THE LARGE DAVENPORT CONSTANT I: GROUPS WITH A CYCLIC, INDEX 2 SUBGROUP

ALFRED GEROLDINGER AND DAVID J. GRYNKIEWICZ

ABSTRACT. Let G be a finite group written multiplicatively. By a sequence over G, we mean a finite sequence of terms from G which is unordered, repetition of terms allowed, and we say that it is a product-one sequence if its terms can be ordered so that their product is the identity element of G. The *small Davenport constant* $\mathsf{d}(G)$ is the maximal integer ℓ such that there is a sequence over G of length ℓ which has no nontrivial product-one subsequence. The *large Davenport constant* $\mathsf{D}(G)$ is the maximal length of a minimal product-one sequence—this is a product-one sequence which cannot be factored into two nontrivial product-one subsequences. Otherwise put, $\mathsf{D}(G)$ is the maximal integer ℓ such that there is a product-one sequence S over G of length ℓ which has no nontrivial product-one subsequence T whose compliment sequence $T^{-1}S$ is also a nontrivial product-one subsequence. It is easily observed that $\mathsf{d}(G) + 1 \le \mathsf{D}(G)$, and if G is abelian, then equality holds. However, for non-abelian groups, these constants can differ significantly. Now suppose G has a cyclic, index 2 subgroup. Then an old result of Olson and White (dating back to 1977) implies that, with regards to the small Davenport constant, we have $\mathsf{d}(G) = \frac{1}{2}|G|$ if G is non-cylic, and $\mathsf{d}(G) = |G| - 1$ if G is cyclic. In this paper, we determine the large Davenport constant of such groups, showing that $\mathsf{D}(G) = \mathsf{d}(G) + |G'|$, where $G' = [G, G] \le G$ is the commutator subgroup of G.

1. Introduction and Main Result

Let G be a multiplicatively written finite group. A sequence S over G means a finite sequence of terms from G which is unordered, repetition of terms allowed. We say that S is a product-one sequence if its terms can be ordered so that their product equals 1, the identity element of the group. The *small Davenport constant* $\mathsf{d}(G)$ is the maximal integer ℓ such that there is a sequence over G of length ℓ which has no nontrivial product-one subsequence. The *large Davenport constant* $\mathsf{D}(G)$ is the maximal length of a minimal product-one sequence—this is a product-one sequence which cannot be partitioned into two nontrivial product-one subsequences. A simple argument (see Lemma 2.3) shows that

$$\mathsf{d}(G) + 1 \le \mathsf{D}(G) \le |G| \,.$$

Suppose for the moment that G is abelian. Then $\mathsf{d}(G) + 1 = \mathsf{D}(G)$ (see Section 2). The problem of finding the precise value of the Davenport constant and what is now know as the Erdős–Ginzburg–Ziv Theorem became the starting points of Zero-Sum Theory. Since that time (dating back to the early 1960s), it has developed into a flourishing branch of Additive and Combinatorial Number Theory (see the surveys [3, 5, 8] or the monographs [12, 10]). Apart from abelian groups, the Davenport constant has also been studied for finite abelian (non-cancellative) semigroups (see [18], [10, Proposition 2.8.13]).

2010 *Mathematics Subject Classification.* 20D60, 11B75.

Key words and phrases. zero-sum, product-one, Davenport constant, Cyclic Index 2 Subgroup.

This work was supported by the *Austrian Science Fund FWF* (Project No. P21576-N18).

Although the main focus of Zero-Sum Theory has been on abelian groups, research was never restricted to the abelian setting alone. To provide one example apart from the Davenport constant, let $\mathsf{E}(G)$ denote the smallest integer ℓ guaranteeing that every sequence S over G of length $|S| \ge \ell$ has a product-one subsequence of length $|G|$. Motivated by the classical Erdős–Ginzburg–Ziv Theorem, the study of $\mathsf{E}(G)$ has attracted much attention for non-abelian groups ([19, 1, 7, 6]). In all cases studied so far (abelian and non-abelian), it has turned out that $\mathsf{E}(G) = |G| + \mathsf{d}(G)$.

The Davenport constant was first introduced in the abelian setting by Rogers [17] (though Davenport was more famous for promoting it) in the context of its relation to Algebraic Number Theory. Here there is no difference between the combinatorially defined small davenport constant $\mathsf{d}(G) + 1$ and the monoid theoretic large Davenport Constant $\mathsf{D}(G)$. Later work expanded the role of the Davenport constant in relation to factorization problems over algebraic number rings and, more generally, Krull monoids; see [10]. In this setting, the definition of the large Davenport constant is the more natural one. The first attempts to study a Davenport constant in a non-abelian setting were carried out by Olson and White [15], who defined the small Davenport constant of a non-abelian group and gave a general upper bound that was shown to be tight for groups having a cyclic, index 2 subgroup; see Theorem 3.1. However, the definition of the small Davenport constant is not as fully satisfying in this setting. The first reason for this is simple: there is no monoid factorization interpretation of the small Davenport constant over a non-abelian group. The second reason for this regards Invariant Theory. Let G be a group, let $\mathbb{F}$ be a field whose characteristic does not divide $|G|$, and let $\beta(G)$ denote the maximal degree of an invariant polynomial in a minimal generating set of the invariant ring $\mathbb{F}[V]^G$. When G is abelian, the algebraically defined constant $\beta(G)$ is equal to $\mathsf{d}(G)+1$. However, when G is non-abelian, there are examples in which $\beta(G) > \mathsf{d}^*(G) + 1$ [14] [11].

In view of both these issues, we have defined the large Davenport constant simply by taking the natural monoid theoretic definition and extending it to non-abelian groups. This results in a constant with a monoid factorization interpretation which is also larger than $\mathsf{d}(G) + 1$, thus leaving open later potential use as an upper bound for $\beta(G)$. Our main result is the following theorem, in which we parallel the early result of Olson and White that determined the small Davenport constant of a finite group having a cyclic, index 2 subgroup, by instead determining the large Davenport constant for all such groups. Note that Theorem 1.1 covers dihedral groups, semi-dihedral groups, and generalized quaternion or dicyclic groups, as well as many more. Building upon the results of this paper, we will give more general upper bounds for $\mathsf{D}(G)$ in a sequel [9].

Theorem 1.1. *Let G be a finite group having a cyclic, index 2 subgroup. Then*

$$\mathsf{D}(G) = \mathsf{d}(G) + |G'| \quad \text{and} \quad \mathsf{d}(G) = \begin{cases} |G| - 1 & \text{if } G \text{ is cyclic} \\ \frac{1}{2}|G| & \text{if } G \text{ is non-cyclic,} \end{cases}$$

where $G' = [G, G] \le G$ is the commutator subgroup of G.

The paper is divided as follows. In Section 2, we introduce and adapt notation used for sequences and sumsets over abelian groups and prove several basic facts. In Section 3, we give some general upper bounds that can be used in conjugation with inductive arguments. Section 4 deals entirely with classical results for abelian groups, needed for later proofs, and the proof of one axillary lemma needed for handling

dicyclic groups. The main bulk of the proof of Theorem 1.1 is then carried out in Section 5, beginning with an overview of the possible isomorphism classes of groups having a cyclic, index 2 subgroup.

2. Notation and Preliminaries

All intervals will be discrete, so for real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} : \ a \le x \le b\}$. If A and B are subsets, then whenever addition or multiplication between elements of A and B is allowed, we define their sumset and product-set as

$$A + B = \{a + b : \ a \in A, \, b \in B\} \qquad \text{and} \qquad AB = \{ab : \ a \in A, \, b \in B\}.$$

Of course, we use the abbreviations $A + g = \{a + g : \ a \in A\}$, $Ag = \{ag : \ a \in A\}$ and $gB = \{gb : \ b \in B\}$ when dealing with a single element g for which the respective addition or multiplication is defined.

In our main applications, all groups will be finite, but we will encounter groups written both additively and multiplicatively, reserving addition only for cases where it is a commutative operation. For the moment, assume that G is a group written multiplicatively except when otherwise noted.

If $A \subseteq G$ is a finite subset, then we use $\langle A \rangle \le G$ to denote the subgroup generated by A and use $\mathsf{H}(A) := \{g \in G : \ gA = A\}$ to denote the left *stabilizer* of A. Then $\mathsf{H}(A) \le G$ is a subgroup, and A is a union of right $\mathsf{H}(A)$-cosets; moreover, $\mathsf{H}(A) \le G$ is the unique maximal subgroup H for which A is a union of right H-cosets. Of course, if G is abelian, then we do not need to differentiate between left and right stabilizers and simply speak of the stabilizer of A, and when G is written additively, we have $\mathsf{H}(A) = \{g \in G : \ g + A = A\}$. For $n \ge 1$, we let C_n denote a cyclic group of order n.

Given a normal subgroup $H \lhd G$, we let

$$\phi_H \colon G \to G/H$$

denote the canonical homomorphism. The index a subgroup $H \le G$ is denoted $|G : H|$. When G is finite, $|G : H| = |G|/|H|$. We use the following standard notation for the following important subgroups:

$Z(G) = \{g \in G : \ gx = xg \quad \text{for all } x \in G\} \lhd G$ is the *center* of G,

$[x, y] = x^{-1}y^{-1}xy \in G$ is the *commutator* of the elements $x, y \in G$,

$G' = [G, G] = \langle [x, y] : \ x, y \in G \rangle \lhd G$ is the *commutator subgroup* of G,

$C_G(A) = C_G(\langle A \rangle) = \{g \in G : \ ga = ag \quad \text{for all } a \in A\} \le G$ is the *centralizer* of $A \subseteq G$, and

$N_G(A) = \{g \in G : \ gA = Ag\} \le G$ is the *normalizer* of $A \subseteq G$.

Sequences Over Groups. These are our main objects of study. We fix our notation, which is consistent with the monographs [10, 12] and with the surveys [5, 8]. We generally assume multiplicative group notation, but summarize the necessary variations for additive notation as we go.

By a *sequence* over G, we mean a finite, unordered sequence where the repetition of elements is allowed. The term multi-set would also be appropriate, but is rarely used. When a sequence is viewed as an unordered string of terms from G, it obtains a natural free abelian monoid structure whose operation, written multiplicatively, is simply the concatenation of sequences. Thus we let $\mathcal{F}(G)$ denote the free abelian monoid with basis G, whose elements $S \in \mathcal{F}(G)$ are then simply the sequences over G equipped

with the sequence concatenation product. The identity in $\mathcal{F}(G)$ is the sequence having no terms, called the *empty* or *trivial* sequence. When G is written additively, a sequence $S \in \mathcal{F}(G)$ has the form

$$S = g_1 \cdot \ldots \cdot g_\ell \in \mathcal{F}(G)$$

with $g_i \in G$ the terms of S and $\ell \ge 0$ the length of S. Every element $g \in G$ is viewed as a singleton sequence $g \in \mathcal{F}(G)$ consisting solely of the single term g. However, when G is written multiplicatively, we must exercise more care to avoid confusing the group theoretic multiplication of 2 elements $g, h \in G$ and the sequence theoretic multiplication of 2 singleton sequences $g, h \in \mathcal{F}(G)$. To do so, we consider an injective map $\diamond\colon G \to \mathcal{F}(G)$. Then $\diamond(g)$, or just $\diamond g$ for short, denotes the singleton sequence consisting of the element g. In this way, we can avoid confusion between products in G and products in $\mathcal{F}(G)$ even in the trickiest of situations as the sequence

$$S = \diamond g_1 \cdot \ldots \cdot \diamond g_\ell \in \mathcal{F}(G) \tag{1}$$

is easily differentiated from the product $g_1 \cdots g_\ell \in G$.

By viewing sequences monoid theoretically, we gain for sequences all the standard notation used to describe other monoids. In particular, if $S \in \mathcal{F}(G)$ is as given by (1), then

$$\begin{aligned}
&|S| = \ell \ge 0 \quad \text{is the } \textit{length} \text{ of } S,\\
&\mathrm{supp}(S) = \{g_1, \ldots, g_\ell\} \subseteq G \quad \text{is the } \textit{support} \text{ of } S,\\
&\mathsf{v}_g(S) = \{i \in [1,\ell] :\ g_i = g\} \quad \text{is the } \textit{multiplicity} \text{ of the term } g \in G, \quad \text{and}\\
&\mathsf{h}(S) = \max\{\mathsf{v}_g(S) :\ g \in G\} \quad \text{is the } \textit{maximum multiplicity} \text{ of a term of } S.
\end{aligned}$$

Also, $T \mid S$ denotes that T is a subsequence of S, i.e., that $T \in \mathcal{F}(G)$ with $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in G$. In such case, ST^{-1} or $T^{-1}S$ denotes the sequence obtained by taking the sequence S and removing the terms from T, i.e., $ST^{-1} \in \mathcal{F}(G)$ with $\mathsf{v}_g(ST^{-1}) = \mathsf{v}_g(S) - \mathsf{v}_g(T)$ for all $g \in G$.

We use

$$\pi(S) = \{g_{\tau(1)} \cdots g_{\tau(l)} :\ \tau \text{ a permutation of } [1,\ell]\} \subseteq G$$

to denote the *set of products* of S. In view of the basic properties of the commutator subgroup $G' = [G,G] \le G$, it is readily seen that

$$\pi(S) \quad \text{is contained in a } G'\text{-coset.}$$

When G is written additively with commutative operation, we likewise let

$$\sigma(S) = g_1 + \ldots + g_\ell \in G$$

denote the *sum* of S. More generally, for any integer $n \ge 0$, the *n-sums* and *n-products* of S are respectfully denoted by

$$\Sigma_n(S) = \{\sigma(T) :\ T \,|\, S \quad \text{and} \quad |T| = n\} \subseteq G \qquad \text{and} \qquad \Pi_n(S) = \bigcup_{\substack{T \,|\, S\\ |T|=n}} \pi(T) \subseteq G$$

and the *subsequence sums* and *subsequence products* of S are respectively denoted by

$$\Sigma(S) = \bigcup_{n \ge 1} \Sigma_n(T) \subseteq G \qquad \text{and} \qquad \Pi(S) = \bigcup_{n \ge 1} \Pi_n(T).$$

The sequence S is called

- a *product-one sequence* if $1 \in \pi(S)$
- *product-one free* if $1 \notin \pi(S)$

Zero-sum and zero-sum free sequences are analogously defined when G is written additively using σ in place of π and 0 in place of 1.

Every map of groups $\varphi\colon G \to G'$ extends to a monoid homomorphism $\varphi\colon \mathcal{F}(G) \to \mathcal{F}(G')$ by setting

$$\varphi(S) = \diamond\varphi(g_1) \cdot \ldots \cdot \diamond\varphi(g_\ell) \in \mathcal{F}(G').$$

If φ is a group homomorphism, then $\varphi(S)$ is a product-one sequence if and only if $\pi(S) \cap \mathrm{Ker}(\varphi) \neq \emptyset$. We use

$$\mathcal{B}(G) = \{S \in \mathcal{F}(G) : \ 1 \in \pi(S)\}$$

to denote the set of all product-one sequences. Clearly, $\mathcal{B}(G) \subseteq \mathcal{F}(G)$ is a submonoid, and we denote by $\mathcal{A}(G) = \mathcal{A}\big(\mathcal{B}(G)\big)$ the set of atoms of $\mathcal{B}(G)$, i.e., those nontrivial product-one sequences that cannot be factored into 2 nontrivial product-one subsequences. We call

$$\mathsf{D}(G) = \sup\{|S| : \ S \in \mathcal{A}(G)\}$$

the *large Davenport constant* of G and

$$\mathsf{d}(G) = \sup\{|S| : \ S \in \mathcal{F}(G) \text{ is product-one free}\}$$

the *small Davenport constant* of G. If $S \in \mathcal{F}(G)$ is product-one free and $g \in \pi(S)$, then $S \diamond g^{-1} \in \mathcal{A}(G)$, and hence $\mathsf{d}(G) + 1 \le \mathsf{D}(G)$. When G is abelian, a simple argument shows that equality holds [10, Proposition 5.1.3.2]: $\mathsf{d}(G) + 1 = \mathsf{D}(G)$.

