Journal of Algebra **224,** 151–165 (2000)
doi:10.1006/jabr.1999.8157, available online at http://www.idealibrary.com on IDEAL®

Semisimple Orbits of Lie Algebras and Card-Shuffling Measures on Coxeter Groups

Jason Fulman

Department of Mathematics, Stanford University, Building 380, MC 2125,
Stanford, California 94305
E-mail: fulman@math.stanford.edu

Communicated by Michel Broué

Received February 15, 1999

Random walk on the chambers of hyperplane arrangements is used to define a family of card shuffling measures $H_{W,x}$ for a finite Coxeter group W and real $x \neq 0$. By algebraic group theory, there is a map Φ from the semisimple orbits of the adjoint action of a finite group of Lie type on its Lie algebra to the conjugacy classes of the Weyl group. Choosing such a semisimple orbit uniformly at random thereby induces a probability measure on the conjugacy classes of the Weyl group. For types A, B, and the identity conjugacy class of W for all types, it is proved that for q very good, this measure on conjugacy classes is equal to the measure arising from $H_{W,q}$. The possibility of refining Φ to a map to elements of the Weyl group is discussed. © 2000 Academic Press

Key Words: card shuffling; hyperplane arrangement; conjugacy class; adjoint action.

1. INTRODUCTION

In a mathematical study of ordinary riffle shuffles of cards, Bayer and Diaconis [1] introduced a 1-parameter class of probability measures (which we denote by $H_{S_n,x}$) on the symmetric group. When $x = 2$, these correspond to a model of shuffling due to Gilbert–Shannon–Reeds which seems close to the way real people shuffle. Repeated shuffling k times (convolution on the symmetric group) was shown in [1] to correspond to $H_{S_n,2^k}$. Further, a closed formula was found for $H_{S_n,x}$. This was used to prove that $\frac{3}{2}\log_2 n + c$ shuffles are necessary and suffice to mix up n cards. In later work [9], a formula was given for the $H_{S_n,x}$ measure of a conjugacy class in S_n. Letting a_i be the number of i-cycles in a permutation in this conjugacy

0021-8693/00 $35.00

class, this formula was shown to equal the chance that a random monic polynomial of degree n chosen over F_q (with $x = q$) has a_i irreducible factors of degree i. This result seemed mysterious. One of the aims of the present paper is to explain the mystery and show how the results generalize to other Coxeter groups.

The first part of this paper defines signed measures $H_{W,x}$ for a finite Coxeter group W and real $x \neq 0$. The meaning of a signed measure is an element of the group algebra of W whose coefficients sum to 1. The key tool in defining the measures $H_{W,x}$ will be the theory of random walks on the chambers of hyperplane arrangements, as initiated in [5] and developed in [6]. As noted in [12] (a follow-up to this paper), the measures defined here generalize to any real hyperplane arrangement. The point of Sect. 2 is to focus on the case of arrangements coming from finite Coxeter groups. The paper [5] had a hyperplane definition for type A shuffling, but not using group theoretically defined face weights.

For type A these measures (not expressed using hyperplane walks) were discovered by Bayer and Diaconis [1] in their analysis of riffle shuffling. Their work was extended to type B in [2]. (It is amusing to note as in [1] that for tarot cards, which often have up/down directions, type B shuffling is a better model than type A shuffling.) For types A and B these measures also arise in explicit versions of the Poincaré–Birkhoff–Witt theorem [4] and in splittings of Hochschild homology [18]. Section 3.8 of [22] describes the type A measure in the language of Hopf algebras. Richard Stanley [26] has studied the measure on partitions obtained by applying the RSK algorithm to permutations distributed as shuffles. This gives an elementary probabilistic interpretation to Schur functions and connects card shuffling with representation theory of the symmetric group.

Section 3 connects the measures $H_{W,x}$ with the finite groups of Lie type. As mentioned, there is a natural map Φ from the semisimple orbits of the adjoint action of a finite group of Lie type on its Lie algebra to the conjugacy classes of the Weyl group. Choosing such a semisimple orbit uniformly at random gives a probability measure on the conjugacy classes of the Weyl group. For q very good, we show that in some cases this measure on conjugacy classes is equal to the measure arising from $H_{W,q}$. For instance in type A the semisimple orbits correspond to monic degree n polynomials with vanishing coefficient of x^{n-1}. When the characteristic p is a very good prime (i.e., p does not divide n), the chance that such a polynomial factors into a_i irreducibles of degree i is equal to the chance that a random monic degree n polynomial has a_i irreducible factors of degree i.

A long term goal is to refine this map Φ so that it associates to each semisimple orbit an *element* of W. Furthermore, at least when Problem 1 has an affirmative answer, choosing an orbit at random and applying the refined map should give the measures $H_{W,q}$. In Section 4 of this paper we indicate how to do this unnaturally for types A and B. A refinement of Φ which is both natural and general remains elusive, but as explained in the second paragraph of Sect. 4, could have important applications in algebraic number theory. It would also be interesting to relate these results to Kirillov's method of coadjoint orbits.

