doi:10.1006/jabr.2001.8814, available online at http://www.idealibrary.com on IDEAL®

Applications of the Brauer Complex: Card Shuffling, Permutation Statistics, and Dynamical Systems

Jason Fulman

Department of Mathematics, Stanford University, Stanford, California 94305
E-mail: fulman@math.stanford.edu

Communicated by Jan Saxl

Received February 28, 2000

By algebraic group theory, there is a map from the semisimple conjugacy classes of a finite group of Lie type to the conjugacy classes of the Weyl group. Picking a semisimple class uniformly at random yields a probability measure on conjugacy classes of the Weyl group. Using the Brauer complex, it is proved that this measure agrees with a second measure on conjugacy classes of the Weyl group induced by a construction of Cellini using the affine Weyl group. Formulas for Cellini's measure in type A are found. This leads to new models of card shuffling and has interesting combinatorial and number-theoretic consequences. An analysis of type C gives another solution to a problem of Rogers in dynamical systems: the enumeration of unimodal permutations by cycle structure. The proof uses the factorization theory of palindromic polynomials over finite fields. Contact is made with symmetric function theory. © 2001 Academic Press

Key Words: Brauer complex; card shuffling; conjugacy class; dynamical systems; symmetric function.

1. INTRODUCTION

In performing a definitive analysis of the Gilbert–Shannon–Reeds (GSR) model of card shuffling, [BaD] defined a one-parameter family of probability measures on the symmetric group S_n called k-shuffles. Given a deck of n cards, one cuts it into k piles with probability of pile sizes $j_1, \ldots, j_k$ given by $\binom{n}{j_1,\ldots,j_k}/k^n$. Then cards are dropped from the packets with probability proportional to the pile size at a given time. (Thus, if the current pile sizes are $A_1, \ldots, A_k$, the next card is dropped from pile i with probability $A_i/(A_1 + \cdots + A_k)$.) They proved that $\frac{3}{2}\log_2(n)$ 2 shuffles are necessary and sufficient to mix up a deck of n cards. Aldous [A] had previously

0021-8693/01 $35.00

obtained this bound asymptotically in n; the paper [F4] shows that the use of cuts does not help speed things up.

One motivation for the current paper is the fact that GSR measures are well-studied and appear in many mathematical settings. Hanlon [Han] is a good reference for applications to Hochschild homology (tracing back to [Ger]), and [BW] describes the relation with explicit versions of the Poincaré–Birkhoff–Witt theorem. Section 3.8 of [SSt] describes GSR shuffles in the language of Hopf algebras. Stanley [Sta] has related biased riffle shuffles to the Robinson–Schensted–Knuth correspondence, thereby giving an elementary probabilistic interpretation of Schur functions and a different approach to some work of interest to the random matrix community. He recast many of the results of [BaD] and [F1] using quasi-symmetric functions. Connections of riffle shuffling with dynamical systems appear in [BaD], [La1], and [La2]. Generalizations of the GSR shuffles to other Coxeter groups, building on [BBHT] and [BiHaRo], appear in [F2] and [F3].

For further motivation, it is useful to recall one of the most remarkable, yet mysterious, properties of these k-shuffles. Since k-shuffles induce a probability measure on conjugacy classes of S_n, they induce a probability measure on partitions λ of n. Consider the factorization of random degree n polynomials over a field F_q into irreducibles. The degrees of the irreducible factors of a randomly chosen degree n polynomial also give a random partition of n. The fundamental result of Diaconis–McGrath–Pitman (DMP) [DMP] is that this measure on partitions of n agrees with the measure induced by card shuffling when $k = q$. This allowed natural questions on shuffling to be reduced to known results on factors of polynomials and vice versa. The DMP result is remarkable since k-shuffles (like the shuffles studied here) are not constant on conjugacy classes.

There are three different proofs of the DMP result, each of them mysterious in their own way. The first proof, in [DMP], is combinatorial and makes use of magical bijection of Gessel and Reutenauer [GesR]; they include a self-contained proof of this bijection. The second proof, in [Han], proves an equivalent assertion about induced characters, but also uses the Gessel–Reutenauer bijection. (The equivalence between the DMP theorem and the results on induced characters is not completely obvious; see Section 4 of [F4] for an explanation.) The third, and perhaps most principled, proof of the equivalent assertion about induced characters appears in [BBGar], using facts about free Lie algebras [Gar]. But it is unclear how to generalize free Lie algebras to arbitrary types. Motivated by the observation that degree n polynomials over F_q are the semisimple orbits of $GL(n, q)$ on its Lie algebra, [F3] gave Lie theoretic reformulations and generalizations of the DMP result. However, the proofs still seem unnatural, and it is not clear when the generalizations hold. In fairness, we should point out that there is hope of a uniform generalization of the Gessel–Reutenauer bijection, at least for the conjugacy class of Coxeter elements ([Rei1], [Rei2]) and that there is an analog of the free Lie algebra in type B [B].

The goal of this paper is to study a setting in which these complications vanish and an analog (Theorem 1) of the DMP result holds in all types and can be proved in a uniform and natural way. The key idea is to study semisimple conjugacy classes in groups such as $SL(n, q)$ rather than $GL(n, q)$; then these polynomials can be viewed as points in Euclidean space, and the extra geometric structure forces natural choices.

The precise contents of this paper are as follows. Section 2 begins by describing the algebraic group setup and the map Φ from semisimple conjugacy classes to conjugacy classes of the Weyl group, giving examples. It makes a connection with the Gessel–Reutenauer map, demystifying it somewhat. Section 3 gives a probabilistic version of a construction of Cellini [Ce1] and states the analog of the DMP theorem, which is proved in Section 7.

Section 4 focuses on understanding Cellini's construction in type A. It emerges that in type A, the probability of a permutation involves both its number of cyclic descents and its major index. This is interesting, because while combinatorialists have thoroughly studied the joint distribution of permutations by descents, major index, and cycle structure [Ges], problems involving cyclic descents have not been treated and are regarded by the experts as harder. It is also shown that the type A construction leads to new models of card shuffling. Section 4 then shows that even for the identity conjugacy class in type A, Theorem 1 gives an interesting result—a number-theoretic reciprocity law. For more general conjugacy classes, Theorem 1 is given a formulation in terms of generating functions which highlights the connections with number theory.

Section 5 studies Cellini's construction in type C. Unlike in the type A case, formulas for type C follow easily from work of Cellini. (This is one of the few times in mathematics when the hyperoctahedral group is easier to understand than the symmetric group.) Thus the main point of this section is to give interpretations in terms of card shuffling. This unifies work of [BaD] and [BB] and implies a simple formula for Bayer–Diaconis hyperoctahedral shuffles. Some work of Bob Beals on total variation distance of hyperoctahedral shuffles to uniform is understood is a new way.

Section 6 gives applications of the type C analog of the DMP theorem to dynamical systems. Specifically, it gives an alternate solution to a problem posed by [Ro] and solved in [Ga]—the enumeration of unimodal permutations by cycle structure. The mathematics in this section were accepted by *J. Algebra* in 1/01, before the appearance of the preprint [T]; hence Section 6 gives the first derivation of the cycle index of unimodal permutations. (The proof in [T], however, gives the first derivation using only symmetric functions.) The cycle index leads to interesting asymptotic results.

The section closes by giving a more conceptual proof of a combinatorial result of Reiner.

Section 7 uses the Brauer complex (an object originally introduced in modular representation theory) to prove Theorem 1, conjectured in an early version of this paper [F5]. The proof presented here is definitive and was provided by Roger Carter in October 2000; he selflessly declined to be a coauthor. His work supersedes my type C odd characteristic proof and efforts to exploit the viewpoint of semisimple conjugacy classes as points in Euclidean space; these partial results remain in the eprint [F5] but have been cut from this final version. The recent preprint [F6] derives some of the results in this paper using symmetric functions.

2. ALGEBRAIC GROUPS

Here notation about algebraic groups conforms to that in [C1], which with [Hu1] contains all the relevant background for this paper. Humphrey's [Hu2] is a good reference for information about Coxeter groups. Throughout, G is a simple, simply connected group over an algebraically closed field of characteristic p. Letting F be a Frobenius automorphism of G, we suppose that G is F split; [C1, pp. 39–41] lists the groups G^F. For instance, in type A_{n-1}, the group is $SL(n, q)$, and in type C_n, the group is $Sp(2n, q)$. Let W denote the Weyl group. This is the symmetric group in the first example and the hyperoctahedral group in the second example.

There is a natural map Φ from semisimple conjugacy classes c of G^F to conjugacy classes of the Weyl group. Let x be an element in the class c. Theorem 2.11 of [Hu1] implies that the centralizers of semisimple elements of G are connected. Consequently, $C_G(x)$, the centralizer in G of x, is determined up to G^F conjugacy. As is possible from [C1, p. 33], let T be an F-stable maximally split maximal torus in $C_G(x)$; T is determined up to G^F conjugacy. Proposition 3.3.3 of [C1] gives that the G^F conjugacy classes of F-stable maximal tori of G are in bijection with conjugacy classes of W. Define $\Phi(c)$ to be the corresponding conjugacy class of W.

Lemma 1 makes the map Φ explicit. Recall from Proposition 3.7.3 of [C1] that there is a bijection between the semisimple conjugacy classes of G^F and the F-stable orbits in T/W.

LEMMA 1. *Let T_0 be a maximally split torus of G, and let $t_0 \in T_0$ be a representative for the semisimple conjugacy class c. Let Ψ_0 be the root system of $C_G(t_0)$, i.e., all roots α such that $\alpha(t_0) = 1$. Suppose that $F(t_0) = t_0^w$ and that $w^{-1}(\Psi_0^+) = \Psi_0^+$ for some positive system of Ψ_0. Then $\Phi(c)$ is the conjugacy class of w.*

Proof. Let T be an F-stable maximal torus of G obtained by twisting T_0 by w. Let t be the image of t_0 under the corresponding conjugation map.