Ordered Sequences Over Groups. These are an important tool used to study (unordered) sequences over non-abelian groups. Indeed, it is quite useful to have related notation for sequences in which the order of terms matters. Thus we let $\mathcal{F}^*(G)$ denote the free (non-abelian) monoid with basis G, whose elements will be called the *ordered sequences* over G. In other terminology, $\mathcal{F}^*(G)$ is the semigroup of words on the alphabet G, and the elements are called words or strings. Again, in order to avoid confusion between products in G and elements of $\mathcal{F}^*(G)$, we will occasionally need to fix an embedding $\diamond\colon G \to \mathcal{F}^*(G)$ and consider ordered sequences as products of terms of the form $\diamond g$ with $g \in G$.

Taking an ordered sequence in $\mathcal{F}^*(G)$ and considering all possible permutations of its terms gives rise to a natural equivalence class in $\mathcal{F}^*(G)$, yielding a natural map

$$[\cdot] : \mathcal{F}^*(G) \to \mathcal{F}(G)$$

given by abelianizing the sequence product in $\mathcal{F}^*(G)$. An ordered sequence $S^* \in \mathcal{F}^*(G)$ with $[S^*] = S$ is called an *ordering* of the sequence $S \in \mathcal{F}(G)$.

All notation for sequences extends naturally to ordered sequences. In particular, every map of groups $\varphi\colon G \to G'$ extends uniquely to a monoid homomorphism $\varphi\colon \mathcal{F}^*(G) \to \mathcal{F}^*(G')$ and, for an ordered sequence $S^* \in \mathcal{F}^*(G)$ with $S = [S^*]$, we set $\mathsf{h}(S^*) = \mathsf{h}(S)$, $\mathrm{supp}(S^*) = \mathrm{supp}(S)$, $|S^*| = |S|$, and $\mathsf{v}_g(S^*) = \mathsf{v}_g(S)$ for every $g \in G$.

Let

$$S^* = \diamond g_1 \cdot \ldots \cdot \diamond g_\ell \in \mathcal{F}^*(G)$$

be an ordered sequence. For every subset $I \subseteq [1, \ell]$, we set

$$S^*(I) = \prod_{i \in I} \diamond g_i \in \mathcal{F}^*(G), \tag{2}$$

where the product is taken in the natural order given by $I \subseteq \mathbb{Z}$, and every sequence of such a form in $\mathcal{F}^*(G)$ is called an *(ordered) subsequence* of S^*. We use the abbreviation

$$S^*(x, y) = S^*([x, y])$$

for integers x, $y \in \mathbb{Z}$. If $I = \emptyset$, then $S^*(I) = 1_{\mathcal{F}^*(G)}$ is the identity of $\mathcal{F}^*(G)$ (in other words, the empty ordered sequence), and if $T^* = S^*(I)$ with $I \subseteq [1, \ell]$ an interval, then we say that T^* is a subsequence of *consecutive terms*, or simply a *consecutive subsequence*, and we write $T^* \mid S^*$. If $i \in [1, |S^*|]$, then

$$S^*(i) \in G \quad \text{denotes the } i\text{-th term of } S^*.$$

Let $\pi \colon \mathcal{F}^*(G) \to G$ denote the unique homomorphism that maps an ordered sequence onto its product in G, so

$$\pi(S^*) = \prod_{i=1}^{\ell} g_i \in G.$$

If $\pi(S^*) = 1$, then S^* is called an *ordered product-one sequence*.

By a *factorization* of $S^* \in \mathcal{F}^*(G)$ of length r, we mean an r-tuple $(S_1^*, \ldots, S_r^*)$ of nontrivial consecutive subsequences $S_i^* \mid S^*$ such that $S^* = S_1^* \cdot \ldots \cdot S_r^*$. Informally speaking, we may refer to $S^* = S_1^* \cdot \ldots \cdot S_r^*$ as a factorization of S^* as well. Then, for each $i \in [1, r]$, we have $S_i^* = S^*(I_i)$ for some $I_i \subseteq [1, |S|]$ such that

$$\bigcup_{i=1}^{r} I_i = [1, |S|] \quad \text{and} \quad \max I_j = \min I_{j+1} - 1 \ \text{ for } j \in [1, r-1].$$

Given such a factorization of S^*, we can define a new ordered sequence

$$T^* = \diamond\pi(S_1^*) \cdot \ldots \cdot \diamond\pi(S_r^*) \in \mathcal{F}^*(G),$$

so T^* is obtained from S^* by replacing consecutive subsequences with the product of their terms. It is then readily noted that

$$\pi(T^*) = \pi(S^*) \quad \text{and} \quad \pi([T^*]) \subseteq \pi([S^*]).$$

Moreover, if $[S^*] \in \mathcal{A}(G)$ was an atom, then $[T^*] \in \mathcal{A}(G)$ must remain an atom.

Basic Lemmas Regarding Sequences. We now prove several basic lemmas and observations that will be needed repeatedly in the paper. The first two are rather straightforward but frequently needed.

Lemma 2.1. *Let G be a finite group and let $U \in \mathcal{F}^*(G)$ be an ordered sequence with $\pi(U^*) = 1$ and $[U^*] \in \mathcal{A}(G)$ an atom. Then there are no consecutive product-one subsequences of U^* that are proper and nontrivial.*

Proof. Observe that removing a consecutive product-one sequence from an ordered sequence does not affect its product. Thus, if the product-one ordered sequence U^* had a consecutive product-one subsequence that was proper and nontrivial, say $U^*(I)$ with $I \subset [1, |U|]$ an interval, then $[U^*] = [U^*(I)][U^*([1, |U| \setminus I)]$ would be a factorization of $[U^*]$ into 2 nontrivial product-one sequences, contradicting that $[U^*] \in \mathcal{A}(G)$ is an atom. □

Lemma 2.2. *Let G be group with $G' = [G, G] \le G$ its commutator subgroup, and let $S \in \mathcal{F}(G)$ be a product-one sequence. If $T \mid S$ is a subsequence with $\pi(T) \subseteq G'$, then $\pi(T^{-1}S) \subseteq G'$. In particular, if $T \mid S$ is a product-one subsequence, then $\pi(T^{-1}S) \subseteq G'$.*

Proof. As remarked earlier in the section, we know that every sequence $R \in \mathcal{F}(G)$ has $\pi(R)$ contained in a G'-coset. In other words, $\phi_{G'}(\pi(R))$ is a single-element, and any product-one sequence R has $1 \in \pi(R) \subseteq G'$. Thus $\pi(S) \subseteq G'$ and $\pi(T) \subseteq G'$ follow from our hypotheses and, consequently,

$$\phi_{G'}(\pi(T^{-1}S)) = \phi_{G'}(\pi(T))^{-1}\phi_{G'}(\pi(S)) = 1^{-1} \cdot 1 = 1,$$

which means $\pi(T^{-1}S) \subseteq G'$, as desired. □

The next lemma is proved by a standard argument. We provide the proof so that the reader may become acquainted with the notation.

Lemma 2.3. *Let G be a finite group. Then every ordered sequence $S \in \mathcal{F}^*(G)$ of length $|S| \ge |G|$ has a nontrivial consecutive product-one subsequence. In particular, $\mathsf{d}(G) + 1 \le \mathsf{D}(G) \le |G|$.*

Proof. Let $S \in \mathcal{F}^*(G)$ be an ordered sequence of length $|S| = \ell \ge |G|$. For $j \in [1, \ell]$, we consider the elements $\pi\Big(S(1, j)\Big) \in G$. If $\pi\Big(S(1, j)\Big) = 1$ for some $j \in [1, \ell]$, then $S(1, j)$ is the desired consecutive product-one subsequence. Otherwise, $\ell = |S| \ge |G|$ together with the pigeonhole principle guarantees that there are j, $k \in [1, \ell]$ with $j < k$ and $\pi\Big(S(1, j)\Big) = \pi\Big(S(1, k)\Big)$, and then $S(j + 1, k)$ is the desired consecutive product-one subsequence. It is now clear from Lemma 2.1 that $\mathsf{D}(G) \le |G|$, while the lower bound $\mathsf{d}(G) + 1 \le \mathsf{D}(G)$ was already explained at the beginning of Section 2. □

The next lemma shows that an ordered product-one sequence can have its terms cyclically shifted while preserving its product.

Lemma 2.4. *Let G be a group and let $S = \diamond s_1 \cdot \ldots \cdot \diamond s_n \in \mathcal{F}^*(G)$ be an ordered product-one sequence. Then $\diamond s_j \cdot \ldots \cdot \diamond s_n \diamond s_1 \cdot \ldots \cdot \diamond s_{j-1}$ is also an ordered product-one sequence for every $j \in [1, n]$.*

Proof. Let $S' = \diamond s_n \diamond s_1 \cdot \ldots \cdot \diamond s_{n-1} \in \mathcal{F}^*(G)$. Since S has product-one, we have

$$\pi(S') = s_n s_1 \cdots s_{n-1} = s_n(s_1 \cdots s_n)s_n^{-1} = s_n 1 s_n^{-1} = 1.$$

Therefore S' is also an ordered product-one sequence. Iterating this argument $n - j + 1$ times shows that $\diamond s_j \cdot \ldots \cdot \diamond s_n \diamond s_1 \cdot \ldots \cdot \diamond s_{j-1}$ is an ordered product-one sequence, as desired. □

Now we give an equivalent definition for the large Davenport constant.

Lemma 2.5. *Let G be a finite group. Then $\mathsf{D}(G)$ is the minimal integer such that, given any sequence $S \in \mathcal{F}(G)$ with $|S| \ge \mathsf{D}(G)$ and any $x \in \pi(S)$, there exists a nontrivial product-one subsequence $T \mid S$ with $x \in \pi(T^{-1}S)$.*

Proof. Suppose $S \in \mathcal{F}(G)$ with $|S| \ge \mathsf{D}(G)$ and $x \in \pi(S)$. Then $S \diamond x^{-1} \in \mathcal{F}(G)$ is a product-one sequence with length $|S \diamond x^{-1}| = |S| + 1 > \mathsf{D}(G)$. Thus the definition of $\mathsf{D}(G)$ ensures that there is a factorization $S \diamond x^{-1} = T_1 T_2$ with T_1 and T_2 both nontrivial product-one subsequences. Without restriction, we may assume $x^{-1} \in \operatorname{supp}(T_2)$, and then it is clear that $T_1 \mid S$ is a nontrivial product-one subsequence with

$$T_1^{-1}S = T_2(\diamond x^{-1})^{-1}.$$

Since T_2 is a product-one sequence, there is an ordering of the terms of T_2 having product 1, say $T_2 = \diamond x_1 \cdot \ldots \cdot \diamond x_n$ with $x_1 \cdots x_n = 1$. In view of Lemma 2.4, we can cyclically shift the ordering so that $x^{-1} \in \supp(T_2)$ is the last term while preserving that the product of terms is 1, i.e., we may w.l.o.g. assume $x_n = x^{-1}$. But now it is clear that $x = x_n^{-1} = x_1 \cdots x_{n-1} \in \pi(T_2(\diamond x^{-1})^{-1}) = \pi(T_1^{-1}S)$. Thus $T = T_1$ is the desired product-one subsequence of S.

To show that $\mathsf D(G)$ is the minimal integer with the desired property, consider an atom $U \in \mathcal A(G)$ with $|U| = \mathsf D(G)$, let $x^{-1} \in \supp(U)$, and set $S = U(\diamond x^{-1})^{-1}$. Then $|S| = \mathsf D(G) - 1$. Moreover, as argued above using Lemma 2.4, we have $x \in \pi(U(\diamond x^{-1})^{-1}) = \pi(S)$. If by contradiction S contained a nontrivial product-one subsequence $T_1 \mid S$ with $x \in \pi(T_1^{-1}S)$, then $U = T_1\big(T_1^{-1}S \diamond x^{-1}\big) = T_1\big(T_1^{-1}U\big)$ would be a factorization of U into nontrivial product-one subsequences, contradicting that $U \in \mathcal A(G)$ is an atom. □

Finally, we briefly need the concept of a *setpartition* over G, which is a (unordered) sequence whose terms, rather than being elements from G, are finite and *nonempty* subsets of G. A setpartition $\mathcal A = A_1 \cdot \ldots \cdot A_n$, where $A_i \subseteq G$ are finite and nonempty, naturally partitions the terms from the sequence

$$\mathsf S(\mathcal A) = \prod_{i=1}^{n} \prod_{a \in A_i} \diamond a \in \mathcal F(G),$$

and the length of $\mathcal A$ is then simply n. A setpartition of length n is called an *n-setpartition*, it is said to have its terms being of *as near equal a size as possible* if

$$|A_i| \in \left\{ \left\lfloor \frac{|\mathsf S(\mathcal A)|}{n} \right\rfloor, \left\lceil \frac{|\mathsf S(\mathcal A)|}{n} \right\rceil \right\} \quad \text{for all } i \in [1,n],$$

and a sequence $S \in \mathcal F(G)$ is said to *have an n-setpartition* if there is an n-setpartition $\mathcal A$ with $\mathsf S(\mathcal A) = S$. The following is the standard existence result for setpartitions. It can be found in [12, Proposition 10.2] or [2] in an equivalent formulation.

Lemma 2.6. *Let G be a group, let $S \in \mathcal F(G)$ be a sequence, and let $\ell \ge 0$ and $n \ge 1$ be integers. Then there is a subsequence $S' \mid S$ with $|S'| = \ell + n$ having an n-setpartition if and only if*

$$|S| \ge \ell + n \quad \text{and,} \quad \text{for every nonempty subset } X \subseteq G \text{ with } |X| \le \tfrac{\ell-1}{n} + 1,$$
$$\text{there are at most } |S| - \ell + (|X|-1)n \text{ terms of } S \text{ from } X.$$

Moreover, if this is the case, then S' has an n-setpartition with terms of as near equal a size as possible.

In particular, S has an n-setpartition if and only if $\mathsf h(S) \le n \le |S|$, and if this is the case, then S has an n-setpartition with terms of as near equal a size as possible.

3. General Upper Bounds

We begin with the following upper bound of Olson and White [15] for the small Davenport constant.

Theorem 3.1. *Let G be a noncyclic, finite group. Then*

$$\mathsf d(G) \le \frac{1}{2}|G|$$

with equality if G contains a cyclic, index 2 subgroup.

The following gives an inductive upper bound for the large Davenport constant. We are indebted to an anonymous referee for having suggested the key idea at the heart of its proof.

Theorem 3.2. *Let G be a finite group and let $H \le G$ be a subgroup. Then*

$$\mathsf{D}(G) \le \mathsf{D}(H)|G : H|.$$

Proof. The proof is similar to that of Lemma 2.3. We need to show that $|U| \le \mathsf{D}(H)|G : H|$ for all $U \in \mathcal{A}(G)$. Assume by contradiction that there is some $U \in \mathcal{A}(G)$ with $|U| > \mathsf{D}(H)|G : H|$. Since $U \in \mathcal{A}(G)$, there exists an ordered product-one sequence $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$.

For every $j \in [1, |U|]$, we consider the elements $\pi\Big(U^*(1, j)\Big) \in G$. Since $|U| > \mathsf{D}(H)|G : H|$, the pigeonhole principle guarantees that there exists some left H-coset, say gH, for which $\pi\Big(U^*(1, j)\Big) \in gH$ holds for at least $\mathsf{D}(H) + 1$ values of $j \in [1, |U|]$. Let $j_1 < j_2 < \ldots < j_r$, where $r \ge \mathsf{D}(H) + 1$, be all those indices $j_i \in [1, |U|]$ with $\pi\Big(U^*(1, j_i)\Big) \in gH$. Our next goal is to show that, by cyclically shifting the ordered sequence U^*, we can w.l.o.g. assume $j_r = |U|$.