To close the introduction, we mention two follow-up papers. The paper [14] considers analogous issues for semisimple conjugacy classes of the finite groups of Lie type. The combinatorics there is significantly more intricate, involving the affine Weyl group and leading to new shuffles which we call affine shuffles. These seem quite interesting; for instance, the formula for type A affine shuffles involves Ramanujan sums and depends on a permutation through both its number of cyclic descents and major index. Remarkably, the results of [14] analogous to those here seem to need no restriction on the characteristic, and the conjectured refinement of the map analogous to Φ uses the affine Weyl group and is much more natural than the refinement considered here. Connections with dynamical systems are also given. The follow-up paper [10] relates affine shuffles to shuffles followed by a uniform cut. It also proves the surprising fact (of interest in casinos) that the use of cuts does not speed the convergence rate of riffle shuffles to randomness.

2. DEFINITION AND PROPERTIES OF $H_{W,x}$

To begin we review work of Bidigare, Hanlon, and Rockmore [5]. Let $\mathcal{A} = \{H_i : i \in I\}$ be a central hyperplane arrangement (i.e., $\bigcap_{i \in I} H_i = 0$) for a real vector space V. Let γ be a vector in the complement of $\mathcal{A}$. Every H_i partitions V into three pieces: $H_i^0 = H_i$, the open half-space H_i^+ of V containing γ, and the open half-space H_i^- of V not containing γ. The faces of $\mathcal{A}$ are defined as the non-empty intersections of the form

$$\bigcap_{i \in I} H_i^{\epsilon_i},$$

where $\epsilon_i \in \{0, -, +\}$. Equivalently, $\mathcal{A}$ cuts V into regions called chambers and the faces are the faces of these chambers viewed as polyhedra.

A random process (henceforth called the BHR walk) on chambers is then defined as follows. Assign weights $v(F)$ to the faces of $\mathcal{A}$ in such a way that $v_F \geq 0$ for all F and $\sum_F v(F) = 1$. Pick a starting chamber C_0. At step i, pick a face F_i with chance of face F equal to $v(F)$ and define C_i to be the chamber adjacent to F_i which is closest to C_{i-1} (separated from C_{i-1} by the fewest number of hyperplanes.) Such a chamber always exists.

To give our definition of $H_{W,x}$, some additional notation is needed. Let L be the set of intersections of the hyperplanes in $\mathcal{A}$, taking $V \in L$. Partially order L by reverse inclusion. (This lattice is not the same as the face lattice.) Recall that the Moebius function μ is defined by $\mu(X, X) = 1$ and $\sum_{X \leq Z \leq Y} \mu(Z, Y) = 0$ if $X < Y$ and $\mu(X, Y) = 0$ otherwise. The characteristic polynomial of L is defined as

$$\chi(L, x) = \sum_{X \in L} \mu(V, X) x^{\dim(X)}.$$

Let Π be a base of the positive roots of W. For $J \subseteq \Pi$, let $\mathrm{Fix}(W_J)$ denote the fixed space of the parabolic subgroup W_J in its action on V. Let $L^{\mathrm{Fix}(W_J)}$ denote the restricted poset $\{Y \in L(\mathscr{A}) \mid Y \geq \mathrm{Fix}(W_J)\}$. Define $\mathrm{Des}(w)$ to be the simple positive roots which w maps to negative roots (also known as the descent set of w) and let $d(w) = |\mathrm{Des}(w)|$. Let $N_W(W_K)$ be the normalizer of W_K in W and let $\lambda(K)$ be the subsets of Π equivalent to K under the action of W.

Definition. For W a finite Coxeter group and $x \neq 0$, define $H_{W,x}(w)$ to be

$$\sum_{K \subseteq \Pi - \mathrm{Des}(w)} \frac{|W_K| \chi(L^{\mathrm{Fix}(W_K)}, x)}{x^n |N_W(W_K)| |\lambda(K)|}.$$

To give a feeling for these measures and for later use, we recall formulas for types A and B (obtained using descent algebras and also arising from the above definition).

- ([1], [5])

$$H_{S_n, x}(w) = \frac{\binom{x + n - 1 - d(w)}{n}}{x^n}.$$

Physically, the inverse of this measure is obtained by cutting at card k with probability $\binom{n}{k}/2^n$, then doing a uniformly chosen random interleaving of the piles. The papers [9] and [11] investigate the cycle structure and inversion structure of a random permutation chosen from $H_{S_n, x}$.

- ([2], [12])

$$H_{B_n, x}(w) = \frac{(x + 2n - 1 - 2d(w))(x + 2n - 3 - 2d(w)) \cdots (x + 1 - 2d(w))}{x^n n!}.$$

The inverse of this measure also has a physical description if x is odd, verified for $x = 3$ in [2]. One cuts multinomially into an odd number of piles, flips over the even numbered piles, and then does a random interleaving. This is different from the type B notion in [1], which cuts into two piles. However, these two types of shuffles can be placed in a unified setting, using the affine Weyl group [14]. In future work we hope to study physical models of the shuffles $H_{W,x}$ for other finite Coxeter groups, viewed as permutation groups.

Next we comment on some properties of the measures $H_{W,x}$, and give a computationally useful expression for them.

- ([12]) For types A, B, C, H_3 and rank-2 groups (but not for all types as is explained below), the measures $H_{W,x}$ convolve in the sense that

$$\left(\sum_{w\in W} H_{W,x}(w)w\right)\left(\sum_{w\in W} H_{W,y}(w)w\right) = \sum_{w\in W} H_{W,xy}(w)w.$$

Thus n x-shuffles is the same as an x^n shuffle. Observe also that in the $x \to \infty$ limit the measures $H_{W,x}$ become the uniform distribution. The eigenvalues of an x-shuffle viewed as a Markov chain are $1/x^i$, $i = 0, \ldots, r$ with multiplicities, the number of w with an r-i dimensional fixed space in its geometric representation.

