PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

PERMUTATIONAL AND REWRITABLE GROUPS

D. S. PASSMAN

Abstract. Permutational groups and rewritable groups were introduced in 1985 and 1988, respectively. In this note, we briefly survey key properties of these groups. In addition, we consider certain related parameters and we compute a number of examples of interest.

1. Introduction

Let G be a multiplicative group. Following [CLMR], G is said to satisfy the n-permutational property P_n if for all $g_1, g_2, \ldots, g_n \in G$ (in that order), there exists a nonidentity permutation $\pi \in \mathrm{Sym}_n$, depending on these elements, such that

$$g_1 g_2 \cdots g_n = g_{\pi(1)} g_{\pi(2)} \cdots g_{\pi(n)}.$$

Somewhat later, the n-rewritable property Q_n was introduced in [B]. Here G is said to have Q_n if for all $g_1, g_2, \ldots, g_n \in G$, there exist two distinct permutations $\sigma, \tau \in \mathrm{Sym}_n$, depending on these elements, such that

$$g_{\sigma(1)} g_{\sigma(2)} \cdots g_{\sigma(n)} = g_{\tau(1)} g_{\tau(2)} \cdots g_{\tau(n)}.$$

Obviously, P_n implies Q_n, but examples in [B] show that the reverse implication is not true in general. One of the goals of the next section is to show that $G = \mathrm{Sym}_n$ also affords such an example.

Now it is clear that property P_n implies P_{n+1} and that property Q_n implies Q_{n+1}. Thus for any group G with these properties it makes sense to define the *permutational degree* $p(G) = \min\{n \mid G \text{ has } P_n\}$ and the *rewritable degree* $q(G) = \min\{n \mid G \text{ has } Q_n\}$.

There are two key results from [CLMR] which show that certain groups have the permutational property. For convenience, we include their short but clever proofs. The following contains the obvious fact that any abelian group satisfies P_2.

Lemma 1.1. *If the commutator subgroup G' of G is finite of order n, then G satisfies the property P_{n+1}.*

Proof. Let $g = g_0 g_1 \cdots g_n$ be a product of $n+1$ elements of G and, for each $i = 0, 1, \ldots, n$, write this product as $\alpha_i \beta_i$ where $\alpha_i = g_0 g_1 \cdots g_i$ is the product of its initial segment and $\beta_i = g_{i+1} \cdots g_{n-1} g_n$ is its final product. Of course, $\beta_n = 1$. Now let β_i^* be the product of the factors of β_i in the opposite order, so that $\beta_i^* = g_n g_{n-1} \cdots g_{i+1}$, and note that $\beta_i^* \alpha_i$ is a product of the elements

2010 *Mathematics Subject Classification.* 20E25, 20B30, 16S34.

Key words and phrases. permutational groups, rewritable groups, finite conjugate center, group algebras, polynomial identities.

Research support in part by NSF grant DMS 1712663.

$g_0, g_1, \ldots, g_n$ in some permuted order. In particular, $\beta_i^* \alpha_i$ is congruent to g modulo G' and hence these $n+1$ elements are all contained in the same coset of G'. But the cosets of G' all have size $|G'| = n$ and hence at least two of these $n+1$ elements must be equal, say $\beta_i^* \alpha_i = \beta_j^* \alpha_j$ for some $i < j$. For simplicity, write $\alpha = \alpha_i$, $\beta = \beta_j$ and $\gamma = g_{i+1} \cdots g_j$. Then $\alpha_j = \alpha\gamma$, $\beta_i = \gamma\beta$ and $\beta_i^* = \beta^*\gamma^*$, so $\beta^*\gamma^*\alpha = \beta_i^*\alpha_i = \beta_j^*\alpha_j = \beta^*\alpha\gamma$. Thus $\gamma^*\alpha = \alpha\gamma$ and $g = \alpha\gamma\beta = \gamma^*\alpha\beta$. Since γ and α are nonempty products, the latter is a nontrivial permutation of the factors of g and hence G satisfies P_{n+1}. □

Next, we have

Lemma 1.2. *Let H be a subgroup of G of finite index a. If H satisfies P_b, then G satisfies P_{ab}. Similarly, if H satisfies Q_b, then G satisfies Q_{ab}. In particular, if H is abelian, then G satisfies P_{2a}.*