Consider the ordered sequence $U'^* = U^*(j_r + 1, |U|)U^*(1, j_r) \in \mathcal{F}^*(G)$. Clearly, we have $[U'^*] = [U^*] = U$. However, we also have

$$\begin{aligned}\pi\Big(U'^*\Big) &= \pi\Big(U^*(j_r + 1, |U|)\Big)\pi\Big(U^*(1, j_r)\Big) = \pi\Big(U^*(j_r + 1, |U|)\Big)\pi\Big(U^*\Big)\pi\Big(U^*(j_r + 1, |U|)\Big)^{-1} \\ &= \pi\Big(U^*(j_r + 1, |U|)\Big)1\Big(U^*(j_r + 1, |U|)\Big)^{-1} = 1.\end{aligned}$$

Thus U'^* is a product-one ordered sequence with $[U'^*] = U$. Moreover, letting $s = |U^*(j_r + 1, |U^*|)| = |U^*| - j_r$ and $g' = \pi\Big(U^*(j_r + 1, |U^*|)\Big)$, we see (in view of the definition of the j_i) that

$$\pi\Big(U'^*(1, j_i + s)\Big) = g'\pi\Big(U(1, j_i)\Big) \in g'gH \quad \text{for all } i \in [1, r].$$

Consequently, repeating the above arguments using the ordered sequence U'^* in place of U^* allows us to w.l.o.g. assume $j_r = |U^*|$. But then $1 = \pi(U^*) = \pi\Big(U^*(1, |U^*|)\Big) = \pi\Big(U^*(1, j_r)\Big) \in gH$ forces $gH = H$. Thus we now have

$$\pi\Big(U^*(1, j_i)\Big) \in H \quad \text{for } i \in [1, r]. \tag{3}$$

Let $U_i = U^*(j_{i-1} + 1, j_i)$ for $i \in [1, r]$, where $j_0 := 0$. Since $j_r = |U|$, we have

$$U_1 \cdot \ldots \cdot U_r = U^*. \tag{4}$$

In view of (3), we have

$$\pi(U_1),\, \pi(U_1U_2),\, \pi(U_1U_2U_3), \ldots, \pi(U_1 \cdot \ldots \cdot U_r) \in H.$$

A simple inductive argument now shows

$$\pi(U_i) \in H \quad \text{for all } i \in [1, r]. \tag{5}$$

In view of (4) and (5), consider the sequence $S = \diamond\pi(U_1) \cdot \ldots \cdot \diamond\pi(U_r) \in \mathcal{F}(H)$. Since $\pi(U_1) \cdots \pi(U_r) = \pi(U_1 \cdot \ldots \cdot U_r) = \pi(U^*) = 1$, we see that $S \in \mathcal{B}(H)$. However, since $|S| = r \ge \mathsf{D}(H) + 1$, the definition of $\mathsf{D}(H)$ ensures that we have some factorization of S, say

$$S = \left(\prod_{i \in I} \diamond\pi(U_i)\right)\left(\prod_{i \in [1,r]\setminus I} \diamond\pi(U_i)\right),$$

where $I \subseteq [1, |U|]$, with both $\prod_{i\in I} \diamond\pi(U_i)$ and $\prod_{i\in[1,r]\setminus I} \diamond\pi(U_i)$ nontrivial product-one sequences over $H \le G$. But then it is clear that both $\left[\prod_{i\in I} U_i\right]$ and $\left[\prod_{i\in[1,r]\setminus I} U_i\right]$ are nontrivial product-one sequences over G, whence the factorization (in view of (4))

$$U = [U^*] = \left[\prod_{i\in I} U_i\right] \left[\prod_{i\in[1,r]\setminus I} U_i\right]$$

contradicts that $U \in \mathcal{A}(G)$ is an atom, completing the proof. □

Though we will not need it is in this paper, a similar argument to that of Theorem 3.2 gives the following result.

Theorem 3.3. *Let G be a finite group and let $H \lhd G$ be a normal subgroup with $H \cap G' = \{1\}$, where $G' = [G, G] \le G$ is the commutator subgroup of G. Then*

$$\mathsf{D}(G) \le \mathsf{D}(H)D(G/H).$$

Proof. Assume by contradiction that there is some atom $U \in \mathcal{A}(G)$ with $|U| > \mathsf{D}(H)\mathsf{D}(G/H)$. Since U is a product-one sequence, we have $1 \in \pi(U) \subseteq G'$. Since $|U| > \mathsf{D}(H)\mathsf{D}(G/H)$, repeatedly applying Lemma 2.5 to the product-one sequence $\phi_H(U) \in \mathcal{F}(G/H)$ taking $x = 1$ each time yields a factorization

$$U = U_1 \cdot \ldots \cdot U_r \quad \text{with} \quad \pi(U_i) \in H \quad \text{for } i \in [1, r] \quad \text{and} \quad r > \mathsf{D}(H).$$

As a result $\pi(U_1) \cdots \pi(U_r) \in H$. However, we also have $\pi(U_1) \cdots \pi(U_r) \in \pi(U) \subseteq G'$. Thus, in view of the hypothesis $H \cap G' = \{1\}$, it follows that $\pi(U_1) \cdots \pi(U_r) = 1$. But this shows that

$$U' := \diamond\pi(U_1) \cdot \ldots \cdot \diamond(U_r) \in \mathcal{F}(H)$$

is a product-one sequence of length $r > \mathsf{D}(H)$. Consequently, the definition of $\mathsf{D}(H)$ ensures that there is a factorization

$$U' = \left(\prod_{i\in I} \diamond\pi(U_i)\right) \left(\prod_{i\in[1,r]\setminus I} \diamond\pi(U_i)\right)$$

with $\left(\prod_{i\in I} \diamond\pi(U_i)\right)$ and $\left(\prod_{i\in[1,r]\setminus I} \diamond\pi(U_i)\right)$ both nontrivial product-one subsequences of U', where $I \subseteq [1, r]$. But then $U = \left(\prod_{i\in I} U_i\right) \left(\prod_{i\in[1,r]\setminus I} U_i\right)$ is a factorization of U into 2 nontrivial product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. □

Next, we give an upper bound in the case when G is nearly abelian.

Lemma 3.4. *Let G be a finite group with commutator subgroup $G' = [G, G] \le G$. Suppose $|G'| \le 2$. Then*

$$\mathsf{D}(G) \le \mathsf{d}(G) + |G'|.$$

Proof. If $|G'| = 1$, then G is abelian and $\mathsf{d}(G) + 1 = \mathsf{D}(G)$ holds as noted in Section 2. Therefore we may assume $|G'| = 2$. Assume by contradiction that we have an atom $U \in \mathcal{A}(G)$ with

$$|U| = \mathsf{D}(G) \ge \mathsf{d}(G) + |G'| + 1 = \mathsf{d}(G) + 3. \tag{6}$$

If all the terms of U commute with each other, then $\mathrm{supp}(U)$ generates an abelian group, whence

$$|U| \le \mathsf{D}(\langle \mathrm{supp}(U)\rangle) = \mathsf{d}(\langle \mathrm{supp}(U)\rangle) + 1 \le \mathsf{d}(G) + 1,$$

contrary to (6). Therefore we may assume there are terms x, $y \in \supp(U)$ which do not commute with each other: $xy \neq yx$. Let $T = \diamond x \diamond y$ be the subsequence consisting of these 2 terms. Since the terms of T do not commute with each other, we have $|\pi(T)| \geq 2 = |G'|$, and since $\pi(T)$ must be contained in a G'-coset (as noted in Section 2), this ensures that $\pi(T)$ is an entire G'-coset. In view of (6), we have $|T^{-1}U| = |U| - 2 \geq d(G) + 1$. Thus the definition of $\mathsf{d}(G)$ ensures that there is a nontrivial product-one subsequence $R \mid T^{-1}U$. From Lemma 2.2, we know that $\pi(R^{-1}U) \subseteq G'$. Thus, since $|\pi(T)| = |G'|$ with $T \mid R^{-1}U$, we conclude that $\pi(R^{-1}U) = G'$. In particular, $1 \in \pi(R^{-1}U)$, meaning $R^{-1}U$ is also a product-one subsequence, which is nontrivial in view of $T \mid R^{-1}U$ and $|T| = 2$. But now $U = R(R^{-1}U)$ is a factorization of U into 2 nontrivial product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. □

4. Some Tools from Additive Theory

In this section, we present the results from Additive Theory needed for Theorem 1.1. To simplify notation, all groups in this section will be abelian and written additively. We begin with the classical Cauchy-Davenport Theorem [12, Theorem 6.2] [13, Theorem 2.2].

Theorem 4.1 (Cauchy-Davenport Theorem)**.** *Let G be an abelian group of prime order p and let $A_1, \ldots, A_n \subseteq G$ be nonempty subsets. Then*

$$|\sum_{i=1}^{n} A_i| \geq \min\{p, \sum_{i=1}^{n} |A_i| - n + 1\}.$$

Next, we state the following special case of either the DeVos-Goddyn-Mohar Theorem or the Partition Theorem (see [12, Chapters 13 and 14] or [4]). In the case when $|G|$ is prime, which is the only case we will use, Theorem 4.2 is a simple consequence of the Cauchy-Davenport Theorem and Lemma 2.6.

Theorem 4.2. *Let G be an abelian group, let $S \in \mathcal{F}(G)$ be a sequence, let $n \in [1, |S|]$, and let $H = \mathsf{H}(\Sigma_n(S))$. Then*

$$|\Sigma_n(S)| \geq \Big(\sum_{g \in G/H} \min\{n, \mathsf{v}_g(\phi_H(S))\} - n + 1 \Big) |H|. \tag{7}$$

For the proof of Theorem 1.1, the case when G is isomorphic to the dicyclic group Q_{4p} of order $4p$ with $p \geq 2$ prime proves to be particularly difficult. One of the key ideas for handling this case is to reduce the basic product-one question for the non-abelian group Q_{4p} into a more complicated zero-sum question over the abelian group C_{2p}: Lemma 4.3. However, we first need some additional notation.

Given an additively written abelian group G, we let

$$2G = \{2g : \ g \in G\} \leq G$$

denote the homomorphic image of G under the multiplication by 2 homomorphism. Likewise, given a sequence $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$, we let

$$2S = 2s_1 \cdot \ldots \cdot 2s_\ell \in \mathcal{F}(2G).$$

For the following lemma, we will make use of the fact that

$$\bigcup_{T|S,\ |T|=n} \big(\sigma(T) - \sigma(ST^{-1})\big) = \Sigma_n(2S) - \sigma(S) \tag{8}$$

for any sequence $S \in \mathcal{F}(G)$ with $|S| \ge n \ge 1$—the equality follows routinely from the definitions involved. We will actually show Lemma 4.3 holds with $|U_1| = |U_2| \le 2$. We remark that Lemma 4.3 remains true without assuming $p \ge 3$ is prime. However, the proof is much more technical and requires a somewhat detailed case distinction for defining and dealing with the subsequence S'. As we only need the case when p is prime, we have opted to present the simplified proof.

Lemma 4.3. *Let $G \cong C_{2p}$ with $p \ge 2$ prime, let $x \in G$ be the unique element with $\mathrm{ord}(x) = 2$, and let $S \in \mathcal{F}(G)$ be a sequence of even length $|S| \ge 2p + 4$. Suppose there is a factorization*

$$S = T_1T_2 \quad \text{with} \quad |T_1| = |T_2| = \frac{1}{2}|S| \quad \text{and} \quad \sigma(T_1) - \sigma(T_2) = |T_1|x,$$

where $T_1, T_2 \in \mathcal{F}(G)$. Then there is a factorization $S = U_1U_2V_1V_2$, where $U_1, U_2, V_1, V_2 \in \mathcal{F}(G)$ are nontrivial, such that

$$|U_1| = |U_2|, \quad |V_1| = |V_2|, \quad \sigma(U_1) - \sigma(U_2) = |U_1|x \quad \text{and} \quad \sigma(V_1) - \sigma(V_2) = |V_1|x\,. \tag{9}$$

Proof. Let $|S| = 2\ell \ge 2p + 4 \ge 8$, so that

$$|T_1| = |T_2| = \ell \ge p + 2 \ge 4. \tag{10}$$

Note $x = -x$ and

$$|T_1|x = \begin{cases} 0, & \text{if } |T_1| = \ell \text{ is even} \\ x, & \text{if } |T_1| = \ell \text{ is odd.} \end{cases}$$

If $g \in \mathrm{supp}(T_1)$ with $g + x \in \mathrm{supp}(T_2)$ for some $g \in G$, then the lemma follows setting $U_1 = g$, $U_2 = x + g$, $V_1 = T_1g^{-1}$ and $V_2 = T_2(x + g)^{-1}$—in view of the hypotheses $|T_1| = |T_2| = \ell \ge 2$ and $\sigma(T_1) - \sigma(T_2) = |T_1|x$. Likewise, if there is some $g \in G$ with $\mathsf{v}_g(T_1), \mathsf{v}_g(T_2) \ge 2$, then the lemma follows setting $U_1 = U_2 = g^2$, $V_1 = T_1g^{-2}$ and $V_2 = T_2g^{-2}$—in view of $|T_1| = |T_2| = \ell \ge 3$. Therefore, we may assume

$$(\mathrm{supp}(T_1) + x) \cap \mathrm{supp}(T_2) = \emptyset \quad \text{and} \tag{11}$$

$$\min\{\mathsf{v}_g(T_1), \mathsf{v}_g(T_2)\} \le 1 \quad \text{for all } g \in G. \tag{12}$$

In particular,

$$\mathsf{h}(S) = \mathsf{h}(T_1T_2) \le \max\{|T_1| + 1, |T_2| + 1\} = \ell + 1. \tag{13}$$

Since $G \cong C_{2p}$, given any $\alpha \in G$, there are exactly 2 distinct elements $g, h \in G$ such that $2g = 2h = \alpha$.

Observing that it suffices to prove the lemma for any translated sequence $-g + S$, where $g \in G$ (the conclusions and hypotheses of the lemma are translation invariant), we may w.l.o.g. translate our sequence S so that

$$\mathsf{v}_0(2S) = \mathsf{h}(2S). \tag{14}$$

Note that

$$2S \in \mathcal{F}(2G) \quad \text{with} \quad 2G \cong C_p.$$

If $\mathsf{h}(2S) \le 2$, then (10) gives $2p + 4 \le 2\ell = |S| = |2S| \le \mathsf{h}(2S)|2G| \le 2p$, a contradiction. Therefore we have

$$\mathsf{v}_0(2S) = \mathsf{h}(2S) \ge 3. \tag{15}$$

By translating by $-x$ if need be, which preserves (14) since $2x = 0$, we may w.l.o.g. assume

$$\mathsf{v}_0(S) \ge \mathsf{v}_x(S). \tag{16}$$

We distinguish two cases.

Case 1: $x \in \mathrm{supp}(S)$.

In view of $x \in \mathrm{supp}(S)$ and (16), we have $0,\, x \in \mathrm{supp}(S)$. Set $S' = S0^{-1}x^{-1}$ and $\ell' = \frac{1}{2}|S'| = \ell - 1$. Since $0,\, x \in \mathrm{supp}(S)$, it follows from (11) that either $\mathrm{supp}(T_1) \cap \{0, x\} = \emptyset$ or $\mathrm{supp}(T_2) \cap \{0, x\} = \emptyset$. Combining this with (14), we conclude that

$$\mathsf{h}(2S) = \mathsf{v}_0(2S) \le \max\{|T_1|,\, |T_2|\} = \ell. \tag{17}$$

We will show that

$$\ell' x \in \bigcup_{T \mid S',\ |T| = \ell'} \big(\sigma(T) - \sigma(S'T^{-1})\big) = \Sigma_{\ell'}(2S') - \sigma(S'), \tag{18}$$

where the equality above was noted in (8). Once (18) is established, we will know there exists some subsequence $T \mid S' = S0^{-1}x^{-1}$ such that

$$\ell' = |T| = 2\ell' - \ell' = |S'| - |T| = |S'T^{-1}| \qquad \text{and} \qquad \sigma(T) - \sigma(S'T^{-1}) = \ell' x = |T|x,$$

whence the lemma will follow setting $U_1 = 0,\ U_2 = x,\ V_1 = T$ and $V_2 = S'T^{-1}$. Thus it remains to establish (18) for the sequence S' to complete Case 1. For this, we apply Theorem 4.2 to $\Sigma_{\ell'}(2S')$.