- The Coxeter complex of W has as faces the left cosets wW_K and as chambers the elements of W. Consider the BHR walks on the chambers of the Coxeter complex with face wieghts

$$v(wW_K) = \frac{|W_K|\chi(L^{\mathrm{Fix}(W_K)}, x)}{x^n|N_W(W_K)||\lambda(K)|}.$$

When these weights are non-negative, $H_{W,x}(w)$ can be interpreted as the probability of moving from the identity chamber to w. Equations from p. 282 of [20] imply that $v(wW_K)$ can be rewritten as

$$(-1)^{n-|K|}\frac{\chi(L^{\mathrm{Fix}(W_K)}, x)}{x^n\chi(L^{\mathrm{Fix}(W_K)}, -1)}.$$

As observed in [12], this leads to a notion of card shuffling for any real hyperplane arrangement or oriented matroid. The Coxeter case gives rise to the factorization

$$\chi(L^{\mathrm{Fix}(W_K)}, x) = \prod_{i=1}^{\dim(\mathrm{Fix}(W_K))} (x - b_i^K)$$

from [20] where the b_i^K are integers called coexponents. From the results and tables in [20], all b_i^K are less than or equal to the maximum exponent of W. From the table of bad primes for crystallographic types on p. 28 of [7], the bad primes are precisely the primes less than the maximum exponent of W which are not equal to exponents of W. (Equivalently, a prime is good if it divides no coefficient of any root expressed as a linear combination of simple roots.) Thus $H_{W,q}(w) \geq 0$ if W is crystallographic and q is a good prime, because then every face weight is non-negative. This may be regarded as evidence in favor of the philosophy underlying the statement in Problem 1 in Section 3.

- Orlik and Solomon [20] have calculated and tabulated $\chi(L^{\mathrm{Fix}(W_K)}, x)$ for all types. By the previous remark, this gives a simple and unified method for computing the measure $H_{W,x}$. Applied to W of type H_3, one concludes that

$$H_{H_3,x}(w) = \begin{cases} \dfrac{(x+9)(x+5)(x+1)}{120x^3} & \text{if } d(w) = 0 \\ \dfrac{(x+5)(x+1)(x-1)}{120x^3} & \text{if } d(w) = 1 \\ \dfrac{(x+1)(x-1)(x-5)}{120x^3} & \text{if } d(w) = 2 \\ \dfrac{(x-1)(x-5)(x-9)}{120x^3} & \text{if } d(w) = 3. \end{cases}$$

This formula, together with the formulas for $H_{W,x}$ for W of types A, B which appeared earlier in this paper, suggest that $H_{W,x}$ satisfies the following factorization and reciprocity properties:

(1) $H_{W,x}(w)$ splits into linear factors as a function of x.

(2) $H_{W,x}(w) = H_{W,-x}(ww_0)$ where w_0 is the longest element of W.

In fact neither of these properties holds. This is evident from the following formula for $H_{H_4,x}$ which is obtained by using tables of Orlik and Solomon as just described:

$$H_{H_4,x}(w) = \begin{cases} \dfrac{(x+29)(x+19)(x+11)(x+1)}{14400x^4} & \text{if } d(w) = 0 \\ \dfrac{(x+1)(x-1)(x^2+30x+149)}{14400x^4} & \text{if } \mathrm{Des}(w) = \{\alpha_1\} \text{ or } \\ & \quad \mathrm{Des}(w) = \{\alpha_2\} \\ \dfrac{(x+1)(x-1)(x^2+30x+269)}{14400x^4} & \text{if } \mathrm{Des}(w) = \{\alpha_3\} \text{ or } \\ & \quad \mathrm{Des}(w) = \{\alpha_4\} \\ \dfrac{(x+11)(x+1)(x-1)(x-11)}{14400x^4} & \text{if } d(w) = 2 \text{ and } \\ & \quad \mathrm{Des}(w) \neq \{\alpha_3, \alpha_4\} \\ \dfrac{(x+1)^2(x-1)^2}{14400x^4} & \text{if } \mathrm{Des}(w) = \{\alpha_3, \alpha_4\} \\ \dfrac{(x+1)(x-1)(x-11)(x-19)}{14400x^4} & \text{if } d(w) = 3 \\ \dfrac{(x-1)(x-11)(x-19)(x-29)}{14400x^4} & \text{if } d(w) = 4. \end{cases}$$

Incidentally this remark shows that $H_{H_4,x}$ does not convolve, because $H_{W,-1}$ places all mass on the longest element w_0. The convolution property would imply that $H_x(w) = H_x(w)H_{-1}(w_0) = H_{-x}(ww_0)$. Since w and ww_0 have complementary descent sets, this equality does not hold for w with $\mathrm{Des}(w) = \{\alpha_3, \alpha_4\}$. The same argument disproves the convolution property in many cases.

Let id be the identity element of W and w_0 the longest element of W. Theorem 1 calculates the values of the measure $H_{W,x}$ on these elements.

