Generalized Orbits-Fixedpoints Relations

Jamil Daboul

Physics Department
Ben Gurion University of the Negev
Beer Sheva, Israel
E-mail: jdaboul@gmail.com

Abstract

I prove the following equality for $t$-transitive groups $G$

$$
\frac{1}{|G|} \sum_{g \in G} f_{Z_N}(g)^k = N_{orbits}(G, Z_N^k) = \sum_{j=1}^{\min(k, N)} d_j(G) S(k, j),
$$

where $S(k, j)$ are Stirling numbers of the second kind, and $d_j(G) = 1$ for $1 \leq j \leq t$, and $d_j(G) \geq 2$ for $j > t$. The above equality extends further, using new proofs, two generalizations of an earlier fixedpoints-orbits theorem for finite group actions $(S_N, Z_N^k)$. An illustration using Mathieu group $M_{24}$ is discussed. Possible applications using tensor products of matrix permutation representations is indicated.

Keywords: group action, orbits, fixed points, Burnside lemma, multiply transitive finite groups, Bell numbers, Stirling numbers of the second kind, symmetry group $S_N$, Mathieu groups, permutation representations.

MSC-class: 20B20 (primary); 20Cxx, 20C35 (secondary)
1 Introduction

In 1975 Goldman [1] proved the following equality, by using interesting statistical (!) arguments:

**Theorem 1.** The following equality holds for the symmetric group $S_N$:

$$
\langle f_{Z_N}^k \rangle := \frac{1}{|S_N|} \sum_{g \in S_N} f_{Z_N}(g)^k = \sum_{j=1}^{\min(N,k)} S(k, j), \quad \text{for } k, N \geq 1, \quad (1)
$$

where $S(k, j)$ are the Stirling numbers of the second type.

**Definition.** The Stirling numbers of the second kind $S(k, j)$ count the number of ways to partition the set $\mathbb{Z}_k = \{1, 2, \ldots, k\}$ into $j$ nonempty subsets. For example, the three integers in $\mathbb{Z}_3 = \{1, 2, 3\}$ can be separated into $j = 2$ subsets in $3 = S(3, 2)$ different ways:

$$
\{\{1\}, \{23\}\}, \quad \{\{2\}, \{13\}\}, \quad \{\{3\}, \{12\}\}.
$$

The $S(k, j)$ can be calculated by using their generating function [2] :

$$
x^k = \sum_{j=0}^{k} S(k, j)(x)_j = S(k, 0) + \sum_{j=1}^{k} S(k, j)x(x-1)\cdots(x-j+1). \quad (2)
$$

where $k \in \mathbb{N}$ and $(x)_j$ is the falling factorial, with $(x)_0 = 1$. It follows from (2) that $S(k, 0) = \delta_{k,0}$. Hence, by substituting $x = N \in \mathbb{N}$ in (2) we obtain for $k \geq 1$:

$$
N^k = \sum_{j=1}^{k} S(k, j)(N)_j, \quad \forall \ N, k \geq 1. \quad (3)
$$

where

$$
(N)_j := N(N-1)\cdots(N+1-j) = \frac{N!}{(N-j)!}, \quad \text{for } 1 \leq j \leq N. \quad (4)
$$

Note that $(N)_j := 0$ for $j > N$, and $(N)_{(N-1)} = (N)_N = N!$. 


For $k \leq N$ Eq. (1) reduces to [3, 4]:

$$\langle f^k_{Z_N} \rangle := \frac{1}{|S_N|} \sum_{g \in S_N} f_{Z_N}(g)^k = B_k, \quad \text{for } N \geq k \geq 1,$$

where $B_k$ denotes the Bell numbers which are related to $S(k, j)$ by [2]

$$B_k := \sum_{j=1}^{k} S(k, j), \quad \text{for } k \geq 1.$$

A second generalization of Eq. (5) was obtained by extending the validity of (5) to general $t$-transitive groups $G$ instead of just the symmetric group $S_N$:

**Theorem 2.** [5] [6] $G$ is $t$-transitive on $X$, if and only if

$$\frac{1}{|G|} \sum_{g \in G} f_{Z_N}(g)^k = B_k, \quad \text{for } k \leq t \leq N := |X|.$$

The equality (7) was first proved by Merris and Pierce (1971) [5] by induction on $k$. A second proof was given by Monro and Taylor (1978) [6], by mapping subsets of $Z^k_k$ onto partitions of $Z_k$.