In view of the hypotheses $S = T_1T_2$ with $\sigma(T_1) - \sigma(T_2) = |T_1|x = \ell x$, we know

$$\sigma(S) = 2\sigma(T_2) + \ell x = 2\sigma(T_2) + \ell' x + x.$$

Thus

$$\sigma(S') + \ell' x = \sigma(S) - x + \ell' x = 2\sigma(T_2) + 2\ell' x = 2\sigma(T_2) \in 2G.$$

Consequently, if $\Sigma_{\ell'}(2S') = 2G$, then $2\sigma(T_2) = \sigma(S') + \ell' x \in \Sigma_{\ell'}(2S')$ follows, yielding (18), as desired. Therefore we may assume

$$|\Sigma_{\ell'}(2S')| \le |2G| - 1 = p - 1. \tag{19}$$

Consequently, since $2G \cong C_p$ has no nontrivial, proper subgroups, we must have $\mathsf{H}(\Sigma_{\ell'}(2S'))$ trivial. Since $\mathsf{H}(\Sigma_{\ell'}(2S'))$ is trivial and $\ell' = \ell - 1 \ge p + 1$ (by (10)), Theorem 4.2 will contradict (19) if $2S'$ contains 2 distinct terms having multiplicity at least $\ell' + 1$. Thus there can be at most one term with multiplicity at least $\ell' + 1$ in $2S'$. Furthermore, Theorem 4.2 will again contradict (19) unless such a term from $2S'$ exists having multiplicity at least $2\ell' - p + 2 = 2\ell - p \ge \ell + 2$, where the inequality follows from (10). However the latter case contradicts (17) in view of the trivial inequality $\mathsf{h}(2S') \le \mathsf{h}(2S)$, completing Case 1.

Case 2: $x \notin \mathrm{supp}(S)$.

Since $x \notin \mathrm{supp}(S)$, it follows from (15) that

$$\mathsf{v}_0(S) = \mathsf{v}_0(S) + \mathsf{v}_x(S) = \mathsf{v}_0(2S) \ge 3.$$

If $\mathsf{h}(S0^{-2}) \le 1$, then it follows in view of the case hypothesis that

$$2p + 2 \le |S| - 2 = |S0^{-2}| \le |G \setminus \{x\}| = 2p - 1,$$

a contradiction. Therefore we must instead have some $g \in \mathrm{supp}(S0^{-2})$ with $\mathsf{v}_g(S) \ge 2$, allowing us to define $S' := S0^{-2}g^{-2}$. Let $\ell' = \ell - 2 = \frac{1}{2}|S'|$. Note that S' is nontrivial in view of $|S| = 2\ell \ge 2p + 4 \ge 8$.

For the moment, $g \in \text{supp}(S0^{-2})$ is an arbitrary element with $\mathsf{v}_g(S) \ge 2$. We will choose g more carefully later in the proof.

Next, we will show that

$$\ell' x \in \bigcup_{T \mid S',\ |T|=\ell'} \big(\sigma(T) - \sigma(S'T^{-1})\big) = \Sigma_{\ell'}(2S') - \sigma(S'), \tag{20}$$

where the equality above was noted in (8). Once (20) is established, we will know there exists some subsequence $T \mid S' = S0^{-2}g^{-2}$ such that

$$\ell' = |T| = 2\ell' - \ell' = |S'| - |T| = |S'T^{-1}| \quad \text{and} \quad \sigma(T) - \sigma(S'T^{-1}) = \ell' x = |T|x,$$

whence the lemma will follow setting $U_1 = 0g,\ U_2 = 0g,\ V_1 = T$ and $V_2 = S'T^{-1}$. Thus it remains to establish (20) for the sequence S' to complete Case 2. For this, we apply Theorem 4.2 to $\Sigma_{\ell'}(2S')$.

In view of the hypotheses $S = T_1T_2$ with $\sigma(T_1) - \sigma(T_2) = |T_1|x = \ell x$, we know

$$\sigma(S) = 2\sigma(T_2) + \ell x = 2\sigma(T_2) + (\ell - 2)x = 2\sigma(T_2) + \ell' x.$$

Thus

$$\sigma(S') + \ell' x = \sigma(S) - 2g + \ell' x = 2\sigma(T_2) - 2g + 2\ell' x = 2\sigma(T_2) - 2g \in 2G.$$

Consequently, if $\Sigma_{\ell'}(2S') = 2G$, then $\sigma(S') + \ell' x \in \Sigma_{\ell'}(2S')$ follows, yielding (20), as desired. Therefore we may assume

$$|\Sigma_{\ell'}(2S')| \le |2G| - 1 = p - 1. \tag{21}$$

Consequently, since $2G \cong C_p$ has no nontrivial, proper subgroups, we must have $\mathsf{H}(\Sigma_{\ell'}(2S'))$ trivial, in which case Theorem 4.2 yields

$$|\Sigma_{\ell'}(2S')| \ge \sum_{y \in 2G} \min\{\ell',\, \mathsf{v}_y(2S')\} - \ell' + 1. \tag{22}$$

Since $\ell' = \ell - 2 \ge p$ holds by (10), we see that if there are 2 distinct terms of $2S'$ having multiplicity at least $\ell' + 1$, then (22) will contradict (21). Therefore, there is at most one term of $2S'$ having multiplicity at least $\ell' + 1$. Moreover, (22) will again contradict (21) unless such a term of $2S'$ exists having multiplicity at least $2\ell' - p + 2 = 2\ell - p - 2$. Thus

$$\mathsf{h}(2S') \ge 2\ell - p - 2 \ge \ell, \tag{23}$$

where the latter inequality follows from (10). In view of our case hypothesis, (14) and (13), it follows that

$$\mathsf{h}(2S') \le \mathsf{h}(2S) = \mathsf{v}_0(2S) = \mathsf{v}_0(S) \le \ell + 1.$$

Suppose $\mathsf{h}(2S) = \mathsf{v}_0(2S) = \ell + 1$. Then all nonzero elements will have multiplicity at most $|2S| - \ell - 1 = \ell - 1$ in $2S$, and thus also in $2S'$, while $\mathsf{v}_0(2S') \le \mathsf{v}_0(2S) - 2 = \ell - 1$ follows in view of $S' = S0^{-2}g^{-2}$. In such case, it follows that $\mathsf{h}(2S') \le \ell - 1$, contradicting (23). So we must have $\mathsf{h}(2S) = \mathsf{v}_0(2S) \le \ell$. On the other hand, if $\mathsf{h}(2S) \le \ell - 1$, then (23) will again be contradicted in view of the trivial inequality $\mathsf{h}(2S') \le \mathsf{h}(2S)$. So we conclude that

$$\mathsf{h}(2S) = \mathsf{v}_0(2S) = \ell.$$

Now $\mathsf{v}_0(2S') \le \mathsf{v}_0(2S) - 2 = \ell - 2$. Thus (23) ensures that there must be a nonzero element having multiplicity ℓ in $2S'$, and thus also in $2S$. Since 0 also has multiplicity ℓ in $2S$ with $|2S| = |S| = 2\ell$, this is only possible if $|\mathrm{supp}(2S)| = 2$ with both elements from $\mathrm{supp}(2S)$ having multiplicity ℓ in $2S$. As a result, since $\ell \ge p + 2 \ge 3$, the pigeonhole principle guarantees that we can take g with $2g \neq 0$ when defining $S' = S0^{-2}g^{-2}$, whence $\mathsf{v}_0(2S') = \mathsf{v}_0(2S) - 2 = \ell - 2$ and $\mathsf{v}_{2g}(2S') = \mathsf{v}_{2g}(2S) - 2 = \ell - 2$ follow, contradicting (23) for the final time. □

5. Groups with a Cyclic, Index 2 Subgroup

In this section, we determine the large Davenport constant of all finite groups containing a cyclic, index 2 subgroup. The possible isomorphism classes of such groups can be determined by standard methods from Group Theory, and despite the simple formulation of Theorem 1.1, we will need some specialized information regarding these groups for the proof. Thus we begin by summarizing the classification of all finite groups G containing a cyclic, index 2 subgroup, which can be found for instance in the forthcoming book [].

Lemma 5.1. *Let G be a finite group of order $|G| = 2n = 2^{s+1}m$, where $\gcd(2, m) = 1$, $s \ge 0$, $m \ge 1$, and $n = 2^s m$. Suppose G has a cyclic, index 2 subgroup. Then G has a presentation of one of the following forms:*

(A) $G = \langle \alpha, \tau \mid \alpha^n = 1, \quad \alpha\tau = \tau\alpha^r, \quad \tau^2 = 1 \rangle$,

(B) $G = \langle \alpha, \tau \mid \alpha^n = 1, \quad \alpha\tau = \tau\alpha^r, \quad \tau^2 = \alpha^{\frac{1}{2}n} \rangle$, *or*

(C) $G = \langle \alpha, \tau \mid \alpha^n = 1, \quad \alpha\tau = \tau\alpha^r, \quad \tau^2 = \alpha^m \rangle$

for some $r \in [1, n-1]$ with (B) only possible if $s \ge 1$. In particular, $G = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} \cup \{\tau, \tau\alpha, \tau\alpha^2, \ldots, \tau\alpha^{n-1}\}$.

Of course, not all values of $r \in [1, n-1]$ are possible nor necessarily give rise to isomorphically distinct groups. However, throughout this section, we will use the format given by Lemma 5.1 for G, saying that G has type (A) if it has a presentation given by (A) in Lemma 5.1, and likewise defining types (B) and (C). Note that if G is of type (C) with $r = 1$, then $\mathrm{ord}(\tau\alpha) = 2n$, which corresponds to when G is cyclic. Also, when $s = 0$, type (C) coincides with type (A), and when $s = 1$, type (C) coincides with type (B). Type (C) is really only needed when $s \ge 2$, but it will be convenient to state Lemma 5.1 with this slight amount of overlap between types.

In order to unify the notation in the proofs and statements of theorems in this section, we list a set of assumptions regarding hypotheses and notation that we will use throughout this section. The importance of the parameters n^-, n^+, m^- and m^+ will become apparent later in the section.

General Assumptions for Section 5

- G is a finite group of order $|G| = 2n = 2^{s+1}m$, where $\gcd(2, m) = 1$, $s \ge 0$, $m \ge 1$, and $n = 2^s m$.
- G has a cyclic, index 2 subgroup, notated as in Lemma 5.1, with parameter $r \in [1, n-1]$.
- $G' = [G, G] \le G$ is the commutator subgroup of G.

- $P \le G$ is a Sylow 2-subgroup of G.
- $n^- = \gcd(r-1, n)$ and $n = n^+n^-$.
- $m^- = \gcd(r-1, m)$ and $m^+ = \gcd(r+1, m)$.

We continue with the full characterization for 2-groups.

Lemma 5.2. *Let G satisfy the General Assumptions for Section 5. Suppose G is a 2-group, so $m = 1$ and $G = P$. Then G is isomorphic to one of the following 6 isomorphically distinct groups.*

(i) *$s \ge 0$ and G is a cyclic group:*

$$G \cong C_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha, \quad \tau^2 = \alpha \rangle.$$

(ii) *$s \ge 1$ and G is an abelian but non-cyclic group:*

$$G \cong C_2 \times C_{2^s} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha, \quad \tau^2 = 1 \rangle.$$

(iii) *$s \ge 2$ and G is a dihedral group:*

$$G \cong D_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{-1}, \quad \tau^2 = 1 \rangle.$$

(iv) *$s \ge 2$ and G is a generalized quaternion group:*

$$G \cong Q_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{-1}, \quad \tau^2 = \alpha^{2^{s-1}} \rangle.$$

(v) *$s \ge 3$ and G is a semi-dihedral group:*

$$G \cong SD_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{-1+2^{s-1}}, \quad \tau^2 = 1 \rangle.$$

(vi) *$s \ge 3$ and G is an ordinary meta-cyclic group:*

$$G \cong M_{2^{s+1}} = \langle \alpha, \tau \mid \alpha^{2^s} = 1, \quad \alpha\tau = \tau\alpha^{1+2^{s-1}}, \quad \tau^2 = 1 \rangle.$$

In view of Lemma 5.2, given a finite 2-group P of order 2^{s+1} having a cyclic, index 2 subgroup, we let $\rho(P) \in [1, 2^s - 1]$ be the value of r in its presentation given by Lemma 5.1, i.e.,

$$\rho(P) = \begin{cases} 1, & \text{for } P \text{ given by Lemma 5.2(i)(ii) with } s \ge 0 \\ -1 + 2^s, & \text{for } P \text{ given by Lemma 5.2(iii)(iv) with } s \ge 2 \\ -1 + 2^{s-1}, & \text{for } P \text{ given by Lemma 5.2(v) with } s \ge 3 \\ 1 + 2^{s-1}, & \text{for } P \text{ given by Lemma 5.2(vi) with } s \ge 3. \end{cases}$$

The full classification of finite groups having a cyclic, index 2 subgroup is then the following.

Theorem 5.3. *Let G satisfy the General Assumptions for Section 5. Then its Sylow 2-group P is of one of the six types (i)–(vi) given by Lemma 5.2 and*

$$r \in [1, n-1] \quad \textit{satisfies} \quad r^2 \equiv 1 \mod m \quad \textit{and} \quad r \equiv \rho(P) \mod 2^s.$$

Furthermore,

1. *if P is of type (ii), (iii), (v) or (vi), then G has type (A) in Lemma 5.1;*
2. *if P is of type (iv), then G has type (B) in Lemma 5.1;*
3. *if P is of type (i), then G has type (C) in Lemma 5.1.*

Different allowed values of $r \in [1, n-1]$ correspond to non-isomorphic groups, and any group described above indeed has a cyclic, index 2 subgroup.

From Theorem 5.3, we see that the parameter $r \in [1, n-1]$ must satisfy the equation

$$(r+1)(r-1) = r^2 - 1 \equiv 0 \mod m. \tag{24}$$

Now consider a prime $p \mid m$ and let $p^{\mathsf{v}_p(m)}$ be the maximal power of p dividing m. Since p must be odd (as m is odd), either $\gcd(r+1, p) = 1$ or $\gcd(r-1, p) = 1$. Thus (24) implies that either $r + 1 \equiv 0 \mod p^{\mathsf{v}_p(m)}$ or $r - 1 \equiv 0 \mod p^{\mathsf{v}_p(m)}$. This means that we can factor

$$\begin{aligned} &m = m^+ m^- \quad \text{with} \quad \gcd(m^+, m^-) = 1, \quad \text{where} \\ &m^+ \geq 1 \quad \text{contains all those primes } p \mid m \text{ with } r + 1 \equiv 0 \mod p \quad \text{and} \\ &m^- \geq 1 \quad \text{contains all those primes } p \mid m \text{ with } r - 1 \equiv 0 \mod p. \end{aligned} \tag{25}$$

In other words

$$m^+ = \gcd(r+1, m) \quad \text{and} \quad m^- = \gcd(r-1, m).$$

Recall that $n = 2^s m$. Let us next consider the divisibility of $r+1$ and $r-1$ by 2. Given the possibilities for $\rho(P)$, there are five cases, which we summarize below. Note $\mathsf{v}_2(x)$ denotes below the 2-adic valuation of x, which is the maximal integer such that $2^{\mathsf{v}_2(x)} \mid x$.

$$\begin{array}{llll} \mathsf{v}_2(r-1) \geq s & \text{and} & \mathsf{v}_2(r+1) \geq s & \text{if } \rho(P) = 1 \text{ with } s \leq 1, \\ \mathsf{v}_2(r-1) \geq s & \text{and} & \mathsf{v}_2(r+1) = 1 & \text{if } \rho(P) = 1 \text{ with } s \geq 2, \\ \mathsf{v}_2(r-1) = 1 & \text{and} & \mathsf{v}_2(r+1) \geq s & \text{if } \rho(P) = -1 + 2^s \text{ with } s \geq 2, \\ \mathsf{v}_2(r-1) = 1 & \text{and} & \mathsf{v}_2(r+1) = s-1 & \text{if } \rho(P) = -1 + 2^{s-1} \text{ with } s \geq 3, \text{ and} \\ \mathsf{v}_2(r-1) = s-1 & \text{and} & \mathsf{v}_2(r+1) = 1 & \text{if } \rho(P) = 1 + 2^{s-1} \text{ with } s \geq 3. \end{array} \tag{26}$$

Consequently, letting

$$n = n^+ n^- \quad \text{with} \quad n^- = \gcd(r-1, n),$$

we discover that

$$\begin{array}{llll} n^- = 2^s m^- & \text{and} & n^+ = m^+ & \text{if } \rho(P) = 1 \text{ with } s \geq 0, \\ n^- = 2m^- & \text{and} & n^+ = 2^{s-1} m^+ & \text{if } \rho(P) = -1 + 2^s \text{ or } -1 + 2^{s-1} \text{ with } s \geq 2, \text{ and} \\ n^- = 2^{s-1} m^- & \text{and} & n^+ = 2m^+ & \text{if } \rho(P) = 1 + 2^{s-1} \text{ with } s \geq 3. \end{array} \tag{27}$$

Observe that $n^+ \mid r+1$ in all cases, while n^- is even except when $s = 0$. With the above notation in hand, let us now characterize some of the important subgroups of G.

