Bull. Austral. Math. Soc. **77** (2008), 31–36
doi: 10.1017/S0004972708000038

COMMUTATIVITY DEGREES OF WREATH PRODUCTS OF FINITE ABELIAN GROUPS

IGOR V. EROVENKO and B. SURY

(Received 12 April 2007)

Abstract

We compute commutativity degrees of wreath products $A \wr B$ of finite Abelian groups A and B. When B is fixed of order n the asymptotic commutativity degree of such wreath products is $1/n^2$. This answers a generalized version of a question posed by P. Lescot. As byproducts of our formula we compute the number of conjugacy classes in such wreath products, and obtain an interesting elementary number-theoretic result.

2000 *Mathematics subject classification*: 20E22, 20J06.
Keywords and phrases: wreath product, commutativity degree.

1. Introduction

For a finite group G let $\mathcal{G}$ denote the set of pairs of commuting elements of G:

$$\mathcal{G} = \{(g, h) \in G \times G \mid gh = hg\}.$$

The quantity $|\mathcal{G}|/|G|^2$ measures the probability of two random elements of G commuting and is called the *commutativity degree* of G. In [1] Lescot computes the commutativity degree of dihedral groups and shows that it tends to $1/4$ as the order of the group tends to infinity. He then asks whether there are other natural families of groups with the same property. In this paper we show that if B is an Abelian group of order n and A is a finite Abelian group, then the commutativity degree of the wreath product $A \wr B$ tends to $1/n^2$ as the order of A tends to infinity.

THEOREM 1.1. *Let $G = A \wr B$, where A is a finite Abelian group and $B = \{b_1, b_2, \ldots, b_n\}$ is an Abelian group of order n. Then*

$$|\mathcal{G}| = \sum_{s,t=1}^{n} |A|^{n+\alpha(s,t)}, \tag{1}$$

where $\alpha(s, t)$ denotes the index of the subgroup of B generated by b_s and b_t.

The exact value of the quantity $\alpha(s, t)$, of course, depends on the structure of B as an Abelian group. We show how to obtain it in Section 3. Here we just note that when $B = \mathbb{Z}_n = \{1, 2, \ldots, n\}$ is a cyclic group of order n, $\alpha(s, t) = (n, s, t)$ (where (n, s, t) denotes the greatest common divisor of n, s, and t). More generally, for a fixed value of n the farther B is away from a cyclic group, the larger the commutativity degree of the wreath product $A \wr B$ is. For example, the commutativity degree of $A \wr \mathbb{Z}_4$ is $1/16 + 3|A|^{-2} + 12|A|^{-3}$, while that of $A \wr (\mathbb{Z}_2 \times \mathbb{Z}_2)$ is $1/16 + 9|A|^{-2} + 6|A|^{-3}$. However, the asymptotic behaviour of the commutativity degree of the wreath product $A \wr B$ as $|A| \to \infty$ does not depend on the structure of B as an Abelian group.

COROLLARY 1.2. *Let A be a finite Abelian group and B be an Abelian group of order n. Then the commutativity degree of the wreath product $A \wr B$ tends to $1/n^2$ as $|A| \to \infty$.*

A straightforward computation with indices of centralizers shows that the number of conjugacy classes in a finite group G is equal to $|\mathcal{G}|/|G|$, hence (1) yields the formula for the number of conjugacy classes in wreath products of finite Abelian groups.

COROLLARY 1.3. *Let A and B be as in Theorem 1.1. Then the number of conjugacy classes in the wreath product $A \wr B$ is $(1/n) \sum_{s,t=1}^{n} |A|^{\alpha(s,t)}$.*

By taking $B = \mathbb{Z}_n$ in Corollary 1.3, we obtain the following interesting elementary number-theoretic result. We have not been able to find an elementary proof of this fact.

