Math. Z. 137, 257–264 (1974)

Rearrangements of the Symmetric Group and Enumerative Properties of the Tangent and Secant Numbers

Dominique Foata and Volker Strehl

In a recent note [6] the first author has announced the discovery of a family of transformation groups $(G_n)_{n>0}$ which have the following property: G_n acts on the $n!$ elements of the symmetric group $\mathfrak{S}_n$ and the number of its orbits is equal to the n-th tangent or secant number, according as n is odd or even. The purpose of this paper is to give a complete description of these groups. Applications to enumeration problems will appear in a subsequent paper.

The *tangent* (or *Euler*) number are defined by the series expansion of $\tan u$

$$\tan u=(u/1!)\,1+(u^3/3!)\,2+(u^5/5!)\,16+(u^7/7!)\,272+\cdots$$

and the *secant* numbers by that of $\sec u=1/\cos u$

$$\sec u=1+(u^2/2!)\,1+(u^4/4!)\,5+(u^6/6!)\,61+\cdots.$$

Let $D(u)=\tan u+\sec u=1+\sum_{n>0}(u^n/n!)\,D_n$, so that D_n is equal to the tangent or secant number of order n, according as n is odd or even. It is readily verified (see e.g. Frobenius [9], Netto [10], § 63, Nielsen [11]) that the coefficients D_n satisfy the identities

$$2D'(u)=1+D^2(u),\qquad D(0)=1$$

$$D''(u)=D(u)\,D'(u),\qquad D(0)=D'(0)=1,$$

where $D'(u)$ and $D''(u)$ are the first and second derivatives of $D(u)$, namely

$$D'(u)=\sum_{n>0}(u^n/n!)\,D_{n+1}\quad\text{and}\quad D''(u)=\sum_{n>0}(u^n/n!)\,D_{n+2}.$$

The above identities can also be written, the first

$$(1)\qquad 2D_{n+1}=\sum_{0\leqq i\leqq n}\binom{n}{i}D_i\,D_{n-i}\quad(n\geqq 0),\qquad D_0=1$$

and the second one

$$(2) \qquad D_{n+2} = \sum_{0 \leqq i \leqq n} \binom{n}{i} D_i D_{n+1-i} \quad (n \geqq 0), \qquad D_0 = D_1 = 1.$$

Thus, the coefficients D_n are positive integers determined by any one of the preceding two recurrence formulas.

The purpose of this paper is to give a new characterization of these coefficients. The only combinatorial interpretations of these numbers (see [1, 2, 8]) known so far were obtained by introducing remarkable classes of permutations whose cardinalities were equal to the tangent or secant numbers. Here we construct a family of *transformation groups* $(G_n)_{n>0}$, the group G_n acting on the symmetric group $\mathfrak{S}_n$ for $n>0$ and we show that the number of orbits of G_n is equal to the tangent or secant number D_n. The groups are introduced at the end of Section 1. They are generated by a family of involutions φ_x whose definition is based upon a remarkable factorization, called the *x-factorization*, of the elements of $\mathfrak{S}_n$ (see Lemma 1). When $n>1$, the group G_n, as an *abstract* group, is simply the direct product of $(n-1)$ groups of two elements. It is then abelian and of order 2^{n-1}. It is the purpose of Section 2 to establish this result. In Section 3 we give the main result of this paper, i.e. we show that the number of orbits of G_n is equal to D_n. Let $1 \leqq i \leqq n$ and $w: i \to x_i$ be a permutation. We say that x_i is a *peak* (local maximum) of w if the following two conditions hold

(3) (i) either $i=1$ or $1<i$ and $x_{i-1}<x_i$:
(ii) either $i=n$ or $i<n$ and $x_i>x_{i+1}$.