Lemma 5.4. *Let G satisfy the General Assumptions for Section 5. Then*

$$G' = \langle \alpha^{r-1} \rangle = \langle \alpha^{n^-} \rangle \quad \text{and} \quad Z(G) = \begin{cases} G, & \text{if } r = 1 \\ \langle \alpha^{n^+} \rangle, & \text{if } r \neq 1. \end{cases}$$

In particular, G is non-abelian if and only if $r \neq 1$, in which case $|G'| = n^+$ and $|Z(G)| = n^-$.

Proof. Let $\tau^a \alpha^x$, $\tau^b \alpha^y \in G$ be arbitrary elements, where $a, b \in \{0, 1\}$ and $x, y \in [0, n-1]$. Then

$$\begin{aligned} [\tau^a \alpha^x, \tau^b \alpha^y] &= \alpha^{-x} \tau^{-a} \alpha^{-y} \tau^{-b} \tau^a \alpha^x \tau^b \alpha^y \\ &= \alpha^{-x - r^a y + r^b x + y} = \alpha^{(r^b - 1)x - (r^a - 1)y}. \end{aligned} \tag{28}$$

Since $r-1$ divides both r^a-1 and r^b-1, we see from (28) that all commutator elements live in the subgroup $\langle \alpha^{r-1} \rangle$. Moreover, taking $a = y = 1$ and $x = 0$, we see that α^{r-1} is itself a commutator element. This shows that $G' = \langle \alpha^{r-1} \rangle$. In particular, G is abelian if and only if $r = 1$. Moreover, $\mathrm{ord}(\alpha^{r-1}) = \frac{n}{\gcd(r-1,n)} = n^+ = \mathrm{ord}(\alpha^{n^-})$, so that $|G'| = n^+$ and $G' = \langle \alpha^{r-1} \rangle = \langle \alpha^{n^-} \rangle$ (in view of a finite cyclic group of order n containing a unique subgroup of any given order dividing n).

If $r = 1$, then G is abelian and $Z(G) = G$. Let us next determine $Z(G)$ when $r \neq 1$. The element $\tau^a \alpha^x$ lies in the center of G precisely when (28) is equal to 1 for all $b \in \{0, 1\}$ and $y \in [0, n-1]$. If $a = 1$, then the values $b = 0$ and $y = 1$ yield a non-identity value in (28) in view of $r \neq 1$. Therefore $Z(G) \subset \langle \alpha \rangle$. If $a = 0$, then taking the value $b = 1$ in (28) shows that only values $x \in [1, n-1]$ with $(r-1)x \equiv 0 \mod n$ can correspond to elements of the center. Hence we must have $x \equiv 0 \mod n^+$, which means that $Z(G) \subset \langle \alpha^{n^+} \rangle$. However, it is easily seen from (28) that $\alpha^{n^+} \in Z(G)$, whence $Z(G) = \langle \alpha^{n^+} \rangle$. Since $\mathrm{ord}(\alpha^{n^+}) = n^-$, we have $|Z(G)| = n^-$. □

The following lemma gives a subgroup isomorphic to $C_2 \times C_{n^-}$ in most cases, which can then be combined with Theorem 3.2 to bound $\mathsf{D}(G)$.

Lemma 5.5. *Let G satisfy the General Assumptions for Section 5. If P is neither cyclic nor dicyclic, then*

$$C_G(\tau) = \langle \alpha^{n^+}, \tau \rangle \cong C_2 \times C_{n^-} \quad \text{is non-cyclic.}$$

Proof. Since P is neither cyclic nor dicyclic, Theorem 5.3 shows that G must have type (A) with $s \geq 1$. In view of (27) and $s \geq 1$, we have n^- even, whence $\cong C_2 \times C_{n^-}$ is non-cyclic.

Let $\tau^a \alpha^x \in G$ be arbitrary, where $a \in \{0, 1\}$ and $x \in [0, n-1]$. Then

$$[\tau, \tau^a \alpha^x] = \tau^{-1} \alpha^{-x} \tau^{-a} \tau \tau^a \alpha^x = \alpha^{-(r-1)x}. \tag{29}$$

Thus (29) is equal to 1 precisely when $x \equiv 0 \mod n^+$, which means that $C_G(\tau) = \langle \alpha^{n^+}, \tau \rangle$ with $|C_G(\tau)| = 2n^-$. In view of Lemma 5.4, we know $\alpha^{n^+} \in Z(G)$, which forces $C_G(\tau) = \langle \alpha^{n^+}, \tau \rangle$ to be abelian. Consequently, since $\mathrm{ord}(\alpha^{n^+}) = n^-$ and $|C_G(\tau)| = 2n^-$, we conclude that $C_G(\tau)$ is isomorphic to either $C_2 \times C_{n^-}$ or C_{2n^-}. Thus to complete the proof, we simply need to show that

$$\mathrm{ord}(\tau \alpha^{x n^+}) < 2n^- \quad \text{for all } x \in [0, n^- - 1].$$

To this end, let $x \in [0, n^- - 1]$ be arbitrary.

Since G has type (A), we have

$$(\tau \alpha^{x n^+})^2 = \alpha^{(r+1) x n^+} \quad \text{with} \quad \mathrm{ord}(\tau \alpha^{x n^+}) = 2 \, \mathrm{ord}(\alpha^{(r+1) x n^+}). \tag{30}$$

Recall that n^- is even (in view of $s \geq 1$), that $m^+ \mid n^+$, that $m^- \mid n^-$ and that $m^+ m^- = m$ is odd. Thus

$$\frac{1}{2} n^- (r+1) x n^+ \equiv m^- m^+ \equiv m \equiv 0 \mod m.$$

As a result, $\mathrm{ord}(\alpha^{(r+1) x n^+}) \leq \frac{1}{2} n^-$ will follow, proving that $C_G(\tau)$ is non-cyclic in view of (30), provided

$$\mathsf{v}_2(\frac{1}{2} n^- (r+1) n^+) = \mathsf{v}_2((r+1)n) - 1 \geq s = \mathsf{v}_2(n),$$

i.e., provided $\mathsf{v}_2(r+1) \geq 1$. However, in view of (26) and $s \geq 1$, we see that this is indeed the case, completing the proof. □

Next, we give the lower bound for $\mathsf{D}(G)$.

Lemma 5.6. *Let G satisfy the General Assumptions for Section 5. Then*

$$\frac{1}{2}|G| + |G'| \le \mathsf{D}(G).$$

Proof. From Lemma 5.4, we know $|G'| = n^+$. Consider the sequence

$$U = (\diamond\tau^{-1}\alpha)(\diamond\alpha)^{n^+-1}(\diamond\tau\alpha^{1-n^+})(\diamond\alpha)^{n-1} \in \mathcal{F}(G).$$

Then $|U| = n + n^+ = \frac{1}{2}|G| + |G'|$. Since $(\tau^{-1}\alpha)\alpha^{n^+-1}(\tau\alpha^{1-n^+})\alpha^{n-1} = 1$—as is easily seen by recalling from Lemma 5.4 that $\alpha^{n^+} \in Z(G)$—it is clear that U is a product-one sequence. Thus to complete the proof, we need to show that $U \in \mathcal{A}(G)$ is an atom.

Assume to the contrary that we have a factorization $U = VW$ with $V, W \in \mathcal{B}(G)$ both nontrivial. Since V and W are product-one sequences, we have (without restriction) $V \in \mathcal{F}(\langle\alpha\rangle)$ and $\diamond\tau^{-1}\alpha\diamond\tau\alpha^{1-n^+} \mid W$. Hence $V = (\diamond\alpha)^n$ and $W = (\diamond\alpha)^{n^+-2} \diamond \tau^{-1}\alpha \diamond \tau\alpha^{1-n^+}$. Therefore there exists a $k \in [0, n^+ - 2]$ such that $1 = (\tau^{-1}\alpha)\alpha^k(\tau\alpha^{1-n^+})\alpha^{n^+-2-k} \in \pi(W)$—in view of Lemma 2.4, cyclically shifting the terms in a product-one ordered sequence preserves that the sequence has product-one, so we can w.l.o.g. assume our product-one expression starts with $\tau^{-1}\alpha$. Since $1 = (\tau^{-1}\alpha)\alpha^k(\tau\alpha^{1-n^+})\alpha^{n^+-2-k} = \alpha^{(r-1)(k+1)}$, it follows that $k+1 \in [1, n^+ - 1]$ must be a multiple of $\mathrm{ord}(\alpha^{r-1})$. However, since $n^- = \gcd(r-1, n)$ with $n = n^+n^-$, it follows that $\mathrm{ord}(\alpha^{r-1}) = n^+$, so that $k+1 \in [1, n^+ - 1]$ cannot be a multiple of $\mathrm{ord}(\alpha^{r-1})$. This contradiction establishes the desired lower bound for $\mathsf{D}(G)$. □

The next lemma reduces the problem of finding a matching upper bound for $\mathsf{D}(G)$ to the case when $|G'| = n^+$ is prime.

Lemma 5.7. *Let G satisfy the General Assumptions for Section 5. Suppose G is non-abelian, let p be a prime divisor of $|G'| = n^+$, and let*

$$H = \langle \alpha^{\frac{n^+}{p}}, \tau\rangle \le G.$$

Then H has a cyclic, index 2 subgroup and $|H'| = p$, where $H' = [H, H] \le H$ is the commutator subgroup of H. In particular, if $\mathsf{D}(H) \le \frac{1}{2}|H| + |H'|$, then $\mathsf{D}(G) \le \frac{1}{2}|G| + |G'|$.

Proof. Observe that $\mathrm{ord}(\alpha^{\frac{n^+}{p}}) = \mathrm{ord}(\alpha)\frac{p}{n^+} = n^-p$. If G has type (A), then $\tau^2 = 1 \in \langle\alpha^{\frac{n^+}{p}}\rangle$. If G has type (B), then $s \ge 1$ and n^- is even. Thus $\tau^2 = \alpha^{\frac{n}{2}} \in \langle\alpha^{\frac{n^+}{p}}\rangle$ since $(\frac{n^+}{p})\frac{pn^-}{2} = \frac{n}{2}$ with $2 \mid n^-$. If G has type (C), then P is cyclic. Hence (27) implies that $m^+ = n^+$, and now $\tau^2 = \alpha^m \in \langle\alpha^{\frac{n^+}{p}}\rangle$ holds in view of $\left(\frac{n^+}{p}\right)m^-p = \frac{m^+m^-p}{p} = m$. In all cases, we conclude that

$$|H| = 2\,\mathrm{ord}(\alpha^{\frac{n^+}{p}}) = 2n^-p,$$

so that $\langle\alpha^{\frac{n^+}{p}}\rangle \le H$ is a cyclic, index 2 subgroup.

Next, let us compute $H' \le H$. Let $\tau^a\alpha^x, \tau^b\alpha^y \in H$ be arbitrary elements, where $a, b \in \{0, 1\}$, $x, y \in [0, n-1]$ and $x \equiv y \equiv 0 \mod \frac{n^+}{p}$. Then (as in Lemma 5.4)

$$[\tau^a\alpha^x, \tau^b\alpha^y] = \alpha^{(r^b-1)x-(r^a-1)y}.$$

Since $x \equiv y \equiv 0 \mod \frac{n^+}{p}$ and since $r-1$ divides both $r^b - 1$ and $r^a - 1$, we see from (31) that all commutator elements live in the subgroup $\langle\alpha^{(r-1)\frac{n^+}{p}}\rangle$. Moreover, taking $a = 1$, $y = \frac{n^+}{p}$ and $x = 0$, we

see that $\alpha^{(r-1)\frac{n^+}{p}}$ is itself a commutator element. This shows that $H' = \langle \alpha^{(r-1)\frac{n^+}{p}} \rangle$. In consequence, since $\gcd(r-1,n) = n^-$ and $n = n^+n^-$, it follows that $|H'| = p$.

Now $|H| = 2n^-p$, $|H'| = p$, $|G'| = n^+$ (from Lemma 5.4) and $|G : H| = \frac{2n}{2n^-p} = \frac{n^+}{p}$. Thus, if $\mathsf D(H) \le \frac{1}{2}|H| + |H'|$, then Theorem 3.2 yields

$$\mathsf D(G) \le \mathsf D(H)|G:H| \le (\frac{1}{2}|H| + |H'|)|G:H| = \frac{1}{2}|G| + |H'||G:H| = n + n^+ = \frac{1}{2}|G| + |G'|,$$

competing the proof. □

The following lemma handles the case when there are a sufficient number of terms from $\langle \alpha \rangle$.

Lemma 5.8. *Let G satisfy the General Assumptions for Section 5. Suppose $n^+ = p$ is prime and let $U \in \mathcal F(G)$ be a product-one sequence. If $|U| \ge n + p + 1$ and U contains at least $p-1$ terms from $\langle \alpha \rangle \setminus Z(G)$, then U is not an atom.*

Proof. Since $n^+ = p$ is prime, we have $n^+ = p \ge 2$. Thus Lemma 5.4 implies that G is non-abelian with $Z(G) = \langle \alpha^{n^+} \rangle$ and $G' = \langle \alpha^{n^-} \rangle = \langle \alpha^p \rangle = \langle \alpha^{r-1} \rangle$. In particular, $|G'| = n^+ = p \ge 2$ and $|Z(G)| = n^-$.

By hypothesis, there is a subsequence $V \mid U$ with $\mathrm{supp}(V) \subseteq \langle \alpha \rangle \setminus Z(G)$ and $|V| = p-1$, say $V = \diamond v_1 \cdot \ldots \cdot \diamond v_{p-1}$ with

$$v_i = \alpha^{x_i} \quad \text{for} \quad i \in [1, p-1],$$

where $x_i \in [0, n-1]$. Since $v_i \notin Z(G) = \langle \alpha^p \rangle$ for all $i \in [1, p-1]$, we see that

$$x_i \not\equiv 0 \mod p \quad \text{for all } i \in [1, p-1]. \tag{31}$$

If $\mathrm{supp}(U) \subseteq \langle \alpha \rangle$, then $|U| \ge n + p + 1 > n = |\langle \alpha \rangle| \ge \mathsf D(\langle \alpha \rangle)$ ensures that U cannot be an atom, as desired, where the final inequality follows from Lemma 2.3. Therefore we can assume there is some $z = \tau\alpha^x \in \mathrm{supp}(U)$ with $x \in [0, 2p-1]$.

As remarked in Section 2, $\pi(V \diamond z)$ is contained in a G'-coset. Let us next show that

$$|\pi(V \diamond z)| = p = |G'|, \tag{32}$$

so that $\pi(V \diamond z)$ is an entire G'-coset.

