PROBABILITY
AND
MATHEMATICAL STATISTICS
Vol. 24, Fasc. 1 (2004), pp. 173–180

NOTE ON THE FACTORIZATION OF THE HAAR MEASURE ON FINITE COXETER GROUPS

BY

ROMAN URBAN* (WROCŁAW)

Abstract. In this note we show that for the finite Coxeter groups of types A_n, B_n, D_n, F_4, G_2 and $I_2(m)$ it is possible to choose an appropriate set S of generators of order not greater than 2 and a finite set of probability measures $\{\mu_1, \ldots, \mu_k\}$ with their supports in S such that $\mu_1 * \ldots * \mu_k = \lambda$, where $\lambda(g) = |G|^{-1}$ for every $g \in G$.

2000 Mathematics Subject Classification: 60B15, 43A05.

Key words and phrases: Finite Coxeter groups, factorization, Haar measure, Fourier transform.

1. INTRODUCTION

Let G be a finite group and let S be a set of generators of G. It is known that if S is not contained in a coset of a subgroup H of G, then for every probability measure μ such that $\operatorname{supp} \mu = S$ we have $\lim_{n \to \infty} \mu^{*n} = \lambda$, where λ is the uniform (the Haar) probability measure on G, i.e., $\lambda(g) = |G|^{-1}$ (cf. [5] and [2]). More generally, there are known conditions that guarantee that for a given sequence of probability measures $\mu_1, \mu_2, \ldots$ on a finite group G we have

$$\lim_{n \to \infty} \mu_1 * \mu_2 * \ldots * \mu_n = \lambda.$$

For example, from the proof of the result of Ullrich and Urbanik about compact groups (see [10]) we can immediately deduce the following

PROPOSITION 1.1. *Let G be a finite group, $S = S^{-1}$ be a (symmetric) set of generators and $\mu_1, \mu_2, \ldots$ be a sequence of symmetric (i.e., $\mu_k(g) = \mu_k(g^{-1})$) probability measures with supports in S. Let $m_n = \min_{x \in S} \mu_n(x)$. Then $\sum_{n=1}^{\infty} m_n = \infty$ implies that $\mu_1 * \ldots * \mu_n \to \lambda$.*

* The author was partly supported by contract HPRN-CT-2001-00273-HARP from RTN Harmonic Analysis and Related Problems and by KBN grant 1PO3A01826.

Proof. In the proof of the main theorem in [10] we take $\tau = |S|^{-1} 1_S$, $a_n = |S| m_n$. Then for every $x \in S$ we have $\mu_n(x) \geqslant a_n \tau(x)$. Now we conclude that in the case of finite group the above condition, satisfied only on generating elements, allows us to proceed further as in [10]. ∎

In this note we are interested in questions concerning possibilities of getting the uniform measure as a product of a finite number of probability measures with their supports contained in a fixed set S of generators. If possible we try to take $S = S^{-1}$ or, even more, we would like to take S which consists of elements of order not greater than 2.

It has been noticed (see e.g. [3] and Proposition 3.1 in this note) that in an important case of the symmetric group $\mathscr{S}_n$ and the set of generators $S = S^{-1}$ consisting of transpositions there exist n probability measures $\mu_1, \ldots, \mu_n$ supported on S such that

$$\lambda = \mu_1 * \ldots * \mu_n. \tag{1.1}$$

There are, however, groups and symmetric sets S of generators for which (1.1) does not hold for any finite set of probability measures supported on S. Some examples are given in [11].

In this note we prove the following result about the factorization (1.1) of the Haar measure λ on finite Coxeter groups. (For the definition of finite Coxeter groups see Section 2.)

THEOREM 1.2. *Let G be a finite Coxeter group of type A_n, $n \geqslant 1$, B_n, $n \geqslant 2$, D_n, $n \geqslant 4$, F_4, G_2 or $I_2(m)$, $m = 5$ or $7 \leqslant m < \infty$. Then there exists a generating set $S = S^{-1} \neq G$ consisting of elements of order not greater than 2 and a finite set of probability measures with their support in S such that the factorization* (1.1) *holds.*

Inspired by the above theorem we state the following questions:

OPEN QUESTION. Is it possible to find symmetric sets of generators consisting of elements of order not greater than 2 for all finite Coxeter groups (i.e., also for remaining groups of types E_6, E_7, E_8, H_3, and H_4)?