Then T is a maximally split torus in $C(t)$ if and only if there is an F-stable Borel subgroup of $C(t)$ containing T, which happens if and only if there is a positive system of Ψ_0 such that $w^{-1}(\Psi_0^+) = \Psi_0^+$. ∎

Next we give two examples, which are used later in this paper.

1. The first example is $SL(n, q)$ with Weyl group the symmetric group on n symbols. The semisimple conjugacy classes c correspond to monic degree n polynomials over F_q with constant term $(-1)^n$. Such a polynomial factors into irreducible polynomials. Let n_i be the number (counted with multiplicity) of these irreducible factors of degree i. Then the corresponding conjugacy class $\Phi(c)$ has n_i cycles of length i.

To see this from Lemma 1, note that t takes the form of a diagonal matrix, where the entries along the diagonal are the roots of the characteristic polynomial in the algebraic closure. The Frobenius map F acts by raising elements to the qth power, thus permuting the elements along the diagonal. (This permutation is unique if, for instance, all of the irreducible factors of the characteristic polynomial are distinct. If the irreducible factors are not all distinct, then the root system Ψ_0 is nontrivial, since the root $e_i - e_j$ sends a diagonal matrix with diagonal entries $(x_1, \ldots, x_n)$ to x_i/x_j, and hence some roots send t to 1.) If one considers the particular positive subsystem $\Psi_0 \cap \{e_i - e_j : i < j\}$ of Ψ_0, it is easy to see explicitly that there is a unique w satisfying $F(t_0) = t_0^w$, $w^{-1}(\Psi_0^+) = \Psi_0^+$ and that w has n_i cycles of length i.

We remark that the map Φ is closely related to the Gessel–Reutenauer map. The Gessel–Reutenauer map associates a permutation w to each multiset of primitive (i.e., not equal to any of its proper rotations) necklaces on the symbols $\{0, 1, \ldots, q-1\}$. This map is carefully exposited in [GesR] and is used in shuffling work in [DMP]; we omit its definition here.

If one fixes generators for the multiplicative group of each finite extension of F_q, then the monic degree n polynomials ϕ correspond to multisets of primitive necklaces [Go]. For example, suppose that θ is a generator of the multiplicative group of F_{q^3}. Then a degree-3 monic irreducible polynomial corresponds to an orbit of θ^i under the Frobenius map for some i. Writing this i base q gives a size-3 primitive necklace. For each necklace entry, one can associate a root of ϕ by taking θ^j, where j is a number base q obtained by rotating i so that the specified necklace entry is the leftmost digit of j. For example, if the necklace is (01011) and one is working base 2, then the middle 0 would correspond to θ^j, where j is 01101 base 2. In what follows, it is helpful to make 01101 an infinite word by repeating it 0110101101.... Now associated with ϕ, one can form a diagonal matrix whose elements are the roots of ϕ, ordered lexicographically by their associated infinite word. Then the permutation associated with this matrix through Lemma 1 is equal to the permutation which the Gessel–

Reutenauer map associates with the corresponding multiset of primitive necklaces.

2. The second example is type C. The group in question is $Sp(2n, q)$, with Weyl group C_n the group of signed permutations. The semisimple conjugacy classes c correspond to monic degree $2n$ polynomials, $\phi(z)$ with nonzero constant term that are invariant under the involution sending $\phi(z)$ to $\bar{\phi}(z) = (z^{2n}\phi(1/z))/\phi(0)$. Such polynomials can be more simply described as monic degree $2n$ polynomials which are palindromic in the sense that the coefficient of z^i is equal to the coefficient of z^{2n-i}. These factor uniquely into irreducibles as

$$\prod_{\{\phi_j, \bar{\phi}_j\}} [\phi_j \bar{\phi}_j]^{r_{\phi_j}} \prod_{\phi_j : \phi_j = \bar{\phi}_j} \phi_j^{s_{\phi_j}},$$

where the ϕ_j are monic irreducible polynomials and $s_{\phi_j} \in \{0, 1\}$. The conjugacy classes of C_n correspond to pairs of vectors $(\vec{\lambda}, \vec{\mu})$, where $\vec{\lambda} = (\lambda_1, \ldots, \lambda_n)$, $\vec{\mu} = (\mu_1, \ldots, \mu_n)$, and λ_i (resp. μ_i) is the number of positive (resp. negative) i cycles of an element of C_n, viewed as a signed permutation. From Lemma 1, one can see that the conjugacy class of C_n corresponding to c is then determined by setting $\lambda_i = \sum_{\phi : \deg(\phi) = i} r_\phi$ and $\mu_i = \sum_{\phi : \deg(\phi) = 2i} s_\phi$.

3. CELLINI'S WORK

Next, we recall the work of [Ce1]. (The definition which follows differs slightly form hers, being inverse, making use of her Corollary 2.1, and renormalizing so as to have a probability measure.) We follow her in supposing that W is a Weyl group (i.e., a finite reflection group which arises from a Chevalley group). Let $\Delta = \{\alpha_1, \ldots, \alpha_r\}$ be a simple root system for W. Letting α_0 denote the negative of the highest root, let $\widetilde{\Pi} = \Pi \cup \alpha_0$. Define the cyclic descent $C\mathrm{des}(w)$ to be the elements of $\widetilde{\Pi}$ mapped to negative roots by w, and let $cd(w) = |C\mathrm{des}(w)|$. For future use, we remark that the descent set of w is defined as the subset of Δ mapped to negative roots by w.

For instance, for S_n, the simple roots with respect to a basis $e_1, \ldots, e_n$ are $e_i - e_{i+1}$ for $i = 1, \ldots, n-1$ and $\alpha_0 = e_n - e_1$. Thus the permutation 4 1 3 2 5 (in two-line form) has three cyclic descents and two descents. Type C examples are treated in Section 5.

Now we use cyclic descents to define shuffles. For $I \subseteq \widetilde{\Pi}$, put

$$U_I = \{w \in W | C\mathrm{des}(w) \cap I = \emptyset\}.$$

Let Y be the coroot lattice. Then define $a_{k,I}$ by

$$|\{y \in Y | \langle -\alpha_0, y\rangle = k, \langle \alpha_i, y\rangle = 0 \text{ for } \alpha_i \in I - \alpha_0, \langle \alpha_i, y\rangle > 0 \\ \text{for } \alpha_i \in \widetilde{\Pi} - I\}| \text{ if } \alpha_0 \in I$$

or

$$|\{y \in Y | \langle -\alpha_0, y\rangle < k, \langle \alpha_i, y\rangle = 0 \text{ for } \alpha_i \in I, \langle \alpha_i, y\rangle > 0 \\ \text{for } \alpha_i \in \Pi - I\}| \text{ if } \alpha_0 \notin I.$$

Finally, define an element x_k of the group algebra of W by

$$x_k = \frac{1}{k^r} \sum_{I \subseteq \widetilde{\Pi}} a_{k,I} \sum_{w \in U_I} w.$$

Equivalently, the coefficient of an element w in x_k is

$$\frac{1}{k^r} \sum_{I \subseteq \widetilde{\Pi} - C\mathrm{des}(w)} a_{k,I}.$$

This coefficient is denoted by $x_k(w)$ throughout the paper. We refer to these x_k as affine k-shuffles. Note that $X_k(w)$ is not constant on conjugacy classes.

In type A_{n-1}, this says that the coefficient of w is x_k is equal to $1/(k^{n-1})$ multiplied by the number of integer vectors $(v_1, \ldots, v_n)$ satisfying the following conditions:

1. $v_1 + \cdots + v_n = 0$.
2. $v_1 \geq v_2 \geq \cdots \geq v_n, v_1 - v_n \leq k$.
3. $v_i > v_{i+1}$ if $w(i) > w(i+1)$ (with $1 \leq i \leq n-1$).
4. $v_1 < v_n + k$ if $w(n) > w(1)$.

From [Ce1], it follows that the x_k satisfy the following two desirable properties:

1. (Measure) The sum of the coefficients in the expansion of x_k in the basis of group elements is 1. Equivalently,

$$\sum_{I \subseteq \widetilde{\Pi}} a_{k,I} |U_I| = k^r.$$

In probabilistic terms, the element x_k defines a probability measure on the group W.

2. (Convolution) $x_k x_h = x_{kh}$.

The foregoing definition of x_k is computationally convenient for this paper. We note that [Ce1] constructed the x_k in the following more conceptual way, when k is a positive integer. Let W_k be the index k^r subgroup of the affine Weyl group that is generated by reflections in the hyperplanes corresponding to $\{\alpha_1, \ldots, \alpha_r\}$ and also the hyperplane $\{\langle x, -\alpha_0\rangle = k\}$. There are k^r unique minimal-length coset representatives for W_k in the affine Weyl group, and x_k is obtained by projecting them to the Weyl group.

The following problem is very natural. We remark that for GSR riffle shuffles, Problem 1 was studied in [Han]. Diaconis [D] has been a vigorous advocate of such questions, emphasizing the link with convergence rates of Markov chains.

PROBLEM 1. Determine the eigenvalues (and multiplicities) of x_k acting on the group algebra by left multiplication. More generally, recall that the Fourier transform of a probability measure P at an irreducible representation ρ is defined as $\sum_{w \in W} P(w)\rho(w)$. For each ρ, what are the eigenvalues of this matrix?

To close the section, we state the analog of the DMP theorem.