Let W^* be an ordering of the terms of $V \diamond z$, so $W^* \in \mathcal F^*(G)$ with $[W^*] = V \diamond z$. Then

$$\pi(W^*) = \tau\alpha^{x + \sum_{i=1}^{p-1} \epsilon_i x_i}, \tag{33}$$

where $\epsilon = 1$ if the term x_i occurs to the right of $z = \tau\alpha^x$ in W^*, and $\epsilon = r$ if if the term x_i occurs to the left of $z = \tau\alpha^x$ in W^*. The possible exponents for α in (33) (as we range over all orderings W^* of $V \diamond z$) are then

$$x + \{x_1, rx_1\} + \ldots + \{x_{p-1}, rx_{p-1}\} = x + \sum_{i=1}^{p-1} x_i + \{0, (r-1)x_1\} + \ldots + \{0, (r-1)x_{p-1}\}.$$

Consequently,

$$\pi(V \diamond z) = \tau\alpha^{x + \sum_{i=1}^{p-1} x_i} \{(\alpha^{r-1})^y : \ y \in Y\}, \tag{34}$$

where $Y = \{0, x_1\} + \ldots + \{0, x_{p-1}\}$. Recall that α^{r-1} is a generator for G' having $\mathrm{ord}(\alpha^{r-1}) = n^+ = p$. Thus the cardinality of $\pi(V \diamond z)$ is just the number of residue classes modulo p in $Y = \{0, x_1\} + \ldots + \{0, x_{p-1}\}$. From (31), we see that each set $\{0, x_i\}$ consists of 2 elements that are distinct modulo p, in

which case applying the Cauchy-Davenport Theorem to Y shows that $|Y| = p = |G'|$, which combined with (34) establishes (32), as claimed.

Now $|U(V \diamond z)^{-1}| = |U| - p \geq n + 1 = \mathsf{d}(G) + 1$, with the first inequality by hypothesis and the final equality from Theorem 3.1. But now Lemma 2.2 shows that $\pi(UT^{-1}) \subseteq G'$. As a result, since $V \diamond z \mid UT^{-1}$ follows from the definition of T, it follows in view of (32) that $\pi(UT^{-1}) = G'$. In particular, $1 \in G' \in \pi(UT^{-1})$. Thus $U = (UT^{-1})T$ is a factorization of U into two nontrivial product-one subsequences, ensuring that U is not an atom, as desired. □

When either n^+ or n^- is too small, the general strategy for proving Theorem 1.1 breaks down, requiring the cases when $n^- \leq 2$ or $n^+ \leq 2$ to be handled separately. Most of these remaining cases can be handled by simple arguments. However, the case when when G is isomorphic to a dicyclic group Q_{4p} with p odd is particularly difficult, so we handle it separately now.

Lemma 5.9. *Let G be a dicyclic group of order $4p$ with p an odd prime, so*

$$G \cong Q_{4p} = \langle \alpha, \tau \mid \alpha^{2p} = 1, \quad \tau^2 = \alpha^p, \quad \alpha\tau = \tau\alpha^{-1} \rangle.$$

Then $\mathsf{D}(G) \leq \frac{1}{2}|G| + |G'| = 3p$, where $G' = [G, G] \leq G$ is the commutator subgroup.

Proof. By hypothesis, we have $G \cong Q_{4p}$ with p an odd prime. This corresponds to when G satisfies the Standard Assumptions of Section 5 having types (B) and (C) (since these types coincide for $s = 1$) with

$$s = 1, \quad P \leq G \text{ cyclic}, \quad n = 2p, \quad r = 2p - 1, \quad n^- = 2, \quad m^- = 1, \qquad \text{and} \qquad n^+ = m^+ = p.$$

As a result, Lemma 5.4 tells us that

$$G' = \langle \alpha^2 \rangle \cong C_p \qquad \text{and} \qquad Z(G) = \langle \alpha^p \rangle \cong C_2. \tag{35}$$

Assume by contradiction that we have some atom $U \in \mathcal{A}(G)$ with $|U| = \mathsf{D}(G) \geq 3p + 1$. Since U is a product-one sequence, there is an ordering of its terms with product 1, say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$ and $\pi(U^*) = 1$.

Suppose $Z(G) \cap \operatorname{supp}(U) \neq \emptyset$. Since U is an atom and G is nontrivial, we cannot have $1 \in \operatorname{supp}(U)$. Thus, in view of (35), we must have $\alpha^p \in \operatorname{supp}(U)$. By Lemma 2.4, we can w.l.o.g. assume α^p is equal to the first term of U^*, so $U^*(1) = \alpha^p$. But then $|U^*(2, |U| - 1)| = |U| - 2 \geq 3p - 1 \geq 2p = |G/Z(G)|$, which means we can apply Lemma 2.3 to $\phi_{Z(G)}\Big(U^*(2, |U| - 1)\Big)$ and thereby find a nontrivial consecutive subsequence of $U^*(2, |U| - 1)$ with product from $Z(G) = \{1, \alpha^p\}$, say $U^*(I)$ with $I \subseteq [2, |U| - 1]$ an interval. Since $U = [U^*] \in \mathcal{A}(G)$ is an atom, Lemma 2.1 ensures that $\pi\Big(U^*(I)\Big) \neq 1$. Thus $\pi\Big(U^*(I)\Big) = \alpha^p \in Z(G)$, in which case $\pi\Big(U^*(1)U^*(I)U^*([2, |U|] \setminus I)\Big) = \pi(U^*) = 1$. However, $\pi\Big((U^*(1)U^*(I)\Big) = \alpha^p\alpha^p = \alpha^{2p} = 1$, so that $U = [U^*] = [U^*(1)U^*(I)][U^*([2, |U|] \setminus I)]$ is a factorization of U into 2 nontrivial, product-one subsequences—the subsequence $[U^*([2, |U|] \setminus I)]$ is nontrivial since $I \subseteq [2, |U| - 1]$—contradicting that $U \in \mathcal{A}(G)$ is an atom in this case as well. So we instead conclude that

$$Z(G) \cap \operatorname{supp}(U) = \emptyset. \tag{36}$$

In view of Lemma 5.8 and (36), we may assume

$$\text{there are at most } p - 2 \text{ terms of } U \text{ from } \langle \alpha \rangle. \tag{37}$$

Let $J \subseteq [1, |U|]$ be all those indices $j \in [1, |U|]$ with $U^*(j) \in \tau\langle\alpha\rangle$. Since $\pi(U^*) = 1$, it is easily deduced from the group presentation for G that $|J|$ must be even. In view of (37), we have $|J| \ge |U| - p + 2 \ge 2p + 3$. Thus, since $|J|$ must be even, it follows that

$$|J| \ge 2p + 4. \tag{38}$$

Let

$$j_1 < j_2 < \ldots < j_{2w-1} < j_{2w}$$

be the distinct elements of J, where

$$w = \frac{1}{2}|J| \ge p + 2.$$

In view of Lemma 2.4, we can cyclically shift the ordering U^* of U until the first term of U^* is from $\tau\langle\alpha\rangle$, i.e., such that $j^- = 1$.

Now define an ordered sequence

$$U'^* = \diamond U^*(j_1, j_2 - 1) \diamond U^*(j_2, j_3 - 1) \cdot \ldots \cdot \diamond U^*(j_{2w-1}, j_w - 1) \diamond U^*(j_{2w}, |U|) \in \mathcal{F}^*(G).$$

The ordered sequence U'^* is obtained from the ordered product-one sequence U^* by repeatedly replacing a consecutive subsequence with a single term equal to its product. As noted in Section 2, since $[U^*] = U \in \mathcal{A}(G)$ was an atom, this ensures that

$$U' := [U'^*] \in \mathcal{A}(G)$$

is also an atom. From the definition of the j_x, each $U^*(j_x, j_{x+1} - 1)$, for $x \in [1, w]$ where $j_{2w+1} = |U| + 1$, has its first term from $\tau\langle\alpha\rangle$ and all other terms from $\langle\alpha\rangle$. In consequence, we have

$$\mathrm{supp}(U') \subseteq \tau\langle\alpha\rangle \quad \text{and} \quad |U'| = |J| = 2w \ge 2p + 4,$$

where the inequality follows from (38).

For $x \in \mathbb{Z}$, define a map $\overline{\cdot} : \tau\langle\alpha\rangle \to \mathbb{Z}/2p\mathbb{Z}$ by setting $\overline{\tau\alpha^x} := \phi_{2p\mathbb{Z}}(x) \in \mathbb{Z}/2p\mathbb{Z}$, i.e., $\tau\alpha^x$ maps to the residue class represented by x modulo p. Since $\mathrm{ord}(\alpha) = 2p$, the map $\overline{\cdot}$ is well-defined. We continue with a straightforward claim.

Claim A. Let $R \in \mathcal{F}(G)$ with $\mathrm{supp}(R) \subseteq \tau\langle\alpha\rangle$. Then R is a product-one sequence precisely when there there exists a factorization $R = R^+R^-$ such that $|\overline{R^+}| = |\overline{R^-}|$ and $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = \frac{1}{2}|R|p$.

Proof. Suppose R is a product-one sequence. Then there exists an ordering of R, say $R^* \in \mathcal{F}^*(G)$ with $[R^*] = R$, such that $\pi(R^*) = 1$. Since $\pi(R^*) = 1$ and $\mathrm{supp}(R) \subseteq \tau\langle\alpha\rangle$, it is easily deduced from the group presentation for G that $|R|$ must be even. Thus let

$$R^* = \diamond\tau\alpha^{r_1^-} \diamond \tau\alpha^{r_1^+} \cdot \ldots \cdot \diamond\tau\alpha^{r_w^-} \diamond \tau\alpha^{r_w^+} \in \mathcal{F}^*(G),$$

where r_i^-, $r_i^+ \in [0, 2p-1]$ and $w = \frac{1}{2}|R|$. Repeatedly applying the group presentation relations for G yields

$$1 = \pi(R^*) = (\tau\alpha^{r_1^-}\tau\alpha^{r_1^+})(\tau\alpha^{r_2^-}\tau\alpha^{r_2^+}) \cdots (\tau\alpha^{r_t^-}\tau\alpha^{r_t^+}) = \alpha^{wp + \sum_{i=1}^{w} r_i^+ - \sum_{i=1}^{w} r_i^-}, \tag{39}$$

thus implying

$$wp + \sum_{i=1}^{w} r_i^+ - \sum_{i=1}^{w} r_i^- \equiv 0 \mod 2p. \tag{40}$$

Let

$$R^- = [R^*(I^-)] = \diamond\tau\alpha^{r_1^-} \cdot \ldots \cdot \diamond\tau\alpha^{r_w^-} \quad \text{and} \quad R^+ = [R^*(I^+)] = \diamond\tau\alpha^{r_1^+} \cdot \ldots \cdot \diamond\tau\alpha^{r_w^+},$$

where $I^- = \{1, 3, \ldots, 2w-1\}$ and $I^+ = \{2, 4, \ldots, 2w\}$. Since $I^- \uplus I^+ = [1, 2w] = [1, |R|]$, we see that $R = R^+R^-$ with $|\overline{R^-}| = |R^-| = |R^+| = |\overline{R^+}| = w = \frac{1}{2}|R|$. Moreover, (40) is equivalent to saying $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = w = \frac{1}{2}|R|p$. Thus one direction of the claim in established.

Now suppose that we have a factorization $R = R^+R^-$ such that $|\overline{R^+}| = |\overline{R^-}|$ and $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = \frac{1}{2}|R|p$. Let $R^* \in \mathcal{F}^*(G)$ be an ordering of R such that $[R^*(I^-)] = R^-$ and $[R^*(I^+)] = R^+$, where $I^- \subseteq [1, |R|]$ is the subset of odd indices and $I^+ \subseteq [1, |R|]$ is the subset of even indices. Since $R = R^+R^-$ with $|R^+| = |\overline{R^+}| = |\overline{R^-}| = |R^-|$, it follows that $|R|$ is even, so that $|I^+| = |I^-| = \frac{1}{2}|R|$. Let $w = \frac{1}{2}|R|$ and let

$$R^*(2i-1) = \tau\alpha^{r_i^-} \quad \text{and} \quad R^*(2i) = \tau\alpha^{r_i^+} \quad \text{for } i \in [1, \tfrac{1}{2}|R|] = [1, w].$$

Then, in view of $\sigma(\overline{R^-}) - \sigma(\overline{R^+}) = \frac{1}{2}|R|p$, we see that (40) holds, and consequently also (39). Thus $1 = \pi(R^*) \in \pi([R^*]) = \pi(R)$, showing that R is a product-one sequence, which completes the claim. □

Using Claim A, we see that Lemma 4.3 is equivalent to saying that the maximal length of an atom $U \in \mathcal{A}(G)$ with $\operatorname{supp}(U) \subseteq \tau\langle\alpha\rangle$ is $|U| \le 2p+3$. However, this contradicts that we constructed above an atom $U' \in \mathcal{A}(G)$ with $\operatorname{supp}(U') \subseteq \tau\langle\alpha\rangle$ and $|U'| \ge 2p+4$, completing the proof. □

With the above preparatory work complete, we are now ready to begin the proof of Theorem 1.1

Proof of Theorem 1.1. If G is cyclic, then $\mathsf{d}(G) = |G| - 1$ is well-known ([10, Theorem 5.1.10]), while $\mathsf{d}(G) = \frac{1}{2}|G|$ follows for non-cyclic G having a cyclic, index 2 subgroup by Theorem 3.1. If G is abelian, then $|G'| = 1$ and $\mathsf{D}(G) = \mathsf{d}(G)+1$ follows routinely as noted in Section 2. Therefore we may assume G is non-abelian, hence non-cyclic. We may assume G satisfies the General Assumptions for Section 5. Lemma 5.6 gives $\mathsf{d}(G) + |G'| = \frac{1}{2}|G| + |G'| \le \mathsf{D}(G)$. Since G is non-abelian, Lemma 5.4 gives $|G'| = n^+ \ge 2$, and it remains to show the upper bound

$$\mathsf{D}(G) \le \frac{1}{2}|G| + |G'| = n + n^+. \tag{41}$$

Since G is now assumed to be non-abelian, we have $n^+ \ge 2$. Thus, by Lemma 5.7, it suffices to prove (41) when $|G'| = n^+ = p$ is prime. Furthermore, if $n^+ = 2$, then Lemma 3.4 yields (41). Consequently, we can assume

$$|G'| = n^+ = p \ge 3 \quad \text{is prime.} \tag{42}$$

In particular, only the cases where $n^+ = p$ is odd remain, which in view of (27) means that $\rho(P) = 1$. From the definition of ρ, we see that $\rho(P) = 1$ corresponds to when $P \cong C_{2^{s+1}}$ or $P \cong C_2 \times C_{2^s}$. However, if $P \cong C_2 \times C_{2^s}$ is non-cyclic, then Lemma 5.5 shows that $C_G(\tau) \cong C_2 \times C_{n^-}$ is non-cyclic. Since $\mathsf{D}(C_2 \times C_{n^-}) = n^- + 1$ is well-known ([10, Theorem 5.8.3]), invoking Theorem 3.2 would then yield

$$\mathsf{D}(G) \le \mathsf{D}(C_G(\tau))|G : C_G(\tau)| = \mathsf{D}(C_2 \times C_{n^-})\, n^+ = (n^- + 1)n^+ = n + n^+,$$

yielding (41). So it remains to prove (41) when

$$P \cong C_{2^{s+1}} \quad \text{is cyclic with } \rho(P) = 1.$$

In particular, Theorem 5.3 now tells us that G has type (C).

If $n^- = 1$, then (27) and the definition of n^- and m^- ensure that $s = 0$, $r = n-1$ and $p = n^+ = n$. This corresponds to the case when G is dihedral of order $2n$ with n odd. In this case, Lemma 2.3 implies $\mathsf D(G) \le |G| = 2n = n + n^+$, yielding (41). Therefore we may assume $n^- \ge 2$.

