PROBABILITY
AND
MATHEMATICAL STATISTICS
Vol. 31, Fasc. 1 (2011), pp. 141–148

ON THE FACTORIZATION OF THE HAAR MEASURE ON FINITE COXETER GROUPS

BY

ROMAN URBAN[*] (WROCŁAW)

Abstract. Let W be a finite Coxeter group and let λ_W be the Haar measure on W, i.e., $\lambda_W(w) = |W|^{-1}$ for every $w \in W$. We prove that there exist a symmetric set $T \neq W$ of generators of W consisting of elements of order not greater than 2 and a finite set of probability measures $\{\mu_1, \ldots, \mu_k\}$ with their supports in T such that their convolution product $\mu_1 * \ldots * \mu_k = \lambda_W$.

2000 AMS Mathematics Subject Classification: Primary: 60B15; Secondary: 20F55.

Key words and phrases: Finite Coxeter groups, parabolic subgroups, convolution of probability measures, factorization of measure, uniform distribution, Haar measure, subgroup algorithm.

1. INTRODUCTION

The aim of this note is to prove in a constructive way the following factorization of the Haar measure on finite Coxeter groups (for the definition of finite Coxeter groups see Section 2).

THEOREM 1.1. *Let W be a finite Coxeter group and let $\lambda_W(w) = |W|^{-1}$ for every $w \in W$. Then there exist a symmetric set $T \neq W$ of generators of W consisting of elements of order not greater than 2 and a finite set of probability measures $\{\mu_1, \ldots, \mu_k\}$, $k \geqslant 2$, with their supports in T such that their convolution product $\mu_1 * \ldots * \mu_k$ takes the form*

$$\mu_1 * \ldots * \mu_k = \lambda_W. \tag{1.1}$$

If W is a symmetric group $\mathcal{S}_n$, then the result of Theorem 1.1 is well known and widely used both in practical and theoretical problems (see e.g. the classical book by Knuth [8] and the lectures by Diaconis [3]). In this case one can take the set of generators consisting of transpositions $T = \{(i,j) : 1 \leqslant i, j \leqslant n\}$

[*] The author was supported in part by the MNiSW research grant N N201 393937.

© for this edition by CNS

and define $n-1$ probability measures as follows. Let μ_j, $1 \leqslant j \leqslant n$, be a probability measure which is uniformly distributed on the set $\{(j,j),(j,j+1),\ldots,(j,n)\}$. Then it is clear that $\mu_1 * \ldots * \mu_{n-1} = \lambda_{\mathcal{S}_n}$.

The result for $\mathcal{S}_n$ motivated us to consider other finite Coxeter groups. In the case when W is 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 $7 \leqslant m < \infty$, Theorem 1.1 was proved, in a constructive way, by the author in [15]. Here we consider the remaining types: E_6, E_7, E_8, H_3 and H_4. In some steps of the proof a computer algebra system GAP (see [10]) will be used. In particular, we use the functions contained in the CHEVIE share package of GAP. (See [5] and [2] for more information on CHEVIE.)

The problem of factorization of a given probability measure on a finite or compact group goes back to Lévy [9]. Recently, this problem and its particular case – the problem of existence of the "square root" from a given probability measure – has been studied by Diaconis [3], Diaconis and Shahshahani [4], Turnwald [13], and Sherstnev [11], [12].

We should also mention that there are, however, groups and symmetric sets T of generators for which (1.1) does not hold for any finite set of symmetric probability measures supported on T. Some examples are given in [14].

The paper is organized as follows. In Section 2 we recall some basic facts about Coxeter groups and state classification of finite Coxeter groups. In Section 3 we prove Theorem 1.1.

Acknowledgments. The author would like to thank Ms. Monika Tomczak for a discussion on the subject of the paper.

2. COXETER GROUPS

For basic references on the subject of this section see [1] and [7].

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

$$\bullet \overset{m(s,t)}{\text{———}} \bullet$$

If $m(s,t) = 3$, then the edge is not labeled.

With every Coxeter graph (Γ, m) we associate the corresponding *Coxeter group* $W(\Gamma, m)$ (we also use the notation $W(\Gamma)$, $W(S,m)$ or, simply, $W(S)$ if there is no reason for confusion) specifying its presentation:

$$W(\Gamma, m) = \langle s \in S \mid s^2 = 1, (st)^{m(s,t)} = 1, s \neq t \in S \rangle,$$

i.e., $W(S)$ is generated by the symbols $s \in S$ satisfying the following relations: $s^2 = 1$ for every $s \in S$ and $(st)^{m(s,t)} = 1$ for all pairs $s, t \in S$ with $m(s,t) \geqslant 3$.