THEOREM 1. *Let G be a simple, simply connected group defined over an algebraically closed field of characteristic P. Letting F be a Frobenius automorphism of G, suppose that G is F-split. Let c be a semisimple conjugacy class of G^F chosen uniformly at random. Then for all conjugacy classes C of the Weyl group W,*

$$\sum_{w \in C} \text{Probability } (\Phi(c) = C) = \sum_{w \in C} \text{Coef. of } w \textit{ in } x_q.$$

4. TYPE A AFFINE SHUFFLES

To begin, we derive four expressions for x_k in type A_{n-1}. For this, recall that the major index of w is defined by $\operatorname{maj}(w) = \sum_{\substack{i:1 \le i \le n-1 \\ w(i) > w(i+1)}} i$. This is the sum of the positions of the descents of w. The notation $\left[{n \atop k}\right]$ denotes the q-binomial coefficient $\frac{(q^n-1)\cdots(q-1)}{(q^k-1)\cdots(q-1)(q^{n-k}-1)\cdots(q-1)}$. Let $C_m(n)$ denote the Ramanujan sum $\sum_k e^{\frac{2\pi i k n}{m}}$, where k runs over integers prime to m satisfying $1 \le k \le m$.

The following lemma of von Sterneck (see [Ram] for a proof in English) will be helpful. We emphasize that it is used only in the derivation of the fourth formula for x_k; the first three expressions do not require it.

LEMMA 2. *The number of ways of expressing n as the sum* mod m *of $k \ge 1$ integers of the set $0, 1, 2, \ldots, m-1$ repetitions being allowed is*

$$\frac{1}{m} \sum_{d \mid m, k} \binom{\frac{m+k-d}{d}}{\frac{k}{d}} C_d(n).$$

Recall that $x_k(w)$ is the coefficient of w in x_k. For our purposes, partitions have the standard number theoretic meaning as in [HarW].

THEOREM 2. *In type* A_{n-1}, $x_k(w)$ *is equal to any of the following*:

1. $1/(k^{n-1})$ *multiplied by the number of partitions with* $\leq n-1$ *parts of size at most* $k - cd(w)$, *such that the total number being partitioned has size congruent to* $-\text{maj}(w) \bmod n$

2. $1/(k^{n-1})$ *multiplied by the number of partitions with* $\leq k - cd(w)$ *parts of size at most* $n-1$, *such that the total number being partitioned has size congruent to* $-\text{maj}(w) \bmod n$

3.

$$\frac{1}{k^{n-1}} \sum_{r=0}^{\infty} \text{Coef. of } q^{r\cdot n} \textit{ in } \left(q^{\text{maj}(w)} \begin{bmatrix} k+n-cd(w)-1 \\ n-1 \end{bmatrix} \right)$$

4.

$$\begin{cases} \dfrac{1}{nk^{n-1}} \displaystyle\sum_{d|n,\, k-cd(w)} \binom{\frac{n+k-cd(w)-d}{d}}{\frac{k-cd(w)}{d}} C_d(-\text{maj}(w)) & \textit{if } \ k-cd(w)>0 \\ \dfrac{1}{k^{n-1}} & \textit{if } \ k-cd(w)=0, \\ & \quad \text{maj}(w) = 0 \bmod n \\ 0 & \textit{otherwise}. \end{cases}$$

Proof. From the definition of x_k,

$$\begin{aligned} x_k(w) &= \frac{1}{k^{n-1}} \sum_{I \subseteq \widetilde{\Pi} - C\text{des}(w)} a_{k,I} \\ &= \frac{1}{k^{n-1}} \sum_{\substack{v_1+\cdots+v_n=0,\, v_1 \geq \cdots v_{n-1} \geq v_n,\, v_1-v_n \leq k,\, \vec{v} \in Z^n, \\ v_i > v_{i+1} \text{ if } e_i - e_{i+1} \in C\text{des}(w), \text{ and } v_1 - v_n < k \text{ if } \alpha_0 \in C\text{des}(w)}} 1 \\ &= \frac{1}{k^{n-1}} \text{Coef. of } q^0 \text{ in} \\ &\qquad \sum_{\substack{v_1 \geq \cdots v_{n-1} \geq v_n,\, v_1 - v_n \leq k,\, \vec{v} \in Z^n, \\ v_i > v_{i+1} \text{ if } e_i - e_{i+1} \in \text{Cdes}(w), \text{ and } v_1 - v_n < k \text{ if } \alpha_0 \in \text{Cdes}(w)}} q^{v_1+\cdots+v_n}. \end{aligned}$$

Given a vector $(v_1, \ldots, v_n)$ with $\sum_i v_i = 0$, one can translate it to $(v_1 - v_n, v_2 - v_n, \ldots, 0)$. The last coordinate of the new vector is 0, and the sum of the coordinates in this new vector is a multiple of n. Abusing notation, we call this new vector $(v_1, \ldots, v_n)$. Thus

$$x_k(w) = \frac{1}{k^{n-1}} \sum_{r=0}^{\infty} \text{Coef. of } q^{r\cdot n} \text{ in} \sum_{\substack{k \geq v_1 \geq \cdots v_{n-1} \geq v_n = 0, \vec{v} \in Z^n \\ v_i > v_{i+1} \text{ if } e_i - e_{i+1} \in \text{Cdes}(w), \text{ and } v_1 < k \text{ if } \alpha_0 \in \text{Cdes}(w)}} q^{\sum v_i}.$$

Now let $v_i' = v_i - |\{j : i \leq j \leq n-1, w(j) > w(j+1)\}|$. Then the expression for $x_k(w)$ simplifies to

$$\frac{1}{k^{n-1}} \sum_{r=0}^{\infty} \text{Coef. of } q^{r\cdot n} \text{in} \sum_{k-cd(w) \geq v_1' \geq \cdots v_{n-1}' \geq v_n' = 0, \vec{v} \in Z^n} q^{\sum v_i' + \sum_i |\{j : i \leq j \leq n-1, w(j) > w(j+1)\}|}$$

$$= \frac{1}{k^{n-1}} \sum_{r=0}^{\infty} \text{Coef. of } q^{r\cdot n} \text{ in } q^{\text{maj}(w)} \sum_{k-cd(w) \geq v_1' \geq \cdots v_{n-1}' \geq v_n' = 0, \vec{v} \in Z^n} q^{\sum v_i'}.$$

This proves the first assertion of the theorem. The second assertion follows from the first by viewing partitions diagrammatically and taking transposes. The third assertion follows from either the first or second assertions together with the well-known fact that the generating function for partitions with at most a parts of size at most b is the q-binomial coefficient $\left[{a+b \atop a} \right]$. The fourth assertion follows from the second assertion and Lemma 2. ∎

Next, we connect x_k in type A with card shuffling. First, we consider the case $k = 2$. Writing $x_k = \sum c_w w$ in the group algebra, the notation x_k^{-1} denotes $\sum c_w w^{-1}$.

THEOREM 3. *When W is the symmetric group S_{2n}, the element $(x_2)^{-1}$ has the following probabilistic interpretation*:

Step 1. *Choose an even number between* 1 *and* $2n$ *with the probability of getting* $2j$ *equal to* $\binom{2n}{2j}/2^{2n-1}$. *From the stack of* $2n$ *cards, form a second pile of size* $2j$ *by removing the top* j *cards of the stack, and then putting the bottom* j *cards of the first stack on top of them.*

Step 2. *Now one has a stack of size* $2n - 2j$ *and a stack of size* $2j$. *Drop cards repeatedly according to the rule that if stacks* 1 *and* 2 *have sizes* A *and* B *at some time, then the next card comes from stack* 1 *with probability* $A/(A+B)$ *and from stack* 2 *with probability* $B/(A+B)$. (*This is equivalent to choosing uniformly at random one of the* $\binom{2n}{2j}$ *interleavings preserving the relative orders of the cards in each stack.*)

The description of x_2^{-1} *is the same for the symmetric group* S_{2n+1}, *except that at the beginning of Step* 1, *the chance of getting* $2j$ *is* $\binom{2n+1}{2j}/2^{2n}$ *and at the beginning of Step* 2, *one has a stack of size* $2n+1-2j$ *and a stack of size* $2j$.

Proof. We argue for the case S_{2n}, the case of S_{2n+1} being similar. Recall that in type A_{2n-1}, the coroot lattice is all vectors with integer components and zero sum with respect to a basis $e_1, \ldots, e_{2n}$, that $\alpha_i = e_i - e_{i+1}$ for $i = 1, \ldots, 2n-1$ and that $\alpha_0 = e_{2n} - e_1$. The elements of the coroot lattice contributing to some $a_{2,I}$ are

$$\begin{array}{ll}
(0,0,\ldots,0,0) & I = \widetilde{\Pi} - \alpha_0 \\
(1,0,0,\ldots,0,0,-1) & I = \widetilde{\Pi} - \{\alpha_1, \alpha_{2n-1}\} \\
(1,1,0,0,\ldots,0,0,-1,-1) & I = \widetilde{\Pi} - \{\alpha_2, \alpha_{2n-2}\} \\
\cdots & \cdots \\
(1,1,\ldots,1,0,0,-1,\ldots,-1,-1) & I = \widetilde{\Pi} - \{\alpha_{n-1}, \alpha_{n+1}\} \\
(1,1,\ldots,1,1,-1,-1,\ldots,-1,-1) & I = \widetilde{\Pi} - \alpha_n.
\end{array}$$

One observes that the inverses of the permutations in the foregoing card-shuffling description for a given j contribute to u_I, where

$$I = \begin{cases} \widetilde{\Pi} - \alpha_0 & \text{if } 2j = 0 \\ \widetilde{\Pi} - \{\alpha_k, \alpha_{2n-k}\} & \text{if } 2j = 2\min(k, 2n-k) \\ \widetilde{\Pi} - \alpha_n & \text{if } 2j = 2n. \end{cases}$$

The total number of such permutations for a fixed value of j is $\binom{2n}{2j}$, the number of interleavings of $2n-2j$ cards with $2j$ cards preserving the relative orders in each pile. Since $\sum_{j=0}^{n} \binom{2n}{2j} = 2^{2n-1}$ and $\sum_{I \subseteq \widetilde{\Pi}} a_{2,I} |U_I| = 2^{2n-1}$, the proof is complete. ∎

Note that when n is prime and k is a power of n, the only contribution in the fourth formula comes from $d = 1$. Using this observation, the follow-up paper [F4] shows that under these conditions, the element x_k^{-1} is the same as a k riffle shuffle followed by a cut at a uniform position. This observation (and Theorem 3) suggest the following

PROBLEM 2. Is there a useful "physical" description of the elements x_k in type A for integer $k > 2$ which renders some of its algebraic properties more transparent? Such a description exists for GSR riffle shuffles [BaD] and explains why a k_1 shuffle followed by a k_2 shuffle is a $k_1 k_2$ shuffle.