COROLLARY 1.4. *For any natural number a, the sum $\sum_{s,t=1}^{n} a^{(n,s,t)}$ is divisible by n. If n is prime, this gives Fermat's little theorem.*

2. Notation and terminology for wreath products

We shall use some of the notation from [2]. Let A and B be groups and let A^* be the direct sum of copies of A indexed by elements of B. We shall write this as $A^* = \sum_{b \in B} A_b$, where each group A_b is a copy of A. Elements of A^* can be thought of as functions from B to A with finite support. An element $f \in A^*$ such that

$$f(b) = \begin{cases} a & \text{if } b = b_0 \in B, \\ e_A & \text{otherwise,} \end{cases}$$

will be denoted by $\sigma_a(b_0)$. In this notation, every element of A^* can be uniquely written in the form

$$\sigma_{a_1}(b_1) \cdots \sigma_{a_s}(b_s),$$

where $b_1, \ldots, b_s$ are *distinct* elements of B, and $a_1, \ldots, a_s$ are any elements of A. Such a presentation will be called a *canonical word*. Define an action of B on A^* by

$$f^c(b) = f(bc^{-1}), \quad c \in B, \ b \in B. \tag{2}$$

The (standard restricted) wreath product of A and B, denoted by $A \wr B$, is the semidirect product of A^* and B with the action of B on A^* given by (2). If we denote the elements of the canonical copy of B in $A \wr B$ by τ_c, $c \in B$, then (2) becomes

$$\tau_c \sigma_a(b) = \sigma_a(bc)\tau_c,$$

and thus every element of $A \wr B$ can be uniquely written in the canonical form

$$\sigma_{a_1}(b_1) \cdots \sigma_{a_s}(b_s)\tau_b,$$

where $\sigma_{a_1}(b_1) \cdots \sigma_{a_s}(b_s)$ is a canonical word in A^*. We shall work with wreath products where the group B is finite, in which case the restricted wreath product and the complete wreath product are the same.

3. Proof of Theorem 1.1

Since both groups A and B are Abelian we shall use additive notation for their group operations. To make the proof transparent we first work out in detail the case when $B = \mathbb{Z}_n$ is the cyclic group of order n. We may represent elements of B by arbitrary integers assuming that one takes the residue modulo n to obtain an actual element of $\mathbb{Z}_n$.

We shall count the number of commuting pairs of elements of $G = A \wr \mathbb{Z}_n$ as follows. Fix s and t in $\{1, \ldots, n-1, n\}$ and let

$$g = \sigma_{a_0}(0)\sigma_{a_1}(1) \cdots \sigma_{a_{n-1}}(n-1)\tau_{-s},$$

and

$$h = \sigma_{x_0}(0)\sigma_{x_1}(1) \cdots \sigma_{x_{n-1}}(n-1)\tau_{-t}.$$

We then count the number of commuting pairs (g, h) with prescribed values of s and t but allowing the a_i and x_i to be arbitrary elements of A. To do so we think of an element g as being 'fixed' and count the number of elements h that commute with every such given g. As we shall see shortly, there might be some conditions on the a_i for g to commute with at least one such h.

We shall make a convention that a_u and a_v represent the same element of the group A if u and v are equal modulo n; similarly for x_u and x_v. With this notation, the elements g and h as above commute if and only if

$$\begin{aligned} x_0 - x_s &= a_0 - a_t, \\ x_1 - x_{s+1} &= a_1 - a_{t+1}, \\ &\vdots \\ x_{n-1} - x_{s+(n-1)} &= a_{n-1} - a_{t+(n-1)}, \end{aligned}$$

which can be thought of as a 'linear system' in unknowns $x_0, x_1, \ldots, x_{n-1}$. Let $d+1$ be the order of s in $\mathbb{Z}_n$, then $d+1 = n/(n,s)$ and there are (n,s) cosets of the cyclic subgroup $\langle s\rangle$ generated by s in $\mathbb{Z}_n$.

The above linear system will split into (n,s) independent subsystems in unknowns $\{x_i, x_{i+s}, x_{i+2s}, \ldots, x_{i+ds}\}$ where i varies over the representatives of the cosets of $\langle s\rangle$ in $\mathbb{Z}_n$, say $0 \leqslant i \leqslant (n,s)-1$. The matrix of each such subsystem has rank d; hence for the subsystem to be consistent the 'constant' column consisting of differences of a_i must add up to zero. This gives the following condition for consistency of the ith subsystem:

$$a_i + a_{i+s} + \cdots + a_{i+ds} = a_{i+t} + a_{i+s+t} + \cdots + a_{i+ds+t}, \qquad 0 \leqslant i \leqslant (n,s)-1. \tag{3}$$

If $t \in \langle s\rangle$ then the conditions (3) are automatically satisfied for all i, and hence for any choice of the elements $a_0, a_1, \ldots, a_{n-1}$ the number of elements h commuting with given g is $|A|^{(n,s)}$ since each subsystem has one free variable.