Let $p(w)$ be the number of peaks of w. To establish the main result we proceed in two steps. First, we show that the number of orbits of G_n is equal to

$$(4) \qquad \theta_n = \sum \{2^{-n+p(w)}: w \in \mathfrak{S}_n\}.$$

It is then easy to see that θ_n verifies the recurrence formula (1) that defines uniquely the sequence of numbers $(D_n)_{n>0}$. As a matter of fact, (4) is a new formula for the tangent or secant number D_n. We conclude the paper by giving the table of the $D_4=5$ orbits of G_4. In a subsequent paper we shall show how the present results provide with a new refinement of the tangent or secant numbers and make the connection with the previous works on Eulerian numbers ([4, 7, 8]).

1. The *x*-Factorization

A permutation w of the set $[n]=\{1, 2, \ldots, n\}$ $(n>0)$ is a bijection of $[n]$ onto itself. The set of the $n!$ permutations of $[n]$ will be denoted by the usual symbol $\mathfrak{S}_n$. A permutation $w: i \to x_i$ of $[n]$ will be identified with the *word* $w = x_1 x_2 \dots x_n$. The empty word is denoted by e. The *reverse* image of $w = x_1 x_2 \dots x_n$ $(n > 0)$ is the word $x_n \dots x_2 x_1$, denoted by Rw. Also $Re = e$. The word u obtained by *juxtaposing* two words v and w in this order is written $u = vw$. The word v (resp. w) is the *left* (resp. *right*) *factor* of u. More generally, a *factorization of length* q $(q > 0)$ of a word w is any sequence $(w_1, w_2, \dots, w_q)$ of words (some of them possibly empty) such that the juxtaposition product $w_1 w_2 \dots w_q$ is equal to w.

1. Lemma. *Let $w = x_1 x_2 \dots x_n$ $(n > 0)$ be a permutation and x be one of the letters x_i $(1 \leqq i \leqq n)$. Then w has a unique factorization (w_1, w_2, x, w_4, w_5) of length 5, called its x-factorization, which is characterized by the three properties*

(i) *w_1 is empty or its last letter is less than x;*

(ii) *w_2 (resp. w_4) is empty or all its letters are greater than x;*

(iii) *w_5 is empty or its first letter is less than x.*

Proof. As x is a letter of w, we have $w = w' x w''$ for some words w' and w''. Let w_2 (resp. w_4) be the longest right (resp. left) factor of w' (resp. w'') all letters of which are greater than x. If the last (resp. first) letter of w' (resp. w'') is smaller than x or if w' (resp. w'') is empty, then w_2 (resp. w_4) is the empty word. We can then write $w' = w_1 w_2$ and $w'' = w_4 w_5$ for some words w_1, w_5. Clearly, the factorization (w_1, w_2, x, w_4, w_5) satisfies the three properties of the lemma.

Conversely, let (w_1, w_2, x, w_4, w_5) be a factorization verifying (i), (ii) and (iii). Then (i) and (ii) (resp. (iii)) imply that w_2 (resp. w_4) is the longest right (resp. left) factor of $w_1 w_2$ (resp. $w_4 w_5$) whose letters are all greater than x. So there can exist only one factorization of w with properties (i), (ii), (iii). Q.E.D.

For instance, for $x = 4$ the x-factorization of $w = 7\,8\,3\,1\,4\,5\,6\,2$ is given by $(7831, e, 4, 56, 2)$.

The keyrole in the construction of our groups G_n is played by the involutions φ_x we are now defining. Let (w_1, w_2, x, w_4, w_5) be the x-factorization of a permutation w containing the letter x. We let

$$\varphi_x w = w_1 w_4 x w_2 w_5 . \tag{5}$$

Clearly (w_1, w_4, x, w_2, w_5) is the x-factorization of $\varphi_x w$. Accordingly

$$\varphi_x \varphi_x w = w . \tag{6}$$

Thus φ_x is an involution that maps $\mathfrak{S}_n$ onto itself. We denote by G_n the subgroup of the permutation group acting on $\mathfrak{S}_n$, which is generated by the set $\{\varphi_x : 1 \leqq x \leqq n\}$.

2. The Rearrangement Group G_n

Our first task is to show that any two involutions φ_x and φ_y commute. To do so it will be convenient to deal with the natural *linear ordering* $w(.,.)$ of $[n]$ associated to any word w of $\mathfrak{S}_n$ $(n \geqq 2)$ rather than w itself. Let z, z' belong to $[n]$ with $z \neq z'$; then

(7) $w(z, z')$ iff w admits a factorization of the form (w_1, z, w_3, z', w_5).

