satisfies

$$PM_nQ = \operatorname{diag}(d_0, \ldots, d_{n-1}, 0, \ldots, 0).$$

The image has rank n, so precisely $p(n) - n$ entries vanish. This proves Theorem 1.1. □

7 The prime cases

The factors in Theorem 1.1 specialize to the two conjectured lists.

Corollary 7.1. *If $n = p$ is an odd prime, the nonzero invariant factor at index r is $r!$ for even r and $2r!$ for odd r, for $0 \leq r < p$. If $n = 2p$ for an odd prime p, the list is $0!, 1!, \ldots, (2p-1)!$ with $p!$ replaced by $(p-1)!$.*

Proof. For $1 \leq r < p$, $\gcd(p, r) = 1$, and $r \equiv p \pmod 2$ means r is odd. This proves the first assertion, including $r = 0$ separately. When $n = 2p$, even r with $0 < r < 2p$ have gcd two and $a_r = 2$. Odd $r \neq p$ have gcd one and $a_r = 1$. At $r = p$ the factor is $p!/p = (p-1)!$. Again $d_0 = 1$. □

The theorem also gives

$$Z(\mathbb{Z}S_n)/K_{(n)}Z(\mathbb{Z}S_n) \cong \mathbb{Z}^{p(n)-n} \oplus \bigoplus_{r=0}^{n-1} \mathbb{Z}/d_r\mathbb{Z}.$$

8 Formal verification

The theorem `StanleySnf.stanley_class_sum_snf` has the statement

$$\forall n \in \mathbb{N}, \quad 0 < n \Longrightarrow (\mathrm{HasStanleySNF}(n, M_n) \ \wedge \ \forall r \in \mathbb{N},\ r+1 < n \Longrightarrow d_r \mid d_{r+1}).$$

Here $\mathrm{HasStanleySNF}(n, A)$ means that there is a finite index set κ and an integral basis of the integer-valued functions on partitions of n, indexed by $\{0, \ldots, n-1\} \sqcup \kappa$, for which the range of multiplication of column vectors by A is the span of $d_r b_r$. Independence makes this the direct sum in (3); the factors are exactly (2), with division proved exact and the values positive.

The formal permutations act on $\{0,\dots,n-1\}$ and include fixed points in their cycle types. Class sums contain each permutation of the prescribed type once. The formal coefficient definition uses a chosen representative of the output type; proved conjugacy and class-sum identities give exactly (1), with the same row and column conventions. In the formal proof, the hook characters are traces of exterior powers of the permutation representation with its trivial summand removed; their generating-function coefficients give (4). This exterior-algebra construction proves (5) directly from the group-ring definitions. The lattice argument then uses that proved identity. Its only numerical hypothesis is $n > 0$. The diagonal equivalence, the $p(n) - n$ zero entries, and Corollary 7.1 are the written deductions above. The accompanying checking notes and Lean guide give the logical dependencies and explain how to check the formalization.[1]

Appendix A The coefficient identity

We give the routine coefficient calculation for Lemma 2.2.

Proof. The coefficient $[x^k](x-1)^i$ is $(-1)^{i-k}\binom{i}{k}$. Using $k!\binom{i}{k}(N-k)! = i!(N-i)!\binom{N-k}{N-i}$, the sum in the lemma becomes

$$(-1)^{i+s} i!(N-i)! \sum_{k=0}^{s} (-1)^k \binom{s}{k}\binom{N-k}{N-i}.$$

Pascal's identity, applied successively s times, gives

$$\sum_{k=0}^{s} (-1)^k \binom{s}{k}\binom{N-k}{m} = \binom{N-s}{m-s},$$

where an out-of-range lower index means zero. Take $m = N - i$ and simplify factorials to obtain (6). Now set $g_\mu(x) = \prod_j (1-x^{\mu_j})/(1-x)$. Equation (4) implies $\chi_k(\mu) = (-1)^k [x^k] g_\mu(x)$, and substitution gives

$$g_\mu(1+y) = \epsilon_\mu H_\mu(y)/y = \epsilon_\mu \sum_i \eta_\mu(i) y^i.$$

Apply the first assertion to (5). □

Appendix B Examples

For $n = 1$, the matrix is $[1]$. The nonzero factors for $n = 2, 3, 4, 5$ are respectively

$$(1,1), \quad (1,2,2), \quad (1,1,2,6), \quad (1,2,2,12,24).$$

The formula at $n = 9$ gives

$$0!,\ 2\cdot 1!,\ 2!,\ \tfrac{2}{3}\,3!,\ 4!,\ 2\cdot 5!,\ \tfrac{1}{3}\,6!,\ 2\cdot 7!,\ 8!,$$

agreeing term by term with Stanley's example [9]. At $n = 12$, it gives

$$0!,\ 1!,\ 2!,\ \tfrac{1}{3}\,3!,\ \tfrac{1}{2}\,4!,\ 5!,\ \tfrac{1}{3}\,6!,\ 7!,\ \tfrac{1}{2}\,8!,\ \tfrac{1}{3}\,9!,\ 10!,\ 11!.$$

The entry at index six is $6!/3$. The displayed $n = 12$ example in [9], revision 2, instead has $2 \cdot 6!$ at this position; that entry does not divide the following $7!$, so the displayed entries do not form a divisibility chain. Our formula gives $6!/3$ instead. The other entries agree. These examples illustrate the formula and are not inputs to its proof.

[1] https://github.com/6/clank-lab/tree/stanley-class-sum-snf-v4/results/stanley-class-sum-snf

Acknowledgments

The question, the two prime-case conjectures, and the motivating examples are due to Richard P. Stanley. The proof uses classical character theory, as presented in the works of Sagan and Grinberg, and the mathematical infrastructure provided by Lean and mathlib. Cai and Stanley's work is credited as related background, not as a prior proof for the operator considered here.

References

[1] P. Biane, *Nombre de factorisations d'un grand cycle*, Séminaire Lotharingien de Combinatoire **51** (2004), Article B51a. https://www.mat.univie.ac.at/~slc/wpapers/s51biane.pdf.

[2] T. W. Cai and R. P. Stanley, *The Smith Normal Form of a Matrix Associated with Young's Lattice*, Proceedings of the American Mathematical Society **143** (2015), 4695–4703. arXiv:1502.00922v1.

[3] A. Goupil and G. Schaeffer, *Factoring n-cycles and counting maps of given genus*, European Journal of Combinatorics **19** (1998), no. 7, 819–834. doi:10.1006/eujc.1998.0215.

[4] D. Grinberg, *An introduction to the symmetric group algebra*, version 1, 2025. arXiv:2507.20706v1.

[5] N. Lindzey, *Smith Normal Form of a Cayley Graph of the Symmetric Group*, MathOverflow, June 27, 2019. https://mathoverflow.net/questions/334899.

[6] B. E. Sagan, *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*, second edition, Graduate Texts in Mathematics 203, Springer, 2001. doi:10.1007/978-1-4757-6804-6.

[7] R. P. Stanley, *Factorization of permutations into n-cycles*, Discrete Mathematics **37** (1981), 255–262. doi:10.1016/0012-365X(81)90224-7.

[8] R. P. Stanley, *Smith Normal Form in Combinatorics*, 2016, version 2. arXiv:1602.00166v2.

[9] R. P. Stanley, *Smith normal form of conjugacy class actions*, MathOverflow, revision 2, July 1, 2019. https://mathoverflow.net/questions/335226.