Suppose $n^- = 2$. Then it follows in view of $\rho(P) = 1$ and (27) that

$$s = 1, \quad m^- = 1, \quad n^+ = m^+ = m = p \quad \text{and} \quad n = 2m = 2p.$$

Since P is cyclic with $s = 1$, Theorem 5.3 ensures that G has types (C) and (B) (these types coincide for $s = 1$) with

$$(r-1)(r+1) = r^2 - 1 \equiv 0 \mod m \quad \text{and} \quad r \equiv 1 \mod 2.$$

In consequence, since $1 = m^- = \gcd(r-1, m)$ and $r \in [0, n-1]$, it follows that $r = n-1 = 2p-1$. As a result, we see that $G \cong Q_{4p}$ is dicyclic, in which case Lemma 5.9 yields (41). So we may assume

$$n^- \ge 3. \tag{43}$$

To establish (41), assume by contradiction that we have an atom $U \in \mathcal A(G)$ with

$$|U| = \mathsf D(G) \ge n + n^+ + 1 = n^+ n^- + n^+ + 1. \tag{44}$$

Factor $U = U_\alpha U_\tau$ with U_α the subsequence consisting of all terms from $\langle \alpha \rangle$ and U_τ the subsequence consisting of all terms from $\tau\langle \alpha \rangle$. In view of Lemma 5.4, we know

$$Z(G) = \langle \alpha^{n^+} \rangle = \langle \alpha^p \rangle \quad \text{and} \quad G' = \langle \alpha^{n^-} \rangle = \langle \alpha^{r-1} \rangle \quad \text{with} \quad |G'| = n^+ = p.$$

Let $U'_\alpha \mid U_\alpha$ be the subsequence consisting of all terms from $\langle \alpha \rangle \setminus Z(G)$. Then, since $Z(G) = \langle \alpha^p \rangle$, we see that $U_\alpha {U'_\alpha}^{-1}$ is the subsequence of U consisting of all terms from $Z(G)$.

Let us next show that

$$|U'_\alpha| \le n^+ - 2, \quad |U_\alpha {U'_\alpha}^{-1}| \le n^- - 1 \quad \text{and} \quad |U_\alpha| \le n^+ + n^- - 3. \tag{45}$$

In view of Lemma 5.8, we have $|U'_\alpha| \le n^+ - 2$. Thus, if (45) fails, then we must have $|U_\alpha {U'_\alpha}^{-1}| = |U_\alpha| - |U'_\alpha| \ge n^-$. In other words, there are at least $n^- = |Z(G)|$ terms of U from $Z(G)$. Since $U \in \mathcal A(G)$ is an atom, let $U^* \in \mathcal F^*(G)$ with $[U^*] = U$ be an ordering of U such that $\pi(U^*) = 1$. Any term from $Z(G)$ can be moved around in the ordered sequence U^* without changing the value of $\pi(U^*)$. Thus we can w.l.o.g. assume all terms from $U_\alpha {U'_\alpha}^{-1}$ are consecutive in U^*. In consequence, since $|U_\alpha {U'_\alpha}^{-1}| \ge |Z(G)| = n^-$, we can apply Lemma 2.3 to $U_\alpha {U'_\alpha}^{-1}$ to find a nontrivial, consecutive product-one subsequence $U^*(I)$, where $I \subseteq [1, |U|]$ is an interval. Moreover, $|U^*(I)| \le |Z(G)| = n^- < |U|$, meaning $U^*(I) \mid U$ is proper. But since $U = [U^*] \in \mathcal A(G)$ is an atom, this contradicts Lemma 2.1. So (45) is established, as claimed.

Define a map $\iota : G \to \mathbb Z$ by setting

$$\iota(\tau^y \alpha^x) = x, \quad \text{where } x \in [0, n-1] \text{ and } y \in [0, 1],$$

and define a map $\bar{\cdot} : G \to \mathbb Z/p\mathbb Z$ by setting

$$\overline{g} = \phi_{p\mathbb Z}(\iota(g)) \quad \text{for } g \in G,$$

so $g \in G$ maps to the residue class modulo p given by $\iota(g)$.

Let $R \in \mathcal{F}(G)$ be a sequence and let $R^* \in \mathcal{F}^*(G)$ be an arbitrary ordering of R, so $[R^*] = R$. Factor $R = R_\alpha R_\tau$ with $\mathrm{supp}(R_\alpha) \subseteq \langle\alpha\rangle$ and $\mathrm{supp}(R_\tau) \subseteq \tau\langle\alpha\rangle$. We proceed to describe $\pi(R)$ under the assumption that

$$|R_\tau| \geq 1.$$

First note that from the defining relations for G, it is clear that $\pi(R^*) \in \langle\alpha\rangle$ if and only if the number of terms of R from $\tau\langle\alpha\rangle$ is even, that is, if $|R_\tau|$ is even. Let $\omega = \lfloor \frac{1}{2}|R_\tau| \rfloor$, so that $|R_\tau| = 2\omega$ when $\pi(R^*) \in \langle\alpha\rangle$ and $|R_\tau| = 2\omega + 1$ when $\pi(R^*) \in \tau\langle\alpha\rangle$.

Next, since G has type (C), a routine application of the defining relations from Lemma 5.1 for G shows that

$$\pi(R^*) = \tau^\epsilon \alpha^{\omega m + \sum_{i=1}^{|R|} d_i \iota(R^*(i))}, \tag{46}$$

where $\epsilon = 1$ if $|R_\tau|$ is odd, $\epsilon = 0$ if $|R_\tau|$ is even, $d_i = 1$ if the number of terms of R^* from $\tau\langle\alpha\rangle$ to the right of $R^*(i)$ is even, and $d_i = r$ if the number of terms of R^* from $\tau\langle\alpha\rangle$ to the right of $R^*(i)$ is odd.

There are some important consequences of the formula (46). Let $I \subseteq [1, |R|]$ be the set of indices such that $[R^*(I)] = R_\tau$. If we fix the position of every term $R^*(i)$ with $i \notin I$ but allow ourselves to permute the terms within $R^*(I)$, this maintains that $[R^*(I)] = R_\tau$ while each coefficient d_i, for $i \in [1, |R|] \setminus I$, remains unaffected and constant. In consequence, when trying to determine the possible values for (46) over all orderings R^*, we can first decide how to distribute the terms from R_α into R^*, thus fixing and determining the subset of indices $I \subseteq [1, |R|]$ with $[R^*(I)] = R_\tau$, and then decide how to permute the terms within $R^*(I)$. Since $|R_\tau| \geq 1$, every term of R_α can either be placed in R^* such that the number of terms of R^* from $\tau\langle\alpha\rangle$ to its right is even, or such that this number is odd. Changing this choice has the effect on (46) of switching d_i between 1 and r. Once we have fixed how the terms of R from $\langle\alpha\rangle$ are to be distributed in R^*, the set $I \subseteq [1, |R|]$ is then fixed, but we are free to re-order the terms from R_τ so long as we preserve $[R^*(I)] = R_\tau$ and this will not effect whether $d_i = 1$ or $d_i = r$ holds for any $i \in [1, |R|] \setminus I$.

Concerning the terms of R^* from R_τ, whether $d_i = 1$ or $d_i = r$ holds for $i \in I$ depends entirely on whether $R^*(i) = (R^*(I))(j)$ with $j \equiv \epsilon \mod 2$ or $j \equiv \epsilon - 1 \mod 2$. If $j \equiv \epsilon \mod 2$, then $d_i = 1$, and if $j \equiv \epsilon - 1 \mod 2$, then $d_i = r$. Letting

$$J = \{1 + \epsilon, 3 + \epsilon, \ldots, 2\omega - 1 + \epsilon\} \subseteq [1, |R_\tau|]$$

be the subset of indices congruent to $\epsilon - 1$ modulo 2, we are free to arrange for $[(R^*(I))(J)]$ to be any subsequence of R_τ having length $\omega = \lfloor \frac{1}{2}|R_\tau| \rfloor$, and then $d_i = r$ will hold for all these terms, while $d_i = 1$ will hold for all remaining terms of R_τ.

In summary, the above works shows that

$$\pi(R) = \tau^\epsilon \alpha^{\omega m} \{\alpha^x : \ x \in X\},$$

where

$$\begin{aligned} X &= \sum_{i=1}^{|R_\alpha|} \Big\{ \iota\Big(R_\alpha^*(i)\Big), \ r\,\iota\Big(R_\alpha^*(i)\Big) \Big\} + \Big\{ r\,\sigma(\iota(R'_\tau)) + \sigma(\iota(R_\tau {R'_\tau}^{-1})) : \ R'_\tau \mid R_\tau, \ |R'_\tau| = \omega = \Big\lfloor \frac{1}{2}|R_\tau| \Big\rfloor \Big\} \\ &= \sigma(\iota(R)) + (r-1)\Big(\big\{0, \iota\big(R_\alpha^*(1)\big)\big\} + \ldots + \big\{0, \iota\big(R_\alpha^*(|R_\alpha|)\big)\big\} + \Sigma_{\lfloor \frac{1}{2}|R_\tau| \rfloor}(\iota(R_\tau)) \Big). \end{aligned}$$

Consequently,

$$\pi(R) = \tau^\epsilon \alpha^{xm + \sigma(\iota(R))} \{(\alpha^{r-1})^y : \ y \in Y\}, \tag{47}$$

where

$$Y = \Big\{0, \iota\Big(R^*_\alpha(1)\Big)\Big\} + \ldots + \Big\{0, \iota\Big(R^*_\alpha(|R_\alpha|)\Big)\Big\} + \Sigma_{\lfloor \frac{1}{2}|R_\tau|\rfloor}(\iota(R_\tau)).$$

Since $\mathrm{ord}(\alpha^{r-1}) = \mathrm{ord}(\alpha^{n^-}) = n^+ = p$, we conclude that $|\pi(R)|$ is equal to the number of distinct residue classes modulo p in Y.

Let us next apply some of the above reasoning to the sequence U in the following claim, which shows that any sufficiently small subsequence can be placed in an ordering of U so as to avoid some long length consecutive subsequence.

Claim A. If $T \mid U$ is a subsequence with $|T| \le n^+ - 1$, then there exists an ordering of U, say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$, and an interval $J \subseteq [1, |U|]$ such that $\pi(U^*) = 1$, $T \mid \Big[U^*\Big([1, |U|] \setminus J\Big)\Big]$ and $|J| \ge 2n^-$.

Proof. Since $U \in \mathcal{A}(G)$ is an atom, there is an ordering of U, say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$, such that $\pi(U^*) = 1$. In view of (45) and (44), we know $\mathrm{supp}(U) \cap \tau\langle\alpha\rangle \ne \emptyset$. Thus, in view of Lemma 2.4, we can cyclically shift the terms of U^* until w.l.o.g. $U^*(1) \in \tau\langle\alpha\rangle$. In view of the formula (46) for $U^* = R^*$, we see that we can shift the position of a term x of U^* from $\langle\alpha\rangle$ while preserving that $\pi(U^*) = 1$ so long as we maintain the parity of the number of terms of U^* from $\tau\langle\alpha\rangle$ that follow to the right of x. In particular, we can put all terms of U^* from $\langle\alpha\rangle$ for which this number is odd into a consecutive block starting with the second term of U^*, while also putting all terms of U^* from $\langle\alpha\rangle$ for which this number is even into a consecutive block at the very end of U^*, and this will preserve that $\pi(U^*) = 1$. In other words, we may w.l.o.g. assume U^* has the form

$$U^* = \diamond\tau\alpha^{x_1}(\diamond\alpha^{y_i} \cdot \ldots \diamond \alpha^{y_t})(\diamond\tau\alpha^{x_2} \cdot \ldots \cdot \diamond\tau\alpha^{x_{2w}})(\diamond\alpha^{y'_1} \cdot \ldots \cdot \diamond\alpha^{y'_{t'}}),$$

for some t, $t' \ge 0$ with

$$t + t' = |U_\alpha|, \quad 2w = |U_\tau| \ge 2, \qquad \text{and} \qquad x_i,\, y_i,\, y'_i \in [0, n-1].$$

Let $J' \subseteq [1, |U|]$ be those indices $j \in [1, |U|]$ such that $U^*(j) \in \tau\langle\alpha\rangle$, i.e.,

$$J' = \{1\} \cup [t+2, t+2w].$$

Now $T = U^*(I)$ for some $I \subseteq [1, |U|]$. Factor $T = T_\alpha T_\tau$ with T_α the subsequence consisting of terms from $\langle\alpha\rangle$ and T_τ the subsequence with terms from $\tau\langle\alpha\rangle$. Since $\mathrm{supp}(U^*(J')) \subseteq \tau\langle\alpha\rangle$, we see that T_α is disjoint from $U^*(J')$. For the remaining terms of T, we must have $T_\tau = (U^*(J'))(X)$ for some subset $X \subseteq [1, 2w]$. Let $X = X^+ \cup X^-$, where $X^+ \subseteq X$ is the subset of indices $x \in X$ with x odd and $X^- \subseteq X$ is the subset of indices $x \in X$ with x even. Consider an arbitrary term of T from $\tau\langle\alpha\rangle$, say $(U^*(J'))(x)$ with $x \in X \subseteq [1, 2w]$. If $x \in X^+$, then $(U^*(J'))(x)$ can be moved freely about in $(U^*(J'))(\{1, 2, \ldots, 2w-1\})$ without changing that $\pi(U^*) = 1$. Likewise, if $x \in X^-$, then $(U^*(J'))(x)$ can be moved freely about in $(U^*(J'))(\{2, 4, \ldots, 2w\})$ without changing that $\pi(U^*) = 1$. Consequently, we can w.l.o.g assume that X^+ consists of the first $|X^+|$ elements from $\{1, 3, \ldots, 2w-1\}$ and that X^- consists of the first $|X^-|$ elements from $\{2, 4, \ldots, 2w\}$. But this means that

$$T_\tau \mid U^*\Big(\{1\} \cup [t+2, t+2|X|]\Big).$$

As a result, setting

$$J := [t + \max\{2|X|, 1\} + 1, t + 2w] \subseteq J'$$

and recalling from the beginning o the paragraph that T_α is disjoint from $U^*(J')$, we find that $T \mid \Big[U^*\Big([1,|U|] \setminus J\Big)\Big]$. It remains to estimate $|J|$.

Since $|X| = |T_\tau| \le |T| \le n^+ - 1$ holds by hypothesis, it follows in view of (42) that

$$|J| = 2w - \max\{2|X|, 1\} = |U_\tau| - \max\{2|X|, 1\} \ge |U_\tau| - \max\{2|T|, 1\} \ge |U_\tau| - 2n^+ + 2. \tag{48}$$

From (45) and (44), we know

$$|U_\tau| = |U| - |U_\alpha| \ge (n + n^+ + 1) - (n^+ + n^- - 3) = n^+n^- - n^- + 4.$$

Combining this with (48) and making use of (42) and (43), we find that

$$|J| \ge n^+n^- - 2n^+ - n^- + 6 = 3n^- - 6 - n^- + 6 = 2n^-,$$

completing the proof of Claim A. □

We will say that a subsequence $T \mid U$ is *good* if it has an ordering $T^* \in \mathcal{F}^*(G)$, so $[T^*] = T$, such that

$$T^* = \diamond y_1 \diamond z_1 \cdot \ldots \cdot \diamond y_w \diamond z_w \diamond x_1 \cdot \ldots \cdot \diamond x_v \tag{49}$$

with v, $w \ge 0$,

$$x_i \in \langle\alpha\rangle \setminus Z(G) \quad \text{for } i \in [1, v], \quad \text{and} \quad y_i,\, z_i \in \tau\langle\alpha\rangle \quad \text{and} \quad \iota(y_i) \not\equiv \iota(z_i) \mod p \quad \text{for } i \in [1, w].$$

Furthermore, we define

$$\varphi(T^*) = \diamond y_1 z_1 \cdot \ldots \cdot \diamond y_w z_w \diamond x_1 \cdot \ldots \diamond x_v \in \mathcal{F}^*(\langle\alpha\rangle) \quad \text{and} \quad \ell(T) = |\varphi(T^*)| = v + w.$$

We continue with the following claim.