If $z \neq z'$ and $w(z, z')$, we denote by $I_{zz'} w$ the factor of w whose first and last letters are z, z'. With the notations of (7) for instance we have $I_{zz'} w = z w_3 z'$. The minimum letter – with respect to the natural order of the integers – of $I_{zz'} w$ is denoted by $\mu_w(z, z')$. Iff $w(z', z)$, then $w(z, z')$ does not hold and we let $\mu_w(z, z') = \mu_w(z', z)$. Thus μ_w is defined for all couples (z, z') of integers of $[n]$ with $z \neq z'$. It is called the *minimum function* of w.

Let us go back to the definition of φ_x given in (5). The involution φ_x permutes the words w_2 and w_4 only. Thus φ_x reverses the ordering $w(.,.)$ for exactly those pairs (z, z') such that $z \neq z'$, z is a letter of $w_2 x$ and z' of $x w_4$. On the other hand, z is a letter of $w_2 x$ and z' of $x w_4$ with $z \neq z'$ iff $w(z, z')$ and $\mu_w(z, z') = x$. Hence the linear ordering $\varphi_x w(.,.)$ can also be defined by

(8) if $w(z, z')$, then $\begin{cases} \varphi_x w(z', z) & \text{if } \mu_w(z, z') = x \\ \varphi_x w(z, z') & \text{otherwise.} \end{cases}$

Clearly, w and $w' = \varphi_x w$ have the *same* minimum function, i.e.

(9) $$\mu_w = \mu_{w'} \quad \text{with } w' = \varphi_x w.$$

Let $x \neq y$, $w' = \varphi_x w$ and assume $w(z, z')$ with $z \neq z'$. If $\mu_w(z, z') = x$, we have $w'(z', z)$ (from (8)) and $\mu_{w'}(z, z') = x$ (from (9)). From (8) again with w' instead of w and y in place of x, we obtain $\varphi_y w'(z', z)$, i.e. $\varphi_y \varphi_x w(z', z)$. If $\mu_w(z, z') \neq x$, then $\varphi_x w(z, z')$, i.e. $w'(z, z')$. Another application of (8) with w' and y in place of w and x yields

$$\begin{array}{ll} \varphi_y w'(z', z) & \text{if } \mu_{w'}(z, z') = y \\ \varphi_y w'(z, z') & \text{if } \mu_{w'}(z, z') \neq y. \end{array}$$

Altogether, we obtain

(10) if $w(z, z')$, then $\begin{cases} \varphi_y \varphi_x w(z', z) & \text{if } \mu_w(z, z') \in \{x, y\} \\ \varphi_y \varphi_x w(z, z') & \text{otherwise.} \end{cases}$

In (10) the role played by x and y is symmetric. As $\varphi_y \varphi_x w(.,.)$ is a linear ordering of $[n]$, we then have

(11) $$\varphi_x \varphi_y = \varphi_y \varphi_x.$$

In fact, relation (11) holds for any couple (x, y) of integers of $[n]$, since it is trivial for $x = y$.

As all the φ_x's commute, it makes sense, when the subset X of $[n]$ is non-empty, to define

$$(12) \qquad \varphi_X = \prod_{x \in X} \varphi_x .$$

When X is empty, we let φ_X be the identity map of $\mathfrak{S}_n$. On the other hand, as n can never be the minimum letter of any factor of a word w of $\mathfrak{S}_n$, we can restrict X to be a subset of $[n-1]$. From (6) and (12) it follows that

$$(13) \qquad \varphi_X \varphi_Y = \varphi_{X \Delta Y},$$

where X and Y are subsets of $[n-1]$ and $X \Delta Y$ denotes the symmetric difference between X and Y (i.e. $(X \setminus Y) \cup (Y \setminus X)$). By induction on Card X we deduce from (8) and (10) the following proposition.

