Canad. Math. Bull. Vol. **33** (4), 1990

THE COHERENCE NUMBER OF 2-GROUPS

BY
JAMES McCOOL

ABSTRACT. Let G be a finite group. A natural invariant $c(G)$ of G has been defined by W.J. Ralph, as the order (possibly infinite) of a distinguished element of a certain abelian group associated to G. Ralph has shown that $c(Z_n) = 1$ and $c(Z_2 \oplus Z_2) = 2$. In the present paper we show that $c(G)$ is finite whenever G is a dihedral group or a 2-group, and obtain upper bounds for $c(G)$ in these cases.

1. **Introduction.** Let G be a finite group. In [2] Ralph has defined a somewhat mysterious invariant $c(G)$ of G, called the coherence number of G. Although the motivation for introducing $c(G)$ comes from algebraic topology, the definition itself is completely algebraic, and may be described as follows. Let $H = H(G)$ be a free group with basis B consisting of elements $\alpha_g, \beta_g (g \in G)$, so that H has rank $2|G|$. Next, for each $g \in G$ define H_g to be the normal closure of the set of elements $\alpha_x \beta_{xg}^{-1} (x \in G)$, and let K be the intersection of all these subgroups. Now consider the quotient group H/KH', where H' is the commutator subgroup of H, and note that any torsion element of this group must be a power of the image of the element $\theta = \prod_{x \in G} \alpha_x \beta_x^{-1}$ of H, since any element of K not in H' must coincide with a power of θ, modulo H'. Thus H/KH' can be described as $Z_m \oplus Z^{2|G|-1}$, where m is the order of θ in H/KH' (cf. Corollary 1.16 of [2]). As we show below, this number m is the coherence number $c(G)$ of G as defined in [2].

Despite its ease of definition, and some general results obtained in [2], some very basic questions about $c(G)$ remain unanswered. Thus, for example, it is not known whether or not $c(G)$ is always finite, even in the case where G is abelian. Indeed, the only groups for which $c(G)$ is known seem to be the cyclic groups Z_n and the group $Z_2 \oplus Z_2$. The object of the present note is to provide a modest increase of our knowledge in this regard. More precisely, our main result is to show that if G is an extension of degree two of a group G_0 with $c(G_0)$ finite, then $c(G)$ itself is finite. As a consequence we obtain that $c(G)$ is finite whenever G is a dihedral group D_k, and whenever G is a 2-group. The method of proof shown that $c(D_k)$ is a divisor of k, while if $|G| = 2^k$ then $c(G)$ is a divisor of 2^{2^k-k-1} (it is conjectured in [2] that this is the value of $c(Z_2^k)$).

2. **Notation and preliminary results.** We begin by recalling a form of the definition of $c(G)$ given in [2]. Let $|G| = n$, and consider the G-set $S = \{(g,i);\ g \in G,\ 1 \leqq i \leqq n\}$, where $y(g,i) = (yg,i)$ for each $y \in G$. Let $F_i \quad (1 \leqq i \leqq n)$ be the free group with basis the subset S_i of S, where $S_i = \{(g,i);\ g \in G\}$, and take P to be the direct

Received June 19, 1990.
AMS subject classification: Primary 20D60; Secondary 20E05.

Research supported by a grant from the Natural Sciences and Engineering Research Council of Canada.

product $F_1 \times \cdots \times F_n$. Observe that the action of G on S induces a corresponding action on P. We define elements α_g, β_g of P, for $g \in G$, as follows. Firstly, we put

$$\alpha = \alpha_e = \prod_{i=1}^{n} (g_i, i), \qquad \beta = \beta_e = \prod_{i=1}^{n} (e, i),$$

where e is the identity element of G, and $g_1, g_2, \ldots, g_n$ is some chosen ordering of the elements of G. Then we define $\alpha_g = g\alpha_e$ and $\beta_g = g\beta_e$ for each $g \in G$. Taking $\tilde{H} = \tilde{H}(G)$ to be the subgroup of P generated by the α_g and $\beta_g (g \in G)$, and $\tilde{\theta}$ to be the element $\prod_{i=1}^{n} \alpha_{g_i}\beta_{g_i}^{-1}$, the coherence number $c(G)$ is then defined to be the order of the image of $\tilde{\theta}$ in the quotient $\tilde{H}/\tilde{H}'$ of $\tilde{H}$ by its commutator subgroup.

