THE LARGE DAVENPORT CONSTANT II: GENERAL UPPER BOUNDS

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 partitioned into two nontrivial, product-one subsequences. The goal of this paper is to present several upper bounds for $\mathsf{D}(G)$, including the following:

$$\mathsf{D}(G) \le \begin{cases} \mathsf{d}(G)+2|G'|-1, & \text{where } G'=[G,G]\le G \text{ is the commutator subgroup;} \\ \frac{3}{4}|G|, & \text{if } G \text{ is neither cyclic nor dihedral of order } 2n \text{ with } n \text{ odd;} \\ \frac{2}{p}|G|, & \text{if } G \text{ is noncyclic, where } p \text{ is the smallest prime divisor of } |G|; \\ \frac{p^2+2p-2}{p^3}|G|, & \text{if } G \text{ is a non-abelian } p\text{-group.} \end{cases}$$

As a main step in the proof of these bounds, we will also show that $\mathsf{D}(G)=2q$ when G is a non-abelian group of order $|G|=pq$ with p and q distinct primes such that $p \mid q-1$.

1. INTRODUCTION

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 [5, Lemma 2.4] shows that

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

with equality in the first bound when G is abelian, and equality in the second when G is cyclic.

The study of $\mathsf{D}(G)$, for G abelian, is a classical and very difficult problem in Combinatorial Number Theory. When G is non-abelian, there is more than one way to naturally extend the definition of the Davenport constant. This was first done by Olson and White [13] who introduced the small Davenport constant $\mathsf{d}(G)$ and gave the general upper bound $\mathsf{d}(G) \le \frac{1}{2}|G|$ (for G non-cyclic) that was observed to be tight for non-cyclic groups having a cyclic, index 2 subgroup.

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

Key words and phrases. zero-sum, product-one, Davenport constant.

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

This paper is a continuation of [5]. There, paralleling the result of Olson and White, the author along with A. Geroldinger determined the large Davenport constant $\mathsf{D}(G)$ for groups having a cyclic, index 2 subgroup. Here, we parallel the result of Olson and White in a different fashion, proving several general upper bounds for $\mathsf{D}(G)$. In view of (1), the bounds proved here, in many cases, also improve upon the upper bound of Olson and White for the small Davenport constant. For detailed background and motivation concerning the study of $\mathsf{D}(G)$, including connections with Invariant Theory, we direct the reader to the prior paper [5]. We follow the notation outlaid in detail in [5] and will make frequent use of the results cited and proved there.

The paper is organized as follows. In Section 2, we describe the prerequisite notation and results, including a summary of what is needed from [5]. In Section 3, we that the closer a group is to being abelian, the closer the lower bound $\mathsf{d}(G)+1 \le \mathsf{D}(G)$ is to being accurate. Specifically, we prove the upper bound $\mathsf{D}(G) \le \mathsf{d}(G)+2|G'|-1$, where $G'=[G,G] \le G$ is the commutator subgroup, with equality holding if and only if G is abelian. We will also prove a crucial technical lemma needed for later sections as well as a refinement of the bound $\mathsf{D}(G) \le \mathsf{d}(G)+2|G'|-1$ under additional hypotheses. In Section 4, we prove several upper bounds for $\mathsf{D}(G)$ when G is a p–group. Chief among these, that $\mathsf{D}(G) \le \frac{p^2+2p-2}{p^3}|G|$ holds for a non-abelian p–group G. In Section 5, we tackle the main group of difficulty in this paper—the non-abelian group of order pq—and determine the exact value of the large Davenport constant for such groups (the small Davenport constant of these groups was previously computed by Bass [1]). The methods used in Section 5 will then be put to further use in Section 6 to determine the small Davenport constant of another problematic group: $G=\langle \alpha, \tau : \ \alpha^q=1, \quad \tau^4=1, \quad \alpha\tau=\tau\alpha^r\rangle$, where q is an odd prime and $r^2 \equiv -1 \mod q$. Finally, in Section 7, making full use of the previous results as well as the main result from [5], we prove two general upper bounds for $\mathsf{D}(G)$ when G is non-cyclic. First, that $\mathsf{D}(G) \le \frac{2}{p}|G|$, where p is the smallest prime divisor of $|G|$; and second, that $\mathsf{D}(G) \le \frac{3}{4}|G|$, provided that G is also not dihedral of order $2n$ with n odd (it is known that $\mathsf{D}(G)=|G|$ for such groups [5]). The latter mirrors a similar upper bound for the Noether constant from Invariant Theory [12].

2. Notation and Preliminaries

Much of the following notation can be found in [5] and is repeated here for the convenience of the reader. 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 sets, 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 may 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 nonempty 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 $H \trianglelefteq G$, we let

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

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

$$\begin{aligned}
&\mathsf{Z}(G) = \{g \in G : \ gx = xg \quad \text{for all } x \in G\} \trianglelefteq G \quad \text{is the } \textit{center} \text{ of } G,\\
&[x, y] = x^{-1}y^{-1}xy \in G \quad \text{is the } \textit{commutator} \text{ of the elements } x,\, y \in G,\\
&G' = [G, G] = \langle [x, y] : \ x,\, y \in G\rangle \trianglelefteq G \quad \text{is the } \textit{commutator subgroup} \text{ of } G, \quad \text{and}\\
&\mathsf{C}_G(A) = \mathsf{C}_G(\langle A\rangle) = \{g \in G : \ ga = ag \quad \text{for all } a \in A\} \le G \quad \text{is the } \textit{centralizer} \text{ of } A \subseteq G.
\end{aligned}$$

Many of our arguments rely upon the use of a subgroup $H \le G$ acting upon the finite group G by conjugation (see [14, Chapter 1]). We use fairly standard notation for this. For a subset $A \subseteq G$ and $x \in G$, we let

$$x^A = \{a^{-1}xa : \ a \in A\}.$$

More generally, if $A,\, B \subseteq G$, then

$$A^B = \{b^{-1}ab : \ a \in A,\, b \in B\}.$$

Thus a^H is the H-orbit of a under the action of conjugation by elements from $H \le G$, which has size

$$|a^H| = |H|/|\mathsf{C}_G(a) \cap H|. \tag{2}$$

For a set P, we denote by $\mathcal{F}(P)$ the *free abelian monoid* with basis P. Then every $a \in \mathcal{F}(P)$ has a unique representation in the form

$$a = p_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} p_\ell = \prod_{p \in P} p^{\mathsf{v}_p(a)}, \quad \text{where } p_1, \ldots, p_\ell \in P, \quad \mathsf{v}_p(a) \in \mathbb{N}_0 \ \text{ and } \ \mathsf{v}_p(a) = 0 \ \text{ for almost all } \ p \in P\,,$$

and we use all notation from elementary divisibility theory. In particular, $\mathsf{v}_p(a)$ is the *p-adic valuation* of a, $\operatorname{supp}(a) = \{p \in P : \ \mathsf{v}_p(a) > 0\} \subseteq P$ is the *support* of a, $|a| = \ell = \sum_{p \in P} \mathsf{v}_p(a)$ is the *length* of a, and $\mathsf{h}(a) = \max\{\mathsf{v}_p(a) : \ p \in P\}$.