For these groups one can prove factorization using the so-called subgroup algorithm (see [3]), however the resulting set S of generators does not necessarily contain elements of order 2. See Remark 3.4.

Is it an important feature that we deal exactly with Coxeter groups or maybe the crucial role is that the group is generated by elements of order 2? In other words, we hope that the following conjecture holds:

CONJECTURE. *Let G be a finite group generated by a set S such that every element $s \in S$ has order 2, i.e., $s^2 = e$. Then there exist a generating set S_0 consisting of elements of order not greater than 2 and a finite number of probability measures $\mu_1, \mu_2, \ldots, \mu_n$ with $\operatorname{supp} \mu_k \subset S_0$, $k = 1, 2, \ldots, n$, such that the factorization* (1.1) *holds.*

It is clear that the above Conjecture works if G is Abelian. In fact, if G is as in the Conjecture and we assume that G is Abelian, then we see that every element $g \in G$ is of order 2. But since G is finite, we get $G = \boldsymbol{Z}_2^m$ for some positive integer m. For this group our Conjecture is true. In fact, in [11] the following proposition has been proved and will be used in this note.

PROPOSITION 1.3 (Proposition 5.3 in [11]). *Let* $G = \boldsymbol{Z}_2^m$ *and*

$$S = \{\pm e_1, \ldots, \pm e_m, \mathbf{0}\},$$

where $\mathbf{0} = (0, \ldots, 0)$, $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$. *Then* λ *has a factorization.*

In this place it should be mentioned that the problem of factorization has been studied by Diaconis in [3], however he did not make any constraints on the generating set S, in particular his measures had supports on the whole groups.

The paper is organized as follows. In Section 2 we recall some elementary facts from harmonic analysis on finite groups since we use the Fourier transform in the proof of Theorem 1.2 in the case of the dihedral group. In order to make the paper self-contained we also recall some facts about finite Coxeter groups. We use mainly the classification of finite Coxeter groups by presentations given by so-called Coxeter–Dynkin diagrams. Finally, in Section 3 we prove Theorem 1.2.

Acknowledgements. The author is grateful to Ryszard Szwarc for his helpful remarks concerning the contents of this paper. The author wishes to thank Ziemowit Rzeszotnik for long discussions in Zakopane in winter 2001 and the referee for a number of helpful suggestions.

2. PRELIMINARIES

2.1. Fourier analysis on finite groups. All facts we included here can be found in [9] or [5].

A *representation* π of G is a homomorphism of G into the group of invertible linear maps of a complex finite-dimensional vector space V. We say that the representation π is *d-dimensional* if $\dim V = d$. We may think of $\pi(x)$ as a $\dim V \times \dim V$ matrix. Without loss of generality we may assume that representations π are *unitary*, i.e., $\pi(x)$ is a unitary matrix for all $x \in G$. A representation π is *irreducible* if V admits no $\pi(G)$ invariant subspaces other than $\{0\}$ or V. Two representations $\pi_1\colon G \to GL(V_1)$ and $\pi_2\colon G \to GL(V_2)$ are *equivalent* if there is a linear isomorphism $\varrho\colon V_1 \to V_2$ such that $\varrho\pi_1(x) = \pi_2(x)\varrho$ for all $x \in G$. Let G be a product of two groups $G = G_1 \times G_2$ with multiplication defined coordinatewise. Let $\pi_1\colon G_1 \to V_1$ and $\pi_2\colon G_2 \to V_2$ be representations. Define the representation

$$\pi_1 \otimes \pi_2\colon G_1 \times G_2 \to GL(V_1 \otimes V_2)$$

by

$$\pi_1 \otimes \pi_2 (x, y) v_1 \otimes v_2 = \pi_1 (x) v_1 \otimes \pi_2 (y) v_2 .$$

Consequently, if π_1 and π_2 are irreducible, then $\pi_1 \otimes \pi_2$ is irreducible. Moreover, each irreducible representation of $G_1 \times G_2$ is equivalent to a representation $\pi_1 \otimes \pi_2$, where π_i is an irreducible representation of G_i.