We now reconcile this with the description of $c(G)$ as given above. Let γ_i be the projection homomorphism from P to F_i, so that $\gamma_i(f_1, \ldots, f_n) = f_i$. Clearly we have $\bigcap_{i=1}^{n} \ker \gamma_i = \{e\}$. Also (regarding each F_i as embedded in P), $\gamma_i(\alpha_g) = (gg_i, i)$ and $\gamma_i(\beta_{gg_i}) = (gg_i, i)$, so that $\alpha_g\beta_{gg_i}^{-1} \in \ker\gamma_i$. Thus if $\tilde{H}_{g_i}$ is the normal closure in $\tilde{H}$ of all elements $\alpha_g\beta_{gg_i}^{-1}$ of $\tilde{H}$, then $\tilde{H}_{g_i} < \tilde{H} \cap \ker\gamma_i$. Now $\tilde{H}/(\tilde{H} \cap \ker\gamma_i)$ is isomorphic to F_i, since the fact that $\gamma_i(\alpha_g) = (gg_i, i)$ tells us that γ_i maps the set $\alpha_{g_1}, \ldots, \alpha_{g_n}$ onto the basis S_i of F_i; it follows that $\tilde{H}/\tilde{H}_{g_i}$ is free with basis $\alpha_{g_1}\tilde{H}_{g_i}, \ldots, \alpha_{g_n}\tilde{H}_{g_i}$, because it is generated by the images of the α_{g_j} and maps onto the free group $\tilde{H}/(\tilde{H} \cap \ker\gamma_i)$. Using the well known result that free groups of finite rank are hopfian (see, e.g. proposition 3.5 of [1]) we see that $\tilde{H}_{g_i} = \tilde{H} \cap \ker\gamma_i$, and hence that $\bigcap_{i=1}^{n} \tilde{H}_{g_i} = \{e\}$. Now consider the groups H, H_g and $K = \bigcap_{g \in G} H_g$ as defined above, and let π be the homomorphism from H to $\tilde{H}$ which is the identity map on the set $B = \{\alpha_g, \beta_g;\ (g \in G)\}$. Then clearly $\pi(H_g) = \tilde{H}_g$ for each $g \in G$, and we have

LEMMA 1. $\ker \pi = K$.

PROOF. Since $\bigcap_{i=1}^{n} \tilde{H}_{g_i} = \{e\}$, it follows from the remarks above that $K < \ker\pi$. On the other hand, since H/H_{g_i} is free on the cosets $\alpha_{g_1}H_{g_i}, \ldots, \alpha_{g_n}H_{g_i}$, and $\tilde{H}/\tilde{H}_{g_i}$ is free with corresponding basis noted above, it is clear that $\ker\pi < H_{g_i}$ for $1 \leqq i \leqq n$. This proves the lemma.

We thus have H/K isomorphic to $\tilde{H}$ via the identity map on B, and the equivalence of the two descriptions of $c(G)$ is now obvious.

We now introduce automorphisms r_y, ℓ_y and s_y $(y \in G)$ of the group H, by specifying their effect on elements of the basis B, as follows

$$\begin{array}{lcl} r_y(\alpha_g) = \alpha_g, & & r_y(\beta_g) = \beta_{gy^{-1}}, \\ \ell_y(\alpha_g) = \alpha_{gy^{-1}}, & & \ell_y(\beta_g) = \beta_g, \\ s_e(\alpha_g) = \beta_g, & & s_e(\beta_g) = \alpha_g, \end{array}$$

and $s_y = \ell_y r_y^{-1} s_e$, so that

$$s_y(\alpha_g) = \beta_{gy}, \qquad s_y(\beta_g) = \alpha_{gy^{-1}}.$$

It is an easy matter to check that the mapping $r_y \longrightarrow (e, y, e)$, $\ell_y \longrightarrow (y, e, e)$, $s = s_e \longrightarrow (e, e, s)$ is a isomorphism from the subgroup $\mathcal{G}_1$ of Aut H generated by the r_y, ℓ_y and s to the group $(G \times G) \rtimes Z_2$, noting that $s_y r_y = \ell_y s_y$ for all $y \in G$, and in particular for $s = s_e$.