Proof. Let $g = g_1 g_2 \cdots g_{ab}$ be a product of ab elements of G and consider the $ab+1$ initial products $\alpha_i = g_1 g_2 \cdots g_i$ with $0 \le i \le ab$ and $\alpha_0 = 1$. Since H has precisely a left cosets in G, some left coset xH must contain at least $b+1$ of these initial products. Now suppose α_i and α_j with $i < j$ are both contained in xH and that they are adjacent with this property. If we write $\gamma = g_{i+1} \cdots g_j$, then $\alpha_j = \alpha_i \gamma$ implies that $\gamma \in H$. It follows that the product g contains b nonempty adjacent products each of which is contained in H. In particular, if H satisfies P_b, then this product of b segments is equal to a permuted product of these segments, and hence G satisfies P_{ab}. On the other hand, if H satisfies Q_b, then there are two permuted products of these b segments that are equal, and hence G satisfies Q_{ab}. □

The above result with H abelian goes back to the 1949 paper [K]. Now groups with properties P_n or Q_n were characterized to some extent in references [CLMR], [B] and [EP]. To start with, the *F.C.* or *finite conjugate center* of a group G is defined by

$$\Delta(G) = \{x \in G \mid |G : \mathcal{C}_G(x)| < \infty\}.$$

Thus $\Delta(G)$ is the set of elements of G having only finitely many G-conjugates, and hence it is a characteristic subgroup of G containing the center $\mathcal{Z}(G)$. Next, a result of [CLMR] asserts that if G has property P_n, then $|G : \Delta(G)| \le f(n)$, for some function $f(n)$, and furthermore the commutator subgroup $\Delta(G)'$ is finite. Of course, if G itself is finite, then $G = \Delta(G)$, so this result really offers no information about the group. Indeed, one cannot hope to bound $|\Delta(G)'|$ as a function of n. For example, let $G = A \rtimes X$ be a finite dihedral group with A abelian of odd order and $|X| = 2$. Then by the previous lemma, G satisfies P_4, and yet $G' = A$ can be arbitrarily large. Fortunately, there is a sharper result in [EP] based on the polynomial identity methods of [P]. Specifically, we have

Theorem 1.3. *There exist integer valued functions $a(n)$ and $b(n)$ with the following property. If G is a group satisfying P_n, then G has a characteristic subgroup $N \subseteq \Delta(G)$ with $|G : N| \le a(n)$ and $|N'| \le b(n)$.*

The functions given here are quite big and hence not particularly useful. Indeed, starting with n, we set $k = n!$, $\ell = k \cdot (k+1)!$ and $m = k^{4^\ell}$. Then $a(n) = \ell$ and $b(n) = (m^4)^{m^4}$. Note that N is generated by all elements of G having at most $k = n!$ conjugates under the action of G.

The situation with the rewritable property is similar, but much more difficult. Fortunately [B] was able to show that if G satisfies Q_n then $|G : \Delta(G)| \leq \bar{f}(n)$ for some function $\bar{f}(n)$, and $|\Delta(G)'|$ is finite. Again, this yields no information when G is finite, but the methods of [B] and [P] combine in [EP] to yield

Theorem 1.4. *There exist integer valued functions $\bar{a}(n)$ and $\bar{b}(n)$ with the following property. If G is a group satisfying Q_n, then G has a characteristic subgroup $N \subseteq \Delta(G)$ with $|G : N| \leq \bar{a}(n)$ and $|N'| \leq \bar{b}(n)$.*

The functions here are exponentially larger than those for property P_n, and the subgroup N is defined in a similar manner. To understand how these results fit into the general theory, we briefly prove the following corollary from [EP], that was a conjecture of [B].

Corollary 1.5. *There exists an integer valued function $\bar{c}(n)$ with the following property. If G is a group satisfying the rewritable property Q_n, then G satisfies the permutational property $P_{\bar{c}(n)}$.*

Proof. Since G satisfies Q_n it has the structure of the preceding theorem. Then, by Lemma 1.1, the subgroup N has property $P_{\bar{b}(n)+1}$, and it follows from Lemma 1.2 that G satisfies $P_{\bar{c}(n)}$ where

$$\bar{c}(n) = \bar{a}(n) \cdot (\bar{b}(n) + 1).$$

This is obviously a converse of sorts to the simple fact that P_n implies Q_n. □

2. The Rewritable Degree

The remainder of this note is concerned with finite examples of interest. We start with symmetric groups. For this, we first need the following rewritable analog of Lemma 1.1 that comes from paper [B].