Next, we observe that for the identity conjugacy class in type A, Theorem 1 has the following consequence.

COROLLARY 1. *For any positive integer n and prime power q, the number of ways* (*disregarding order and allowing repetition*) *of writing* $0 \bmod q-1$ *as the sum of n integers from the set* $0, 1, \ldots, q-1$ *is equal to the number of ways* (*disregarding order and allowing repetition*) *of writing* $0 \bmod n$ *as the sum of $q-1$ integers from the set* $0, 1, \ldots, n-1$.

Proof. Consider k^{n-1} multiplied by the coefficient of the identity in x_q in type A_{n-1}. By part 2 of Theorem 2, this is the number of ways of writing 0 mod n as the sum of $q-1$ integers from the set $0, 1, \ldots, n-1$. Theorem 1 states that this is the number of monic degree n polynomials over F_q with constant term 1 which factor into linear terms. Working in the multiplicative group of F_q, this is clearly the number of ways of writing 0 mod $q-1$ as the sum of n integers from the set $0, 1, \ldots, q-1$. ∎

We remark that Corollary 1 holds for any positive integers n, q. This can be seen from Lemma 2. It independently appeared in an invariant theoretic setting in [EJP].

Next, we reformulate Theorem 1 in type A in terms of generating functions. This makes its number-theoretic content more visible, because one side is mod n and the other side is mod $k-1$. For its proof, Lemma 3 will be helpful. We use the notation that $f_{m,k,i,d}$ is the coefficient of Z^m in $(\frac{Z_{kd}-1}{Z-1})^{i/d}$.

LEMMA 3. $\frac{1}{i}\sum_{d|i}\mu(d)f_{m,\,k,\,i/d}$ *is the number of size i aperiodic necklaces on the symbols* $\{0, 1, \ldots, k-1\}$ *with total symbol sum m.*

Proof. This is an elementary Mobius inversion running along the lines of a result in [Rei1]. ∎

THEOREM 4. *Let $n_i(w)$ be the number of i-cycles in a permutation w. Then Theorem* 1 *in type A implies the assertion* (*which we intentionally do not simplify*) *that for all n, k,*

$$\sum_{m=0 \bmod n} \text{Coef. of } q^m u^n t^k \text{ in}$$
$$\sum_{n=0}^{\infty}\frac{u^n}{(1-tq)\cdots(1-tq^n)}\sum_{w\in S_n} t^{cd(w)}q^{\mathrm{maj(w)}}\prod x_i^{n_i(w)}$$
$$= \sum_{m=0 \bmod k-1} \text{Coef. of } q^m u^n t^k \text{ in}$$
$$\sum_{k=0}^{\infty} t^k \prod_{i=1}^{\infty}\prod_{m=1}^{\infty}\left(\frac{1}{1-q^m x_i u^i}\right)^{1/i\sum_{d|i}\mu(d)f_{m,\,k,\,i,d}}.$$

Proof. The left-hand side is equal to

$$\sum_{w\in S_n}\sum_{m=0 \bmod n} \text{Coef. of } q^m t^{k-cd(w)} \text{ in } \frac{1}{(1-tq)\cdots(1-tq^n)} q^{\mathrm{maj}(w)}\prod x_i^{n_i(w)}$$
$$= \sum_{w\in S_n}\sum_{m=0 \bmod n} \text{Coef. of } q^m \text{ in } \begin{bmatrix} n+k-cd(w)-1 \\ n-1 \end{bmatrix} q^{\mathrm{maj}(w)}\prod x_i^{n_i(w)},$$

where the last step uses Theorem 349 on page 280 of [HarW]. Note that by part 3 of Theorem 2, this expression is precisely the cycle structure-generating function under the measure x_k, multiplied by k^{n-1}.

To complete the proof of the theorem, it must be shown that the right-hand side gives the cycle structure-generating function for degree n polynomials over a field of k elements with constant term 1 (by complex analysis it is enough to argue for k a prime power). Let ϕ be a fixed generator of the multiplicative group of the field F_k of k elements, and let τ_i be a generator of the multiplicative group of the degree i extension of F_k, with the property that $\tau_i^{(k^i-1)/(k-1)} = \phi$. Recall Golomb's correspondence [Go] between degree i irreducible, monic polynomials over F_k and size i aperiodic necklaces on the symbols $\{0, 1, \ldots, k-1\}$. This correspondence goes by taking any root of the polynomial, expressing it as a power of τ_i, and then writing this power base k and forming a necklace out of the coefficients of $1, k, k^2, \ldots, k^{i-1}$. It is then easy to see that the norm of the corresponding polynomial is ϕ raised to the sum of the necklace entries. The result now follows from Lemma 3. Note that there is no $m = 0$ term, because the polynomial z cannot divide a polynomial with constant term 1. ∎

It is perhaps interesting to compare the generating function in Theorem 4 with a generating function with a similar flavor. For $w \in S_n$, let $d(w) = 1 + |\{i : w(i) > w(i+1), 1 \leq i \leq n-1|$. Thus $d(w)$ is one more than the number of linear descents. Gessel [Ges] proved that

$$\sum_{n=0}^{\infty} \frac{u^n}{(1-t)(1-tq)\cdots(1-tq^n)} \sum_{w \in S_n} t^{d(w)} q^{\mathrm{maj(w)}} \prod x_i^{n_i(w)}$$
$$= \sum_{k=1}^{\infty} t^k \prod_{i=1}^{\infty} \prod_{m=0}^{\infty} \left(\frac{1}{1 - q^m x_i u^i} \right)^{1/i \sum_{d|i} \mu(d) f_{m,k,i,d}}.$$

This raises the following:

PROBLEM 3. What is the joint generating function for permutations by cyclic descents, major index, and cycle structure? Can it be used to resolve Statement 1 in Section 5 of [F4]?

We remark that Theorem 8 in [F4] is equivalent to a generating function for permutations by cyclic descents and cycle structure.

5. TYPE C AFFINE SHUFFLES

This section studies the x_k in type C_n. Recall that the elements of C_n can be viewed as signed permutations w on the symbols $1, \ldots, n$. From the description of the root system of [Hu2, p. 42], it follows that (ordering the integers $1 < 2 < 3 < \cdots < \cdots < -3 < -2 < -1$ as in [Rei1])

1. w has a descent at position i for $1 \le i \le n-1$ if $w(i) > w(i+1)$.
2. w has a descent at position n if $w(n) < 0$.
3. w has a cyclic descent at position 1 if $w(1) > 0$.

For example, the permutation $3\ 1\ {-2}\ 4\ 5$ has a cyclic descent at position 1 and descents at positions 1 and 3.

Lemma 4, which follows easily from Theorem 1 of [Ce2], gives a formula for x_k.

LEMMA 4. *Let $d(w)$ and $cd(w)$ denote the number of descents and cyclic descents of $w \in C_n$. Then the coefficient of w in x_k is*

$$\frac{1}{k^n}\binom{\frac{k-1}{2}+n-d(w)}{n} \quad k \text{ odd}$$

$$\frac{1}{k^n}\binom{\frac{k}{2}+n-cd(w)}{n} \quad k \text{ even}.$$

Proof. For the first assertion, from Theorem 1 of [Ce2], the coefficient of w in x_k is

$$\begin{aligned}\frac{1}{k^n}\sum_{l=d(w)}^{n}\binom{\frac{k-1}{2}}{l}\binom{n-d(w)}{l-d(w)} &= \frac{1}{k^n}\sum_{l=d(w)}^{n}\binom{\frac{k-1}{2}}{l}\binom{n-d(w)}{n-l}\\ &= \frac{1}{k^n}\sum_{l=0}^{n}\binom{\frac{k-1}{2}}{l}\binom{n-d(w)}{n-l}\\ &= \frac{1}{k^n}\binom{\frac{k-1}{2}+n-d(w)}{n}.\end{aligned}$$

The second assertion is similar and involves two cases. ∎

Proposition 1 shows that the elements x_k in type C arise from physical models of card shuffling. (A careful reading of [Ce2] suggests that Cellini essentially knew this for $k = 2$.) The models which follow were previously considered in the literature for the special cases $k = 2$ in [BaD] and $k = 3$ (and implicitly for higher odd k) in [BB]. The higher k models and the implied formulas for card shuffling resulting from combining Lemma 4 and Proposition 1 may be of interest. (No formula is given for the $k = 2$ case in [BaD].)