If f is a function on G and π is a representation, define

$$\hat{f}(\pi) = \sum_{x \in G} f(x) \pi(x).$$

The transform $\hat{f}$ is the analog of the Fourier transform. It converts convolution into multiplication of linear transformations

$$\widehat{f * g}(\pi) = \hat{f}(\pi) \hat{g}(\pi).$$

Moreover, if $\hat{\mu} = \hat{\nu}$, then $\mu = \nu$.

Let λ denote the probability measure which is uniformly distributed on a finite group G, i.e. $\lambda(x) = |G|^{-1}$ for all $x \in G$. For λ we have

$$\hat{\lambda}(\pi) = \begin{cases} \mathrm{Id} & \text{for the trivial representation,} \\ 0 & \text{for a nontrivial irreducible representation.} \end{cases}$$

2.2. Coxeter graphs and finite Coxeter groups. All facts we cite here can be found e.g. in [8], [6] and [1].

A *Coxeter graph* is a pair (Γ, m), where $\Gamma = (\Gamma_0, \Gamma_1)$ is a finite graph (Γ_0 is a set of vertices, Γ_1 is a set of the edges) in which every two vertices are joined by at most one edge, while $m\colon \Gamma_0 \times \Gamma_0 \to \{2, 3, 4, \ldots\} \cup \{\infty\}$ is a function such that $m(i, j) = 2$ if and only if there are no edges joining i and j. Therefore $m(i, j) \geqslant 3$ if and only if there exists exactly one edge joining i with j. Such an edge will be denoted as follows:

$$\bullet \overset{m(i,j)}{\text{———}} \bullet$$

With every Coxeter graph (Γ, m) we associate an appropriate *Coxeter group* specifying its presentation:

$$W(\Gamma, m) = \langle X_i,\, i \in \Gamma_0 \mid X_i^2 = 1,\, (X_i X_j)^{m(i,j)} = 1,\, i \neq j \in \Gamma_0 \rangle,$$

i.e., $W(\Gamma, m)$ is generated by the symbols X_i, $i \in \Gamma_0$, satisfying the following relations: $X_i^2 = 1$ for every $i \in \Gamma_0$ and $(X_i X_j)^{m(i,j)} = 1$ for all pairs i, j such that $m(i, j) \geqslant 3$.

The next theorem answers the following question: When is a given Coxeter group finite?

THEOREM 2.1. *Let (Γ, m) be a connected Coxeter graph and $W(\Gamma, m)$ be the Coxeter group of the Coxeter graph (Γ, m). Then $W(\Gamma, m)$ is finite if and only if the graph (Γ, m) is one of the following Coxeter–Dynkin diagrams:*

A_n: $\bullet \overset{3}{\text{——}} \bullet \overset{3}{\text{——}} \ldots \overset{3}{\text{——}} \bullet \overset{3}{\text{——}} \bullet$ $\quad$ (n *vertices*, $n \geqslant 1$);

B_n: $\bullet \overset{4}{\text{——}} \bullet \overset{3}{\text{——}} \ldots \overset{3}{\text{——}} \bullet \overset{3}{\text{——}} \bullet$ $\quad$ (n *vertices*, $n \geqslant 2$);

D_n:
$$\begin{array}{ccccccc} & & \bullet & & & & \\ & & |3 & & & & \\ \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} \ldots \overset{3}{\text{——}} & \bullet \end{array} \quad (n \textit{ vertices}, n \geqslant 4);$$

E_6:
$$\begin{array}{ccccccccc} & & & & \bullet & & & & \\ & & & & |3 & & & & \\ \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet; \end{array}$$