Sequences Over Groups. These are our main objects of study. As it is traditional in Combinatorial Number Theory, by a *sequence* over a group G we mean a finite, unordered sequence where the repetition of elements is allowed. We view sequences over G as elements of the free abelian monoid $\mathcal{F}(G)$ (this point of view provides many technical advantages and was pushed forward by applications of Zero-Sum Theory in more algebraic fields, such as Multiplicative Ideal Theory and Factorization Theory; see the monographs [6, 7]). So we freely use all notation from free abelian monoids for sequences, though for reason explained in the next paragraph, we denote multiplication in $\mathcal{F}(G)$ by the boldsymbol $\boldsymbol{\cdot}$ rather than by juxtaposition and use brackets for all exponentiation in $\mathcal{F}(G)$. In particular, a sequence $S \in \mathcal{F}(G)$ has the form

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell = \bullet_{i \in [1,\ell]} g_i \in \mathcal{F}(G) \tag{3}$$

with the $g_i \in G$ the terms of S. The identity $1_{\mathcal{F}(G)} \in \mathcal{F}(G)$ is called the *empty* or *trivial* sequence, which is simply the sequence having no terms. For $g \in G$,

$$\mathsf{v}_g(S) = |\{i \in [1,\ell] :\ g_i = g\}| \quad \text{denotes the } \textit{multiplicity} \text{ of } g \text{ in } S,$$
$$\mathsf{h}(S) = \max\{\mathsf{v}_g(S) :\ g \in G\} \quad \text{denotes the } \textit{maximum multiplicity} \text{ of a term of } S,$$

and $T \mid S$ denotes that T is a *subsequence* of S. Of course, for $T \in \mathcal{F}(G)$, we have $T \mid S$ if and only if $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in G$, and in such case, $T^{[-1]} \cdot S$ or $S \cdot T^{[-1]}$ denotes the subsequence of S obtained by removing the terms of T from S, i.e., $\mathsf{v}_g(T^{[-1]} \cdot S) = \mathsf{v}_g(S) - \mathsf{v}_g(T)$ for all $g \in G$. If $X \subseteq G$ is a subset and $S \in \mathcal{F}(G)$ is a sequence over G, then we extend the notation $\mathsf{v}_g(S)$ be letting

$$\mathsf{v}_X(S) = \sum_{x \in X} \mathsf{v}_x(S)$$

denote the number of terms of S from X.

In order to distinguish between the group operation in G and the sequence operation in $\mathcal{F}(G)$, we use the boldsymbol $\cdot$ for the operation in $\mathcal{F}(G)$, so $\mathcal{F}(G) = (\mathcal{F}(G), \cdot)$ (which coincides with the convention in the monographs [6, 7]) and only denote multiplication in G by juxtaposition of elements. In particular, if $S_1, S_2 \in \mathcal{F}(G)$ and $g_1, g_2 \in G$, then $S_1 \cdot S_2 \in \mathcal{F}(G)$ has length $|S_1|+|S_2|$, $S_1 \cdot g_1 \in \mathcal{F}(G)$ has length $|S_1|+1$, $g_1 g_2 \in G$ is an element of G, but $g_1 \cdot g_2 \in \mathcal{F}(G)$ is a sequence of length 2. In order to avoid confusion between exponentiation of the group operation in G and exponentiation of the sequence operation $\cdot$ in $\mathcal{F}(G)$, we use brackets to denote exponentiation in $\mathcal{F}(G)$:

$$g^{[k]} = \underbrace{g \cdot \ldots \cdot g}_{k} \in \mathcal{F}(G) \qquad \text{and} \qquad T^{[k]} = \underbrace{T \cdot \ldots \cdot T}_{k} \in \mathcal{F}(G),$$

for $g \in G$, $T \in \mathcal{F}(G)$ and $k \in \mathbb{N}_0$. When $T^{[k]} \mid S$, we extend exponentiation to include negative exponents by setting $S \cdot T^{[-k]} = S \cdot (T^{[k]})^{[-1]} \in \mathcal{F}(G)$. In particular, if $S \in \mathcal{F}(G)$, $g \in G$ and $k \in \mathbb{Z}$ with $k \ge -\mathsf{v}_g(S)$, then $S \cdot g^{[k]} \in \mathcal{F}(G)$ has length $|S| + k$.

Let $S \in \mathcal{F}(G)$ be a sequence notated as in (3). When G is written multiplicatively, we use

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

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

$$\pi(S) \quad \text{is contained in a } G'\text{-coset.} \tag{4}$$

Thus $\pi(S) = Ag$ for some $A \subseteq G'$ and $g \in G$. Consequently, if we have sequences $S_1, \ldots, S_\ell \in \mathcal{F}(G)$, then, for each $i \in [1,\ell]$, we have

$$\pi(S_i) = A_i g_i \quad \text{for some} \quad A_i \subseteq G' \quad \text{and} \quad g_i \in G.$$

Furthermore, since $G' \trianglelefteq G$ is a normal subgroup, and thus invariant under conjugation automorphisms, it follows, for each $j \in [1,\ell]$, that $g_1 \ldots g_{j-1} A_j = A_j' g_1 \ldots g_{j-1}$ for some $A_j' \subseteq G'$ with $|A_j'| = |A_j| = |\pi(S_j)|$. Specifically, $A_j' = A_j^{(g_1 \ldots g_{j-1})^{-1}}$. Thus

$$\pi(S_1)\pi(S_2)\ldots\pi(S_\ell) = (A_1 g_1)(A_2 g_2)\ldots(A_\ell g_\ell) = A_1' A_2' \ldots A_\ell' g,$$

where $g = g_1 \ldots g_\ell$. In particular, if $G' \cong C_q$ with q prime, then theorems estimating the cardinality of a sumset in C_q, such as the Cauchy-Davenport Theorem (stated below), can be applied to estimate the

cardinality of the product-set $\pi(S_1)\ldots\pi(S_\ell)$. We will frequently do this without further reference to the intermediary sets $A_i' \subseteq G'$.

Note that $|S| = 0$ if and only if S is trivial, and in this case we use the convention that $\pi(S) = \{1\}$. 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 *sub(sequence) sums* and *sub(sequence) products* of S are respectively denoted by

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

For sub-sums and sub-products of restricted length, we have the following analogous notation:

$$\Sigma_{\le n}(S) = \bigcup_{h\in[1,n]} \Sigma_h(S) \qquad \text{and} \qquad \Pi_{\le n}(S) = \bigcup_{h\in[1,n]} \Pi_h(S).$$

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 $\varphi\colon G \to H$ extends to a monoid homomorphism $\varphi\colon \mathcal{F}(G) \to \mathcal{F}(H)$ by setting

$$\varphi(S) = \varphi(g_1)\boldsymbol{\cdot}\ldots\boldsymbol{\cdot}\varphi(g_\ell) \in \mathcal{F}(H)\,.$$

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, hence a commutative, cancellative semigroup with unit element, and we denote by $\mathcal{A}(G) = \mathcal{A}\big(\mathcal{B}(G)\big)$ the set of atoms (irreducible elements) of $\mathcal{B}(G)$. In other words, $\mathcal{A}(G)$ consists of the minimal product-one sequences, which are the nontrivial, product-one sequences that cannot be factored into two nontrivial, product-one subsequences. We call

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

the *large Davenport constant* of G and

$$\mathsf{d}(G) = \sup\{|S| : \ S \in \mathcal{F}(G) \text{ is product-one free}\} \in \mathbb{N}_0 \cup \{\infty\}$$

the *small Davenport constant* of 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 $\mathcal{F}^*(G) = (\mathcal{F}^*(G), \boldsymbol{\cdot})$ 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.

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

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

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

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

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

$$S^*(I) = \bullet_{i \in I} g_i \in \mathcal{F}^*(G), \tag{5}$$

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 $T^* \in \mathcal{F}^*(G)$ is a subsequence of *consecutive terms*, or simply a *consecutive subsequence*, and we indicate this by writing $T^* \mid S^*$. If $i \in [1, |S^*|]$, then

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

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 a *product-one ordered 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 $S^* = S_1^* \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} S_r^*$. Informally speaking, we may refer to $S^* = S_1^* \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} S_r^*$ 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

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

Preliminary Results. We begin with the Cauchy-Davenport Theorem [5, Theorem 4.1] [11, Theorem 2.2] [7, Theorem 6.2], which gives the basic lower bound for sumsets in C_p with p prime.

Theorem 2.1 (Cauchy-Davenport Theorem). *Let $G \cong C_p$ with p prime and let $A, B \subseteq G$ be nonempty subsets. Then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

The case when equality holds was characterized by Vosper [11, Theorem 2.4] [7, Theorem 8.1].

Theorem 2.2 (Vosper's Theorem). *Let $G \cong C_p$ with p prime and let $A, B \subseteq G$ be nonempty subsets with $|A|, |B| \geq 2$. If*

$$|A + B| < \min\{p - 1, |A| + |B|\},$$

then A and B are arithmetic progressions of common difference.