https://doi.org/10.4153/CMB-1990-080-1 Published online by Cambridge University Press

It is convenient to regard $\mathcal{G}_1$ as a subgroup of $Bij(H)$, the group of bijections of H, and to denote by I the element of $Bij(H)$ such that $I(w) = w^{-1}$ for all $w \in H$. We note that the subgroup $\mathcal{G} = \mathcal{G}(G)$ of $Bij(H)$ generated by $\mathcal{G}_1$ and I is just $\mathcal{G}_1 \times \langle I \rangle = \mathcal{G}_1 \times Z_2$. We now define the element R_y of $\mathcal{G}$, for $y \in G$, to be given by $R_y = s_y I$. Thus we have $R_y(\alpha_g) = \beta_{gy}^{-1}$, $R_y(\beta_g) = \alpha_{gy^{-1}}^{-1}$, and we can now state

LEMMA 2. *Let $w \in H$ and $y \in G$. Then $wR_y(w) \in H_y$.*

PROOF. If $w = \alpha_g^\epsilon$ ($\epsilon = \pm 1$) then $wR_y(w) = \alpha_g^\epsilon \beta_{gy}^{-\epsilon} \in H_y$, and similarly $\beta_g^\epsilon R_y(\beta_g^\epsilon) \in H_y$. We now note that for any $u, v \in H$,

$$R_y(uv) = s_y(v^{-1}u^{-1}) = s_y(v^{-1})s_y(u^{-1}) = R_y(v)R_y(u).$$

Thus if $w = u\alpha_g^\epsilon$, then working modulo H_y we have

$$wR_y(w) = u\alpha_g^\epsilon \beta_{gy}^{-\epsilon} R_y(u) = uR_y(u),$$

and in the same way we see that if $w = u\beta_g^\epsilon$ then $wR_y(w) = uR_y(u)$ modulo H_y. Induction on the length of w now proves the result.

Next we have

LEMMA 3. *Let $g \in G$ and $w \in H$, and put $k = |g|$. Define $f_G(w) = f_{g,G}(w)$ by*

$$f_G(w) = \prod_{r=1}^{2k} (R_{g^r} R_{g^{r-1}} \ldots R_g)(w). \tag{1}$$

Then $f_G(w) \in \bigcap_{j=0}^{k-1} H_{g^j}$.

PROOF. We write $\tau = R_e$ and $\phi = \ell_g r_{g^{-1}}$. It is then easy to check that $R_{g^i} = \phi^i \tau$, and that $\langle \tau, \phi \rangle$ is just a copy of the dihedral group D_k, with $\phi^k = \tau^2 = (\tau\phi)^2 = e$.

In order to show that $f_G(w) \in H_{g^t}$ we may work with any suitable conjugate of $f_G(w)$, since H_{g^t} is a normal subgroup of H. Writing $w_1 = (R_{g^{t-1}} R_{g^{t-2}} \ldots R_g)(w)$, we observe that the subword $w_1 R_{g^t}(w_1)$ of $f_G(w)$ is in H_{g^t}, by Lemma 2. Taking $f_G(w)$ to be written in a circle, and working modulo H_{g^t}, we may therefore delete this subword to obtain a 'smaller' circular word. We claim that at the point in the circle where the subword was deleted we can continue this deletion process until the empty word results. The proof of this is by induction on the number of deletions. At the rth stage the subwords $\lambda_r(w_1)$ and $\rho_r(w_1)$ become adjacent, where $\lambda_r = R_{g^{t-r}} R_{g^{t-r+1}} \ldots R_{g^{t-1}}$ and $\rho_r = R_{g^{t+r}} R_{g^{t+r-1}} \ldots R_{g^t}$ (here we use the fact that $R_{k+i} = R_i$, and $(R_{g^{k-1}} R_{g^{k-2}} \ldots R_e)^2 = e$). We show that $R_g^t \lambda_r = \rho_r$. This is the case for $r = 0$, since $\lambda_0 = e$ and $\rho_0 = g^t$; for $r > 0$ we have