PROPOSITION 1. *The element x_k^{-1} in type C_n has the following description*:

Step 1. *Start with a deck of n cards face down. Choose numbers $j_1, \ldots, j_k$ multinomially with the probability of getting $j_1, \ldots, j_k$ equal to $\binom{n}{j_1,\ldots,j_k}/k^n$. Make k stacks of cards of sizes $j_1, \ldots, j_k$ respectively. If k is odd, then flip over the even numbered stacks. If k is even, then flip over the odd numbered stacks.*

Step 2. *Drop cards from packets with probability proportional to packet size at a given time. Equivalently, choose uniformly at random one of the $\binom{n}{j_1,\ldots,j_k}$ interleavings of the packets.*

Proof. The proof proceeds in several cases, the goal being to show that the inverse of the foregoing processes generate w with the probabilities in Lemma 4. We give details for one subcase (the others being similar)—namely, even k when w satisfies $cd(w) = d(w)$. (The other case for k even is $cd(w) = d(w) + 1$). The inverse of the probabilistic description in the theorem is as follows:

Step 1. Start with an ordered deck of n cards face down. Successively and independently, turn the cards face up and deal then into one of k uniformly chosen random piles. Then flip over the even numbered piles (so that the cards in these piles are face down).

Step 2. Collect the piles from pile 1 to pile k, so that pile 1 is on top and pile k is on the bottom.

Consider, for instance, the permutation w given in two-line form by -2 3 1 4 -6 -5 7. Note that this satisfies $cd(w) = d(w)$, because the top card has a negative value (i.e., is turned face up). It is necessary to count the number of ways that w could have arisen from the inverse description. This is done using a bar and stars argument as in [BaD]. Here the stars represent the n cards, and the bars represent the $k-1$ breaks between the different piles. It is easy to see that each descent in w forces the position of two bars, except for the first descent, which forces only one bar. Then the remaining $(k-1)-(2d(w)-1) = k-2d(w)$ bars must be placed among the n cards as $(k-2d(w))/2$ consecutive pairs (since the piles alternate face-up, face-down). This can be done in $\binom{\frac{k}{2}+n-cd(w)}{n}$ ways, proving the result. ∎

We remark that Proposition 1 leads to a direct proof of the convolution property in type C.

Next, recall the notion of total variation distance $||P_1 - P_2||$ between two probability distributions P_1 and P_2 on a finite set X. It is defined as

$$\frac{1}{2}\sum_{x\in X} |P_1(x) - P_2(x)|.$$

Diaconis [D] explains why this is a natural and useful notion of distance between probability distributions. The remainder of this section computes the total variation distance of an affine type C k-shuffle to uniform in the case where k is even. Bayer and Diaconis [BaD] attribute an equivalent result to Bob Beals (unpublished), but with a quite different method of proof. We omit the case of odd k, because the convergence rate to randomness has been determined in [BB].

LEMMA 5. *Let N_r be the number of w in C_n with r cyclic descents. Let A_r be the number w in S_n with r descents. Then $N_{r+1} = 2^n A_r$.*

Proof. Lemma 4 shows that the chance that an affine type C k-shuffle gives a signed permutation w is

$$\frac{1}{k^n}\binom{k/2+n-cd(w)}{n}.$$

Using the fact that these shuffles are a probability measure and dividing both sides of the resulting equation by 2^n, it follows that

$$\sum_{r=1}^{n} \frac{N_r}{2^n}\binom{k/2+n-r}{n} = (k/2)^n.$$

This can be rewritten as

$$\sum_{r=0}^{n-1} \frac{N_{r+1}}{2^n}\binom{k/2+n-r-1}{n} = (k/2)^n.$$

Since this is true for all k, the relation can be inverted to solve for N_{r+1}. In the theory riffle shuffles [BaD], one gets the equation (Worpitzky's identity)

$$\sum_{r=0}^{n-1} A_r\binom{k+n-r-1}{n} = k^n$$

for all k. Thus $N_{r+1} = 2^n A_r$, as desired. ∎

THEOREM 5. *The total variation distance of an affine type C k-shuffle with k even to uniform is equal to the total distance of a GSR $k/2$ riffle shuffle on S_n to uniform.*

Proof. Lemma 4 shows that the chance that an affine type C k-shuffle gives a signed permutation w is

$$\frac{1}{k^n}\binom{k/2+n-cd(w)}{n}.$$

Thus the total variation distance is equal to

$$\begin{aligned}
&\sum_{r=0}^{n-1} N_{r+1} \left| \frac{1}{k^n} \binom{k/2+n-r-1}{n} - \frac{1}{2^n n!} \right| \\
&\quad = \sum_{r=0}^{n-1} 2^n A_r \left| \frac{1}{k^n} \binom{k/2+n-r-1}{n} - \frac{1}{2^n n!} \right| \\
&\quad = \sum_{r=0}^{n-1} A_r \left| \frac{1}{(k/2)^n} \binom{k/2+n-r-1}{n} - \frac{1}{n!} \right|.
\end{aligned}$$

From [BaD], one recognizes this last expression as the total variation distance between a $k/2$ riffle shuffle and uniform. ∎

6. DYNAMICAL SYSTEMS

Much of this section relates to the enumeration of unimodal permutations by cycle structure. This problem is given two solutions, one using a more fundamental result of [Ga] and symmetric functions, and another using Theorem 1 and the factorization theory of palindromic polynomials (which actually proves a more general result). Some asymptotic consequences are derived. We give a new proof of a result of [Rei1].

A unimodal permutation w on the symbols $\{1, \ldots, n\}$ is defined by requiring that there be some i with $1 \le i \le n$ such that the following two properties hold:

1. If $a < b \le i$, then $w(a) < w(b)$.
2. If $i \le a < b$, then $w(a) > w(b)$.

Thus i is where the maximum is achieved, and the permutations $12 \cdots n$ and $nn-1 \cdots 1$ are counted as unimodal. For each fixed i, there are $\binom{n-1}{i-1}$ unimodal permutations with maximum i, and hence a total of 2^{n-1} such permutations.

Motivated by biology and dynamical systems, [Ro] posed the problem of counting unimodal permutations by cycle structure. This problem was solved by [Ga], who gave a constructive proof of the following elegant (and more fundamental) result. For its statement, one defines the shape s of a cycle $(i_1 \cdots i_k)$ on some k distinct symbols (call them $\{1, \ldots, k\}$) to be the cycle $(\tau(i_1) \cdots \tau(i_k))$, where τ is the unique order preserving bijection between $\{i_1, \ldots, i_k\}$ and $\{1, \ldots, k\}$. Thus the shape of (523) is (312).

THEOREM 6 ([Ga]). *Let $s_1, s_2, \ldots$ denote the possible shapes of transitive unimodal permutations. Then the number of unimodal permutations with n_i cycles of shape s_i is 2^{l-1}, where l is the number of i for which $n_i > 0$.*

Theorem 6 can be rewritten in terms of generating functions.

COROLLARY 2. *Let $n_s(w)$ be the number of cycles of w of shape s. Let $|s|$ be the number of elements in s. Then*

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{2^{n-1}} \sum_{\substack{w \in S_n \\ w \text{ unimodal}}} \prod_{s \text{ shape}} x_s^{n_s(w)} = \prod_{s \text{ shape}} \left(\frac{2^{|s|} + x_s u^{|s|}}{2^{|s|} - x_s u^{|s|}} \right)$$

and

$$(1-u) + \sum_{n=1}^{\infty} \frac{(1-u)u^n}{2^{n-1}} \sum_{\substack{w \in S_n \\ w \text{ unimodal}}} \prod_{s \text{ shape}} x_s^{n_s(w)} = \prod_{s \text{ shape}} \left(\frac{2^{|s|} + x_s u^{|s|}}{2^{|s|} + u^{|s|}} \right) \times \left(\frac{2^{|s|} - u^{|s|}}{2^{|s|} - x_s u^{|s|}} \right).$$

Proof. For the first equation, consider the coefficient of $\prod_s x_s^{n_s} u^{\sum |s| n_s}$ on the left-hand side. This is the probability that a uniformly chosen unimodal permutation on $\sum |s| n_s$ symbols has n_s cycles of shape s. The coefficient on the right-hand side is $2^{|\{s: n_s > 0\}| - n}$. These are equal, by Theorem 6. To deduce the second equation, observe that setting all $x_s = 1$ in the first equation gives that

$$\frac{1}{1-u} = \prod_{s \text{ shape}} \frac{2^{|s|} + u^{|s|}}{2^{|s|} - u^{|s|}}.$$

Taking reciprocals and multiplying by the first equation yields the second equation. ∎

The second equation in Corollary 2 has an attractive probabilistic interpretation. Fix u such that $0 < u < 1$. Then choose a random symmetric group so that the chance of getting S_n is equal to $(1-u)u^n$. Choose a unimodal $w \in S_n$ uniformly at random. Then the random variables $n_s(w)$ are independent, each having distribution a convolution of a binomial $(\frac{u^{|s|}}{2^{|s|} + u^{|s|}})$ with a geometric $(1 - \frac{u^{|s|}}{2^{|s|}})$.

As another illustration of the second equation in Corollary 2, we deduce the following corollary, extending the asymptotic results in [Ga] that asymptotically 2/3 of all unimodal permutations have fixed points and 2/5 have length two cycles.

COROLLARY 3. *In the $n \to \infty$ limit, the random variables n_s converge to the convolution of a binomial$(\frac{1}{2^{|s|}+1})$ with a geometric$(1 - \frac{1}{2^{|s|}})$ and are asymptotically independent.*

Proof. The result follows from the claim that if $f(u)$ has a Taylor series around 0 and $f(1) < \infty$, then the $n \to \infty$ limit of the coefficient of u^n in $\frac{f(u)}{1-u}$ is $f(1)$. To verify the claim, write the Taylor expansion $f(u) = \sum_{n=0}^{\infty} a_n u^n$ and observe that the coefficient of u^n in $\frac{f(u)}{1-u} = \sum_{i=0}^{n} a_i$. ∎

Rogers and Weiss [RogW] used dynamical systems to count the number of transitive unimodal permutation on n symbols. We offer a proof using symmetric function theory.