For a finite group G, we let $\eta(G)$ denote the minimal integer such that every sequence $S \in \mathcal{F}(G)$ with length $|S| \geq \eta(G)$ has a nontrivial product-one subsequence of length at most $\max\{\mathrm{ord}(g) : \ g \in G\}$. When $G = C_n^2$ with $n \geq 2$, we have $\max\{\mathrm{ord}(g) : \ g \in G\} = \exp(G) = n$, and both the constants $\eta(G)$ and $\mathsf{D}(G)$ are known [6, Theorem 5.8.3]:

$$\eta(C_n^2) = 3n - 2 \quad \text{and} \quad \mathsf{d}(C_n^2) + 1 = \mathsf{D}(C_n^2) = 2n - 1. \tag{6}$$

Next, we continue we a series of basic lemmas from [5].

Lemma 2.3. [5, Lemma 2.1] *Let G be a 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.*

Lemma 2.4. [5, Lemma 2.2] *Let G be group with $G' = [G, G] \leq G$ 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 $\pi(T^{[-1]} \cdot S) \subseteq G'$. In particular, if $T \mid S$ is a product-one subsequence, then $\pi(T^{[-1]} \cdot S) \subseteq G'$.*

Lemma 2.5. [5, Lemma 2.3] *Let G be a group and let $S = g_1 \cdot \ldots \cdot g_\ell \in \mathcal{F}^*(G)$ be a product-one ordered sequence. Then $g_j \cdot \ldots \cdot g_\ell \cdot g_1 \cdot \ldots \cdot g_{j-1}$ is also an product-one ordered sequence for every $j \in [1, \ell]$.*

Lemma 2.6. [5, Lemma 2.4] *Let G be a group.*

1. *If G is finite, then every ordered sequence $S \in \mathcal{F}^*(G)$ of length $|S| \geq |G|$ has a consecutive, product-one subsequence that is nontrivial. In particular, we have $\mathsf{d}(G) + 1 \leq \mathsf{D}(G) \leq |G|$.*
2. *G is finite if and only if $\mathsf{d}(G)$ is finite.*
3. *If G is finite abelian, then $\mathsf{d}(G) + 1 = \mathsf{D}(G)$.*
4. *If G is finite cyclic, then $\mathsf{d}(G) + 1 = \mathsf{D}(G) = |G|$.*

Lemma 2.7. [5, Lemma 2.5] *Let G be a finite group. Then $\mathsf{D}(G)$ is the smallest integer $\ell \in \mathbb{N}$ with the following property: for every sequence $S \in \mathcal{F}(G)$ of length $|S| \geq \ell$ and every $x \in \pi(S)$, there exists a nontrivial, product-one subsequence $T \mid S$ with $x \in \pi(T^{[-1]} \cdot S)$ and $|T| \leq \ell$.*

Next, we need the concept of a *setpartition*. Let P be a set and let Q be the set of *finite and nonempty* subsets of P. The elements of $\mathcal{S}(P) := \mathcal{F}(Q)$ are called *setpartitions over P*, and an *n-setpartition*, where $n \geq 0$, is simply a setpartition $\mathcal{A} \in \mathcal{S}(P)$ having length $|\mathcal{A}| = n$. In other words, an n-setpartition

$\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n \in \mathcal{S}(P)$ is a sequence of n finite and *nonempty* subsets $A_i \subseteq P$. The setpartition $\mathcal{A} \in \mathcal{S}(P)$ naturally partitions the sequence

$$\mathsf{S}(\mathcal{A}) = \bullet_{i\in[1,n]} \bullet_{a\in A_i} a \in \mathcal{F}(P)\,,$$

and $\mathcal{A}$ is said to have its terms being of *as near equal a size as possible* if

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

A sequence $S \in \mathcal{F}(P)$ is said to *have an n-setpartition* if there is an n-setpartition $\mathcal{A} \in \mathcal{S}(P)$ with $\mathsf{S}(\mathcal{A}) = S$. The following is the standard existence result for setpartitions. It can be found in [7, Proposition 10.2] or [3].

Lemma 2.8. *Let P be a set, let $S \in \mathcal{F}(P)$ be a sequence over P, 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*

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

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.

The following is a special case of either the DeVos-Goddyn-Mohar Theorem or the Partition Theorem (see [7, Chapters 13 and 14] or [4]).

Theorem 2.9. *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*

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

Next, we continue some general upper bounds for the Davenport constant(s). We begin with the classical upper bound of Olson and White [13] for the small Davenport constant.

Theorem 2.10. *Let G be a finite, noncyclic group. Then*

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

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

Finally, we conclude with two inductive upper bounds for $\mathsf{D}(G)$ from [5].

Theorem 2.11. [5, Theorem 3.2] *Let G be a finite group and let $H \le G$ be a subgroup. Then*

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

Theorem 2.12. [5, 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*

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

3. Upper Bounds Involving $\mathsf{d}(G)$ and $|G'|$

As noted in (1), we have $\mathsf{d}(G) + 1 \le \mathsf{D}(G)$ with equality if G is abelian. In this section, we show that the closer G is to being abelian (as measured by the commutator $G' = [G, G]$), the closer $\mathsf{D}(G)$ is bounded to $\mathsf{d}(G) + 1$. The main result of the section is the following.

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

$$\mathsf{D}(G) \le \mathsf{d}(G) + 2|G'| - 1,$$

where $G' = [G, G] \le G$ is the commutator subgroup of G, with equality if and only if G is abelian.

The proof of Theorem 3.1 will be given at the end of the section. Before continuing, we make the following easy observation.

Lemma 3.2. *Let G be a group. If $x, y \in G$ are elements such that $xy \neq yx$, then $xy \notin \mathsf{Z}(G)$.*

Proof. Assume by contradiction that $xy \in \mathsf{Z}(G)$. Then $xyx^{-1}y^{-1} = x^{-1}xyy^{-1} = 1$, which implies $xy = yx$, contrary to hypothesis. □

We continue with an extremely important technical lemma embodying a simple algorithm at the heart of many of the proofs. We need several variations on the algorithm, which accounts for the rather weighty and technical formulation of Lemma 3.3. Before stating it, let us try to motivate and explain what is going on in the background of Lemma 3.3. When trying to find upper bounds for $\mathsf{D}(G)$, one starts with a product-one sequence S with $|S|$ large and tries to find a nontrivial factorization of S. One strategy for finding such a factorization goes as follows.

Suppose we could find a subsequence $T \mid S$ such that $\pi(T)$ was a full G'-coset. Let $S = T \cdot R$. Now further suppose that R contained a nontrivial product-one subsequence U_2, and let $R = U_1 \cdot U_2$. Then Lemma 2.4 ensures that $\pi(T \cdot U_1)$ is not only contained in a G'-coset but in G' itself. Moreover, since $\pi(T)$ is a full G'-coset, so is $\pi(T \cdot U_1)$, which implies $1 \in G = \pi(T \cdot U_1)$, giving us a nontrivial factorization $S = (T \cdot U_1) \cdot U_2$, as desired.

There are two main issues with the above strategy. First, how to find the subsequence $T \mid S$ with $\pi(T)$ a full G'-coset? Second, how to find a nontrivial product-one subsequence $U_2 \mid S \cdot T^{[-1]}$? Let us focus on the second issue first. If we were able to guarantee the existence of a short subsequence $T \mid S$ with $\pi(T)$ a full G'-coset, then there would be many terms left in $S \cdot T^{[-1]}$, perhaps more than $\mathsf{d}(G)$, in which case the definition of the small Davenport constant will give us the desired product-one subsequence U_2. Alternatively, if we could first find a short-length product-one sequence $U_2 \mid S$, that would leave many terms in $S \cdot U_2^{[-1]}$, perhaps enough that we could more easily guarantee the existence of a subsequence $T \mid S \cdot U_2^{[-1]}$ with $\pi(T)$ an entire G'-coset.