$$\begin{aligned} R_{g^t}\lambda_r &= R_{g^t} R_{g^{t-r}} \lambda_{r-1} = R_{g^t} R_{g^{t-r}} R_{g^t} \rho_{r-1} \\ &= \alpha^r \tau \alpha^{t-r} \tau \alpha^t \tau \rho_{r-1} = \alpha^{t+r} \tau \rho_{r-1} = R_{g^{t+r}} \rho_{r-1} = \rho_r, \end{aligned}$$

as claimed. Thus $R_{g^t}\lambda_r = \rho_r$, and so $\lambda_r(w)\rho_r(w) = \lambda_r(w) R_{g^t} \lambda_r(w) \in H_{g^t}$, by Lemma 2, and hence $\lambda_r(w)\rho_r(w)$ can be deleted. This proves the Lemma.

https://doi.org/10.4153/CMB-1990-080-1 Published online by Cambridge University Press

We note that with f_G defined as in the lemma above, we have

$$f_G(\alpha_e) = \prod_{j=1}^{k} \beta_{g^j}^{-1} \alpha_{g^{-j}},$$

and so, in particular, we recover the result of [2] that $c(G) = 1$ for G cyclic.

If κ is a homomorphism from G to G_1, there will be induced, in a functorial way, corresponding homomorphisms from $H(G)$ to $H(G_1)$ and $\mathcal{G}(G)$ to $\mathcal{G}(G_1)$. Since we will only be concerned with the case of a single monomorphism, the following naive remarks will be sufficient for our purpose. Thus we shall regard G as a subgroup of G_1, and then consider the basis $B(G)$ of $H(G)$ as a subset of the basis $B(G_1)$ of $H(G_1)$. In addition, for $y \in G$, writing $r_y(G)$, $r_y(G_1)$, etc., to distinguish elements of $\mathcal{G}(G)$ and $\mathcal{G}(G_1)$, we have an embedding of $\mathcal{G}(G)$ in $\mathcal{G}(G_1)$ which maps $r_y(G)$ to $r_y(G_1)$, $\ell_y(G)$ to $\ell_y(G_1)$, etc. We note, for use below, that the restrictions of $\ell_y(G_1)$, $r_y(G_1)$, $s_y(G_1)$, $I(G_1)$ to the free factor $H(G)$ of $H(G_1)$ are just the corresponding elements of $H(G)$, for each $y \in G$.

Given G as a subgroup of G_1, we can now replace the function f_G of Lemma 3 by the corresponding function f_{G_1}, mapping $H(G_1)$ to $H(G_1)$, given by

$$f_{G_1}(w) = \prod_{r=1}^{2k} \big(R_{g^r}(G_1) R_{g^{r-1}}(G_1) \ldots R_g(G_1)\big)(w),$$

for each w in $H(G_1)$. Of course, the result of the Lemma now gives us that $f_{G_1}(w) \in \bigcap_{j=0}^{k-1} H_{g^j}(G_1)$ for all w in $H(G_1)$. In order to facilitate discussion of this type of result, we shall define an *$H(G)$-formula* f to be an element $f = (\phi_1, \ldots, \phi_n)$ of $\mathcal{G}(G)^n$, for any positive integer n; the corresponding *$H(G)$-function* $f_G : H(G) \longrightarrow H(G)$ is then given by $f_G(w) = \prod_{i=1}^{n} \phi_i(w)$. Each $H(G)$-formula can be regarded, via the embedding of $\mathcal{G}(G)$ in $\mathcal{G}(G_1)$, as an *$H(G_1)$-formula*, with corresponding $H(G_1)$-function f_{G_1}, and f_{G_1} restricted to $H(G)$ is just f_G again.