Some notation is needed. A subset $D = \{d_1, \ldots, d_k\}$ of $\{1, 2, \ldots, n-1\}$ defines a composition $C(D)$ of n with parts $d_1, d_2 - d_1, \ldots, n - d_k$. A standard Young tableau is said to have a descent at position i if $i+1$ occurs in a row lower than i. The descent set of a standard Young tableau thus defines a composition of n.

LEMMA 6. *The number of transitive unimodal permutations on n symbols is*

$$\frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{\frac{n}{d}}.$$

Proof. Symmetric function notation from Chapter 1 of Macdonald [Mac] is used. Thus $p_\lambda, h_\lambda, e_\lambda$, and s_λ are the power sum, complete, elementary, and Schur symmetric functions parameterized by a partition λ. From Theorem 2.1 of [GesR], the number of n cycles with descent set D is the inner product of a Lie character $L_n = \frac{1}{n} \sum_{d|n} \mu(d) p_d^{\frac{n}{d}}$ and a Foulkes character $F_{C(D)}$. From the proof of Corollary 2.4 of [GesR], $F_{C(D)} = \sum_{|\lambda|=n} \beta_\lambda s_\lambda$, where β_λ is the number of standard tableaux of shape λ with descent composition $C(D)$. Thus the sought number is

$$\left\langle \frac{1}{n} \sum_{d|n} \mu(d) p_d^{\frac{n}{d}}, e_n + \sum_{i=2}^{n-1} s_{i,(1)^{n-i}} + h_n \right\rangle.$$

Expanding these Schur functions using exercise 9 of [Mac, p. 47], using the fact that the p_λ are an orthogonal basis of the ring of symmetric functions with known normalizing constants (p. 64 of [Mac]), and using the expansions of e_n and h_n in terms of the p_λ's (p. 25 of [Mac]), it follows that

$$\begin{aligned} \left\langle \frac{1}{n} \sum_{d|n} \mu(d) p_d^{\frac{n}{d}}, e_n + \sum_{i=2}^{n-1} s_{i,(1)^{n-i}} + h_n \right\rangle &= \left\langle \frac{1}{n} \sum_{d|n} \mu(d) p_d^{\frac{n}{d}}, \sum_{i \text{ even}} h_i e_{n-i} \right\rangle \\ &= \frac{1}{n} \sum_{d|n} \mu(d) \left\langle p_d^{\frac{n}{d}}, \sum_{\substack{i=1,\ldots,\frac{n}{d} \\ di \text{ even}}} h_{di} e_{n-di} \right\rangle \end{aligned}$$

$$= \frac{1}{n}\sum_{d|n}\mu(d)\left\langle p_d^{\frac{n}{d}}, p_d^{\frac{n}{d}} \sum_{\substack{i=1,\dots,\frac{n}{d} \\ di \text{ even}}} \frac{(-1)^{n-di-\frac{n}{d}+i}}{d^{\frac{n}{d}} i!(\frac{n}{d}-i)!}\right\rangle$$

$$= \frac{1}{n}\sum_{d|n}\mu(d)(-1)^{n-\frac{n}{d}} \sum_{\substack{i=1,\dots,\frac{n}{d} \\ di \text{ even}}} (-1)^i \binom{\frac{n}{d}}{i}$$

$$= \frac{1}{2n}\sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) 2^{\frac{n}{d}}. \qquad \blacksquare$$

Corollary 2 and Lemma 6 have the following immediate consequence.

COROLLARY 4. *Let $n_i(w)$ be the number of i-cycles of a permutation w. Then*

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{2^{n-1}} \sum_{\substack{w \in S_n \\ w \text{ unimodal}}} \prod_i x_i^{n_i(w)} = \prod_i \left(\frac{2^i + x_i u^i}{2^i - x_i u^i}\right)^{\frac{1}{2i}\sum_{\substack{d|i \\ d \text{ odd}}} \mu(d) 2^{\frac{i}{d}}}.$$

Theorem 1 will yield a second proof of the enumeration of unimodal permutations by cycle structure by relating the problem to the factorization theory of palindromic polynomials over finite fields. The first step is to reformulate Theorem 1 in type C. The following lemmas, the first of which is well known, will be helpful. Here μ denotes the Moebius function of elementary number theory.

LEMMA 7. *The number of monic degree-n irreducible polynomials over F_q is equal to*

$$\frac{1}{n}\sum_{d|n}\mu(d) q^{n/d}.$$

LEMMA 8 ([FNP]). *Let $e = 1$ if q is even and $e = 2$ if q is odd. Then the number of monic, degree n polynomials $f(z)$ over F_q with nonzero constant coefficient and invariant under the involution $f(z) \mapsto f(0)^{-1} z^n f(\frac{1}{z})$ is*

$$\begin{cases} e & \text{if } n = 1 \\ 0 & \text{if } n \text{ is odd and } n > 1 \\ \frac{1}{n}\sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)(q^{\frac{n}{2d}} + 1 - e) & \text{otherwise.} \end{cases}$$

Recall that $x_q(w)$ denotes the coefficient of w in x_q.

THEOREM 7. *Let $e = 1$ if q is even and $e = 2$ if q is odd. Let $\lambda_i(w)$ and $\mu_i(w)$ be the number of positive and negative i-cycles of a signed permutation*

w in C_n. Then

$$1+\sum_{n\geq 1} u^n q^n \sum_{w\in C_n} x_q(w) \prod_{i\geq 1} x_i^{\lambda_i(w)} y_i^{\mu_i(w)} = \left(\frac{1}{1-x_1 u}\right)^{e-1}$$
$$\times \prod_{m\geq 1} \left(\frac{1+y_m u^m}{1-x_m u^m}\right)^{\frac{1}{2m}\sum_{\substack{d|m \\ d \text{ odd}}} \mu(d)(q^{\frac{m}{d}}+1-e)}.$$

Proof. One argues separately for odd and even characteristics and first for prime powers. Taking the coefficient of $u^n \prod_i x_i^{\lambda_i} y_i^{\mu_i}$ on the left-hand side of this equation and dividing by q^n gives, by Lemma 4, the probability that w chosen according to the x_q probability measure is in a conjugacy class with λ_i positive i-cycles and μ_i negative i-cycles for each i. By Theorem 1, to verify the theorem for even prime powers, it is enough to show that the coefficient of $u^n \prod_i x_i^{\lambda_i} y_i^{\mu_i}$ on the right-hand side of this equation is the number of degree-$2n$ monic palindromic polynomials over F_q which factor as

$$\prod_{\{\phi_j,\bar{\phi}_j\}} [\phi_j \bar{\phi}_j]^{r_{\phi_j}} \prod_{\phi_j:\phi_j=\bar{\phi}_j} \phi_j^{s_{\phi_j}}$$

(with ϕ_j, where $s_{\phi_j} \in \{0,1\}$) and $\lambda_i = \sum_{\phi:\deg(\phi)=i} r_\phi$ and $\mu_i = \sum_{\phi:\deg(\phi)=2i} s_\phi$. This follows readily from Lemmas 7 and 8. The theorem now follows for arbitrary q, since two functions analytic in a region and agreeing on a set with an accumulation point ($q=\infty$) in that region must be equal. ∎

Corollary 5 deduces the enumeration of unimodal permutations by cycle structure.

COROLLARY 5. *Let $n_i(w)$ be the number of i-cycles of $w \in S_n$. Then*

$$1+\sum_{n=1}^{\infty} \frac{u^n}{2^{n-1}} \sum_{\substack{w\in S_n \\ w \text{ unimodal}}} \prod_i x_i^{n_i(w)} = \prod_i \left(\frac{2^i + x_i u^i}{2^i - x_i u^i}\right)^{\frac{1}{2i}\sum_{\substack{d|i \\ d \text{ odd}}} \mu(d) 2^{\frac{i}{d}}}.$$

Proof. Given Theorem 7 with $q=2$, it is enough to define a 2-to-1 map η from the 2^n type C_n characteristic two shuffles to unimodal elements of S_n, such that η preserves the number of i-cycles for each i, disregarding signs. To define η, recalling Proposition 1 observe that the two shuffles are all ways of cutting a deck of size n, then flipping the first pack, and choosing a random interleaving. For instance, if one cuts a 12-card deck at position 6, then such an interleaving could be

$$[-6, -5, 7, 8, -4, 9, -3, 10, -2, 11, -1, 12].$$

Observe that taking the inverse of this permutation and disregarding signs gives

$$[11, 9, 7, 5, 2, 1, 3, 4, 6, 8, 10, 12].$$

Next, conjugate by the involution transposing each i with $n+1-i$, thereby obtaining a unimodal permutation. Note that this map preserves cycle structure and is 2 to 1 because of the first symbol. (In the example, -6 can always have its sign reversed, yielding a possible shuffle.) ∎

The following corollary describes the $n \to \infty$ asymptotics of cycle structure for type C affine q shuffles. We omit the proof, which is essentially the same as for Corollary 3.