E_7:
$$\begin{array}{ccccccccccc} & & & & \bullet & & & & & & \\ & & & & |3 & & & & & & \\ \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet; \end{array}$$

E_8:
$$\begin{array}{ccccccccccccc} & & & & \bullet & & & & & & & & \\ & & & & |3 & & & & & & & & \\ \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet & \overset{3}{\text{——}} & \bullet; \end{array}$$

F_4: $\bullet \overset{3}{\text{——}} \bullet \overset{4}{\text{——}} \bullet \overset{3}{\text{——}} \bullet$;

G_2: $\bullet \overset{6}{\text{——}} \bullet$;

H_3: $\bullet \overset{5}{\text{——}} \bullet \overset{3}{\text{——}} \bullet$;

H_4: $\bullet \overset{5}{\text{——}} \bullet \overset{3}{\text{——}} \bullet \overset{3}{\text{——}} \bullet$;

$I_2(m)$: $\bullet \overset{m}{\text{——}} \bullet$ $\quad$ ($m = 5$ *or* $7 \leqslant m < \infty$).

For the proof see e.g. [6] or [1]. ∎

3. PROOF OF THEOREM 1.2

We use the classification given by Theorem 2.1 in Section 2. We start with the very well-known example of symmetric group $\mathscr{S}_n$ (cf. [3]) which corresponds to the group of type A_{n-1} and which was our model situation for what we can expect:

PROPOSITION 3.1. *Let $G = \mathscr{S}_n$ be a symmetric group and let $S = S^{-1} = \{(i, j)\colon i, j \in \{1, \ldots, n\}\}$ be the set of transpositions. Then λ has a factorization* (1.1).

Proof. We define $n-1$ measures. Let μ_1 be a probability measure which is uniformly distributed on $\{(1, 1), (1, 2), \ldots, (1, n)\}$, μ_2 uniformly distributed on $\{(2, 2), (2, 3), \ldots, (2, n)\}$, and so on. It is clear that $\mu_1 * \ldots * \mu_{n-1} = \lambda$. ∎

Now let G be one of the following types: $I_2(m)$ ($m = 5$ or $m > 7$) or B_2 or G_2 (or A_2 which is a group $\mathscr{S}_3$), merely when G is a dihedral group.

In order to prove that the factorization (1.1) is possible in these cases we are going to use the following general observation (which has already been used in [11]) in order to prove our Proposition 1.3. Let G be a finite group and S (not necessarily symmetric) a set of generators. Suppose that we can show that for every nontrivial unitary representation π of G we can find $k = k(\pi)$ probability measures $\mu_{1,\pi}, \ldots, \mu_{k,\pi}$ with supports in S such that the measure $\mu_\pi := \mu_{1,\pi} * \ldots * \mu_{k,\pi}$ has the property that $\hat{\mu}_\pi(\pi) = 0$. Then the Fourier transform of the measure $*_{\pi \in \hat{G} \setminus \mathrm{Id}} \mu_\pi$ is equal to 0 on every nontrivial unitary representation π, and therefore gives the desired factorization.

PROPOSITION 3.2. *Let G be the finite Coxeter group of type $I_2(m)$ ($m = 5$ or $m > 7$) or of type G_2 or B_2 or A_2, i.e., G is generated by x and y and the following relations hold*: $x^2 = y^2 = (xy)^m = 2$ (see Theorem 2.1). *Let*

$$S = S^{-1} = \{e, x, y, xyx, x(yx)^2, \ldots, x(yx)^m\}.$$

Then λ has a factorization.