THEOREM 1. *Let $m_1, \ldots, m_r$ be the exponents of W. Then*

$$H_{W,x}(w_0) = \frac{\prod_{i=1}^r (x - m_i)}{x^r|W|},$$

$$H_{W,x}(\mathrm{id}) = \frac{\prod_{i=1}^r (x + m_i)}{x^r|W|}.$$

Proof. The first assertion is easier. In fact,

$$H_{W,x}(w_0) = \frac{\chi(L,x)}{x^r|W|} = \frac{\prod_{i=1}^r (x - m_i)}{x^r|W|}.$$

The first equality is from the definition of $H_{W,x}$ and the second equality is a well-known factorization of the characteristic polynomial of L (e.g., [20]).

For the second assertion, additional concepts are needed. Let L be the lattice in V generated by $\check{\Phi}$ and let

$$\hat{L} = \big\{ v \in V \mid \langle v, \alpha \rangle \in Z \text{ for all } \alpha \in \Phi \big\}.$$

Let $f = [\hat{L} : L]$ be the index L in $\hat{L}$. Let $\Pi = \{\alpha_i\} \subset \Phi^+$ be a set of simple roots contained in a set of positive roots and let θ be the highest root in Φ^+. For convenience set $\alpha_0 = -\theta$. Let $\tilde{\Pi} = \Pi \cup \{\alpha_0\}$. Define coefficients c_α of θ with respect to $\tilde{\Pi}$ by the equations $\sum_{\alpha \in \tilde{\Pi}} c_\alpha \alpha = 0$ and $c_{\alpha_0} = 1$. For $S \neq \tilde{\Pi}$ a proper subset of $\tilde{\Pi}$, define as in [23] $p(S,x)$ to be the number of solutions $\mathbf{y}$ in strictly positive integers to the equation

$$\sum_{\alpha \in \tilde{\Pi} - S} c_\alpha y_\alpha = x.$$

In the equations which follow $W_{K_1}, \ldots, W_{K_l}$ with $K_1, \ldots, K_l \subseteq \Pi$ are representatives for the parabolic subgroups of W under conjugation. In [20] it is proved that $|\lambda(K)|$ is the number of $J \subseteq \Pi$ such that W_J is conjugate to W_K. We also make use of the fact [24] that if x is relatively prime to all c_α, then for any $S \subset \tilde{\Pi}$, $S \neq \tilde{\Pi}$, if $p(S,x)$ is non-zero then W_S is conjugate to one of $W_{K_1}, \ldots, W_{K_l}$. We denote conjugacy of parabolic subgroups by the symbol $\sim$. One concludes that for infinitely many (and hence all) nonzero x,

$$\begin{aligned}
H_{W,x}(\mathrm{id}) &= \sum_{K\subseteq\Pi} \frac{|W_K|\chi(L^{\mathrm{Fix}(W_K)},x)}{x^r|N_W(W_K)||\lambda(K)|}\\
&= \sum_{i=1}^{l} \frac{|W_{K_i}|\chi(L^{\mathrm{Fix}(W_{K_i})},x)}{x^r|N_W(W_{K_i})|}\\
&= \frac{1}{x^r f}\sum_{i=1}^{l} \frac{f|W_{K_i}|\chi(L^{\mathrm{Fix}(W_{K_i})},x)}{|N_W(W_{K_i})|}\\
&= \frac{1}{x^r f}\sum_{i=1}^{l} \sum_{\substack{S\subseteq\tilde{\Pi},S\neq\tilde{\Pi}\\ W_S\sim W_{K_i}}} p(S,x)\\
&= \frac{1}{x^r f}\sum_{\substack{S\subset\tilde{\Pi}\\ S\neq\tilde{\Pi}}} p(S,x)\\
&= \frac{1}{x^r|W|}\prod_{i=1}^{r}(x+m_i).
\end{aligned}$$

The fourth and sixth equalities are results of [23]. ▮

3. SEMISIMPLE ORBITS OF LIE ALGEBRAS

This section connects (in some cases) the signed measures $H_{W,x}$ with semisimple orbits of the adjoint action of finite groups of Lie type on their Lie algebras.

Let G be a connected semisimple group defined over a finite field of q elements. Suppose also that G is simply connected. Let $\mathcal{G}$ be the Lie algebra of G. Let F denote both a Frobenius automorphism of G and the corresponding Frobenius automorphism of $\mathcal{G}$. Suppose that G is F-split (analogous results for the non-split case should be sought). Since the derived group of G is simply connected (the derived group of a simply connected group is itself), a theorem of Springer and Steinberg [25] implies that the centralizers of semisimple elements of $\mathcal{G}$ are connected. Let r be the rank of G.

Now we define a map Φ (studied in [19] in somewhat greater generality) from the F-rational semisimple orbits c of $\mathcal{G}$ to W, the Weyl group of G. Pick $x \in \mathcal{G}^F \cap c$. Since the centralizers of semisimple elements of $\mathcal{G}$ are connected, x is determined up to conjugacy in G^F and $C_G(x)$, the centralizer in G of x, is determined up to G^F conjugacy. Let T be a maximally split maximal torus in $C_G(x)$. Then T is an F-stable maximal torus of G, determined up to G^F conjugacy. By Proposition 3.3.3 of [7], 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.

For example, in type A_{n-1} the semisimple orbits c of $sl(n, q)$ correspond to monic degree n polynomials $f(c)$ whose coefficient of x^{n-1} vanishes. Such a polynomial factors as $\prod_i f_i^{a_i}$ where the f_i are irreducible over F_q. Letting d_i be the degree of f_i, $\Phi(c)$ is the conjugacy class of S_n corresponding to the partition $(d_i^{a_i})$. This follows from Sect. 3 of [8].