Either way, we still need a way to address the first issue. We use a very crude tactic. Observe that if two terms x and y do not commute, then $\pi(x \cdot y) = \{xy, yx\}$ is a cardinality 2 subset. More generally, as we will see in the proof of Lemma 3.3, either $|\pi(T_1 \cdot x)| > |\pi(T_1)|$ or else $\pi(T_1)$ is invariant under conjugation by x, where $T_1 \in \mathcal{F}(G)$. Thus the idea is to slowly build up an increasingly long subsequence $T_1 \mid S$ with $|\pi(T_1)| \ge |T_1|$. In view of the previous observation, there is only one thing that can prevent us from growing T_1 as long as we want. Namely, at some point $\pi(T_1)$ might become invariant under conjugation by all remaining terms $x \in \operatorname{supp}(S \cdot T_1^{[-1]})$. If $\langle \operatorname{supp}(S \cdot T_1^{[-1]}) \rangle = K < G$ is a

proper subgroup, then we will be in the good situation in which our sequence S is structured, containing many terms from a proper subgroup K (more on what to do in this case later). On the other hand, if $\langle \mathrm{supp}(S \cdot T_1^{[-1]}) \rangle = G$, then (as we will see in the proof) we have $\pi(T_1)^G = \pi(T_1)$, so that $\pi(T_1)$ is actually equal to a G-orbit. In particular, since the size of an orbit divides $|G|$, we must have $|\pi(T_1)| \ge p$, where p is the smallest prime divisor of $|G|$. In such case, rather than give up, we simply begin trying to construct a second $T_2 \mid T_1^{[-1]} \cdot S$ with $|\pi(T_2)| \ge |T_2|$ using the remaining terms. Iterating this process, we either find many terms from the same proper subgroup $K < G$ or else are able to partition many terms of S into subsequences $T_1 \cdot \ldots \cdot T_r \mid S$ with $|\pi(T_i)| \ge |T_i|$ for $i \in [1, r]$ and $\pi(T_i)$ a G-orbit for $i \in [1, r-1]$. In the second case, if $|T_1 \cdot \ldots \cdot T_r|$ is long enough, we can use results like the Cauchy-Davenport Theorem to show that that product set $\pi(T_1) \cdots \pi(T_r) \subseteq \pi(T)$ is large enough in cardinality to guarantee that $\pi(T)$ is an entire G'-coset, where $T = T_1 \cdot \ldots \cdot T_r$. Moreover, if we know the structure of potential G-orbits, we may be able to use results like Vosper's Theorem to gain even quicker product-set growth (here we are assuming $|G'|$ is prime).

Next, let us return to the "good" situation in which the algorithm is forced to stop prematurely with many terms of S from a proper subgroup $K < G$. If this is all we know, then the situation is actually not as good as we would like. What we really would like to have is an ordering of S with product one with many terms from the proper subgroup K lying in a *consecutive* subsequence. Then we could use the definition of $\mathsf{d}(H) + 1$ and Lemma 2.3 to show S has a nontrivial factorization. Thus, when constructing the sequences T_i, we need to make sure $T_1 \cdot \ldots \cdot T_r$ always remains a consecutive subsequence in some ordering of S having product-one. This requires extra technical care, but can be done.

In summary, we start with an ordering of S with product one, are allowed to rearrange terms in this ordering so long as the result still has product-one, and try to find our subsequences T_i with the desired properties such that $T_1 \cdot \ldots \cdot T_r$ remains a consecutive subsequence. If the algorithm stops prematurely, then we gain many terms of S in a consecutive subsequence all from a proper subgroup K, which we can handle by the means explained above. If the algorithm does not stop prematurely, then we can obtain (near) precise control on how many terms are contained in the T_i, enough so that $|T|$ is small yet still large enough that sumset results can be used to show $\pi(T)$ is an entire G'-coset, where $T = T_1 \cdot \ldots \cdot T_r$. This is ONE variation on how Lemma 3.3 will be employed. It is not the only one.

Needing that $T_1 \cdot \ldots \cdot T_r$ remains consecutive is only necessary if the algorithm stops prematurely (with many terms of S from the same proper subgroup K). If we already know some structural information about the sequence S, enough to guarantee that the algorithm will not stop prematurely, then we can use the alternative (often more effective) method of *first* finding the product-one sequence $U_2 \mid S$ and then running the algorithm on the sequence S' consisting of remaining terms $S \cdot U_2^{[-1]}$ (instead of running the algorithm on S itself). However, this requires having considerable information about the sequence S beforehand. Alternatively, this method can also be used to simply show S contains many terms from some proper subgroup, and thereby used to begin gaining such knowledge about the sequence S.

Sometimes, we will need to run the algorithm on a subsequence $S' \mid S$ (instead of S itself), stop when an undesirable outcome occurs, swap some terms of $S \cdot S'^{[-1]}$ for some terms from S' not yet partitioned in the T_i, and then rerun the algorithm starting up from where we left off (keeping the T_i that we already constructed). This capability is built into Lemma 3.3 via the "seed" sequence S_0, which will generally either be taken to be trivial or equal to the output $T = T_1 \cdot \ldots \cdot T_r$ from a previous use of Lemma 3.3.

As another technical point, it will sometimes be necessary to construct the final sequence T_r manually, i.e., not via Lemma 3.3. In these cases, we will run the algorithm to produce the $T_1, \ldots, T_r$, stop when $|T_1 \cdot \ldots \cdot T_r|$ is not quite long enough for sumset results to guarantee that $\pi(T_1 \cdot \ldots \cdot T_r)$ is a full G'-coset, and then construct a final subsequence T_{r+1} manually that will finish the job. Because of this, we need to have precise control over how long $|T_1 \cdot \ldots \cdot T_r|$ is allowed to be before the algorithm is automatically set to stop. This capability is built into the parameter ω, which is the setting that tells Lemma 3.3 when to stop (assuming it is not forced to stop prematurely with many terms of S from $K < G$).

Finally, we can build into the algorithm any alternative condition that, if met, will cause the algorithm to automatically stop. For some of the most refined uses of Lemma 3.3, it will be important to not exhaust too many terms from a distinguished subgroup $H \le G$. Thus, if we begin to use too many terms from H in the sequences T_i, we need the algorithm to stop immediately so that we can first modify the sequence $S' \mid S$ that we are employing the algorithm on before continuing. This is capability is built into the parameter ω_H. When this capability is not needed, we simply set $\omega_H = -1$ with H trivial. With all this in mind, we now state Lemma 3.3.

Lemma 3.3. *Let G be a non-abelian, finite group, let $S^* \in \mathcal{F}^*(G)$ be an ordered sequence, let $H \le G$ be an abelian subgroup, let*

$$\omega \ge 1, \quad \omega_H \in \mathbb{Z}, \qquad \text{and} \qquad \omega_0 \in \{0\} \cup [2, |S^*|] \ \text{ with } \ \omega_0 \le \omega,$$

and suppose that $|\pi(S_0)| \ge |S_0| = \omega_0$ and $\pi(S_0) \cap \big(G \setminus \mathsf{Z}(G)\big) \ne \emptyset$ (if $\omega_0 > 0$), where $S_0 = [S^*(1, \omega_0)]$, and that there are at least ω_H terms of $S_0^{[-1]} \cdot S$ from H.

Then there exists an ordered sequence $S'^* \in \mathcal{F}(G)$ with

$$[S'^*] = [S^*] \qquad \text{and} \qquad \pi(S'^*) \in \pi(S^*)^G, \tag{8}$$

having a factorization

$$S'^* = T_1^* \cdot \ldots \cdot T_{r-1}^* \cdot T_r^* \cdot R^*, \tag{9}$$

where $T_1^*, \ldots, T_r^*, R^* \in \mathcal{F}^*(G)$ and $r \ge 0$, such that, letting $R = [R^*]$ and $T_i = [T_i^*]$ for $i \in [1, r]$, we have $S_0 \mid T_1$ (if $\omega_0 > 0$),

$$\pi(T_i) \cap \big(G \setminus \mathsf{Z}(G)\big) \ne \emptyset \qquad \text{and} \qquad |\pi(T_i)| \ge |T_i| \ge 2 \quad \text{for } i \in [1, r], \quad \pi(T_i)^G = \pi(T_i) \ \text{ for } i \in [1, r-1], \tag{10}$$

and either

(i) $\sum_{i=1}^{r} |T_i| \le w - 1$ *and* $\langle \mathrm{supp}(R) \rangle < G$ *is a proper subgroup, or*

(ii) $w \le \sum_{i=1}^{r} |T_i| \le w + 1$, *with the upper bound only possible if $|T_r| = 2$ and $\sum_{i=1}^{r-1} |T_i| = \omega - 1$, and there are at least ω_H terms of R from H, or*

(iii) $\sum_{i=1}^{r} |T_i| \le w - 1$ *and there are precisely ω_H terms of R from H.*

Proof. Let $S = [S^*]$. First observe that

$$\pi\Big(S^*(2, |S|) \cdot S^*(1)\Big) = S^*(1)^{-1} \pi(S^*) S^*(1).$$

Thus cyclically shifting the terms of S^* results in an ordered sequence S'^* with $[S'^*] = [S^*] = S$ and product in $\pi(S^*)^G$, as required by (8).