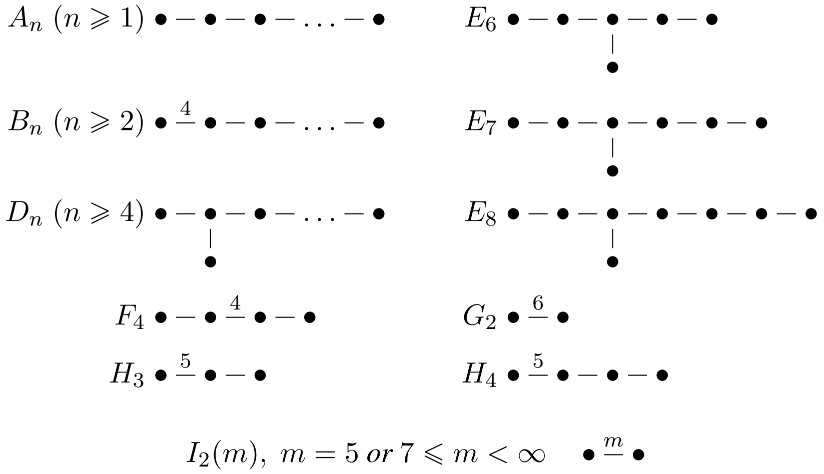
© for this edition by CNS

Let W be a Coxeter group with its distinguished set of generators S. A subgroup $W_J \subset W$ generated by a subset J of S is a Coxeter group and is called a *parabolic subgroup*.

The *length function* $\ell : W \to \mathbb{N} \cup \{0\}$ is defined as follows. Let $w \in W = W(S)$. If $w = 1$, then $\ell(w) = 0$. Otherwise, there exists a minimal $k \geqslant 1$ and elements $s_1, \dots, s_k \in S$ such that $w = s_1 \dots s_k$ (i.e., we have a *reduced expression* for w) and we set $\ell(w) = k$.

We will need the following classification of finite Coxeter groups.

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). *The group* $W(\Gamma, m)$ *is finite if and only if the graph* (Γ, m) *is one of the following Coxeter–Dynkin diagrams*:



Proof. For the proof see, e.g., [1], [7], [6]. ■

3. PROOF OF THEOREM 1.1

It is clear that it is enough to consider only finite Coxeter groups corresponding to connected Dynkin diagrams given in Theorem 2.1 (i.e., *irreducible* Coxeter groups). Otherwise, we have the direct product of such irreducible groups and Theorem 1.1 clearly works for the direct products.

By the result of Urban [15] we are left with the groups E_6, E_7, E_8, H_3 and H_4.

The idea of proof is the following. We show that for a given group W of the above types there exists a parabolic subgroup $W_J = \langle s \mid s \in J \rangle$, $J \subset S$, for which the factorization (1.1) holds and, moreover, there exists a set $\tilde{X}_J$ of right coset representatives of W_J in W consisting of elements of order not greater than 2. Then Theorem 1.1 will follow from the *subgroup algorithm* (see [3]). In the simplest case the subgroup algorithm states the following. Let G be a finite group and let H be a subgroup of G (not necessarily normal). Let C be a set of coset representatives for

© for this edition by CNS

H in G. Then every element $g \in G$ has a unique representation: $g = hc$ with $h \in H$ and $c \in C$. If λ_C is a uniform distribution on C and λ_H is a uniform distribution (the Haar measure) on H, then the convolution $\lambda_H * \lambda_C$ is the factorization of the Haar measure on G.

3.1. Coset representatives. Let W_J be a parabolic subgroup of W. The Coxeter group W is partitioned, with respect to W_J, into right cosets $W_J w = \{vw \mid v \in W_J\}$. The set X_J given in the next proposition will be called a set of *distinguished right coset representatives* of W_J in W.

PROPOSITION 3.1. *Let $J \subset S$ and define*

$$X_J = \{w \in W \mid \ell(sw) > \ell(w) \textit{ for all } s \in J\}.$$

Then:

(a) *For each $w \in W$ there exists a unique $v \in W_J$ and $x \in X_J$ such that $w = vx$. Moreover*, $\ell(w) = \ell(v) + \ell(x)$.

(b) *For any $x \in W$ the following are equivalent*:

(i) $x \in X_J$;

(ii) $\ell(vx) = \ell(v) + \ell(x)$ *for all* $v \in W_J$;

(iii) *x is a unique element of minimal length in $W_J x$.*

In particular, X_J is a complete set of right coset representatives of W_J in W.