Lemma 2.1. *Let G be a group with $|G'| < n!$. Then G satisfies Q_n.*

Proof. Let $g_1, g_2, \ldots, g_n \in G$ be given and consider the $n!$ permuted products $\alpha_\sigma = g_{\sigma(1)} g_{\sigma(2)} \cdots g_{\sigma(n)}$ with $\sigma \in \mathrm{Sym}_n$. These elements are clearly all congruent modulo G' and hence they are contained in the same coset of G'. But all such cosets have size $|G'| < n!$ and hence there must exist two distinct permutations σ and τ with $\alpha_\sigma = \alpha_\tau$. Thus G satisfies Q_n. □

Next we study the permutational property as applied to the symmetric group. To fix notation, let $G = \mathrm{Sym}_n$ act on the right on the set $\{1, 2, \ldots, n\}$. Thus we multiply the elements of G from left to right. If $A = \{a_1, a_2, \ldots, a_k\}$ is a subset of $\{2, 3, \ldots, n\}$ then the product of the k transpositions $(1, a_1), (1, a_2), \ldots, (1, a_k)$ in that order is equal to the $(k+1)$-cycle $(1, a_1, a_2, \ldots, a_k)$. For convenience, we denote this product by $(1, A)$ and use $(1, A) = 1$ if A is the empty set. Obviously this product depends on the ordering of the elements of A, and conversely the $(k+1)$-cycle $(1, A)$ uniquely determines the order of the k factors.

The $n = 3$ case of the following can be found in [B]. Of course, $Q_2 = P_2$.

Theorem 2.2. *Let $G = \mathrm{Sym}_n$ with $n \geq 3$. Then G satisfies Q_n but not P_n.*

Proof. Since $|G'| < n!$, it follows from the preceding lemma that G satisfies Q_n. The hard part is to show that G does not satisfy P_n. To this end, let σ be the n-cycle $(1, 2, \ldots, n) \in G$. We think of σ as the plus map so that $a\sigma = a^+$, where

of course $a^+ \equiv a+1 \bmod n$. Obviously, $\sigma^{-1} = (n, \ldots, 2, 1)$ can be viewed as the minus map so that $a\sigma^{-1} = a^- \equiv a-1 \bmod n$.

Now consider the n elements of G given in order by $\sigma, (1,3), (1,4), \ldots, (1,n), \sigma^{-1}$. Notice that there are $n-2$ transpositions and the two additional n-cycles. The product of these elements in their natural order is

$$\sigma(1,3)(1,4)\cdots(1,n)\sigma^{-1} = \sigma(1,3,4,\ldots,n)\sigma^{-1} = (2,3,4,\ldots,n)$$

and we denote the latter $(n-1)$-cycle by τ. The goal is to show that if a permuted product of these n group elements is equal to τ, then the factors must be in their natural order.

So suppose g is a product of the n elements in some order and that $g = \tau$. By considering where σ and σ^{-1} appear in the product, we can write the product g, grouped into five factors, as $g = \alpha\sigma^{\pm}\beta\sigma^{\pm}\gamma$, where α, β and γ are suitable products of the transpositions. Indeed, $\alpha = (1, A)$, $\beta = (1, B)$ and $\gamma = (1, C)$, where A, B and C are disjoint sets that union to $S = \{3, 4, \ldots, n\}$. Note that the disjointness implies that α fixes all points in $B \cup C$, β fixes all points in $A \cup C$, and γ fixes all points in $A \cup B$. There are three cases to consider, namely (1) $B = \emptyset$, (2) $B \neq \emptyset$ and $g = \alpha\sigma^{-1}\beta\sigma\gamma$, and (3) $B \neq \emptyset$ and $g = \alpha\sigma\beta\sigma^{-1}\gamma$. We study these in turn.