As is standard in Lie theory, call a prime p very good if it divides no coefficient of any root expressed as a linear combination of simple roots and is relatively prime to the index of connection (the index of the coroot lattice in the weight lattice). For example, in type A the very good primes are those not dividing n. A result of Fleischmann shows that very good primes are regular in the sense of [19].

Problem 1. When is the following statement true? "Let G be as above, and suppose that the characteristic is a prime which is very good for G. Choose c among the q^r F-rational semisimple orbits of $\mathcal{G}$ uniformly at random. Then for all conjugacy classes C of W,

$$\text{Probability } (\Phi(c) = C) = \sum_{w \in C} H_{W,q}(w)."$$

Recall from the end of Sect. 2 that under the conditions of Problem 1, $H_{W,q}(w) \geq 0$ for all $w \in W$. This may be taken as evidence that the statement in Problem 1 is correct. Theorems 2, 3, and 4 provide further evidence. In cases where the convolution property of W does not hold, we have doubts as to whether the statement in Problem 1 is always true. Nevertheless, at present we have no examples to the contrary (type D_4 would be a natural first place to look). It would be interesting to classify conjugacy classes for which the equality holds.

THEOREM 2. *The statement in Problem* 1 *holds for G of all types* (*i.e.*, *A–D, $E_{6\text{–}8}$, F_4, G_2*) *when C is the identity conjugacy class of W.*

Proof. Proposition 5.9 of [19]) implies that for q very good, the number of F-rational semisimple orbits c of $\mathcal{G}$ which satisfy $\Phi(c) = \text{id}$ is equal to

$$\prod_{i=1}^{r} \frac{q+m_i}{1+m_i},$$

where r is the rank of G and m_i are the exponents of W. Since there are a total of q^r F-rational semisimple orbits of $\mathcal{G}$, and because $|W| = \prod_{i=1}^{r}(1+m_i)$,

$$\text{Probability } (\Phi(c) = \text{id}) = \frac{\prod_{i=1}^{r}(q+m_i)}{q^r|W|}.$$

The proposition now follows from Theorem 1. ∎

We remark that the analog of Theorem 2 for affine shuffles [14] leads to number theoretic reciprocity laws. Namely for any positive x, y the number of ways (disregarding order and allowing repetition) of writing m (mod y) as the sum of x integers of the set $0, 1, \ldots, y-1$ is equal to the number of ways of writing m (mod x) as the sum of y integers of the set $0, 1, \ldots, x-1$.

THEOREM 3. *The statement of Problem* 1 *holds for G of type A, for all conjugacy classes C of the symmetric group S_n.*

Proof. Note that a monic, degree n polynomial f with coefficients in F_q defines a partition of n, and hence a conjugacy class of S_n, by its factorization into irreducibles. To be precise, if f factors as $\prod_i f_i^{a_i}$ where the f_i are irreducible of degree d_i, then $(d_i^{a_i})$ is a partition of n. If the coefficient of x^{n-1} in f vanishes, then f represents an F-rational semisimple orbit c of $sl(n, q)$, and the conjugacy class of S_n corresponding to the partition $(d_i^{a_i})$ is equal to $\Phi(c)$.

In [9] it is shown that if f is uniformly chosen among all monic, degree n polynomials with coefficients in F_q, then the measure on the conjugacy classes of S_n induced by the factorization of f is equal to the measure induced by $H_{S_n, q}$. Thus, to prove the theorem, it suffices to show that the random partition associated to a uniformly chosen monic, degree n polynomial over F_q has the same distribution as the random partition associated to a uniformly chosen monic, degree n polynomial over F_q with vanishing coefficient of x^{n-1}. Since the characteristic p is assumed to be very good, p does not divide n. Thus for a suitable choice of k, the change of variables $x \to x + k$ gives rise to a bijection between monic, degree n polynomials with coefficient of x^{n-1} equal to b_1 and monic, degree n polynomials with coefficient of x^{n-1} equal to b_2, for any b_1 and b_2. Since this bijection preserves the partition associated to a polynomial, the theorem is proved. ∎

Theorem 4 will confirm the statement of Problem 1 for all G of type B. The proof will use the following combinatorial objects introduced in [21]. As Lemma 1 will show, these objects have interpretations in terms of polynomials. Let a **Z**-word of length m be a vector $(a_1, \ldots, a_m) \in \mathbf{Z}^m$. For such a word define $\max(a) = \max(|a_i|)_{i=1}^m$. The cyclic group C_{2m} acts on **Z**-words of length m by having a generator g act as $g(a_1, \ldots, a_m) = (a_2, \ldots, a_m, -a_1)$. Call a fixed-point free orbit P of this action a primitive twisted necklace of size m. The group $Z_2 \times C_m$ acts on **Z**-words of length m by having the generator r of C_m act as a cyclic shift $r(a_1, \ldots, a_m) = (a_2, \ldots, a_m, a_1)$ and having the generator v of Z_2 act by $v(a_1, \ldots, a_m) = (-a_1, \ldots, -a_m)$. Call an orbit D of this action a primitive blinking necklace of size m if its C_m action is free (though its $Z_2 \times C_m$ action need not be). Let a signed ornament o be a set of primitive twisted necklaces and a multiset of primitive blinking necklaces. Say that o has type $(\vec{\lambda}, \vec{\mu}) = ((\lambda_1, \lambda_2, \ldots), (\mu_1, \mu_2, \ldots))$ if it consists of λ_m primitive blinking necklaces of size m and μ_m primitive twisted necklaces of size m. Also define the size of o to be the sum of the sizes of the primitive twisted and blinking necklaces which make up o, and define $\max(o)$ to be the maximum of $\max(D)$ and $\max(P)$ for the primitive twisted and blinking necklaces which make up o.