Proof. See [6], Proposition 2.1.1. ■

There is an algorithm for computing X_J. In the sequel we use the following convention. The expression $X \leftarrow Y$ means that we assign to a variable X the value of a variable Y.

ALGORITHM 1 ([6], Algorithm B, p. 40). Given $W(S)$ and a subset J of S, the set X_J is constructed.

(1) Set $k \leftarrow 0$, $Y_0 \leftarrow \{1\}$ and $X_0 \leftarrow Y_0$.

(2) Set $k \leftarrow k + 1$ and

$$Y_k \leftarrow \{xs \mid x \in Y_{k-1}, s \in S, \ell(xs) > \ell(x) \text{ and } \ell(txs) > \ell(tx) \text{ for all } t \in J\}.$$

Set $X \leftarrow X \cup Y_k$.

(3) Repeat (2) until $Y_k = \emptyset$. Then set $X_J \leftarrow X$ and stop.

In the proof of Theorem 1.1, for a given $J \subset S$ we are going to find, if possible, the set $\tilde{X}_J$ of right coset representatives consisting of elements of order not greater than 2. For this purpose the following proposition will be useful.

PROPOSITION 3.2. *Let $x \in Y_k \cap X_J$ and let $\tilde{x} \in \tilde{X}_J$ be such that $W_J x = W_J \tilde{x}$. Suppose that $w = xs \in Y_{k+1}$ with $s \in J$. Then the element $\tilde{w} = s\tilde{x}s$ satisfies $\tilde{w}^2 = 1$ and $W_J w = W_J \tilde{w}$.*

© for this edition by CNS

Proof. Clearly, $\tilde{w}^2 = 1$. Since $x\tilde{x} \in W_J$, we have $w\tilde{w} = x\tilde{x}s \in W_J$ and $W_J w = W_J \tilde{w}$. ■

Proposition 3.2 states that if the representative $w \in Y_{k+1}$ is constructed in Algorithm 1 from the previous one by appending $s \in J$ to its end, then the corresponding representative of order 2 is constructed by appending s to the beginning and to the end of the previously constructed one.

The situation is more complicated if we append $s \notin J$ to the end of the previous representative x in Algorithm 1. Then, as will be seen in Section 3.3 and Section 3.6, it may happen that the coset $W_j xs$ does not contain elements of order 2. Hence, our strategy in order to construct $\tilde{X}_J$ is as follows. We choose a parabolic subgroup W_J on which Theorem 1.1 holds. Next we generate X_J (in CHEVIE there is a function `ReducedRightCosetRepresentatives` which produces X_J using Algorithm 1). By Proposition 3.2, it is enough to consider the following subset Z of X_J:

$$\begin{aligned} Z = \{x \in X_J \mid \operatorname{order}(x) > 2\} \\ \cap \{x \in X_J \mid \text{the last letter in the reduced expression of } x \text{ is in } S \setminus J\}, \end{aligned}$$

and for every $z \in Z$ we check if there is an element $w \in W_J$ such that $\operatorname{order}(wz) \leqslant 2$ (simply by checking all elements in the coset $W_J z$). If this fails, we choose a different parabolic subgroup and repeat our procedure.

Remark. It would be interesting to find sufficient (and necessary) conditions on J which guarantee that for every $z \in Z$ there exists $w \in W_J$ such that $\operatorname{order}(wz) \leqslant 2$, i.e., there exists a set $\tilde{X}_J$ of right coset representatives consisting of elements of order not greater than 2.

For a finite set A we write $|A|$ to denote the number of its elements.

3.2. Coxeter group H_3. We take

$$H_3: \quad s_1 \overset{5}{-} s_2 - s_3, \qquad J = \{s_1, s_2\}.$$

Hence W_J is of type $I_2(5)$. We have $|W_J| = 10$, $|X_J| = 12$. The set Z contains only one element $z = s_3 s_2 s_1 s_2 s_1 s_3$. We check that $s_1 z$ can be taken as the corresponding representative of order 2. By [15], Proposition 3.2, there is a factorization of the Haar measure on $I_2(5)$, so Theorem 1.1 is proved in this case.

Alternatively, one can also take the subgroup $J = \{s_2, s_3\}$. Then W_J is of type A_2, $|W_J| = 6$, $|X_J| = 20$, $Z = \{z = s_1 s_2 s_1 s_2 s_1 s_2 s_3 s_2 s_1\}$. The corresponding representative of order 2 is $s_3 z = s_1 s_2 s_3 s_2 s_1 s_2 s_1 s_3$.