2. Proposition. *Let $X \subset [n-1]$ and $w \in \mathfrak{S}_n$. Then $\varphi_X w(.,.)$ is the linear ordering defined by*

$$(14) \quad \text{if } w(z, z'), \text{ then } \begin{cases} \varphi_X w(z', z) & \text{if } \mu_w(z, z') \in X \\ \varphi_X w(z, z') & \text{otherwise.} \end{cases}$$

3. Corollary. *For $n > 1$ the group G_n is isomorphic to the direct product of $(n-1)$ groups of 2 elements. It consists of the 2^{n-1} distinct involutions φ_X $(X \subset [n-1])$.*

Proof. The power set $2^{[n-1]}$ of $[n-1]$ together with the operation Δ is isomorphic to the direct product of $(n-1)$ groups of 2 elements. It follows from (13) that G_n is a homomorphic image of $2^{[n-1]}$ under the mapping $X \to \varphi_X$. It suffices to show that $X \to \varphi_X$ is an isomorphism. Let $X \subset [n-1]$ be non-empty and w a word of the form $n\, z\, w'$ with $z \in X$. As $w(n, z)$ and $\mu_w(n, z) = z \in X$, we have $\varphi_X w(z, n)$ and so $\varphi_X w \neq w$. Hence, the kernel of $X \to \varphi_X$ is reduced to the single element $\emptyset$ of $2^{[n-1]}$. Q.E.D.

Let $w = x_1 x_2 \dots x_n$ be a permutation. We recall that Rw is the reverse image of w, namely $x_n \dots x_2 x_1$. Moreover, let $\{\mu_w\}$ denote the range of μ_w and $|\mu_w|$ the cardinality of that range.

4. Corollary. *Let $X \subset [n-1]$ and $w \in \mathfrak{S}_n$. Then*

$$\varphi_X w = Rw \quad \textit{iff } X \supset \{\mu_w\}.$$

Proof. We have $\varphi_X w = Rw$ iff $\varphi_X w(z', z)$ holds for all couples (z, z') such that $w(z, z')$. From (14) the latter condition is equivalent to the inclusion $X \supset \{\mu_w\}$. Q.E.D.

3. Orbits of G_n

We know from (9) and (12) that μ is an orbit-invariant. In fact, μ is an *orbit-characteristic* as shown in the next proposition.

5. Proposition. *If* $\mu_w = \mu_{w'}$, *then* $w' = \varphi_X w$ *for some* $X \subset [n-1]$, *i.e.* w *and* w' *belong to the same orbit of* G_n. *In fact, let*

(15) $$X = \{\mu_w(z, z') \colon w(z, z') \,\&\, w'(z', z)\}.$$

Then $w' = \varphi_X w$.

Proof. Only the second part of the proposition is to be proved. First, we show that if

(16) $$\mu_w(z'', z''') = x \in X \qquad (z'' \neq z''') \text{ and } w(z'', z'''),$$

then $w'(z''', z'')$. By definition of X there exists a couple (z, z') such that

(17) $$w(z, z'), \quad w'(z', z) \quad \text{and} \quad \mu_w(z, z') = x.$$

Let (w_1, w_2, x, w_4, w_5) (resp. $(w'_1, w'_2, x, w'_4, w'_5)$) be the x-factorization of w (resp. w') and assume $w'(z'', z''')$. The latter condition together with (16) and (17) imply that z'' and z (resp. z and z''', z' and z''', z' and z'') are letters of $w'_2 x$ and $x w'_4$ (resp. $w_2 x$ and $x w_4$, $w'_2 x$ and $x w'_4$, $w_2 x$ and $x w_4$). Consequently, each pair

$$\{z, z''\}, \qquad \{z, z'''\}, \qquad \{z', z'''\}, \qquad \{z', z''\}$$

contains an integer equal to x. If $z = x$, then $z' \neq x$ since $z \neq z'$; it follows that $z'' = x = z'''$, which is a contradiction, since $z'' \neq z'''$. If $z'' = x$, then $z''' \neq x$ since $z'' \neq z'''$; it follows that $z = x = z'$ and, since $z \neq z'$, we again obtain a contradiction. Hence, assumption (16) implies $w'(z''', z'')$. It is equivalent to saying that $\mu_w(z'', z''') \in X$ iff either $w(z'', z''')$ and $w'(z''', z'')$ or $w(z''', z'')$ and $w'(z'', z''')$. Hence