In present paper I give in theorem 5 a new proof of (1), based on Burnside lemma [7]. My proof also shows that the r.h.s. of (1) is equal to the number of orbits of the action $(S_N, Z^k_N)$; this interpretation cannot be deduced from the proof of Goldman [1]. This interpretation is important, since it enables me to give a simple proof of Eq. (15) below, which is valid for any finite group $G$ and also for $k > N$.

## 2 New proofs and results

**Definition.** When a group $G$ acts on a $G$-set $Y$, it decompose it into disjoint orbits. In particular, when $S_N$ acts on $Y = Z^k_N$, it produces $S_N$-orbits of different types, as follows:

$$O_{j,k,N} := S_N \cdot b_{jk} \in Z^k_N, \quad j \leq \min(k, N),$$

where $b_{jk}$ denotes basis ordered $k$-tupels which depend on $j$ distinct integers from $Z_j = \{1, 2, \ldots, j\}$ (not from $Z_N$)

$$b_{jk} := (x_1, \ldots, x_k) \in Z^k_j, \quad \text{where } x_i \in Z_j.$$
Example. To illustrate the above notation, consider an $S_N$-orbit:

$$O_{3,4,N} := S_N \cdot b_{34} = S_N \cdot (1,2,3,2) = \{(g(1), g(2), g(3), g(2)) | g \in S_N\} = \{(i, j, k, j) | i \neq j \neq k \neq i \in \mathbb{Z}_N\}.$$ 

Theorem 3. The number of orbits created by the group action $(S_N, \mathbb{Z}_N^k)$ is given by

$$\mathcal{N}_{\text{orbits}}(S_N, \mathbb{Z}_N^k) = \sum_{j=1}^{\min(k,N)} S(k,j), \text{ for } k, N \geq 1, \tag{9}$$

Proof. The length of an orbit $O_{j,k,N}$ is independent on $k$:

$$|O_{j,k,N}| = |O_{j,j,N}| = (N)_j := N(N-1) \cdots (N+1-j), \quad j \leq N, \tag{10}$$

Let $n(k,j)$ denotes the number of orbits of type $O_{j,k,N}$. It follows that

$$N^k = \sum_{j=1}^{\min(k,N)} n(k,j)|O_{j,k,N}| = \sum_{j=1}^{\min(k,N)} n(k,j)(N)_j. \tag{11}$$

By comparing Eq. (11) with the equality Eq. (3), starting from $N = 1$ and successively $N = 2, 3, \ldots$, we obtain

$$n(k,j) = S(k,j), \quad \forall \quad k \geq j \geq 1. \tag{12}$$

Lemma 4. Let $f_X(g)$ and $f_{X^k}(g)$ denote the number of fixed points of the actions $(G, X)$ and $(G, X^k)$, respectively. Then

$$\langle f_{X^k} \rangle = \langle f_X \rangle = \mathcal{N}_{\text{orbits}}(G, X^k). \tag{13}$$

Proof. We recall that $f_{X^k}(g)$ is equal to the number of ordered $k$-tupels $(x_1, \ldots, x_k) \in X^k$ which are fixed by the action of $g \in G$. Hence, the first equality in (13) follows from

$$f_{X^k}(g) = \sum_{(x_1, \ldots, x_k) \in X^k} \delta_{(x_1, \ldots, x_k), g^k(x_1, \ldots, x_k)} = \prod_{j=1}^{k} \left( \sum_{x_j \in X} \delta_{x_j, g^j x_j} \right) = f_X(g)^k, \tag{14}$$

since the summations over $x_j$ can be carried out independently. The second equality follows immediately from Burnside’s lemma [7] for $(G, X^k)$. ☐
Below I generalize the two equalities Eq. (11) and Eq. (17), as follows:

**Theorem 5.** The group action \((G, \mathbb{Z}_N)\) is \(t\)-transitive, if and only if the following equality holds:

\[
\frac{1}{|G|} \sum_{g \in G} f_{\mathbb{Z}_N}(g)^k = N_{\text{orbits}}(G, \mathbb{Z}_N^k) \tag{15a}
\]

\[
= \sum_{j=1}^{\min(k, N)} d_j(G) S(k, j), \tag{15b}
\]

\[
\Rightarrow \begin{cases} 
B_k, & \text{for } k \leq t \leq N, \\
B_t + \sum_{j=t+1}^{\min(k, N)} d_j(G) S(k, j) & \text{for } t < k,
\end{cases}
\]

where the divisions \(d_j(G)\) depend on the group \(G\) and on \(j\), but not on \(k\):

\[
d_j(G) = 1 \quad \text{for } 1 \leq j \leq t, \quad \text{and} \\
d_j(G) \geq 2 \quad \text{for } j > t. \tag{16}
\]

**Proof.** Eq. (15a) follows from Eq. (13).

Eq. (15b) follows from Eq. (9) after taking into account:

- Every \(G\) which acts on \(\mathbb{Z}_N\) must be a subgroup of \(S_N\).

- If \(G\) is a genuine subgroup of \(S_N\), it would have less group elements. Therefore, we expect

\[
|G \cdot b_{jk}| \leq |S_N \cdot b_{jk}|. \tag{17}
\]

- The equality sign in (17) \((d_j(G) = 1)\) holds for \(j \leq t\), since a \(t\)-transitive group produces exactly the same orbits \(O_{j,k,N}\) as \(S_N\), for \(j \leq t\).

- For \(j > t\) then \(|G \cdot b_{jk}| < |S_N \cdot b_{jk}|\), which means that the corresponding (maximal) orbit \(O_{j,k,N}\) of \(S_N\) must split into \(d_j(G) \geq 2\) orbits of \(G\). Erect
Example. The Mathieu group $M_{24}$ is 5-transitive. Its divisions $d_j$ can be read from the following formula. (Note that since $S(k, j) = 0$ for $k < j$, the formula (18) is valid for all $k \geq 1$.)

$$
\langle f^k_{\mathbb{Z}_{24}} \rangle = \sum_{j=1}^{5} S(k, j) + 2S(k, 6) + 9S(k, 7) + 123S(k, 8) + 1938 \sum_{j=9}^{\min(k,24)} \frac{15!}{(24-j)!} S(k, j).
$$

We can easily understand why the maximal $S_{24}$-orbit $O_{6,6,24}$ has to split: $|O_{6,6,24}| = (24)_6 = (24)5 \cdot 19$ is not a divisor of $|M_{24}| = (24)_5 \cdot 48$. Hence, I conclude that $O_{6,6,24}$ must split into two sub-orbits, with lengths $(24)_5 \cdot 16$ and $(24)_5 \cdot 3$, which are divisors of $|M_{24}|$. Note that $d_7 = 9$ and $d_8 = 123$ yield more predictions.

3 Summary

I gave a new proof of Eq. (1) by using the generating function of $S(k, j)$ and Burnside lemma. Unlike the statistical proof of Goldman [1], my proof led to the equality (15a), between the r.h.s. of (1) to the number of orbits of $(S_N, \mathbb{Z}_N)$. This made it possible to derive Eq. (15), which is a generalization of (7) to $k > N$, by using a simple argument which led to the inequality in Eq. (17).

Note that a finite group action $(G, \mathbb{Z}_N)$ yields an $N \times N$-matrix representation of $G$, which is called permutation representation $\Gamma^P$, so that the action $(G, \mathbb{Z}_N^k)$ yields a k-fold tensor product of $\Gamma^P$.

A detailed version of the present paper is available as a preprint, which includes applications and a review of basic concepts of group action. I will gladly send it by email upon request.

References

[1] Jay R. Goldman, An identity for fixed points of permutations Aequationes Math. 13 (1975), 155-156.
[2] Eric W. Weisstein, *Stirling Number of the Second Kind.* From *MathWorld.*

[3] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, 1968), p. 599.

[4] J. van Lint, Combinatorial Theory Seminar, Eindhoven University of Technology (Springer-Verlag Lecture Notes in Mathematics, 382, Berlin, 1974), p. 31.

[5] R. Merris and S. Pierce, *The Bell numbers and r-fold transitivity,* J. Combinatorial Theory (A) 12 (1971), 155-157.

[6] G. P. Monro and D. E. Taylor, *On Multiply Transitive Permutation Groups,* Austral. Math. Soc. (Series A) 26 (1978), 57-58.

[7] N. L. Biggs and A.T. White, *Permutation Groups and Combinatorial Structures* (Cambridge University Press, London 1979)