Let $S'^* \in \mathcal{F}^*(G)$ be an ordered sequence with a factorization (and all notation) given by (9), satisfying all parts of the lemma apart from (possibly) conclusions (i)–(iii), with at least ω_H terms of R from H, with $|T_r| = 2$ if $\sum_{i=1}^{r}|T_i| = w+1$, and subject to all this, with $\sum_{i=1}^{r}|T_i| \le w+1$ maximal. We begin by showing that such an ordered sequence S'^* exists.

If $\omega_0 = 0$, then all conclusions of the lemma apart from (i)–(iii) hold taking $R^* = S^* = S'^*$ and $r = 0$; moreover, we know $S^* = R^*$ contains at least ω_H terms from H by hypothesis, and clearly $\sum_{i=1}^{r}|T_i| = 0 < \omega$. Thus the S'^* described above exists in the case $\omega_0 = 0$. On the other hand, if $\omega_0 \ge 2$ (note $\omega_0 = 1$ is not allowed by our hypotheses), then all conclusions of the lemma apart from (i)–(iii) hold taking $S^* = S'^*$, $R^* = S^*(\omega_0+1, |S^*|)$, $r = 1$ and $T_1^* = S^*(1, \omega_0)$ (as follows from the hypotheses); moreover, we know that $|T_1| = \omega_0 \le \omega < \omega+1$ and that $R^* = S^*(\omega_0+1, |S^*|)$ contains at least ω_H terms from H by hypothesis. Thus the S'^* described above exists in the case $\omega_0 \ge 2$ as well.

If $\sum_{i=1}^{r}|T_i| \ge \omega$, then (ii) holds and the proof is complete. Therefore we can assume

$$\sum_{i=1}^{r}|T_i| \le \omega - 1. \tag{11}$$

Hence, if there are precisely ω_H terms of R from H, then (iii) holds and the proof is again complete. Therefore, since there are assumed to be at least ω_H terms of R from H, it follows that this estimate must be strict:

$$\mathsf{v}_H(R) \ge \omega_H + 1. \tag{12}$$

If $\langle \mathrm{supp}(R)\rangle < G$ is a proper subgroup, then (i) holds, completing the proof once more. Therefore we can assume

$$\langle \mathrm{supp}(R)\rangle = G. \tag{13}$$

We now aim to show that (11)–(13) allow us to contradict the maximality of $\sum_{i=1}^{r}|T_i|$ for S'^*. We proceed in two cases.

Case 1: $r \ge 1$ and $\pi(T_r)^G \ne \pi(T_r)$.

If $\pi(T_r)^{\mathrm{supp}(R)} = \pi(T_r)$, then it is easily shown that $\pi(T_r)^{\langle \mathrm{supp}(R)\rangle} = \pi(T_r)$. But since (13) gives $\langle \mathrm{supp}(R)\rangle = G$, this would mean $\pi(T_r)^G = \pi(T_r)^{\langle \mathrm{supp}(R)\rangle} = \pi(T_r)$, contrary to case hypothesis. Therefore there must be some $g \in \mathrm{supp}(R)$ such that $g\pi(T_r) \ne \pi(T_r)g$. Let $x \in [1, |R|]$ be minimal such that $R^*(x)\pi(T_r) \ne \pi(T_r)R^*(x)$.

By the minimality of x, we have $R^*(y)\pi(T_r) = \pi(T_r)R^*(y)$ for every $y \in [1, x-1]$. Since $\pi(T_j)^G = \pi(T_j)$ for $j \in [1, r-1]$ (in view of (10) holding for S'^*), we also have $R^*(y)\pi(T_j) = \pi(T_j)R^*(y)$ for every $y \in [1, x-1]$ and $j \in [1, r-1]$. Thus, for each $j \in [1, r]$, there exists ordering T'^*_j of T_j such that

$$\pi\Big(R^*(1, x-1)\Big)\pi(T'^*_j) = \pi(T_j^*)\pi\Big(R^*(1, x-1)\Big).$$

Hence

$$\pi\Big(R^*(1, x-1)\Big)\pi(T'^*_1)\dots\pi(T'^*_r) = \pi(T_1^*)\dots\pi(T_r^*)\pi\Big(R^*(1, x-1)\Big).$$

In other words, allowing re-ordering of the terms of the T_i, we can commute the terms from $R^*(1, x-1)$ past the T_i while preserving that the resulting ordered sequence still has the same product. Then, as

mentioned at the beginning of the proof, we can cyclically shift the terms $R^*(1, x-1)$ until the sequence ${T'}_1^*$ is once again the start of the resulting sequence

$$S''^* := {T'}_1^* \cdot \ldots \cdot {T'}_r^* \cdot R^*(x, |R|) \cdot R^*(1, x-1),$$

and this will preserve that $\pi(S''^*) \in \pi(S'^*)^G = \pi(S^*)^G$ (note that the hypothesis $\pi(S'^*) \in \pi(S^*)^G$ is equivalent to $\pi(S'^*)^G = \pi(S^*)^G$). Moreover, this does not affect any of the defining properties of the T_i, which means that (by replacing S'^* by S''^*, the T_i^* by the ${T'}_i^*$, and R^* by $R^*(x, |R|) \cdot R^*(1, x-1)$), we can w.l.o.g. assume $x = 1$.

Observe that

$$\pi(T_r)R^*(1) \cup R^*(1)\pi(T_r) \subseteq \pi\Big(T_r \cdot R^*(1)\Big).$$

Moreover, we have $\pi(T_r)R^*(1) \neq R^*(1)\pi(T_r)$ in view of $x = 1$ and the definition of x. Thus

$$|\pi\Big(T_r \cdot R^*(1)\Big)| \geq |\pi(T_r)| + 1.$$

If $gR^*(1) = R^*(1)g$ for every $g \in \pi(T_r)$, then $R^*(1)\pi(T_r) = \pi(T_r)R^*(1)$ would follow, contrary to the definition of $x = 1$. Therefore there must be some $g \in \pi(T_r)$ with $R^*(1)g \neq gR^*(1)$, in which case Lemma 3.2 ensures that the element $gR^*(1) \in \pi\Big(T_r \cdot R^*(1)\Big)$ is from $G \setminus \mathsf{Z}(G)$. In view of (12), we see that $R'^* := R^*(2, |R|)$ contains at least ω_H terms from H, and (11) ensures that $\sum_{i=1}^{r} |T_i'| \leq \omega < \omega + 1$, where ${T_i'}^* := {T_i}^*$ for $i \in [1, r-1]$ and ${T_r'}^* := {T_r}^* \cdot R^*(1)$. But now the maximality of $\sum_{i=1}^{r} |T_i|$ for S'^* is contradicted by the factorization $S'^* = {T'}_1^* \cdot \ldots \cdot {T'}_r^* \cdot R'^*$, completing Case 1.

Case 2: $r = 0$ or $\pi(T_r)^G = \pi(T_r)$.

If $gh = hg$ for all $g, h \in \mathrm{supp}(R)$, then $\langle \mathrm{supp}(R) \rangle$ must be abelian. Hence, since G is non-abelian by hypothesis, $\langle \mathrm{supp}(R) \rangle$ is a proper subgroup of G, contrary to (13). Therefore, there must be $g_0, h_0 \in \mathrm{supp}(R)$ with $g_0h_0 \neq h_0g_0$. Swapping the order of adjacent terms of R^* that commute with each other preserves all assumptions from the definition of S'^*. Consequently, performing such swaps, we can either arrange that R^* has the non-commuting terms g_0 and h_0 adjacent to each other or else has g_0 adjacent to another term h_0' that also does not commute with g_0. Either way, we may assume there are consecutive terms in R^* that do not commute, say $R^*(x)R^*(x+1) \neq R^*(x+1)R^*(x)$ with $x \in [1, |R| - 1]$.