Case 1. Here σ and σ^{-1} are adjacent, so these factors cancel. Thus we have $g = (1, A)(1, B)(1, C) = (1, S)$. But $2 \notin S$, so g fixes point 2 and hence $g \neq \tau$.

Case 2. Here B is nonempty and the σ, σ^{-1} factors occur in the wrong order. We show that B is closed under the minus operation. To this end, suppose $b \in B$, but $b^- \notin B$. Then $b^- \notin B \cup \{1\}$ since $2 \notin B$, and thus $\beta = (1, B)$ fixes b^-. Now α and γ fix $b \in B$ so, by considering the five factors of g, we see that the action of g on b is given by $b \mapsto b \mapsto b^- \mapsto b^- \mapsto b \mapsto b$. In other words, $bg = b$. But $g = \tau$ fixes only the point 1, and $1 \notin B$, contradiction.

We conclude that $B^- \subseteq B$. Since B is nonempty, we can start with an element $b \in B$ and get $b^- \in B$. Continuing in this manner with $b^- \in B$, we see finally that $3 \in B$. But then $3^- = 2 \in B$, and this is again a contradiction. Thus only case (3) can occur.

Case 3. Here $g = \alpha\sigma\beta\sigma^{-1}\gamma = (1, A)\sigma(1, B)\sigma^{-1}(1, C)$ and our first goal is to show that $A = C = \emptyset$ or equivalently that $B = S$. To this end, suppose first that $3 \notin B$. Then β fixes point 3 and of course α and γ fix 2 since $2 \notin S$. Thus, the action of g on 2 is given by $2 \mapsto 2 \mapsto 3 \mapsto 3 \mapsto 2 \mapsto 2$ and $2g = 2$. But $g = \tau$ does not fix 2, so this is a contradiction and $3 \in B$.

Next, we show that $B^+ \subseteq B \cup \{1\}$. Suppose by way of contradiction that $b \in B$ and $b^+ \notin B \cup \{1\}$. Then the latter implies that $\beta = (1, B)$ fixes b^+. Thus since α and γ fix $b \in B$, the action of g on b is given by $b \mapsto b \mapsto b^+ \mapsto b^+ \mapsto b \mapsto b$ and $bg = b$. But $g = \tau$ fixes only point 1 and $1 \notin B$, so we have the required contradiction. Hence $B^+ \subseteq B \cup \{1\}$.

Now $3 \in B$, so $4 = 3^+ \in B$ and $5 = 4^+ \in B$. Continuing in this manner, we conclude that $\{3, 4, \ldots, n\} \subseteq B$. Thus $B = S$ and $A = C = \emptyset$. It follows that $g = \sigma(1, S)\sigma^{-1} = \tau$, so $(1, S) = \sigma^{-1}\tau\sigma = (1, 3, 4, \ldots, n)$, and therefore the factors in S must be in their natural order. In other words, if $g = \tau$ then the n factors of g necessarily appear in their natural order and hence G does not satisfy P_n. $\square$

Now we show that for every $n \geq 2$ there exists a finite group with rewritable degree n. Indeed,

Lemma 2.3. *For $n \geq 2$, we have $q(\mathrm{Sym}_n) = n$.*

Proof. As we observed above, $G = \mathrm{Sym}_n$ has property Q_n, and this holds even for $n = 2$. On the other hand, consider the $n-1$ transpositions $(1,2), (1,3), \ldots, (1,n)$. Then we know that any product of these elements in any order is an n-cycle and that this n-cycle uniquely determines the order of the factors. Thus G does not satisfy Q_{n-1}. □

We now consider another context where P_n occurs. We do this by introducing some ring theory into the problem. Let A be an algebra over a field F. Then following [K], we say that A satisfies a *polynomial identity* if there exists $0 \neq f(\zeta_1, \zeta_2, \ldots, \zeta_n)$ in the free algebra $F\langle \zeta_1, \zeta_2, \ldots \rangle$ such that $f(a_1, a_2, \ldots, a_n) = 0$ for all $a_1, a_2, \ldots, a_n \in A$. Thus, for example, A is commutative if and only if it satisfies $f = \zeta_1\zeta_2 - \zeta_2\zeta_1$. In the special case where $A = F[G]$ is the group algebra of G over F, we obtain a relationship between polynomial identities and permutational groups.