3.3. Coxeter group H_4. Let us take

$$H_4: \quad s_1 \overset{5}{-} s_2 - s_3 - s_4, \qquad J = \{s_2, s_3, s_4\}.$$

© for this edition by CNS

Thus W_J is of type A_3. We have $|W_J| = 24$, $|X_J| = 600$, $|Z| = 88$. It turns out that this is a wrong choice for the parabolic subgroup. There are 51 cosets which do contain only elements of order greater than 2, e.g., the coset

$$W_J s_1 s_2 s_1 s_2 s_3 s_2 s_1 s_2 s_1 s_4 s_3 s_2 s_1.$$

Therefore, we try another subgroup and we take

$$J = \{s_1, s_2, s_3\}.$$

Thus W_J is of type H_3. We have $|W_J| = |X_J| = 120$, $|Z| = 22$. For example, the shortest and the longest elements in Z are

$$\begin{aligned} z_1 &= s_4 s_3 s_2 s_1 s_2 s_1 s_3 s_4, \\ z_2 &= s_4 s_3 s_2 s_1 s_2 s_1 s_3 s_2 s_1 s_2 s_3 s_4 s_3 s_2 s_1 s_2 s_1 s_3 s_2 s_1 s_2 s_3 s_4 s_3 s_2 s_1 s_2 s_1 s_3 s_2 s_1 s_2 s_4. \end{aligned}$$

The corresponding representatives of order 2 are

$$s_1 z_1, \qquad s_2 s_1 s_2 s_1 s_3 s_2 s_1 z_2.$$

For all other elements from the set Z we succeeded in finding corresponding representatives of order not greater than 2. Since, by the results of Section 3.2, Theorem 1.1 is valid for groups of type H_3, we have proved that it is also valid for groups of type H_4.

3.4. Coxeter group E_6. We take

$$E_6 : \quad s_1 - s_3 - \underset{\substack{| \\ s_2}}{s_4} - s_5 - s_6, \qquad J = \{s_1, s_3, s_4, s_5, s_6\}.$$

Hence W_J is of type A_5. We have $|W_J| = 720$, $|X_J| = 72$, $|Z| = 4$. The set Z contains the following elements:

$$\begin{aligned} z_1 &= s_2 s_4 s_3 s_1 s_5 s_4 s_2, \\ z_2 &= s_2 s_4 s_3 s_1 s_5 s_4 s_2 s_3 s_6 s_5 s_4 s_2, \\ z_3 &= s_2 s_4 s_3 s_1 s_5 s_4 s_2 s_3 s_4 s_6 s_5 s_4 s_2, \\ z_4 &= s_2 s_4 s_3 s_1 s_5 s_4 s_2 s_3 s_4 s_5 s_6 s_5 s_4 s_2. \end{aligned}$$

The corresponding representatives of order 2 are

$$\begin{aligned} s_1 z_1 &= s_1 s_2 s_4 s_3 s_1 s_5 s_4 s_2, \\ s_4 z_2 &= s_2 s_4 s_2 s_3 s_1 s_5 s_4 s_2 s_3 s_6 s_5 s_4 s_2, \\ s_5 s_4 z_3 &= s_2 s_4 s_3 s_1 s_5 s_4 s_2 s_3 s_1 s_4 s_3 s_6 s_5 s_4 s_2, \\ s_6 s_5 s_4 z_4 &= s_2 s_4 s_3 s_1 s_5 s_6 s_5 s_4 s_2 s_3 s_1 s_4 s_3 s_5 s_4 s_2 s_6. \end{aligned}$$

Thus we are done in this case. We could also choose $J = \{s_1, s_2, s_3, s_4, s_5\}$. Then W_J is of type D_5 (there is a factorization on W_J by the results of [15]), $|W_J| = 1920$, $|X_J| = 27$, $|Z| = 4$, and so $\tilde{X}_J$ exists.

© for this edition by CNS

3.5. Coxeter group E_7. We take

$$E_7: \quad \begin{array}{ccccccccccc} s_1 & - & s_3 & - & s_4 & - & s_5 & - & s_6 & - & s_7, \\ & & & & | & & & & & & \\ & & & & s_2 & & & & & & \end{array} \qquad J = \{s_1, s_3, s_4, s_5, s_6, s_7\}.$$

Hence W_J is of type A_6. We have $|W_J| = 5{,}040$, $|X_J| = 576$, $|Z| = 32$. Since for every $z \in Z$ there exists $w \in W_J$ such that $\mathrm{order}(wz) \leqslant 2$, Theorem 1.1 is proved in this case.