By (9) and case hypothesis, we have $\pi(T_j)g = g\pi(T_j)$ for all $g \in G$ and $j \in [1, r]$. Thus, as we argued in Case 1, we can commute the terms $R^*(1, x-1)$ past the T_i^*, re-ordering each T_i appropriately, and then cyclically shift the terms $R^*(1, x-1)$ to thereby w.l.o.g. assume $x = 1$.

Let $T_{r+1}^* := R^*(1, 2)$, $T_{r+1} = [T_{r+1}^*]$ and $R'^* := R^*(3, |R|)$. Since $R^*(1)R^*(2) \neq R^*(2)R^*(1)$ (in view of the definition of $x = 1$), we have $|\pi(T_{r+1})| \geq 2 = |T_{r+1}|$ while Lemma 3.2 ensures that $\pi(T_{r+1}) \cap (G \setminus \mathsf{Z}(G)) \neq \emptyset$. In view of the case hypothesis, we have $\pi(T_r)^G = \pi(T_r)$, while $\pi(T_j)^G = \pi(T_j)$ holds for $j \in [1, r-1]$ from the hypotheses in the definition of S'^*. Since H is abelian and the terms $R^*(1)$ and $R^*(2)$ do not commute with each other, it follows that at most one term from $R^*(1, 2)$ is from H, whence (12) ensures that R'^* contains at least ω_H terms from H. By its definition, we have $|T_{r+1}| = 2$, and (11) gives $\sum_{i=1}^{r+1} |T_i| \leq \omega - 1 + 2 = \omega + 1$. But now the maximality of $\sum_{i=1}^{r} |T_i|$ for S'^* is contradicted by the factorization $S'^* = T_1^* \cdot \ldots \cdot T_r^* \cdot T_{r+1}^* \cdot R'^*$, completing Case 2 and the proof. □

Next, we give a simple application of Lemma 3.3. Note that the p defined in Corollary 3.4 is always at least as big as the smallest prime divisor of $|G|$.

Corollary 3.4. *Let G be a finite, non-abelian group, let $G' = [G, G] \le G$ be its commutator subgroup, and let*

$$p = \min\{|G|/|\mathsf{C}_G(x)| : \ x \in G \setminus \mathsf{Z}(G)\}.$$

Suppose G' is cyclic of prime order. Then

$$\mathsf{D}(G) \ \le \ \max\left(\left\{\mathsf{d}(G) + |G'| + \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor\right\} \cup \left\{\mathsf{D}(H) + |G'| + \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor - 2 : \ H < G \text{ proper}\right\}\right).$$

In particular, if we also know that all proper subgroups $H < G$ are abelian, then

$$\mathsf{D}(G) \le \mathsf{d}(G) + |G'| + \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor.$$

Proof. Since G is non-abelian, $G' \le G$ is nontrivial and $\mathsf{Z}(G) < G$ is proper. Note that the "in particular" statement of the corollary follows from the main part in view of the inequality $\mathsf{D}(H) = \mathsf{d}(H)+1 \le \mathsf{d}(G)+1$ holding for any abelian subgroup $H \le G$ (care of Lemma 2.6.3). In view of (2), we see that $p \ge 2$ is the minimal size of an orbit of an element $g \in G \setminus \mathsf{Z}(G)$. Assume by contradiction that we have an atom $S \in \mathcal{A}(G)$ with

$$|S| \ge \max\left(\left\{\mathsf{d}(G) + |G'| + \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor + 1\right\} \cup \left\{\mathsf{D}(H) + |G'| + \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor - 1 : \ H < G \text{ proper}\right\}\right). \tag{14}$$

Since $S \in \mathcal{A}(G)$, there is an ordering $S^* \in \mathcal{F}^*(G)$ with $[S^*] = S$ and $\pi(S^*) = 1$.

Apply Lemma 3.3 to S^* taking H trivial, $\omega = |G'| + \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor$, $\omega_H = -1$, and $\omega_0 = 0$ and let

$$S'^* = T_1^* \cdot \ldots \cdot T_r^* \cdot R^*$$

be the resulting factorization, where $T_1^*, \ldots, T_r^*$, $R^* \in \mathcal{F}^*(G)$, $[R^*] = R$ and $[T_i^*] = T_i$ for $i \in [1, r]$. Observe that

$$\omega \ge \frac{p|G'| - p}{p-1}. \tag{15}$$

Since ω_H is negative, Lemma 3.3(iii) cannot hold. This gives us two cases.

Case 1: Lemma 3.3(i) holds.

Since $\pi(S'^*) \in \pi(S^*)^G = 1^G = \{1\}$ (from (8)), we see that S'^* is a product-one ordered sequence. In view of Lemma 3.3(i), we have $\langle \mathrm{supp}(R) \rangle := H < G$ being a proper subgroup. In view of Lemma 3.3(i) and (14), we also know

$$|R| \ge |S| - w + 1 \ge \left(\mathsf{D}(H) + |G'| + \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor - 1\right) - |G'| - \left\lfloor \frac{|G'|-2}{p-1} \right\rfloor + 1 = \mathsf{D}(H).$$

Thus we can apply Lemma 2.7 to R to find a nontrivial, product-one subsequence $T \mid R$ with $|T| \le \mathsf{D}(H) < |S|$ and $\pi(R^*) \in \pi(T^{[-1]} \cdot R)$. Hence

$$1 = \pi(S'^*) = \pi(T_1^*) \ldots \pi(T_r^*)\pi(R^*) \in \pi\Big(T_1 \cdot \ldots \cdot T_r \cdot (T^{[-1]} \cdot R)\Big) = \pi(T^{[-1]} \cdot S),$$

which means $S = T \cdot (T^{[-1]} \cdot S)$ is a nontrivial factorization, contradicting that $S \in \mathcal{A}(G)$ is an atom.

Case 2: Lemma 3.3(ii) holds.

Since $\pi(T_i) \cap \Big(G \setminus \mathsf{Z}(G)\Big) \neq \emptyset$ and $\pi(T_i)^G = \pi(T_i)$ for $i \in [1, r-1]$ (from (10)), it follows, in view of the description of p given at the beginning of the proof, that

$$|\pi(T_r)| \geq 2 \quad \text{and} \quad |\pi(T_i)| \geq p \quad \text{for all } i \in [1, r-1], \tag{16}$$

where the first inequality follows directly from (10).

Suppose we can find a subsequence $T \mid S$ such that $\pi(T)$ is a full G'-coset and $|T| \leq \omega$. Then, in view of (14), we have

$$|T^{[-1]} \cdot S| \geq |S| - \omega \geq \mathsf{d}(G) + 1.$$

As a result, the definition of $\mathsf{d}(G)$ guarantees that there is a nontrivial, product-one subsequence $V_1 \mid T^{[-1]} \cdot S$. Thus $S = V_1 \cdot V_2$ with $T \mid V_2$, where $V_2 = V_1^{[-1]} \cdot S$. Note that $V_2 = {V_1}^{[-1]} \cdot S$ is nontrivial since it contains the subsequence T which must be nontrivial in view of $\pi(T)$ being a full G'-coset with G' nontrivial. By Lemma 2.4, we have

$$\pi(V_2) \subseteq G'. \tag{17}$$

Since $T \mid V_2$, and since $\pi(T)$ is a full G'-coset, it likewise follows that $\pi(V_2)$ is also a full G'-coset, meaning the inclusion in (17) is an equality: $1 \in G' = \pi(V_2)$. Consequently, $S = V_1 \cdot V_2$ is a factorization of S into two nontrivial, product-one subsequences, contradicting that $S \in \mathcal{A}(G)$ is an atom. So we instead assume that

$$\text{there does not exist a subsequence } \ T \mid S \ \text{ with } \quad |\pi(T)| = |G'| \quad \text{ and } \quad |T| \leq \omega. \tag{18}$$

Let $W = T_1 \cdot \ldots \cdot T_{r-1}$. Then

$$|W| = \sum_{i=1}^{r} |T_i| - |T_r| \leq \omega + 1 - 2 = \omega - 1,$$

with the inequality above following from those given in Lemma 3.3(ii) and (10). Thus (18) ensures that

$$|\pi(W)| \leq |G'| - 1. \tag{19}$$

Observe that

$$\pi(T_1) \ldots \pi(T_{r-1}) \subseteq \pi(T_1 \cdot \ldots \cdot T_{r-1}) = \pi(W). \tag{20}$$

Thus, since G' is cyclic of prime order by hypothesis, using (19), (20), the Cauchy-Davenport Theorem, and (16), we obtain

$$|G'| - 1 \geq |\pi(W)| \geq \sum_{i=1}^{r-1} |\pi(T_i)| - r + 2 \geq (r-1)p - r + 2. \tag{21}$$

Rearranging this inequality gives

$$r \leq \frac{|G'| + p - 3}{p - 1}. \tag{22}$$

In view of Lemma 3.3(ii) holding by case hypothesis, we have $\omega \leq \sum_{i=1}^{r} |T_i| \leq \omega + 1$.