LEMMA 1. *Primitive twisted necklaces P of size m and with* $\max(P) \leq \frac{q-1}{2}$ *correspond to irreducible polynomials $f(z)$ over F_q of degree $2m$ satisfying $f(z) = f(-z)$. Primitive blinking necklaces D of size m and with* $\max(D) \leq \frac{q-1}{2}$ *correspond to products $f(z)f(-z)$ with $f(z), f(-z)$ a pair of irreducible polynomial of degree m over F_q. Signed ornaments given as sets of such P's and multisets of such D's correspond to polynomials of degree $2m$ over F_q satisfying $f(z) = f(-z)$.*

Proof. For the first assertion, let $F_{q^{2m}}$ be the degree $2m$ extension of F_q. Choose α in $F_{q^{2m}}$ such that $\{\alpha^{q^i} : 1 \leq i \leq 2m\}$ is a basis over F_q. (Such a basis is called a normal basis and is known to exist.) Let $f(z)$ be an irreducible polynomial of degree $2m$ satisfying $f(z) = f(-z)$. Let β be one of its roots in $F_{q^{2m}}$. Writing $\beta = \sum_{i=1}^{2m} c_i \alpha^{q^i}$, define a vector $(c_1, \ldots, c_m)$ associated to β. Since the automorphism of $F_{q^{2m}}$ defined by $\alpha \to \alpha^{q^m}$ is its unique automorphism of order two, it follows that β^q is assigned the vector $(c_2, \ldots, c_m, -c_1)$. Thus the action of the Frobenius map $x \to x^q$ corresponds to the action of $Z_2 \times C_m$ on the vector $(c_1, \ldots, c_m)$, and irreducible polynomials correspond to primitive orbits.

For the second assertion, choose α in F_{q^m} such that $\{\alpha^{q^i} : 1 \leq i \leq m\}$ is a basis over F_q. Let $f(z)$ be an irreducible polynomial of degree m. Let β be one of its roots in F_{q^m}. Writing $\beta = \sum_{i=1}^{m} c_i \alpha^{q^i}$, define a vector $(c_1, \ldots, c_m)$ associated to β. The C_m action on this vector is free because $f(z)$ is irreducible. The Z_2 action sends $f(z)$ to $f(-z)$.

For the final assertion, note that a polynomial $f(z)$ satisfying $f(z) = f(-z)$ can be factored uniquely as a product

$$\prod_{\{\phi_j(z), \phi_j(-z)\}} [\phi_j(z)\phi_j(-z)]^{r_{\phi_j}} \prod_{\phi_j : \phi_j(z) = \phi_j(-z)} \phi_j(z)^{s_{\phi_j}},$$

where the ϕ_j are monic irreducible polynomials and $s_{\phi_j} \in \{0, 1\}$. ∎

Theorem 4 proves the statement of Problem 1 for type B.

THEOREM 4. *The statement of Problem* 1 *holds for G of type B, for all conjugacy classes C of the hyperoctahedral group B_n.*

Proof. Note that because 2 is a bad prime for type B, it can be assumed that the characteristic is odd. Recall that the type of a signed ornament is parametrized by pairs of vectors $(\vec{\lambda}, \vec{\mu})$, where λ_i is the number of primitive blinking necklaces of size i and μ_i is the number of primitive twisted necklaces of size i. From the theory of wreath products, the conjugacy classes of the hyperoctahedral group B_n are also parametrized by pairs of vectors $(\vec{\lambda}, \vec{\mu})$, where $\lambda_i(w)$ and $\mu_i(w)$ are the number of positive and negative cycles of $w \in B_n$, respectively.

The first step of the proof will be to show that the measure induced on pairs $(\vec{\lambda}, \vec{\mu})$ by choosing a random signed ornament o of size n satisfying $\max(o) \leq \frac{q-1}{2}$ is equal to the measure induced on pairs $(\vec{\lambda}, \vec{\mu})$ by choosing $w \in B_n$ according to the measure $H_{B_n,q}$ and then looking at its conjugacy class. From the definition of descents given in Sect. 2, it is easy to see that if one introduces the linear order Λ on the set of non-zero integers

$$+1 <_\Lambda +2 <_\Lambda \cdots + n <_\Lambda \cdots <_\Lambda -n <_\Lambda \cdots <_\Lambda -2 <_\Lambda -1$$

then $d(w)$, the number of descents of $w \in B_n$, can be defined as $|\{i : 1 \leq i \leq n : w(i) >_\Lambda w(i+1)\}|$. Here $w(n+1) = n+1$ by convention.