(18) $$\begin{aligned} &\mu_w(z'', z''') \in X, \quad w(z'', z''') \text{ imply } w'(z''', z'') \\ &\mu_w(z'', z''') \notin X, \quad w(z'', z''') \text{ imply } w'(z'', z'''). \end{aligned}$$

Comparing (18) with (14) we conclude that $w' = \varphi_X w$. Q.E.D.

It follows from (14) that the orbit of G_n containing w consists of the $2^{|\mu_w|}$ *distinct* elements

$$\varphi_X w \qquad \text{where } X \subset \{\mu_w\}.$$

Hence

$$1 = \sum \{2^{-|\mu_{w'}|} \colon w' \in \text{orbit of } w\}.$$

Let θ_n be the number of orbits of G_n. By summing over all the orbits of G_n the preceding formula we get

$$\theta_n = \sum \{2^{-|\mu_w|} \colon w \in \mathfrak{S}_n\}.$$

It remains to make the connection with formula (4). Let (w_1, w_2, x, w_4, w_5) be the x-factorization of w. Then x is a peak of w iff both w_2 and w_4 are empty words, i.e. iff we can never have $\mu_w(z, z')=x$ for any couple (z, z') with $z \neq z'$. Thus x is a peak of w iff $x \notin \{\mu_w\}$. Consequently

$$|\mu_w| = n - p(w).$$

6. Proposition. *The number of orbits of G_n is equal to the secant or tangent number D_n ($n>0$).*

Proof. By convention let $\theta_0=1$. Also $\theta_1=1$. For $0 \leqq i \leqq n$ and $n \geqq 1$ let $\mathfrak{S}_{n+1,i}$ be the set of permutations $w=x_1 x_2 \ldots x_{n+1}$ whose $(i+1)$-st letter x_{i+1} is equal to 1. Clearly

$$\sum \{2^{-(n+1)+p(w)}\colon w \in \mathfrak{S}_{n+1,i}\} = (1/2) \sum \{2^{-n+p(w)}\colon w \in \mathfrak{S}_n\} = (1/2)\,\theta_n$$

when $i=0$ or n. If $0<i<n$, let us map any permutation $w=x_1 x_2 \ldots x_{n+1}$ in $\mathfrak{S}_{n+1,i}$ onto the couple (w', w'') with $w'=x_1 \ldots x_i$ and $w''=x_{i+2} \ldots x_{n+1}$. The map $w \to (w', w'')$ is a bijection of $\mathfrak{S}_{n+1,i}$ onto the set of couples (w', w'') such that w' is a permutation of a subset I of $\{2, 3, \ldots, n+1\}$ of cardinality i, and w'' a permutation of $\{2, 3, \ldots, n+1\} \setminus I$. Moreover $p(w)=p(w')+p(w'')$ because of our convention on peaks and the fact that 1 is never a peak in a permutation $w \in \mathfrak{S}_{n+1}$ with $n \geqq 1$. On the other hand, the summation $\sum 2^{-i+p(w')}$, where w' runs over all the permutations of I, is equal to $\sum \{2^{-i+p(w')}\colon w' \in \mathfrak{S}_i\} = \theta_i$, since the definition of peak only depends on the mutual order of the elements. In the same manner, when w'' runs over all the permutations of $\{2, 3, \ldots, n+1\} \setminus I$, the summation $\sum 2^{-(n-i)+p(w'')}$ is equal to θ_{n-i}. Consequently,

$$\sum \{2^{-(n+1)+p(w)}\colon w \in \mathfrak{S}_{n+1,i}\} = (1/2) \binom{n}{i} \theta_i \theta_{n-i}$$

and

$$2\theta_{n+1} = \theta_n + \sum_{0<i<n} \binom{n}{i} \theta_i \theta_{n-i} + \theta_n = \sum_{0 \leqq i \leqq n} \binom{n}{i} \theta_i \theta_{n-i}.$$