Suppose $\sum_{i=1}^{r}|T_i| = \omega+1$. In this case, Lemma 3.3(ii) further tells us that $|T_r| = 2$ and $\sum_{i=1}^{r-1}|T_i| = \omega-1$; and from (10), we have $|\pi(T_i)| \ge |T_i|$ for all i. Thus (21) and (22) yield

$$|G'|-1 \ge \sum_{i=1}^{r-1}|\pi(T_i)| - r + 2 \ge \sum_{i=1}^{r-1}|T_i| - r + 2 = \omega + 1 - r \ge \omega + 1 - \frac{|G'|+p-3}{p-1}.$$

Consequently, $\omega \le \frac{p|G'|-p-1}{p-1}$, contradicting (15). So we instead conclude that

$$\sum_{i=1}^{r}|T_i| = \omega. \tag{23}$$

In view of (23), we have $|T_1\boldsymbol{\cdot}\ldots\boldsymbol{\cdot}T_r| \le \omega$. But now we obtain a string of inequalities as follows: the first inequality follows from (18), the second is clear, the third from an application of the Cauchy-Davenport Theorem as argued for (21), the fourth in view of (10), the equality from (23), and the final inequality from (22).

$$\begin{aligned} |G'|-1 \quad &\ge \quad |\pi(T_1\boldsymbol{\cdot}\ldots\boldsymbol{\cdot}T_r)| \ge |\prod_{i=1}^{r}\pi(T_i)| \ge \sum_{i=1}^{r}|\pi(T_i)| - r + 1 \\ &\ge \quad \sum_{i=1}^{r}|T_i| - r + 1 = \omega + 1 - r \ge \omega + 1 - \frac{|G'|+p-3}{p-1} \end{aligned}$$

Rearranging the above inequality gives $\omega \le \frac{p|G'|-p-1}{p-1}$, contrary to (15), which completes the proof. □

We conclude the section with the proof of Theorem 3.1.

Proof of Theorem 3.1. We have $\mathsf{D}(G) = \mathsf{d}(G)+1$ for any abelian group G (care of Lemma 2.6.3). Thus it suffices to show

$$\mathsf{D}(G) \le \mathsf{d}(G) + 2|G'| - 2$$

for a finite, non-abelian group G. Since G is non-abelian, G' is nontrivial.

Let $U \in \mathcal{A}(G)$ be an atom with $|U| = \mathsf{D}(G)$. As in the proof of (18) in Corollary 3.4, may assume

$$\text{there is no subsequence } \ T \mid U \ \text{ with } \ |T^{[-1]}\boldsymbol{\cdot}U| \ge \mathsf{d}(G)+1 \ \text{ and } \ \pi(T) \ \text{ a full } \ G'\text{-coset} \tag{24}$$

and, by way of contradiction, that

$$|U| \ge \mathsf{d}(G) + 2|G'| - 1. \tag{25}$$

Let $\ell \in [2, 2|G'|-2]$ be the maximal integer such that there exists an ordered sequence $U^* \in \mathcal{F}^*(G)$ with

$$[U^*] = U \qquad \text{and} \qquad \pi(U^*) = 1 \tag{26}$$

having a factorization $U^* = T^*\boldsymbol{\cdot}R^*$, where R^*, $T^* \in \mathcal{F}^*(G)$, $R := [R^*]$ and $T := [T^*]$, such that

$$|T| = \ell \qquad \text{and} \qquad |\pi(T)| \ge \frac{1}{2}|T| + 1. \tag{27}$$

To see that $\ell \ge 2$ exists, we argue as follows. If $\langle \mathrm{supp}(U)\rangle := H$ were abelian, then $H < G$ follows since G is non-abelian, and then Lemma 2.6.3 gives $|U| \le \mathsf{D}(\langle \mathrm{supp}(U)\rangle) = \mathsf{D}(H) = \mathsf{d}(H)+1 \le \mathsf{d}(G)+1$, contrary to (25). Therefore we can assume there are terms g_0, $h_0 \in \mathrm{supp}(U)$ that do not commute: $g_0h_0 \ne h_0g_0$. But now, arguing as from the beginning of Case 2 in Lemma 3.3 allows us to w.l.o.g. assume the first

two terms of U^* do not commute, in which case it is clear that $\ell \ge 2$ exists. Also, if ℓ were odd, then taking $T^* \cdot R^*(1)$ in place of T^* would contradict the maximality of ℓ, which means that ℓ must be even. Finally, if $\ell = 2|G'| - 2$, then the sequence T will contradict (24) in view of (25). Thus, since ℓ is even, we must have

$$2 \le \ell \le 2|G'| - 4. \tag{28}$$

In view of $\ell \le 2|G'| - 4$ and (25), we have $|R| = |U| - \ell \ge \mathsf{d}(G) + 3$. Thus the definition of $\mathsf{d}(G)$ guarantees that R has a nontrivial, product-one subsequence. Consequently, we can reorder the terms of R^* so that the resulting ordered sequence R'^* has a nontrivial, product-one consecutive subsequence. Of course, we may have $\pi(R'^*) \ne \pi(R^*)$. It is well-known that the symmetric group on $|R|$ elements can be generated by the cycles $(1, 2)$ and $(1, 2, \ldots, |R|)$. But this means that there is a chain of ordered sequences

$$R_0^*, R_1^*, \ldots, R_n^* \in \mathcal{F}^*(G)$$

such that

$$\begin{aligned} &R_0^* = R^*, \quad R_n^* = R'^*, \quad [R_i^*] = R \quad \text{for all } i \in [1, n], \quad \text{and either} \\ &R_{i+1}^* = R_i^*(2, |R|) \cdot R_i^*(1) \quad \text{or} \quad R_{i+1}^* = R_i^*(2) \cdot R_i^*(1) \cdot R_i^*(3, |R|) \quad \text{for each } i \in [0, n-1]. \end{aligned} \tag{29}$$

Since $1 = \pi(U^*) = \pi(T^* \cdot R^*) = \pi(T^* \cdot R_0^*)$, we have

$$\pi(R_0^*)^{-1} = \pi(T^*) \in \pi(T).$$

If $\pi(R_n^*)^{-1} \in \pi(T)$, then we could order the terms of T, yielding some $T_n^* \in \mathcal{F}^*(G)$ with $[T_n^*] = T$, such that $\pi(T_n^* \cdot R_n^*) = 1$. But then, since $R_n^* = R'^*$ contains a nontrivial, consecutive product-one subsequence, say $R_n^*(I)$ with $I \subseteq [1, |R_n^*|]$ a nonempty interval, it would follow that

$$U = T \cdot R = \Big[T_n^* \cdot R_n^*\Big([1, |R|] \setminus I\Big)\Big] \cdot [R_n^*(I)]$$

was a factorization of U into 2 nontrivial product-one subsequences—note $[T_n^* \cdot R_n^*([1, |R|] \setminus I)]$ is also nontrivial since it contains $[T_n^*] = T$ and $|T| = \ell \ge 2$—contradicting that $U \in \mathcal{A}(G)$ is an atom. Therefore we can instead assume that

$$\pi(R_n^*)^{-1} \notin \pi(T).$$

As a result, let $s + 1 \in [1, n]$ be the minimal integer such that

$$\pi(R_{s+1}^*)^{-1} \notin \pi(T). \tag{30}$$

In view of the minimality of $s + 1 \in [1, n]$, it follows that $\pi(R_s^*)^{-1} \in \pi(T)$, which means that we can order the terms of T, yielding some $T_s^* \in \mathcal{F}^*(G)$ with $[T_s^*] = T$, such that

$$\pi(T_s^* \cdot R_s^*) = 1.$$

In view of (29), there are 2 possibilities for how R_{s+1}^* was obtained from R_s^*.