It is proved in [21] that there is a bijection between signed ornaments o of size n satisfying $\max(o) \leq \frac{q-1}{2}$ and pairs $(w, \vec{s})$ where $w \in B_n$ and $\vec{s} = (s_1, \ldots, s_n) \in \mathbf{N}^n$ satisifies $\frac{q-1}{2} \geq s_1 \geq \cdots \geq s_n \geq 0$ and $s_i > s_{i+1}$ when $w(i) >_\Lambda w(i+1)$ (i.e., when w has a descent at position i). Further, Reiner shows that the type of o is equal to the conjugacy class vector of w. It is easy to see that if w has $d(w)$ descents, then the number of $\vec{s}$ such that $\frac{q-1}{2} \geq s_1 \geq \cdots \geq s_n \geq 0$ and $s_i > s_{i+1}$ when $w(i) <_\Lambda w(i+1)$ is equal to

$$\binom{\frac{q-1}{2} + n - d(w)}{n} = \frac{(q+1-2d(w)) \cdots (q+2n-1-2d(w))}{2^n n!}.$$

Lemma 1 implies that there are q^n signed ornaments f of size n satisfying $\max(f) \leq \frac{q-1}{2}$. Thus choosing a random signed ornament induces a measure on $w \in B_n$ with mass on w equal to

$$\frac{(q+1-2d(w)) \cdots (q+2n-1-2d(w))}{q^n |B_n|}.$$

By the remarks in Sect. 2, this is exactly the mass on w under the measure $H_{B_n,q}$. Since in Reiner's bijection the type of o is equal to the conjugacy class vector of w, we have proved that the measure on conjugacy classes $(\vec{\lambda}, \vec{\mu})$ of B_n induced by choosing w according to $H_{B_n,q}$ is equal to the measure on conjugacy classes $(\vec{\lambda}, \vec{\mu})$ of B_n induced by choosing a signed ornament uniformly at random and taking its type.

The second step in the proof is to show that if f is chosen uniformly among the q^n semisimple orbits of $\mathrm{Spin}(2n+1, q)$ on its Lie algebra, then the chance that $\Phi(f)$ is the conjugacy class $(\vec{\lambda}, \vec{\mu})$ of B_n is equal to the chance that a signed ornament chosen randomly among the q^n signed ornaments o of size n satisfying $\max(o) \leq \frac{q-1}{2}$ has type $(\vec{\lambda}, \vec{\mu})$. It is known that the semisimple orbits of $\mathrm{Spin}(2n+1, q)$ on its Lie algebra correspond to monic, degree $2n$ polynomials f satisfying $f(z) = f(-z)$. From Sect. 3 of [8], one sees that $\Phi(f)$ can be described as follows. Factor f uniquely into irreducibles as

$$\prod_{\{\phi_j(z),\, \phi_j(-z)\}} [\phi_j(z)\phi_j(-z)]^{r_{\phi_j}} \prod_{\phi_j : \phi_j(z)=\phi_j(-z)} \phi_j(z)^{s_{\phi_j}},$$

where the ϕ_j are monic irreducible polynomials and $s_{\phi_j} \in \{0, 1\}$. Then let $\lambda_i(f) = \sum_{\phi : \deg(\phi)=i} r_\phi$ and $\mu_i(f) = \sum_{\phi : \deg(\phi)=2i} s_\phi$. The result now follows from Lemma 1. ∎

4. REFINING THE MAP Φ TO THE WEYL GROUP

As noted in the introduction, one long-term goal is to find a canonical way to associate to an F-rational semisimple orbit c of $\mathcal{G}$ an *element* w of W. The conjugacy class of w should equal $\Phi(c)$ and choosing c uniformly at random should induce the measure $H_{W,q}$ on W.

To see why such a result may be interesting, at least in type A, consider a simple algebraic extension of Q with minimal polynomial $f(x)$. At unramified primes the Frobenius automorphism is defined up to conjugacy in the Galois group. Viewed as a permutation of the roots of $f(x)$, the cycle structure of the Frobenius automorphism is given by the degrees of the irreducible factors of the modulo p reduction of $f(x)$. This is simply the map Φ in type A. Some important constructions in algebraic number theory (see [15] for a survey) create generating functions combining this data over all primes. It is not impossible that a natural refinement of the Frobenius data will yield new number theoretic constructions.

Next we indicate a somewhat unnatural way to refine the map Φ in types A and B. For type A, the refinement proceeds in two steps. Define a necklace on an alphabet to be a sequence of cyclically arranged letters of the alphabet. A necklace is said to be primitive if it is not equal to any of its non-trivial cyclic shifts. For example, the necklace $(a\ a\ b\ b)$ is primitive, but the necklace $(a\ b\ a\ b)$ is not.

The first step is to associate to a monic degree n polynomial over F_q a multiset of primitive necklaces on a lexicographically ordered alphabet of $q-1$ symbols. One way to do this is using the concept of a normal basis, that is to choose for each n an element α_n such that its conjugates $\alpha_n^{p^j}$ for $j = 0, \ldots, n-1$ are a basis of F_{p^n} over F_p. Then a monic irreducible degree i polynomial gives a primitive necklace of size i formed by the coefficients c_j of any one of its roots written as $\sum c_j \alpha_i^{p^j}$. (It is natural to require that for $i|n$, the norm of α_n is α_i.) This is the preferred method in the case of semisimple adjoint orbits, because the involution sending $f(x)$ to $f(-x)$ takes negatives of the necklace entries.

A second way to carry out this first step was noticed by Golomb [17]. For each n, pick an element β_n generating the multiplicative group of the field extension F_{q^n} of F_q. A root of an irreducible polynomial ϕ of degree i can be written β_i^x. Considering the mod q expansion of x gives a primitive necklace of size i on the symbols $\{0, 1, \ldots, q-1\}$. This is the preferred construction in the case of semisimple conjugacy classes, because the involution $f(x) \mapsto t^{\deg(f)} f(\frac{1}{t})/f(0)$ on polynomials with non-zero constant term takes negatives of the necklace entries.