Suppose now that $t \in j + \langle s\rangle$ for some $j \in \{1, \ldots, (n,s)-1\}$. Let u denote the order of t (= order of j) in the quotient group $\mathbb{Z}_n/\langle s\rangle$. Then $u = (n,s)/(n,s,t)$ and the index of the subgroup $\langle t\rangle$ in $\mathbb{Z}_n/\langle s\rangle$ is $(n,s)/u = (n,s,t)$; in the notation of Theorem 1.1 this is nothing but $\alpha(s,t)$.

The conditions (3) split into $\alpha(s,t)$ blocks corresponding to the cosets of $\langle t\rangle$ in $\mathbb{Z}_n/\langle s\rangle$. The kth block $(0 \leqslant k \leqslant \alpha(s,t)-1)$ looks as follows:

$$\begin{aligned} a_k + a_{k+s} + \cdots + a_{k+ds} &= a_{k+t} + a_{k+t+s} + \cdots + a_{k+t+ds},\\ a_{k+t} + a_{k+t+s} + \cdots + a_{k+t+ds} &= a_{k+2t} + a_{k+2t+s} + \cdots + a_{k+2t+ds},\\ &\ \vdots\\ a_{k+(u-1)t} + a_{k+(u-1)t+s} + \cdots + a_{k+(u-1)t+ds} &= a_{k+ut} + a_{k+ut+s} + \cdots + a_{k+ut+ds}. \end{aligned}$$

But ut is a multiple of s, and hence the right-hand side of the last equation is equal to the left-hand side of the first equation. It follows that exactly one of these u equations is a consequence of the others and each block produces $u-1$ independent 'linear' conditions on the a_i.

To summarize, among the $|A|^n$ sequences $(a_0, a_1, \ldots, a_{n-1})$ of elements of A, there are exactly $|A|^{n-\alpha(s,t)(u-1)} = |A|^{n-(n,s)+\alpha(s,t)}$ sequences for which the original linear system in $x_0, x_1, \ldots, x_{n-1}$ is consistent. For each such fixed sequence, the number of sequences $(x_0, x_1, \ldots, x_{n-1})$ satisfying the corresponding system is $|A|^{(n,s)}$ since each of the (n,s) (= index of the subgroup of B generated by s) subsystems contributes one free variable. Thus, for fixed s and t the total number of commuting pairs (g,h) of elements of G where the canonical form of g ends in τ_{-s} and the canonical form of h ends in τ_{-t} is $|A|^{n+\alpha(s,t)}$. The formula (1) now follows.

In the general case, when $B = \{b_1, b_2, \ldots, b_n\}$ is an arbitrary Abelian group, fix $b_s, b_t \in B$ and consider two elements of $G = A \wr B$,

$$g = \sigma_{a_1}(b_1)\sigma_{a_2}(b_2)\cdots\sigma_{a_n}(b_n)\tau_{-b_s},$$

and

$$h = \sigma_{x_1}(b_1)\sigma_{x_2}(b_2)\cdots\sigma_{x_n}(b_n)\tau_{-b_t}.$$

Note that the above proof essentially did not use the fact that B was a cyclic group (it was only used so as to have a convenient way to label the indices of a_i and x_i). Rather, the computation involves the following quantities:

(1) the index of the cyclic subgroup of B generated by b_s, say $\beta(s)$;
(2) the index of the cyclic subgroup of the quotient group $B/\langle b_s\rangle$ generated by the image of b_t, which is precisely $\alpha(s, t)$ in our notation.

The 'linear system' which gives conditions for elements g and h to commute then splits into $\beta(s)$ subsystems each of which corresponds to a coset of the *cyclic* subgroup $\langle b_s\rangle$ of B, and hence the same reasoning carries over verbatim to the general case. Further, the conditions on the a_i will split into $\alpha(s, t)$ blocks each of which corresponds to a coset of the *cyclic* subgroup generated by the image of b_t in $B/\langle b_s\rangle$.