We can also take $J = \{s_1, s_2, s_3, s_4, s_5, s_6\}$. Then W_J is of type E_6. By the above, there is a factorization on W_J. In this case we have $|W_J| = 51{,}840$, $|X_J| = 56$, $|Z| = 9$ and for every z we can construct a corresponding representative of order less than or equal to 2.

3.6. Coxeter group E_8. If we take

$$E_8: \quad \begin{array}{ccccccccccccc} s_1 & - & s_3 & - & s_4 & - & s_5 & - & s_6 & - & s_7 & - & s_8, \\ & & & & | & & & & & & & & \\ & & & & s_2 & & & & & & & & \end{array} \qquad J = \{s_1, s_3, s_4, s_5, s_6, s_7, s_8\}$$

then W_J is of type A_7. We have $|W_J| = 40{,}320$, $|X_J| = 17{,}280$. Unfortunately, this is not a right choice since there are cosets which contain only elements of order greater than 2, as, e.g., the following one:

$$W_J s_2 s_4 s_3 s_1 s_5 s_4 s_3 s_6 s_5 s_4 s_2 s_7 s_6 s_5 s_4 s_3 s_8 s_7 s_6 s_5 s_4 s_2.$$

However, we take $J = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7\}$. That is, W_J is of type E_7. We have $|W_J| = 2{,}903{,}040$, $|X_J| = 240$, $|Z| = 26$. In this case our procedure works. From Section 3.5 we know that there is a factorization on W_J, so the last case of Theorem 1.1 has been proved.

REFERENCES

[1] N. Bourbaki, *Groupes et algèbres de Lie*, Ch. 5, 6, 7, Hermann, 1968.

[2] CHEVIE: `http://www.math.rwth-aachen.de/~CHEVIE`

[3] P. Diaconis, *Application of non-commutative Fourier analysis to probability problems*, Lecture Notes in Math. Vol. 1362, Springer, 1982, pp. 51–100.

[4] P. Diaconis and M. Shahshahani, *On square roots of the uniform distribution on compact groups*, Proc. Amer. Math. Soc. 98 (2) (1986), pp. 341–348.

[5] M. Geck, G. Hiss, F. Lübeck, G. Malle and G. Pfeiffer, *CHEVIE – a system for computing and processing generic character tables. Computational methods in Lie theory (Essen, 1994)*, Appl. Algebra Engrg. Comm. Comput. 7 (3) (1996), pp. 175–210.

[6] M. Geck and G. Pfeiffer, *Characters of Finite Coxeter Groups and Iwahori–Hecke Algebras*, London Math. Soc. Monogr. (2000).

[7] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, Cambridge–New York 1990.

[8] D. E. Knuth, *The Art of Computer Programming, Vol. 2. Seminumerical Algorithms*, second edition, Addison-Wesley Series in Computer Science and Information Processing, Addison-Wesley Publishing Co., Reading, Mass., 1981.

© for this edition by CNS

[9] P. Lévy, *Premiers éléments de l'arithmétique des substitutions aléatoires*, C. R. Acad. Sci. Paris 237 (1953), pp. 1488–1489.

[10] M. Schönert et al., *GAP – Groups, Algorithms, and Programming – version 3 release 4 patchlevel 4*, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 1997; available at `http://www.gap-system.org/gap.html`.

[11] V. I. Sherstnev, *A random variable uniformly distributed on a finite abelian group as a sum of independent summands* (in Russian), Teor. Veroyatnost. i Primenen. 43 (2) (1998), pp. 397–403. Translation in: Theory Probab. Appl. 43 (2) (1999), pp. 329–335.

[12] V. I. Sherstnev, *Decompositions of a uniform distribution on a finite group* (in Russian), Teor. Veroyatnost. i Primenen. 47 (3) (2002), pp. 594–599. Translation in: Theory Probab. Appl. 47 (3) (2003), pp. 550–555.

[13] G. Turnwald, *Roots of Haar measure and topological Hamiltonian groups*, in: *Probability Measures on Groups, IX (Oberwolfach, 1988)*, Lecture Notes in Math. Vol. 1379, Springer, 1989, pp. 364–375.

[14] R. Urban, *Some remarks on the random walk on finite groups*, Colloq. Math. 74 (2) (1997), pp. 287–298.

[15] R. Urban, *Note on the factorization of the Haar measure on finite Coxeter groups*, Probab. Math. Statist. 24 (1) (2004), pp. 173–180.

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

Received on 11.6.2010;
revised version on 23.12.2010

© for this edition by CNS