The next step in the construction is to associate to a multiset of primitive necklaces on $\{0, \ldots, q-1\}$ a permutation with cycle structure equal to that of the necklace. A way to do this was found by Gessel and Reutenauer [16]. To each entry of a necklace, first associate the infinite word obtained by reading the necklace in the clockwise direction. Using the example from [16], consider the multiset of necklaces

$$(1\ 2)(1\ 2)(2)(2\ 3)(2\ 3\ 2\ 3\ 3).$$

Then the entry 2 on the necklace (2 3) would give the word $23232323\cdots$. One then orders lexicographically the words obtained (after imposing an arbitrary order on equal necklaces), and replaces each necklace entry by the lexicographic order of its associated word. The example would thus yield the permutation

$$(1\ 3)(2\ 4)(5)(6\ 9)(7\ 11\ 8\ 12\ 10).$$

Arguing as in [9] (which does not mention correspondences between polynomials and necklaces) shows that choosing a multiset of primitive necklaces on the symbols $\{0, \ldots, q-1\}$ of total size n and applying the Gessel–Reutenauer map gives a permutation distributed according to $H_{S_n, q}$.

For a B_n analog, the bijection of Gessel should be replaced by the bijection of Reiner [21] used in the proof of Theorem 4. The correspondence between signed ornaments and degree $2n$ monic polynomials satisfying $f(z) = f(-z)$ is given in the proof of Lemma 1.

ACKNOWLEDGMENTS

The author thanks Persi Diaconis, Dick Gross, and Vic Reiner for helpful discussions, and Eric Sommers and a referee for corrections. Part of this work was supported by an NSF Postdoctoral Fellowship.

REFERENCES

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

2. F. Bergeron and N. Bergeron, Orthogonal idempotents in the descent algebra of B_n and applications, *J. Pure Appl. Algebra* **79** (1992), 109–129.
3. F. Bergeron, N. Bergeron, R. B. Howlett, and D. E. Taylor, A decomposition of the descent algebra of a finite Coxeter group, *J. Alg. Combinatorics* **1** (1992), 23–44.
4. N. Bergeron and L. Wolfgang, The decomposition of Hochschild cohomology and the Gerstenhaber operations, *J. Pure Appl. Algebra* **104** (1995), 243–265.
5. 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.
6. K. Brown and P. Diaconis, Hyperplane arrangements and random walk, *Ann. Probab.* **26** (1998), 1813–1854.
7. R. Carter, "Finite Groups of Lie Type," Wiley, New York, 1985.
8. R. Carter, Centralizers of semisimple elements in the finite classical groups, *Proc. London Math Soc. (3)* **42** (1981), 1–41.
9. P. Diaconis, M. McGrath, and J. Pitman, Riffle shuffles, cycles, and descents, *Combinatorica* **15** (1995), 11–20.
10. J. Fulman, Affine shuffles, shuffles with cuts, and patience sorting, available at http://xxx.lanl.gov/abs/math.CO/9910087.
11. J. Fulman, The combinatorics of biased riffle shuffles, *Combinatorica* **18** (1998), 173–184.
12. J. Fulman, Descent algebras, hyperplane arrangements, and shuffling cards, *Proc. Amer. Math Soc.*, to appear.
13. J. Fulman, Counting semisimple orbits of finite Lie algebras by genus, *J. Algebra* **217** (1999), 170–179.
14. J. Fulman, Cellini's descent algebra and semisimple conjugacy classes of finite groups of Lie type, available at http://xxx.lanl.gov/abs/math.NT/9909121.
15. S. Gelbart, An elementary introduction to the Langlands program, *Bull. Amer. Math. Soc.* **10** (1984), 177–219.
16. I. Gessel and C. Reutenauer, Counting permutations with given cycle structure and descent set, *J. Combin. Theory Soc. A* **64** (1993), 189–215.
17. 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, North Carolina, 1969.
18. P. Hanlon, The action of S_n on the components of the Hodge decomposition of Hochschild homology, *Michigan Math. J.* **37** (1990), 105–124.
19. G. Lehrer, Rational tori, semisimple orbits and the topology of hyperplane complements, *Comment. Math. Helv.* **67** (1992), 226–251.
20. P. Orlik and L. Solomon, Coxeter arrangements, *Proc. Sympos. Pure Math.* **40** (1983), 269–291.
21. V. Reiner, Signed permutation statistics and cycle type, *European J. Combin.* **14** (1993), 569–579.
22. S. Shnider, and S. Sternberg, "Quantum Groups," Graduate Texts in Mathematical Physics, Vol. II, International Press, Cambridge, MA, 1993.
23. E. Sommers, A family of affine Weyl group representations, *Transform. Groups* **2** (1997), 375–390.
24. E. Sommers, A generalization of the Bala–Carter theorem for nilpotent orbits, *Internat. Math. Res. Notices* **11** (1998), 539–562.
25. T. A. Springer and R. Steinberg, "Conjugacy Classes," Springer Lecture Notes in Mathematics Vol. 131, 1969.
26. R. Stanley, Generalized riffle shuffles and quasi-symmetric functions, available at http://xxx.lanl.gov/abs/math.CO/9904042.