Proof. Facts about representations of the dihedral group, which are used here, can be found e.g. in [7]. If m is odd, then we have one nontrivial character ψ_1:

$$\psi_1((xy)^j) = 1 \qquad \text{for } j = 0, \ldots, m-1$$

and

$$\psi_1(x(xy)^j) = -1 \qquad \text{for } 0 = 1, \ldots, m-1.$$

If m is even, then there are three nontrivial characters: ψ_1 as above and

$$\psi_2((xy)^j) = (-1)^j, \qquad \psi_2(x(xy)^j) = (-1)^{j+1},$$
$$\psi_3((xy)^j) = (-1)^j, \qquad \psi_3(x(xy)^j) = (-1)^j,$$

where $j = 0, \ldots, m-1$. Let U_α, where α is an m-th root of unity, be the unitary representation defined as follows:

$$e \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 0 & \alpha^{m-1} \\ \alpha & 0 \end{pmatrix}.$$

If m is odd, then $U_\alpha, U_{\alpha^2}, \ldots, U_{(m-1)/2}$ are irreducible unitary and pairwise unequivalent representations, while for m even such are $U_\alpha, U_{\alpha^2}, \ldots, U_{(m-2)/2}$. Now it is clear that for every character ψ_i we can construct a measure μ_{ψ_i} with its support in S (even consisting of two points) such that $\hat{\mu}_{\psi_i}(\psi_i) = 0$. Similarly, for two-dimensional representations we take

$$\mu = \frac{1}{m} \sum_{k=1}^{m} \delta_{x(yx)^k}.$$

Then

$$\hat{\mu}(U_{\alpha^l}) = \frac{1}{m}\begin{pmatrix} 0 & \sum_{k=1}^{m} \alpha^{lk} \\ \sum_{k=1}^{m} \alpha^{l(m-1)k} & 0 \end{pmatrix}.$$

This shows that $\hat{\mu}(U_{\alpha^l}) = 0$ for every U_{α^l}. Indeed, it follows from the very elementary fact that if α is an m-th root of unity, then $\sum_{j=1}^{m} \alpha^j = 0$. ■

PROPOSITION 3.3. *Let G be the finite Coxeter group of type B_n ($n \geqslant 2$) or D_n ($n \geqslant 4$) or F_4. Then there exist symmetric sets of generators consisting of elements of order not greater than 2 such that the factorizations* (1.1) *hold for these groups.*

Proof. The case of B_n ($n \geqslant 2$). B_n is a Weyl group of some set of rotations Φ in $\boldsymbol{R}^n$ (cf. [8], p. 42). Let $V = \boldsymbol{R}^n$ ($n \geqslant 2$) with $\varepsilon_1, \ldots, \varepsilon_n$ being the standard basis of $\boldsymbol{R}^n$. Define $\Phi = \{\pm\varepsilon_i \text{ and } \varepsilon_i + \varepsilon_j,\ i < j\}$. Then the group of type B_n (the Weyl group of Φ) is the semidirect product $\mathscr{S}_n$ (which permutes the ε_i) and $\boldsymbol{Z}_2^n$ (acting by sign changes on the ε_i). Therefore, multiplication is given by

$$(x_1, \sigma_1)\cdot(x_2, \sigma_2) = (x_1 + x_2^{\sigma_1}, \sigma_1\sigma_2).$$

Now we define the following measures:

$$\delta_0 \otimes \mu_1, \ldots, \delta_0 \otimes \mu_n,$$

where $\mu_1, \ldots, \mu_n$ give factorization on $\mathscr{S}_n$ (see Proposition 3.1), and

$$\nu_1 \otimes \delta_{\mathrm{Id}}, \ldots, \nu_k \otimes \delta_{\mathrm{Id}},$$

where $\nu_1, \ldots, \nu_k$ give factorization on $\boldsymbol{Z}_2^n$. Then

$$\delta_0 \otimes \mu_1 * \ldots * \delta_0 \otimes \mu_n * \nu_1 \otimes \delta_{\mathrm{Id}} * \ldots * \nu_k \otimes \delta_{\mathrm{Id}}$$

gives us the desired factorization of λ on B_n.