If $f = (\phi_1, \ldots, \phi_n)$ and $h = (\mu_1, \ldots, \mu_m)$ are $H(G)$-formulas, then we define the product hf to be the formula

$$hf = \big(\mu_1(\phi_1, \ldots, \phi_n), \mu_2(\phi_1, \ldots, \phi_n), \ldots, \mu_m(\phi_1, \ldots, \phi_n)\big),$$

where $\mu(\phi_1, \ldots, \phi_n) = (\mu\phi_1, \ldots, \mu\phi_n)$. In other words, hf is the element of $\mathcal{G}(G)^{mn}$ with *rth* entry $\mu_i\phi_j$ if $r = (i-1)n+j$, with $1 \leqq i \leqq m$ and $1 \leqq j \leqq n$. It is not difficult to check that this product is associative, and that the function $(hf)_G$ is just the composition $h_G f_G$.

We shall require one more result concerning the functions f_G, namely that each $H(G)$-function f_G induces a corresponding function, denoted by f'_G, on the commutator quotient group $H(G)/H(G)'$, and f'_G is an endomorphism of this abelian group. In fact, if $f = (\phi_1, \ldots, \phi_n)$ is the formula affording f_G, then it is clear that each ϕ_i induces a corresponding automorphism ϕ'_i of $H(G)/H(G)'$, and then f'_G is just the (usual) sum of the ϕ'_i.

3. **The main result.** In order to state our main result, we need the concept of a *coherence-formula* f for G; by this we mean an $H(G)$-formula f and a positive integer $n = n(f)$ such that whenever G is embedded in G_1 we have

https://doi.org/10.4153/CMB-1990-080-1 Published online by Cambridge University Press

(a) $f_{G_1}(w) \in \bigcap_{g\in G} H_g(G_1)$ for all $w \in H(G_1)$,

and, for each $x \in G_1$,

(b1) $f'_{G_1}(\alpha_x) = \prod_{g\in G}\left(\alpha_{xg}\beta_{xg}^{-1}\right)^n$ (modulo $H(G_1)'$)

and

(b2) $f'_{G_1}(\beta_x) = \prod_{g\in G}\left(\beta_{xg}\alpha_{xg}^{-1}\right)^n$ (modulo $H(G_1)'$).

It is easily checked that the formula given in Lemma 3 is a coherence-formula for the cyclic group $\langle g\rangle$ generated by g. In general, if G has a coherence-formula f then (taking $G = G_1$ above) we see that G has finite coherence number, and $c(G)$ divides $n(f)$.

We can now state our main result.

THEOREM. *Let f be a coherence-formula for the finite group G, and suppose L is an extension of G with $[L : G] = 2$. Then, for any z in $L - G$, $\gamma = f\ell_z f$ is a coherence-formula formula for L, with $n(\gamma) = \{n(f)\}^2|G|$.*

PROOF. Let G_1 be a finite extension of L. We have to verify (a) and (b) above for $\gamma_{G_1} = f_{G_1}\ell_z f_{G_1}$. Taking $w \in H(G_1)$, we have

$$f_{G_1}(w) \in \bigcap_{g\in G} H_g(G_1).$$

Now we note that $\ell_x(\alpha_g\beta_{gy}^{-1}) = \alpha_{gx^{-1}}\beta_{gy}^{-1}$, and it follows that ℓ_x maps $H_y(G_1)$ to $H_{xy}(G_1)$, for each $x, y \in G_1$, so that, in particular,

$$\ell_z f_{G_1}(w) \in \bigcap_{g\in G} H_{zg}(G_1) = \bigcap_{g\in G} H_{gz}(G_1).$$