Lemma 2.4. *If $A = F[G]$ satisfies a polynomial identity of degree n, then the group G has property P_n.*

Proof. It was shown in [K] that, for any A, the given polynomial identity f of degree n can be linearized so that f has the form

$$f(\zeta_1, \zeta_2, \ldots, \zeta_n) = \sum_{\sigma \in \mathrm{Sym}_n} c_\sigma \zeta_{\sigma(1)} \zeta_{\sigma(2)} \cdots \zeta_{\sigma(n)}$$

with coefficients $c_\sigma \in F$. Furthermore, we can assume that $c_1 \neq 0$. Now $G \subseteq A = F[G]$ so we can plug $g_1, g_2, \ldots, g_n \in G$ into the above f and get $0 = f(g_1, g_2, \ldots, g_n)$. But then the nonzero term $c_1 g_1 g_2 \cdots g_n$ must be cancelled by some other summands $c_\pi g_{\pi(1)} g_{\pi(2)} \cdots g_{\pi(n)}$, where $g_1 g_2 \cdots g_n = g_{\pi(1)} g_{\pi(2)} \cdots g_{\pi(n)}$, and therefore G satisfies P_n. □

Group algebras satisfying a polynomial identity were characterized in the 1972 paper [P] and, as we pointed out, the techniques from that paper were used in [EP] to prove Theorems 1.3 and 1.4. We can also use the above lemma along with the Amitsur-Levitzky theorem [AL] to show that certain finite groups satisfy P_n. To this end, we note that the *standard identity* of degree n is defined by

$$s_n(\zeta_1, \zeta_2, \ldots, \zeta_n) = \sum_{\sigma \in \mathrm{Sym}_n} (-1)^\sigma \zeta_{\sigma(1)} \zeta_{\sigma(2)} \cdots \zeta_{\sigma(n)}.$$

In particular, s_n is linear in each of its n variables and behaves somewhat like the determinant function.

Now for any finite group G, let $d(G)$ be the largest degree of an irreducible representation of the complex group algebra $\mathbb{C}[G]$. Properties of these degrees can be found in [I]. For example. $d(G)$ divides $|G|$, $d(G) \leq |G : H|$ if H is an abelian subgroup of G, and $d(G) \leq \sqrt{|G : Z|}$ where $Z = \mathcal{Z}(G)$ is the center of G.

Then we have

Lemma 2.5. *Let G be a finite group with $d = d(G)$. Then G satisfies the permutational property P_{2d}. In particular, if $G \neq 1$, then $p(G) < 2\sqrt{|G|}$.*

Proof. Since $\mathbb{C}[G]$ is semisimple and finite dimensional, the Wedderburn theorem implies that $\mathbb{C}[G] = \oplus \sum_i M_{d_i}(\mathbb{C})$, a direct sum of matrix rings of various degrees d_i at most equal to d. Since the group algebra has dimension equal to $|G|$, we see that $d^2 \leq \sum_i d_i^2 = |G|$, and in particular, $d \leq \sqrt{|G|}$. Furthermore, we have strict inequality for $|G| > 1$ since G has the principal representation of degree 1. Now, it follows from [AL] that each matrix ring $M_{d_i}(\mathbb{C})$ satisfies the standard polynomial identity s_{2d} and hence $\mathbb{C}[G]$ satisfies s_{2d}. Lemma 2.4 now yields the result. □

One wonders whether the $p(G)$ upper bound of this lemma can be proved group theoretically without using the ring theoretic Amitsur-Levitzky theorem.

As a consequence, we get the following rather weak inequality for $p(\mathrm{Sym}_n)$, namely

Proposition 2.6. *For $n \geq 3$, we have $n + 1 \leq p(\mathrm{Sym}_n) < 2\sqrt{n!}$.*

Proof. Since $G = \mathrm{Sym}_n$ does not satisfy P_n, we have $p(G) \geq n + 1$. On the other hand, the previous lemma implies that $p(G) < 2\sqrt{|G|} = 2\sqrt{n!}$. □

Obviously, much more work needs to be done here.

3. The Permutational Degree

Finally, we consider some solvable group examples. The following is a reinterpretation of an example from [B].