Claim B. If $T \mid U$ is a good subsequence with $\ell(T) \ge n^+ - 1 = p - 1$, then $\pi(T)$ is a G'-coset.

Proof. Let $T^* \in \mathcal{F}^*(G)$ be an ordering from the definition of T notated as in (49). Since $\ell(T) \ge n^+ - 1 = p-1$, it follows from (45) that $w \ge 1$. As remarked in Section 2, $\pi(T)$ is contained in a G'-coset. Therefore we need to show that $|\pi(T)| = |G'| = p$.

Since $w \ge 1$, it follows from (47) and the definition of $\overline{g}$ that

$$|\pi(T)| = |\{0, \overline{x_1}\} + \ldots + \{0, \overline{x_v}\} + \Sigma_w(\overline{T_\tau})|, \tag{50}$$

where $T_\tau \mid T$ is the subsequence of terms from $\tau\langle\alpha\rangle$. Note that $|T_\tau| = 2w$. Since T is good, we know $x_i \in \langle\alpha\rangle \setminus Z(G) = \langle\alpha\rangle \setminus \langle\alpha^p\rangle$ for $i \in [1, v]$, which means that $\overline{x_i} \ne 0$ for all $i \in [1, v]$. Consequently, since p is prime, we can apply the Cauchy-Davenport Theorem to $\{0, \overline{x_1}\} + \ldots + \{0, \overline{x_v}\}$ to conclude

$$|\{0, \overline{x_1}\} + \ldots + \{0, \overline{x_v}\}| \ge \min\{p,\, v + 1\}. \tag{51}$$

Since T is good, we have $\overline{y_i} \ne \overline{z_i}$ for $i \in [1, w]$, which together with the pigeonhole principle ensures that $\mathsf{h}(\overline{T_\tau}) \le w$. Consequently, since p is prime, we can apply Theorem 4.2 to $\Sigma_w(\overline{T_\tau})$ to conclude

$$|\Sigma_w(\overline{T_\tau})| \ge \min\{p,\, |T_\tau| - w + 1\} = \min\{p,\, w + 1\}. \tag{52}$$

Applying the Cauchy-Davenport Theorem to the 2-fold sumset $(\{0, \overline{x_1}\} + \ldots + \{0, \overline{x_v}\}) + \Sigma_w(\overline{T_\tau})$, using (51) and (52), and recalling the case hypothesis $\ell(T) \ge p - 1$, it follows that

$$|\,(\{0, \overline{x_1}\} + \ldots + \{0, \overline{x_v}\}) + \Sigma_w(\overline{T_\tau})| \ge \min\{p,\, v + 1 + w + 1 - 1\} = \min\{p,\, \ell(T) + 1\} = p.$$

Combining this with (50) completes the proof of Claim B. □

Let $T \mid U$ be a good subsequence with $\ell(T) \ge 0$ maximal and let $T^* \in \mathcal{F}^*(G)$ be an ordering from the definition of T notated as in (49). We handle two cases.

Case 1: $\ell(T) \ge 2n^+ + n^- - 3$.

We first proceed to show that there is a good subsequence $T' \mid T$ with

$$\ell(T') \ge n^+ - 1, \quad \pi(T') \subseteq G', \qquad \text{and} \qquad \ell(TT'^{-1}) \ge n^+ - 1. \tag{53}$$

To do so, it suffices, in view of the case hypothesis $\ell(T) = |\varphi(T^*)| \ge 2n^+ + n^- - 3$, to show that $[\phi_{G'}(\varphi(T^*))]$ has a product-one subsequence of length $\ell \in [n^+ - 1, n^+ - 2 + n^-]$. Note that

$$[\phi_{G'}(\varphi(T^*))] \in \mathcal{F}(\langle\alpha\rangle/G').$$

Thus, since $\ell(T) \ge n^+ - 2 + n^-$ holds by hypothesis, and since $\mathsf{d}(\langle\alpha\rangle/G') + 1 \le |\langle\alpha\rangle/G'| = n^-$ follows from Lemma 2.3, such a subsequence can be found simply by repeated application of the definition of $\mathsf{d}(\langle\alpha\rangle/G')$ to $[\phi_{G'}(\varphi(T^*))]$. This establishes (53).

In view of (53) and Claim B, we have $\pi(T') = G'$. In particular, T' is a nontrivial product-one subsequence of U. Thus Lemma 2.2 shows that $\pi(UT'^{-1}) \subseteq G'$. As a result, since $TT'^{-1} \mid UT'^{-1}$, it follows in view of (53) and Claim B that $\pi(UT'^{-1}) = G'$, so that UT'^{-1} is also a product-one subsequence. But now $U = T'(UT'^{-1})$ is a factorization of U into 2 nontrivial product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. This completes Case 1.

Case 2: $\ell(T) \le 2n^+ + n^- - 4$.

In view of (45), we know $|U_\alpha U_\alpha'^{-1}| \le n^- - 1$. We have

$$2(2n^+ + n^- - 4) + 1 \le |U| - |U_\alpha U_\alpha'^{-1}|, \tag{54}$$

for if (54) failed, then $|U_\alpha U_\alpha'^{-1}| \le n^- - 1$, (44), (42) and (43) would imply

$$0 > |U| - 4n^+ - 3n^- + 8 \ge n^+n^- - 3n^+ - 3n^- + 9 = (n^+ - 3)(n^- - 3) \ge 0,$$

which is a contradiction. In view of the maximality of $\ell(T)$, we must have $U_\alpha' \mid T$. Let $T_\tau = TU_\alpha'^{-1}$. Then, in view of the case hypothesis, it follows that $T_\tau \mid U_\tau$ is a good subsequence with

$$\ell(T_\tau) = \ell(T) - |U_\alpha'| \le 2n^+ + n^- - |U_\alpha'| - 4 \quad \text{ maximal subject to } T_\tau \mid U_\tau. \tag{55}$$

From (54), we deduce that

$$2(2n^+ + n^- - 4 - |U_\alpha'|) + 1 \le |U| - |U_\alpha U_\alpha'^{-1}| - |U_\alpha'| = |U_\tau|. \tag{56}$$

Now $|U_\tau|$ must be even as remarked above (46), which means that the inequality in (56) must be strict:

$$2(2n^+ + n^- - |U_\alpha'| - 3) \le |U_\tau|. \tag{57}$$

It is readily seen that a subsequence $R \mid U_\tau$ being a good is equivalent to $\overline{R}$ having an $\frac{1}{2}|R|$-setpartition with $|R|$ even. In view of (55) and (45), we see that U_τ does not have a good subsequence $R \mid U_\tau$ with

$$\ell(R) = \frac{1}{2}|R| = \ell := 2n^+ + n^- - |U_\alpha'| - 3 \ge 0.$$

Thus applying Lemma 2.6 to $\overline{U_\tau}$ taking $\ell = n$, we conclude that either $2\ell > |U_\tau|$ or there exists a nonempty subset $X \subseteq G$ with $|X| \le \lfloor \frac{\ell-1}{\ell} + 1 \rfloor = 1$ such that at least $|U_\tau| - \ell + 1$ terms of $|\overline{U_\tau}|$ are all from X. In view of (57), we see that the former is not possible, in which case the latter must hold, and with $|X| = 1$. In other words,

$$\mathsf{h}(\overline{U_\tau}) \ge |U_\tau| - \ell + 1. \tag{58}$$

Now (58) is equivalent to saying that there is some $x_0 \in [0, p-1]$ such that all but at most $\ell - 1$ terms of U_τ have the form $\tau\alpha^x$ with $x \equiv x_0 \mod p$. However, since $p = n^+ = m^+ \mid r + 1$ follows from (27) in view of $\rho(P) = 1$ and the definition of m^+, a short calculation shows that

$$H := \{\tau\alpha^x : \ x \in [0, n-1] \ \text{ and } \ x \equiv x_0 \mod p\} \cup \{\alpha^y : \ y \equiv 0 \mod p\} \le G$$

is a subgroup of G having $|H| = 2n^-$. Indeed, $H = C_G(\tau\alpha^{x_0}) = \langle \alpha^p, \tau\alpha^{x_0} \rangle$, though we will not need this fact.

Let $U_H \mid U$ be the subsequence of U with terms from H. In view of the two previous paragraphs, we see that (58) is equivalent to saying

$$|UU_H{}^{-1}| = \ell(T) \le |U'_\alpha| + \ell - 1 = 2n^+ + n^- - 4. \tag{59}$$

As a result, we have

$$|U_H| \ge 2n^- + n^+ - 1, \tag{60}$$

for if (60) failed, then combining this with (59) and (44) would yield

$$n^+n^- + n^+ + 1 \le |U| = |U_H| + |UU_H{}^{-1}| \le 4n^+ + 2n^- - 6,$$

and then rearranging the above inequality and applying (42) and (43) yields the contradiction

$$0 \ge n^+n^- - 3n^+ - 2n^- + 7 \ge 3n^+ - 3n^+ - 6 + 7 = 1.$$

With these key facts finally established, we are now ready to finish the proof, which we do in 2 short subcases.

Case 2.1. $|UU_H{}^{-1}| = \ell(T) \ge n^+ - 1$.

We must have

$$|U_H| \ge 2n^-, \tag{61}$$

for if (61) failed, then combining this with (59) and (44) would yield

$$2n^- - 1 \ge |U_H| \ge |U| - 2n^+ - n^- + 4 \ge n^+n^- - n^+ - n^- + 5,$$

implying, in view of (42) and (43), that

$$0 \ge n^+n^- - n^+ - 3n^- + 6 \ge 3n^- - 3 - 3n^- + 6 = 3,$$

which is a contradiction.

In view of (61) and (45), we can find a subsequence $U'_H \mid U_H$ with $U_\alpha U'_\alpha{}^{-1} \mid U'_H$ and $|U'_H| = 2n^-$. Since $H \cap \langle\alpha\rangle = \langle\alpha^p\rangle = Z(G)$ and since $U_\alpha U'_\alpha{}^{-1}$ is the subsequence of U consisting of all terms from $Z(G)$, we see that

$$\operatorname{supp}(U_H U'_H{}^{-1}) \subseteq \tau\langle\alpha\rangle. \tag{62}$$

Since $|U'_H| = 2n^- = |H|$, applying Lemma 2.3 to U'_H yields a nontrivial product-one subsequence $R \mid U'_H$. From Lemma 2.2, it follows that

$$\pi(UR^{-1}) \subseteq G'. \tag{63}$$

Since $R \mid U'_H$ and $U'_H \mid U_H$, we have

$$U_H {U'_H}^{-1} \mid U_H R^{-1} \quad \text{and} \quad U {U_H}^{-1} \mid UR^{-1}. \tag{64}$$

From (60), we find that

$$|U_H {U'_H}^{-1}| \ge 2n^- + n^+ - 1 - |U'_H| = n^+ - 1.$$

Consequently, it follows in view of (62) that there are at least $n^+ - 1$ terms of $U_H {U'_H}^{-1}$ from $\tau\langle\alpha\rangle$, which together with the first conclusion of (64) shows that there are at least $n^+ - 1$ terms of $U_H R^{-1}$ from $\tau\langle\alpha\rangle$. Combining this with the second conclusion from (64) shows that UR^{-1} contains a good subsequence $T \mid UR^{-1}$ with $\ell(T) \ge \min\{n^+ - 1, |U {U_H}^{-1}|\} \ge n^+ - 1$, where the latter inequality follows in view of the subcase hypothesis. But now, in view of (63), we can apply Claim B to find that $\pi(UR^{-1})$ is not just contained in G', but must be equal to G', so $\pi(UR^{-1}) = G'$. Hence $U = R(UR^{-1})$ is a factorization of U into 2 nontrivial product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom.

Case 2.2. $|U {U_H}^{-1}| = \ell(T) \le n^+ - 2$.

In this case, we can apply Claim A using $T = U {U_H}^{-1}$ to find an ordering of U, say $U^* \in \mathcal{F}^*(G)$ with $[U^*] = U$, and an interval $J \subseteq [1, |U|]$ such that

$$\pi(U^*) = 1, \quad T = U {U_H}^{-1} \mid U^*\Big([1, |U|] \setminus J\Big) \quad \text{and} \quad |J| \ge |H| = 2n^-.$$

In view of $T = U {U_H}^{-1} \mid U^*([1, |U|] \setminus J)$, we have $U^*(J) \mid U_H$. Thus $U^*(J) \in \mathcal{F}(H)$ with $|U^*(J)| = |J| \ge 2n^- = |H|$. As a result, applying Lemma 2.3 yields a nontrivial, consecutive product-one subsequence R^* in $U^*(J)$ with $|R^*| \le 2n^-$. Since $U^*(J) \mid U^*$ is also consecutive, this means that $R^* \mid U^*$ is a nontrivial consecutive product-one sequence in U^* with $U = [U^*] \in \mathcal{A}(G)$ an atom, in which case Lemma 2.1 ensures that $R^* = U^*$. But then (44) and (42) give

$$2n^- \ge |R^*| = |U^*| = |U| \ge n^- n^+ + n^+ + 1 \ge 3n^- + 4,$$

which is a proof concluding contradiction. □

Acknowledgement

We wish to thank the referee for their suggestions, particularly the idea leading to Theorem 3.2, without which the paper would have remained much more limited in scope.

References

[1] J. Bass, *Improving the Erdős-Ginzburg-Ziv theorem for some non-abelian groups*, J. Number Theory **126** (2007), 217 – 236.

[2] A. Bialostocki, P. Dierker, D. J. Grynkiewicz, and M. Lotspeich, On some developments of the Erdo"s-Ginzburg-Ziv theorem II, *Acta Arith.* 110 (2003), no. 2, 173-184.

[3] Y. Caro, *Zero-sum problems - a survey*, Discrete Math. **152** (1996), 93 – 113.

[4] M. DeVos, L. Goddyn, and B. Mohar, *A generalization of Kneser's addition theorem*, Adv. Math. **220** (2009), 1531 – 1548.

[5] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337 – 369.

[6] W. Gao and Yuanlin Li, *The Erdős-Ginzburg-Ziv theorem for finite solvable groups*, J. Pure Appl. Algebra **214** (2010), 898 – 909.

[7] W. Gao and Zaiping Lu, *The Erdős-Ginzburg-Ziv theorem for dihedral groups*, J. Pure Appl. Algebra **212** (2008), 311 – 319.

[8] A. Geroldinger, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory (A. Geroldinger and I. Ruzsa, eds.), Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1 – 86.

[9] A. Geroldinger and D. J. Grynkiewicz, The Large Davenport Constant II: General Upper Bounds, preprint.

[10] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[11] A. Geroldinger and M.D. Neusel, *On the interplay between invariant theory and zero-sum theory*, manuscript.

[12] D.J. Grynkiewicz, *Structural Additive Theory*, to appear, 2013.

[13] M. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer-Verlag, New York, 1996.

[14] M. D. Neusel, *Degree bounds – an invitation to postmodern invariant theory*, Topology Appl. **154** (2007), 792 – 814.

[15] J.E. Olson and E.T. White, *Sums from a sequence of group elements*, Number Theory and Algebra (H. Zassenhaus, ed.), Academic Press, 1977, pp. 215 – 222.

[16] Derek J. S. Robinson, *A Course in the Theory of Groups*, Graduate Texts in Mathematics 80, Springer-Verlag New York, Inc. (Harrisonburg, VA, USA), 1996.

[17] K. Rogers, A combinatorial problem in abelian groups, *Proc. Cambridge Philos. Soc.*, 59 (1963), 559–562.

[18] Guoquing Wang and Weidong Gao, *Davenport constants for semigroups*, Semigroup Forum **76** (2008), 234 – 238.

[19] J. Zhuang and W. Gao, *Erdős-Ginzburg-Ziv theorem for dihedral groups of large prime index*, Eur. J. Comb. **26** (2005), 1053 – 1059.

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: alfred.geroldinger@uni-graz.at, diambri@hotmail.com