COROLLARY 6. *Let $\lambda_i(w)$ and $\mu_i(w)$ be the number of positive and negative i-cycles of a signed permutation w in C_n.*

1. *Fix u such that $0 < u < 1$. Then choose a random hyperoctahedral group so that the chance of getting C_n is equal to $(1-u)u^n$. Choose $w \in C_n$ according to the affine q shuffle measure. Then the random variables $\{\lambda_m, \mu_m\}$ are independent. The λ_m $(m \geq 2)$ are distributed as the convolution of $\frac{1}{2m}\sum_{d|m}\mu(d)(q^{m/d}+1-e)$ many geometrics with parameter $1-\frac{u^m}{q^m}$, and λ_1 is distributed as the convolution of $\frac{1}{2}(q+e-1)$ many geometrics with parameter $1-\frac{u}{q}$. The μ_m are distributed as the convolution of $\frac{1}{2m}\sum_{d|m}\mu(d)(q^{m/d}+1-e)$ many binomials with parameter $\frac{u^m/q^m}{1+u^m/q^m}$.*
2. *Choose $w \in C_n$ according to the affine q shuffle measure. Then in the $n \to \infty$ limit, the random variables $\{\lambda_m, \mu_m\}$ are independent. The λ_m $(m \geq 2)$ are distributed as the convolution of $\frac{1}{2m}\sum_{d|m}\mu(d)(q^{m/d}+1-e)$ many geometrics with parameter $1-\frac{1}{q^m}$, and λ_1 is distributed as the convolution of $\frac{1}{2}(q+e-1)$ many geometrics with parameter $1-\frac{1}{q}$. The μ_m are distributed as the convolution of $\frac{1}{2m}\sum_{d|m}\mu(d)(q^{m/d}+1-e)$ many binomials with parameter $\frac{1/q^m}{1+1/q^m}$.*

Remark. Type C_n shuffles also relate to dynamical systems in another way, analogous to the type A construction for Bayer–Diaconis shuffles [BaD]. Here we describe the case where $k=2$. One drops n points in the interval $[-1, 1]$ uniformly and independently. Then one applies the map $x \mapsto 2|x|-1$. The resulting permutation can be thought of as a signed permutation, since some points preserve and some reverse orientation. From Proposition 1, this signed permutation obtained after iterating this map r times has the distribution of the type C_n shuffle with $k=2^r$. Lalley [La1] studied the cycle structure of random permutations obtained by tracking n uniformly dropped points after iterating a map a large number of times. His results applied to piecewise monotone maps, and he proved that the limiting cycle structure is a convolution of geometrics. Hence Corollary 6 shows that Lalley's results do not extend to functions such as $x \mapsto 2|x| - 1$.

As a final result, we deduce a new proof of the following result of Reiner. Here $d(w)$ denotes the number of descents of $w \in C_n$.

COROLLARY 7 ([Rei1]).

$$\sum_{n\geq 0} \frac{u^n}{(1-t)^{n+1}} \sum_{w\in C_n} t^{d(w)+1} \prod_i x_i^{\lambda_i(w)} y_i^{\mu_i(w)}$$
$$= \sum_{k\geq 0} t^k \frac{1}{1-x_1 u} \prod_{m\geq 1} \left(\frac{1+y_m u^m}{1-x_m u^m}\right)^{\frac{1}{2m}\sum_{\substack{d|m \\ m \text{ odd}}} \mu(d)((2k-1)^{m/d}-1)}.$$

Proof. Taking coefficients of t^k on both sides of the equation under question and then setting $q = 2k-1$ gives the equation

$$\sum_{n\geq 0} u^n \sum_{w\in C_n} \binom{\frac{q-1}{2}+n-d(w)}{n} \prod_i x_i^{\lambda_i(w)} y_i^{\mu_i(w)}$$
$$= \frac{1}{1-x_1 u} \prod_{m\geq 1} \left(\frac{1+y_m u^m}{1-x_m u^m}\right)^{\frac{1}{2m}\sum_{\substack{d|m \\ m \text{ odd}}} \mu(d)(q^{m/d}-1)}.$$

However, this equation follows from Theorem 7 for odd q and Lemma 4. ∎

7. PROOF OF THEOREM 1: THE BRAUER COMPLEX

The purpose of this section is to report a proof of Theorem 1 due to Roger Carter. The proof uses a geometric object called the Brauer complex. All relevant background (including pictures) can be found in Section 3.8 of [C1]. The early version of this paper [F5] attempted (unsuccessfully) to exploit the geometric set-up.

Let Y be the coroot lattice and W the Weyl group, so that $\langle Y, W\rangle$ is the affine Weyl group. The group $\langle Y, W\rangle$ acts on the vector space $Y \otimes R$ with Y acting by translations T_y: $v \mapsto v + y$ and W acting by orthogonal transformations. The affine Weyl group has a fundamental region in $Y \otimes R$ given by

$$\overline{A}_1 = \{v \in Y \otimes R \mid \langle \alpha_i, v\rangle \geq 0 \text{ for } i = 1, \ldots, r, \langle -\alpha_0, v\rangle \leq 1\}.$$

Let $Q_{p'}$ be the additive group of rational numbers $\frac{s}{t}$, where $s, t \in Z$ and t is not divisible by p (the characteristic). Proposition 3.8.1 of [C1] shows that there is an action of F on $\overline{A}_{p'} = \overline{A}_1 \cap (Y \otimes Q_{p'})$ given by taking the image of $v \in \overline{A}_{p'}$ to be the unique element of $\overline{A}_{p'}$ equivalent to $F(v)$ under $\langle Y, W\rangle$.

We highlight the following facts.

Fact 1 (Proposition 3.7.3 of [C1]). The q^r semisimple conjugacy classes of G^F are in bijection with the q^r elements of $\overline{A}_{p'}$ which are stable under the action of F.

As an example, for type A_2 with $q = 3$, the nine stable points are

1. $(0, 0, 0), (1/2, 0, -1/2)$, corresponding to polynomials that factor into linear pieces

2. $(1/4, 0, -1/4), (4/8, 1/8, -5/8), (5/8, -1/8, -4/8)$, corresponding to polynomials that are a product of a linear and a degree 2 factor

3. $(6/26, 2/26, -8/26), (8/26, -2/26, -6/26), (10/26, 4/26, -14/26), (14/26, -4/26, -10/26)$, corresponding to irreducible polyomials.

For instance, the point $v = (4/8, 1/8, -5/8)$ is stable because $3v = v^{(23)} + (1, 1, -2)$.

We remark that this bijection is not entirely canonical, because the isomorphism between the multiplicative group of the algebraic closure of F_q and $Q_{p'}/Z$ (Proposition 3.1.3 of [C1]) is not entirely canonical. In other words, we have chosen (a consistent set of) generators of the multiplicative groups of all of the finite extensions of F_q. The bijection in Fact 1 is canonical only after this choice.

Fact 2 (Corollary 3.8.3 of [C1]). There is a bijection between semisimple conjugacy classes in G^F and simplices of maximal dimension in the Brauer complex.

For all that follows,

$$\overline{A}_q = \{v \in Y \otimes R : \langle \alpha_i, v\rangle \geq 0 \text{ for } i = 1, \ldots, r, \langle -\alpha_0, v\rangle \leq q\}.$$

Let $I(y)$ be the set of α_i with $i \in \{0, 1, \ldots, r\}$ such that y lies on the i-boundary wall of $\overline{A}_q$.

We now describe Professor Carter's proof of Theorem 1.

Proof of Theorem 1. The proof proceeds in two steps. Step 1 shows that there is a bijection between semisimple classes c in G^F and pairs $(y, w) \in Y \times W$ such that $y \in Y \cap \overline{A}_q$ and $I(y) \cap \mathrm{Cdes}(w^{-1}) = \emptyset$. Step 2 shows that $\Phi(c)$ is conjugate to w. The theorem then follows from the definition of x_q.

Step 1. It is known that there is a bijection between simplices of maximal dimension in the Brauer complex and elements ω in the affine Weyl group such that $\omega(\overline{A}_1) \subset \overline{A}_q$. The alcoves $\omega(\overline{A}_1)$ are all obtained by first transforming by $w \in W$ to give $w(\overline{A}_1)$ and then translating by T_y for some $y \in Y$. Let S be the union of the alcoves $w(\overline{A}_1)$ for $w \in W$; S is called the basic star. The sets $T_y(S)$ are called the stars, and the centers of the stars are the elements of Y.

Each alcove $\omega(\overline{A}_1)$ which lies in $\overline{A}_q$ lies in some star whose center lies in $Y \cap \overline{A}_q$. Conversely, if $y \in Y \cap \overline{A}_q$, then we wish to know which alcoves in the star $T_y(S)$ lie in $\overline{A}_q$. If y does not lie on any boundary wall of $\overline{A}_q$, then all alcoves in $T_y(S)$ lie in $\overline{A}_q$. If y lies on the boundary wall corresponding to $i \in \{0, 1, \dots, r\}$, then the alcove $T_y w(\overline{A}_1)$ lies on the $\overline{A}_q$ side of this boundary wall if and only if $w^{-1}(\alpha_i)$ is a positive root. This can be seen by looking at the star S. Thus there is a bijection between semisimple classes c in G^F and pairs $(y, w) \in Y \times W$ such that $y \in Y \cap \overline{A}_q$ and $I(y) \cap \mathrm{Cdes}(w^{-1}) = \emptyset$.

Step 2. Let T_0 be a maximal split torus of G and let $Y_0 = \mathrm{Hom}(Q_{p'}/Z, T_0)$ be its cocharacter group. Let T be an F-stable maximal torus of G obtained from T_0 by twisting with $w \in W$. We have conjugation maps $T \mapsto T_0$, $Y \mapsto Y_0$. Under these maps, $F : Y \mapsto Y$ maps to $w^{-1}F : Y_0 \mapsto Y_0$.