Lemma 3.1. *Let $n \geq 1$ be an integer. Then there exists a finite solvable group G such that G satisfies P_{2n} but not P_n. Thus $n < p(G) \leq 2n$.*

Proof. Choose an integer $k > n$ and let $A = \langle a \rangle$ be the cyclic group of order $k^n - 1$. Since k is prime to $|A|$, it follows that the kth power map σ is an automorphism of A. Indeed, since $a^{k^n} = a$, but $a^{k^{n-1}} \neq a$, this automorphism has order precisely equal to n. Thus we can let x be an element of order n that acts on A via σ and we set $G = A \rtimes \langle x \rangle$. In other words, in G we have $x^{-1}ax = a^x = a^k$. Since A is an abelian subgroup of G of index n, we see from Lemma 1.2 that G satisfies P_{2n}.

We show now that G does not satisfy P_n. To this end, consider the n elements of G given by $g_0 = a^0x^{-1}, g_1 = a^1x^{-1}, \ldots, g_{n-1} = a^{n-1}x^{-1}$. Then their product in the natural order is

$$\begin{aligned} g = g_0g_1 \cdots g_{n-1} &= a^0x^{-1} \cdot a^1x^{-1} \cdot a^2x^{-1} \cdots a^{n-1}x^{-1} \\ &= a^0(a^1)^x(a^2)^{x^2} \cdots (a^{n-1})^{x^{n-1}} \cdot x^{-n} = a^r \end{aligned}$$

where

$$r = 0 \cdot k^0 + 1 \cdot k^1 + 2 \cdot k^2 + \cdots + (n-1) \cdot k^{n-1}.$$

Notice that since $n < k$, the above uniquely describes the positive integer r in base k and $r < k^n - 1$.

Now consider an arbitrary product of the g_i factors given by

$$\begin{aligned} h = g_{i_0}g_{i_1} \cdots g_{i_{n-1}} &= a^{i_0}x^{-1} \cdot a^{i_1}x^{-1} \cdot a^{i_2}x^{-1} \cdots a^{i_{n-1}}x^{-1} \\ &= a^{i_0}(a^{i_1})^x(a^{i_2})^{x^2} \cdots (a^{i_{n-1}})^{x^{n-1}} \cdot x^{-n} = a^s \end{aligned}$$

where

$$s = i_0 \cdot k^0 + i_1 \cdot k^1 + i_2 \cdot k^2 + \cdots + i_{n-1} \cdot k^{n-1}.$$

Again this describes the positive integer s uniquely in base k and $s < k^n - 1$. In particular, $g = h$ implies that $a^r = a^s$ so $r \equiv s \bmod k^n - 1$. Thus $r = s$ and uniqueness implies that $i_0 = 0, i_1 = 1, \ldots, i_{n-1} = n-1$ so h must be written in the natural order. It follows that G does not satisfy P_n. □

Next we extend this argument to a slightly more complicated situation.

Proposition 3.2. *Let $n \geq 1$ be an integer. Then there exists a finite solvable group G such that G satisfies P_{2n} but not P_{2n-1}. Thus $p(G) = 2n$.*

Proof. Choose an integer k so that $k > 1+2+\cdots+n = n(n+1)/2$ and let $A = \langle a \rangle$ and $B = \langle b \rangle$ be cyclic groups of order $k^n - 1$. Since k is prime to $|A| = |B|$, it follows that the kth power map σ is an automorphism of both A and B and hence of the direct product $A \times B$. Again, this automorphism has order n, so we can let x be an element of order n acting on $A \times B$ via σ and we let $G = (A \times B) \rtimes \langle x \rangle$ be the semidirect product of the abelian group $A \times B$ by the cyclic group $\langle x \rangle$ of order n. Since $[G : A \times B] = n$, it follows from Lemma 1.2 that G satisfies P_{2n}.