Similar observations show that $r_x(H_y) = H_{yx^{-1}}$, $s_x(H_y) = H_{xy^{-1}x}$ and $I(H_y) = H_y$. If we let $W = \bigcap_{g\in G} H_{gz}(G_1)$ then taking $x \in G$ and $y = gz$ we see that W is fixed by each of ℓ_x, r_x, s_x and I. Since f is an $H(G)$-formula, we have $f_{G_1}(u) \in W$ whenever $u \in W$, since $f_{G_1}(u)$ is expressible in terms of $\ell_x(u)$, $\tau_x(u)$, $s_z(u)$ and $I(u)$. It follows that $f_{G_1}\ell_z f_{G_1}(w) \in W$. We also have

$$f_{G_1}\left(\ell_z f_{G_1}(w)\right) \in \bigcap_{g\in G} H_g(G_1),$$

since f is a coherence-formula for G, and combining these results we see

$$f_{G_1}\ell_z f_{G_1}(w) \in \bigcap_{g\in L} H_g(G_1),$$

so that $\gamma = f\ell_z f$ satisfies condition (a) above.

Next, working modulo $H(G_1)'$, we have

$$f'_{G_1}(\alpha_x) = \prod_{g\in G}\left(\alpha_{xg}\beta_{xg}^{-1}\right)^n$$

and

$$f'_{G_1}(\beta_x) = \prod_{g\in G}\left(\alpha_{xg}^{-1}\beta_{xg}\right)^n,$$

https://doi.org/10.4153/CMB-1990-080-1 Published online by Cambridge University Press

where $n = n(f)$ and x is any element of G_1. Thus

$$\ell_z' f_{G_1}'(\alpha_x) = \prod_{g \in G} \left(\alpha_{xgz^{-1}} \beta_{xg}^{-1} \right)^n ,$$

so that

$$\begin{aligned} f_{G_1}' \ell_z' f_{G_1}'(\alpha_x) &= \prod_{g \in G} \prod_{h \in G} \left(\alpha_{xgz^{-1}h}^{n^2} \beta_{xgz^{-1}h}^{-n^2} \alpha_{xgh}^{n^2} \beta_{xgh}^{-n^2} \right) \\ &= \prod_{y \in L} \left(\alpha_{xy} \beta_{xy}^{-1} \right)^{n^2|G|} , \end{aligned}$$

since $z \in L - G$. This verifies that condition (b1) above is satisfied by γ, with $n(\gamma) = n^2|G|$, and a similar computation verifies (b2) holds for this same value. This proves the theorem.

As an application, we obtain

COROLLARY. *Let L be a finite group. We have*
(a) If $L = D_k$ then $c(L)$ divides k.
(b) If $|L| = 2^k$ then $c(L)$ divides $2^{2^k - k - 1}$.

PROOF. For part (a) we note that L has a cyclic subgroup G of index two. Now G has a coherence-formula f with $n(f) = 1$, so L has a coherence-formula γ with $n(\gamma) = k$, as required.

Now suppose $|L| = 2^k$, with $k \geqq 1$. We use induction on k to prove that L has a coherence-formula γ with $n(\gamma) = x^{2^k - k - 1}$. This is certainly the case if $k = 1$, so we suppose that $k > 1$. Then L has a subgroup G of index two, and G has a coherence-formula f with $n(f) = 2^{2^{k-1} - k}$. Hence, by the theorem, L has a coherence-formula γ with

$$n(\gamma) = \{n(f)\}^2 |G| = \left\{ 2^{2^{k-1} - k} \right\}^2 2^{k-1} = 2^{2^k - k - 1} ,$$

as required. This proves the result.

REFERENCES

1. R. C. Lyndon and P.E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, New York, 1977.
2. W. J. Ralph, *The coherence number of a finite group*, J. Algebra **126** (1989), 61–79.

Department of Mathemtics
University of Toronto
Toronto, M5S 1A1, Canada

https://doi.org/10.4153/CMB-1990-080-1 Published online by Cambridge University Press