The case of D_n ($n \geqslant 4$). Let $V = \boldsymbol{R}^n$ and let $\varepsilon_1, \ldots, \varepsilon_n$ be the standard basis of $\boldsymbol{R}^n$. Take $\Phi = \{\pm\varepsilon_i \pm \varepsilon_j\colon 1 \leqslant i < j \leqslant n\}$. Then the Weyl group of Φ or, in our terminology, the group D_n is a semidirect product of $\mathscr{S}_n$ (permuting the ε_i and $\boldsymbol{Z}_2^{n-1}$ acting by an even number of sign changes) (see [8]). Since we have already factorization of $\boldsymbol{Z}_2^{n-1}$ (Proposition 1.3) and $\mathscr{S}_n$ (Proposition 3.1), in the case of D_n the proof is complete (compare with the proof of the previous case).

The case of F_4. The corresponding Weyl group W is a semidirect product of W' and $\mathscr{S}_3$, where W' is of type D_4 (for which we have already the factorization). $\mathscr{S}_3$ acts on $W' \simeq D_4$ by interchanging the three outer vertices of the corresponding Coxeter–Dynkin diagram, using $\mathscr{S}_3$ (see [8]).

Therefore, the desired factorization is as follows:

$$\mu_1 \otimes \delta_{\mathrm{Id}} * \ldots * \mu_k \otimes \delta_{\mathrm{Id}} * \delta_e \otimes \nu_1 * \ldots * \delta_e \otimes \nu_3,$$

where $\mu_1 * \ldots * \mu_k$ is the Haar measure on D_4 (determined in the previous case) and $\nu_1 * \ldots * \nu_3$ gives the factorization on $\mathscr{S}_3$. ■

Remark 3.4. For the remaining groups we can prove the possibility of the factorization (1.1) using the so-called subgroup algorithm described e.g. in [3]; however, the generating sets we construct may contain elements of order different than 2. In the simplest case, the subgroup algorithm states what follows. Let H be a subgroup of G (not necessarily normal). Then if we take a convolution of a uniform measure on H with a uniform measure on the set of right representatives of the cosets of H in G, we get the Haar measure on G.

For example, the groups E_6, E_7, E_8, H_3 and H_4 have symmetric groups as their subgroups. Of course, we have factorization on symmetric groups (Proposition 3.1). Now, it is enough to find the set of representatives of the symmetric groups in our Coxeter groups (which can be constructively done by an algorithm described in [4]).

Added in proof. It turns out that the "Open question" from the Introduction has a positive answer, i.e., there are factorizations for the remaining Coxeter groups: E_6, E_7, E_8, H_3 and H_4. The proof of this fact would appear elsewhere.

REFERENCES

[1] N. Bourbaki, *Groupes et algèbres de Lie*, Ch. 5, 6, 7, Hermann, 1968.
[2] P. Diaconis, *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics Lecture Notes – Monograph Series 11, Institute of Mathematical Statistics, Hayward, CA, 1988.
[3] P. Diaconis, *Application of non-cummutative Fourier analysis to probability problems*, Lecture Notes in Math. No 1362, Springer, 1982, pp. 51–100.
[4] M. Geck and G. Pfeiffer, *Characters of Finite Coxeter Groups and Iwahori–Hecke Algebras*, London Math. Soc. Monographs, 2000.
[5] U. Grenander, *Probability on Algebraic Structures*, Wiley, New York 1963.
[6] L. C. Grove and C. T. Benson, *Finite Reflection Groups*, Graduate Texts in Math. 99, Springer, 1985.
[7] E. Hewitt and K. A. Ross, *Abstract Harmonic Analysis*, Vol. 2, Springer, Berlin 1970.
[8] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, Cambridge–New York 1990.
[9] J. P. Serre, *Linear Representation of Finite Groups*, Springer, New York 1977.
[10] M. Ullrich and K. Urbanik, *A limit theorem for random variables in compact topological groups*, Colloq. Math. 7 (1960), pp. 191–198.
[11] R. Urban, *Some remarks on the random walk on finite groups*, Colloq. Math. 74 (1997), pp. 287–298.

Institute of Mathematics
University of Wrocław
pl. Grunwaldzki 2/4
50-384 Wrocław, Poland
E-mail: urban@math.uni.wroc.pl

Received on 6.12.2003;
revised version on 22.5.2004