We show that G does not satisfy P_{2n-1}. To this end consider the $2n-1$ elements of G given by $g_1 = a^1x^{-1}, g_2 = a^2x^{-1}, \ldots, g_{n-1} = a^{n-1}x^{-1}$ and $h_1 = b^1, h_2 = b^2, \ldots, h_n = b^n$. Notice that $g_n = a^nx^{-1}$ is missing here and we will see later on the reason for this. We order these $2n-1$ elements as

$$h_1, g_1, h_2, g_2, \ldots, h_{n-1}, g_{n-1}, h_n$$

and note that their product in the given order is equal to

$$\begin{aligned} g &= (b^1a^1)x^{-1}\cdot(b^2a^2)x^{-1}\cdot(b^3a^3)x^{-1}\cdots(b^{n-1}a^{n-1})x^{-1}\cdot b^n \\ &= (b^1a^1)\cdot(b^2a^2)^x\cdot(b^3a^3)^{x^2}\cdots(b^{n-1}a^{n-1})^{x^{n-2}}\cdot(b^n)^{x^{n-1}}\cdot x^{-(n-1)} \\ &= a^rb^s\cdot x^{-(n-1)} \end{aligned}$$

where

$$r = 1k^0 + 2k^1 + 3k^2 + \cdots + (n-1)k^{n-2}$$

and

$$s = 1k^0 + 2k^1 + 3k^2 + \cdots + (n-1)k^{n-2} + nk^{n-1}.$$

Since $k > n(n+1)/2 \geq n$, both of these expressions uniquely describe the integer in base k and $r, s < k^n - 1$.

Now consider an arbitrary product h of the $2n-1$ elements and suppose $g = h$. Then by considering the situation in $G/B \cong A \rtimes \langle x \rangle$, the argument of the previous lemma shows that the g_i factors in h must occur in their natural order. Thus

$$h = *g_1 * g_2 * \cdots * g_{n-1}*$$

where the $*$'s indicate products of elements from the set $\{b^1, b^2, \ldots, b^n\}$. In other words,

$$h = b^{\lambda_1}g_1b^{\lambda_2}g_2b^{\lambda_3}\cdots b^{\lambda_{n-1}}g_{n-1}b^{\lambda_n}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are sums of disjoint subsets of the set of exponents $\{1, 2, \ldots, n\}$. In particular, each λ_i satisfies $0 \leq \lambda_i \leq 1 + 2 + \cdots + n < k$.

Now working in $G/A \cong B \rtimes \langle x \rangle$, or equivalently just looking at the x and b factors of h, we see that the image $\bar{h} \in G/A$ looks like

$$\begin{aligned}\bar{h} &= b^{\lambda_1} x^{-1} b^{\lambda_2} x^{-1} \cdots b^{\lambda_{n-1}} x^{-1} b^{\lambda_n} \\ &= b^{\lambda_1} (b^{\lambda_2})^x \cdots (b^{\lambda_{n-1}})^{x^{n-2}} (b^{\lambda_n})^{x^{n-1}} x^{-(n-1)} \\ &= b^{s'} x^{-(n-1)}\end{aligned}$$

where

$$s' = \lambda_1 k^0 + \lambda_2 k^1 + \cdots + \lambda_{n-1} k^{n-2} + \lambda_n k^{n-1}.$$

Again, this describes s' uniquely in its base k expression and $s' < k^n - 1$, the order of b. Thus since $g = h$, we have $b^s = b^{s'}$ and hence $s = s'$. Uniqueness now implies that $\lambda_i = i$ for each i. In particular, since each λ_i is nonzero, we see that each λ_i corresponds to a single h_i factor and we conclude that the g_i and h_i factors of h must appear in their natural order. We conclude that G does not satisfy P_{2n-1} and hence $p(G) = 2n$. □

Note that, in the above proof, if we allowed g to have an additional g_i factor, then s' would have a term involving k^n and this is larger than the order of b. Thus $b^{s'}$ would not uniquely determine s'.

Finally, we obtain the permutational degree analog of Lemma 2.3.

Theorem 3.3. *For every integer $n \geq 2$ there exists a finite solvable group G_n with $p(G_n) = n$.*

Proof. If $n = 2$, take G_2 to be any finite nonidentity abelian group. Now suppose $n \geq 3$ and set $m = n - 1 \geq 2$.