Let ω be an element of the affine Weyl group such that $\omega(\overline{A}_1) \subset \overline{A}_q$. From Section 3.8 of [C1], $\overline{A}$ contains a unique p satisfying $F^{-1}\omega(p) = p$, i.e., $F(p) = p^w + y_0$. Let the walls of $\overline{A}_q$ be $H_0, H_1, \dots, H_n$. Let $J = \{i : p \in H_i\}$. J is a proper subset of $\{0, 1, \dots, n\}$. The roots α_i, $i \in J$ form a simple system Π_J in a subsystem $\Phi_J \subset \Phi$. From page 102 of [C1], the point p maps to an element $t_0 \in T_0$. Then $F(t_0) = t_0^w$, and t_0 lies in the semisimple conjugacy class of G^F corresponding to the point p. Φ_J can be identitied with the root system of the centralizer of the semisimple conjugacy class of G^F corresponding to the point t_0.

To complete the proof of Step 2, it suffices to show (by Lemma 1) that $w(\Phi_J^+) = \Phi_J^+$. The construction of the point p as the intersection of a sequence of increasingly small alcoves, each obtained from the previous one by a map $F^{-1}\omega$ which preserves the type of the walls, shows that p lies in the J-face of $\overline{A}_q$ and of $\omega(\overline{A}_1)$. (The J-face of $\overline{A}_q$ is the intersection of the H_i for $i \in J$.) For $i \in J$, let the wall H_i of $\overline{A}_q$ coincide with the wall of type j of $\omega(\overline{A}_1)$. The root orthogonal to H_i pointing into $\overline{A}_q$ is α_i. Consider the root orthogonal to the wall of type j for $\omega(\overline{A}_1)$ pointing into $\omega(\overline{A}_1)$. Since $\omega(\overline{A}_1) = T_{y_0}(w(\overline{A}_1))$, this is the root orthogonal to the wall of type j for $w(\overline{A}_1)$ pointing into $w(\overline{A}_1)$. This is the root $w(\alpha_j)$ since the wall of type j for $w(\overline{A}_1)$ is the image under w of the wall of type j for $\overline{A}_1$. Hence $\alpha_i = w(\alpha_j)$. This shows that, since $i, j \in J$, $w(\Pi_J) = \Pi_J$. Hence $w(\Phi_J^+) = \Phi_J^+$, as desired. ∎

The results of this section raise

PROBLEM 4. Is there an analog of the Brauer complex that sheds light on the problems in [F3] or gives a general-type Gessel–Reutenauer bijection?

ACKNOWLEDGMENTS

This research was supported by an National Science Foundation postdoctoral fellowship. The author is very indebted to Roger Carter for proving conjectures stated in an early version of this paper, superseding the author's partial results on the problem. Persi Diaconis offered expository feedback and motivated the author to seek a new proof of Beals' work on total variation distance.

REFERENCES

[A] A. Aldous, "Random Walk on Finite Groups and Rapidly Mixing Markov Chains," Lecture Notes in Mathematics **986** Springer, New York, 1983, pp. 243–297.

[BaD] D. Bayer and P. Diaconis, Trailing the dovetail shuffle to its lair, *Ann. Appl. Probab.* **2** (1992), 294–313.

[B] N. Bergeron, A hyperoctahedral analog of the free Lie algebra, *J. Combin. Theory Ser. A* **58** (1991), 256–278.

[BB] F. Bergeron and N. Bergeron, Orthogonal idempotents in the descent algebra of B_n and applications, *J. Pure Appl. Algebra* **79** (1992), 109–129.

[BBGar] F. Bergeron, N. Bergeron, and A. M. Garsia, Idempotents for the free Lie algebra and q-enumeration, *in* "Invariant Theory and Tableaux" IMA Vol. Math. Appl. 19, Springer, New York, 1990.

[BBHT] F. Bergeron, N. Bergeron, R. B. Howlett, and D. E. Taylor, A decomposition of the descent algebra of a finite Coxeter group, *J. Algebraic Combin*. **1** (1992), 23–44.

[BW] N. Bergeron and L. Wolfgang, The decomposition of Hochschild cohomology and the Gerstenhaber operations, *J. Pure Appl. Algebra* **104** (1995), 243–265.

[BiHaRo] P. Bidigare, P. Hanlon, and D. Rockmore, A combinatorial description of the spectrum of the Tsetlin library and its generalization to hyperplane arrangements, *Duke Math J.* **99** (1999), 135–174.

[BD] K. Brown and P. Diaconis, Random walks and hyperplane arrangements, *Ann. Probab*. **26** (1998), 1813–1854.

[C1] R. Carter, "Finite Groups of Lie Type," Wiley, New York, 1985.

[Ce1] P. Cellini, A general commutative descent algebra, *J. Algebra* **175** (1995), 990–1014.

[Ce2] P. Cellini, A general commutative descent algebra II. The Case C_n. *J. Algebra* **175** (1995), 1015–1026.

[D] P. Diaconis, "Group Representations in Probability and Statistics," Lecture Notes Monograph Series 11, Institute of Mathematical Statistics, Hayward, CA 1988.

[DMP] P. Diaconis, M. McGrath, and J. Pitman, Riffle shuffles, cycles, and descents, *Combinatorica* **15** (1995), 11–20.

[EJP] A. Elashvili, M. Jibladze, and D. Pataraia, Combinatorics of necklaces and "Hermite reciprocity," *J. Algebraic Combin*. **10** (1999), 173–188.

[F1] J. Fulman, The combinatorics of biased riffle shuffles, *Combinatorica* **18** (1998), 173–184.

[F2] J. Fulman, Descent algebras, hyperplane arrangements, and shuffling cards, *Proc. Amer. Math. Soc*. **129** (2001), 965–973.

[F3] J. Fulman, Semisimple orbits of Lie algebras and card shuffling measures on Coxeter groups, *J. Algebra* **224** (2000), 151–165.

[F4] J. Fulman, Affine shuffles, shuffles with cuts, the Whitehouse module, and patience sorting, *J. Algebra* **231** (2000), 614–639.

[F5] J. Fulman, Cellini's descent algebra and semisimple conjugacy classes of finite groups of Lie type, preprint math.nt/9909121 at xxx.lanl.gov.

[F6] J. Fulman, Applications of symmetric functions to cycle and increasing subsequence structure after shuffles, parts I and II. Preprints math.co/0102176 and math.co/0104003 at xxx.lanl.gov.

[FNP] J. Fulman, P. M. Neumann, and C. E. Praeger, A generating function approach to the enumeration of cyclic, separable, and semisimple matrices in the classical groups over finite fields, preprint.

[Ga] T. Gannon, The cyclic structure of unimodal permutations, preprint, math.DS/9906207 at xxx.lanl.gov.

[Gar] A. Garsia, Combinatorics of the free Lie algebra and the symmetric group, in "Analysis, et cetera," pp. 309–382, Academic Press, Boston, 1990.

[Ger] M. Gerstenhaber and S. D. Schack, A Hodge type decomposition for commutative algebra cohomology, *J. Pure. Appl. Algebra* **38** (1987), 229–247.

[Ges] I. Gessel, Counting permutations by descents, greater index, and cycle structure, unpublished manuscript.

[GesR] I. Gessel and C. Reutenauer, Counting permutations with given cycle structure and descent set, *J. Combin. Theory Ser. A* **64** (1993), 189–215.

[Go] S. Golomb, Irreducible polynomials, synchronization codes, primitive necklaces, and the cyclotomic algebra, *in* "Combinatorial Mathematics and its Applications" pp. 358–370, Univ. North Carolina Press, Durham, NC 1969.

[Han] P. Hanlon, The action of S_n on the components of the Hodge decomposition of Hochschild homology, *Michigan Math. J.* **37** (1990), 105–124.

[HarW] G. Hardy and E. Wright, "An Introduction to the Theory of Numbers" 5th ed., Clarendon Press, Oxford, U.K., 1979.

[Hu1] J. Humphreys, "Conjugacy Classes in Semisimple Algebraic Groups," Mathematical Surveys and Monographs 43, American Mathematical Society, Providence, RI, 1995.

[Hu2] J. Humphreys, "Reflection Groups and Coxeter Groups," Cambridge Studies in Advanced Mathematics, 29, Cambridge Univ. Press, Cambridge, U.K., 1990.

[La1] S. Lalley, Cycle structure of riffle shuffles, *Ann. Prob*. **24** (1996), 49–73.

[La2] S. Lalley, Riffle shuffles and their associated dynamical systems, *J. Theoret. Probab.* **12** (1999), 903–932.

[Mac] I. Macdonald, "Symmetric Functions and Hall Polynomials," 2nd ed., Clarendon Press, Oxford, U.K., 1995.

[Ram] K. G. Ramanathan, Some applications of Ramanujan's trigonometrical sum $C_m(n)$, *Indian Acad. Sci. Sect. A*. **20** (1944), 62–70.

[Rei1] V. Reiner, Signed permutation statistics and cycle type, *European J. Combin*. **14** (1993), 569–579.

[Rei2] V. Reiner, Quotients of Coxeter complexes and P-partitions, *Mem. Amer. Math. Soc*. **95** (1992), vi + 134pp.

[Ro] T. Rogers, Chaos in systems in population biology, Prog. Theoret. Biol. **6** (1981), 91–146.

[RogW] T. Rogers and A. Weiss, The number of orientation reversing cycles in the quadratic map, *CMS Conf. Proc*. **8** (1986), 703–711.

[SSt] S. Shnider and S. Sternberg, "Quantum Groups," Graduate Texts in Mathematical Physics, II, International Press, Cambridge, MA, 1993.

[Sta] R. Stanley, Generalized riffle shuffles and quasisymmetric functions, preprint math. CO/9912025 at xxx.lanl.gov.

[T] J. Y. Thibon, The cycle enumerator of unimodal permutations, preprint, math. CO/0102051 at xxx.lanl.gov.