It follows that among the $|A|^n$ sequences $(a_1, a_2, \ldots, a_n)$ of elements of A, there are exactly $|A|^{n-\beta(s)+\alpha(s,t)}$ sequences for which the linear system is consistent. For each such fixed sequence, the number of sequences $(x_1, x_2, \ldots, x_n)$ satisfying the corresponding system is $|A|^{\beta(s)}$. Thus, for fixed s and t the total number of commuting pairs (g, h) of elements of G where the canonical form of g ends in τ_{-b_s} and the canonical form of h ends in τ_{-b_t} is $|A|^{n+\alpha(s,t)}$. This completes the proof of Theorem 1.1.

Finally, we give a formula for $\alpha(s, t)$ which depends on the structure of B as an Abelian group. Let $B = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ and let $s = (s_1, \ldots, s_k)$, $t = (t_1, \ldots, t_k)$ be two elements of B. Let $\alpha(s, t) = [B : \langle s, t\rangle]$.

Consider the surjective homomorphism $\pi : \mathbb{Z}^k \to B$ with

$$\ker \pi = n_1\mathbb{Z} \times \cdots \times n_k\mathbb{Z}.$$

Let $a, b \in \mathbb{Z}^k$ be such that $\pi(a) = s$ and $\pi(b) = t$. Then $\mathbb{Z}^k/H \cong B/\langle s, t\rangle$ where $H = \ker \pi + \langle a, b\rangle$. We determine the order of $\mathbb{Z}^k/H$ as follows. Write $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ (thinking of the s_i and t_j as integers one may take $a_i = s_i$ and $b_j = t_j$ for all $i, j \in \{1, \ldots, k\}$), then

$$H = \{(n_1m_1 + ua_1 + vb_1, \ldots, n_km_k + ua_k + vb_k) \mid m_i, u, v \in \mathbb{Z}\}.$$

If $R : \mathbb{Z}^{k+2} \to \mathbb{Z}^k$ is a homomorphism given by the $k \times (k + 2)$ matrix

$$\begin{bmatrix} n_1 & 0 & \cdots & 0 & a_1 & b_1 \\ 0 & n_2 & \cdots & 0 & a_2 & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & n_k & a_k & b_k \end{bmatrix}$$

then $H = \operatorname{Im} R$. Let $P \in GL_k(\mathbb{Z})$ and $Q \in GL_{k+2}(\mathbb{Z})$ be such that

$$PRQ = \begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & d_2 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_k & 0 & 0 \end{bmatrix}$$

where $d_1 \mid d_2 \mid \cdots \mid d_k$ are the elementary divisors of R. We have

$$\mathbb{Z}^k/\mathrm{Im}\, R \cong P(\mathbb{Z}^k)/PR(\mathbb{Z}^{k+2}) = \mathbb{Z}^k/PRQ(\mathbb{Z}^{k+2}),$$

so that

$$\alpha(s, t) = |\mathbb{Z}^k/\mathrm{Im}\, R| = |d_1 d_2 \cdots d_k|.$$

For the reader's convenience we recall a well-known method for finding elementary divisors. For $i = 1, \ldots, k$, let h_i denote the greatest common divisor of all $i \times i$ minors of R; then $h_i = d_1 d_2 \cdots d_i$. This is because the numbers h_i do not change when multiplied on the left and on the right by elementary matrices and these generate all invertible integer matrices. In particular, note that if $k = 1$ then $\alpha(s, t) = (n, s, t)$.

Acknowledgement

The second author would like to thank the Max Planck Institut für Mathematik for its hospitality during his visit in February–March 2007 when this paper was written.

References

[1] P. Lescot, 'Central extensions and commutativity degree', *Comm. Algebra* **29** (2001), 4451–4460.

[2] J. D. P. Meldrum, *Wreath products of groups and semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics, 74 (Longman, Harlow, 1995).

Department of Mathematics and Statistics
University of North Carolina at Greensboro
Greensboro, NC 27402
USA
e-mail: igor@uncg.edu

Stat-Math Unit
Indian Statistical Institute
8th Mile Mysore Rd
Bangalore 560 059
India
e-mail: sury@isibang.ac.in