We first construct the group G_n. To start with, let A be the finite abelian group given by $A = A_1 \times A_2 \times \cdots \times A_{m-1} \times Z$, where each $A_i = \langle a_i \rangle$ is cyclic of order m and where $Z = \langle z \rangle$ is also cyclic of order m. Similarly, let $X = X_1 \times X_2 \times \cdots \times X_{m-1}$, where each $X_i = \langle x_i \rangle$ is cyclic of order m. For each $i = 1, 2, \ldots, m-1$ observe that A admits an automorphism σ_i given by $\sigma_i(a_i) = a_i z$, $\sigma_i(a_j) = a_j$ for $j \neq i$ and $\sigma_i(z) = z$. Indeed, it is easy to verify that each σ_i has order m and that σ_i and σ_j commute for all i, j. Thus we can let X act on A by having x_i act like σ_i. With this, we can now define G_n to be the semidirect product $G = A \rtimes X$. Since $G' = Z$ has order m, it follows from Lemma 1.1 that G satisfies $P_{m+1} = P_n$. Of course, Z is central in G.

We show now that G does not satisfy P_m. To this end consider the m elements of G given by $g_1 = a_1 x_1$, $g_2 = x_1^{-1} a_2 x_2$, $g_3 = x_2^{-1} a_3 x_3, \ldots, g_{m-1} = x_{m-2}^{-1} a_{m-1} x_{m-1}$ and $g_m = x_{m-1}^{-1}$, so that $g = g_1 g_2 \cdots g_m = a_1 a_2 \cdots a_{m-1}$. Now suppose that h is a product of these m elements in some random order. Then h and g are congruent modulo $G' = Z$, so $h = g z^e$ for some integer e and our first goal is to describe this integer. For this, consider the $m - 1$ pairs (x_i^{-1}, x_i) that occur in the product h. We say that the pair (x_i^{-1}, x_i) is "blocked" if a_i appears between the two factors and the pair is "unblocked" otherwise.

Suppose the pair (x_i^{-1}, x_i) is unblocked. Since x_i commutes with all of the generators of G other than a_i, we see that x_i^{-1} and x_i commute with all terms that appear between them in the product h. Thus x_i^{-1} and x_i can be moved, without changing h, until they are adjacent, and then $x_i^{-1} x_i = x_i x_i^{-1} = 1$ implies that they can be cancelled. In other words, an unblocked pair can just be cancelled in h.

On the other hand, if (x_i^{-1}, x_i) is blocked, then x_i and x_i^{-1} commute with all terms that appear between them other than a_i. Thus x_i^{-1} and x_i can be moved, without changing h, until they directly sandwich a_i. Since a_i occurs to the left of x_i in g_i, the sandwiched product must look like $x_i^{-1}a_ix_i = a_i^{x_i} = a_iz$. Thus in this blocked case, we can remove the pair (x_i^{-1}, x_i) provided we adjoin a factor of the central element z to h.

It follows from the above that the integer e is precisely equal to the number of blocked pairs in h. Indeed, since $0 \leq e \leq m-1$ and since z has order m, we see that the element z^e uniquely determines e.

In particular, if $h = g$ then $e = 0$ and h has no blocked pairs. It follows from this that the factor g_2 is to the right of g_1, g_3 is to the right of g_2, and so on. Thus the g_i factors must occur in their natural order in h, and we conclude that no nontrivially permuted product h can equal g. In other words, G does not satisfy P_m and hence $p(G) = m + 1 = n$. □

References

[AL] S. A. Amitsur and J. Levitzki, *Minimal identities for algebras*, Proc. AMS, **1** (1950), 449–463.

[B] R. D. Blyth, *Rewriting products of group elements, I*, J. Algebra, **116** (1988), 506-521.

[CLMR] M. Curzio, P. Longobardi, M. Maj, and D. J. S. Robinson, *A permutational property of groups*, Arch. Math., **44** (1985), 385-389.

[EP] M. I. Elashiry and D. S. Passman, *Rewritable groups*, J. Algebra, **345** (2011), 190–201.

[I] I. M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1994.

[K] I. Kaplansky, *Groups with representations of bounded degree*, Canad. J. Math., **1** (1949), 105–112.

[P] D. S. Passman, *Group rings satisfying a polynomial identity*, J. Algebra, **20** (1972), 103–117.

Department of Mathematics, University of Wisconsin-Madison, Madison, Wisconsin 53706, USA

E-mail address: passman@math.wisc.edu