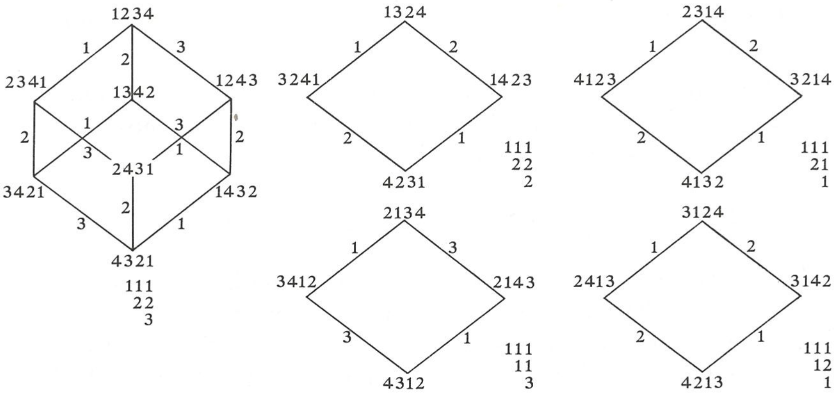
As θ_n satisfies the recurrence formula (4), we have $\theta_n = D_n$. Q.E.D.

7. Remark. To establish that the number of orbits of G_n is equal to D_n, we could have made use of Burnside's lemma ([3], 191, or [5], 90). But the above method provides with a new expression for D_n, namely formula (4).

In the following table the $D_4=5$ orbits of G_4 are presented in the form of a graph. This graph has 4! vertices whose labels are the 4! prmutations. The vertices w and w' are connected by a line labeled x iff $\varphi_x(w)=w'$.

Under each orbit appear the values of μ written in the form

$$\begin{array}{c|ccc} & 2 & 3 & 4 \\ \hline 1 & \dots & \dots & \dots \\ 2 & & \mu(2,3) & \dots \\ 3 & & & \dots \end{array}$$



References

1. André, D.: Développements de sec x et de tan x. C.r. Acad. Sci. Paris **88**, 965–967 (1879)
2. André, D.: Sur les permutations alternées. J. Math. pur. appl. **7**, 167–184 (1881)
3. Burnside, W.: Theory of Groups of Finite Order. New York: Dover 1911, Reprint 1955
4. Carlitz, L., Scoville, R.: Generalized Eulerian numbers: combinatorial applications, J. reine angew. Math. **265**, 110–137 (1974)
5. Comtet, L.: Analyse Combinatoire, Vol. 2. Paris: Presses Universitaires de France 1970
6. Foata, D.: Groupes de réarrangements et nombres d'Euler. C.r. Acad. Sci. Paris **275**, 1147–1150 (1972)
7. Foata, D., Schützenberger, M.-P.: Théorie géométrique des polynômes eulériens. Lecture Notes in Math., 138. Berlin-Heidelberg-New York: Springer 1970
8. Foata, D., Schützenberger, M.-P.: Nombres d'Euler et permutations alternantes. In: A Survey of Combinatorial Theory Sympos. Colorado State Univ. (Colorado 1971). Amsterdam: Horth-Holland 1973, pp. 173–187
9. Frobenius, G.: Über die Bernoullischen Zahlen und die Eulerschen Polynome. Sitzungsberichte der königlichen preussischen Akademie der Wissenschaften zu Berlin 809–847 (1910)
10. Netto, E.: Lehrbuch der Combinatorik. Leipzig: Teubner 1901
11. Nielsen, N.: Traité élémentaire des nombres de Bernoulli. Paris: Gauthier-Villars 1923

Dominique Foata
Institut de Recherche
Mathématique Alsacien
Université Louis-Pasteur
7, rue René Descartes
67084 Strasbourg, France

Volker Strehl
Universität Erlangen
Institut für Informatik I
852 Erlangen
Bismarckstraße 6
Federal Republic of Germany

(Received February 11, 1974)