Suppose first that $R_{s+1}^* = R_s^*(2, |R|) \cdot R_s^*(1)$. If

$$\pi(T) R_s^*(1) = R_s^*(1) \pi(T),$$

then the terms of T can be ordered, yielding some $T_{s+1}^* \in \mathcal{F}^*(G)$ with $[T_{s+1}^*] = T$, such that

$$R_s^*(1) \cdot T_{s+1}^* \cdot R_s^*(2, |R|) \in \mathcal{F}^*(G)$$

has product $\pi(T_s^* \cdot R_s^*) = 1$. But then Lemma 2.5 implies that

$$T_{s+1}^* \cdot R_s^*(2, |R|) \cdot R_s^*(1) = T_{s+1}^* \cdot R_{s+1}^*$$

also has product one, in which case $\pi(R_{s+1}^*)^{-1} \in \pi([T_{s+1}^*]) = \pi(T)$, contradicting (30). Therefore, we instead conclude that $\pi(T)R_s^*(1) \neq R_s^*(1)\pi(T)$. Consequently, since

$$\pi(T)R_s^*(1) \cup R_s^*(1)\pi(T) \subseteq \pi\Big(T \cdot R_s^*(1)\Big),$$

it follows in view of (27) that

$$|\pi\Big(T \cdot R_s^*(1)\Big)| \geq |\pi(T)| + 1 \geq \frac{1}{2}|T| + 2 \geq \frac{1}{2}|T \cdot R_s^*(1)| + 1. \tag{31}$$

Thus, in view of (28), the maximality of $\ell \in [2, 2|G'| - 2]$ is contradicted by $T \cdot R_s^*(1)$ taking $U^* = T_s^* \cdot R_s^*$ for (26). So we may instead assume that

$$R_{s+1}^* = R_s^*(2) \cdot R_s^*(1) \cdot R_s^*(3, |R|).$$

The remainder of the proof is now just a variation on the previous paragraph. If

$$\pi(T)R_s^*(1)R_s^*(2) = \pi(T)R_s^*(2)R_s^*(1),$$

then the terms of T can be ordered, yielding some $T_{s+1}^* \in \mathcal{F}^*(G)$ with $[T_{s+1}^*] = T$, such that

$$T_{s+1}^* \cdot R_{s+1}^* = T_{s+1}^* \cdot R_s^*(2) \cdot R^*(1) \cdot R_s^*(3, |R|) \in \mathcal{F}^*(G)$$

has product $\pi(T_s^* \cdot R_s^*) = 1$, in which case $\pi(R_{s+1}^*)^{-1} \in \pi([T_{s+1}^*]) = \pi(T)$, contradicting (30). Therefore, we instead conclude that $\pi(T)R_s^*(1)R_s^*(2) \neq \pi(T)R_s^*(2)R_s^*(1)$. Consequently, since

$$\pi(T)R_s^*(1)R_s^*(2) \cup \pi(T)R_s^*(2)R_s^*(1) \subseteq \pi\Big(T \cdot R_s^*(1) \cdot R_s^*(2)\Big),$$

it follows in view of (27) that

$$\Big|\pi\Big(T \cdot R_s^*(1) \cdot R_s^*(2)\Big)\Big| \geq |\pi(T)| + 1 \geq \frac{1}{2}|T| + 2 = \frac{1}{2}|T \cdot R_s^*(1) \cdot R_s^*(2)| + 1. \tag{32}$$

Thus, in view of (28), the maximality of $\ell \in [2, 2|G'| - 2]$ is contradicted by $T \cdot R_s^*(1) \cdot R_s^*(2)$ taking $U^* = T_s^* \cdot R_s^*$ for (26), completing the proof. □

4. Upper Bounds for p-Groups

In this section, we give general upper bounds for $\mathsf{D}(G)$ when G is a p-group. The main result of the section is the following.

Theorem 4.1. *Let G be a finite p-group with $p \geq 2$ prime. If G is non-abelian, then*

$$\mathsf{D}(G) \leq \frac{p^2 + 2p - 2}{p^3}|G|. \tag{33}$$

We begin with the following lemma, which follows by standard inductive arguments.

Lemma 4.2. *Let G be a finite group and let $H \trianglelefteq G$ be a normal subgroup with $G/H \cong C_p^2$. Then*

$$\mathsf{d}(G) \leq (\mathsf{d}(H) + 2)p - 2 \leq \frac{1}{p}|G| + p - 2.$$

Proof. From Lemma 2.6.1, we have $\mathsf{d}(H)+1 \le \mathsf{D}(H) \le |H| = \frac{1}{p^2}|G|$. Hence $(\mathsf{d}(H)+2)p-2 \le \frac{1}{p}|G|+p-2$, so that the second inequality for the lemma holds in general.

Let $S \in \mathcal{F}(G)$ be a sequence with length $|S| \ge (\mathsf{d}(H)+2)p-1$. We need to show $1 \in \Pi(S)$, i.e., that S has a nontrivial, product-one subsequence. By hypothesis, we have $G/H \cong C_p^2$, and from (6), we know $\eta(G/H) = \eta(C_p^2) = 3p-2$. Repeatedly applying the definition of $\eta(G/H)$ to $\phi_H(S)$, we can remove product-one subsequences from $\phi_H(S)$ of length at most p until there are at most $3p-3$ terms of $\phi_H(S)$ left. In other words, we obtain a factorization $S = [S_1^*] \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} [S_\ell^*] \boldsymbol{\cdot} [S'^*]$ with $S_1^*, \ldots, S_\ell^*, S'^* \in \mathcal{F}^*(G)$,

$$1 \le |S_i^*| \le p \qquad \text{and} \qquad \pi(S_i^*) \in H \quad \text{for } i \in [1,\ell], \qquad \text{and} \qquad |S'^*| \le 3p-3. \tag{34}$$

Consequently,

$$\ell \ge \frac{|S|-|S'^*|}{p} \ge \frac{(\mathsf{d}(H)+2)p-1-|S'^*|}{p} \ge \frac{(\mathsf{d}(H)+2)p-1-3p+3}{p} = \mathsf{d}(H)-1+\frac{2}{p}. \tag{35}$$

Hence $\ell \ge \mathsf{d}(H)$.

If $\ell > \mathsf{d}(H)$, then applying the definition of $\mathsf{d}(H)$ to the sequence

$$[\pi(S_1^*)] \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} [\pi(S_\ell^*)] \in \mathcal{F}(H)$$

yields a nontrivial product-one subsequence $\bullet_{i\in I}[\pi(S_i^*)] \in \mathcal{F}(H)$, for some nonempty $I \subseteq [1,\ell]$, in which case $\bullet_{i\in I}[S_i^*] \in \mathcal{F}(G)$ is the desired product-one subsequence of S. So we may assume $\ell = \mathsf{d}(H)$.

If $|S'^*| \le 2p-2$, then the estimate in (35) improves to $\ell \ge \mathsf{d}(H)+1$, contrary to what we just established. Therefore $|S'^*| \ge 2p-1 = \mathsf{d}(C_p^2)+1 = \mathsf{d}(G/H)+1$ (in view of (6)). But now we can apply the definition of $\mathsf{d}(G/H)+1$ to the sequence $\phi_H(S')$ to find a nontrivial subsequence $[S_{\ell+1}^*]$ of S' with $\pi(S_{\ell+1}^*) \in H$, where $S_{\ell+1}^* \in \mathcal{F}^*(G)$. Applying the arguments of the previous paragraph to $[\pi(S_1^*)] \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} [\pi(S_{\ell+1}^*)]$ instead of $[\pi(S_1^*)] \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} [\pi(S_\ell^*)]$ now yields the desired product-one subsequence of S, completing the proof. □

Now we can prove Theorem 4.1.

Proof of Theorem 4.1. Since G is a finite, non-abelian group, it must possess a minimal non-abelian subgroup $H \le G$, that is, a subgroup $H \le G$ such that all proper subgroups $K < H$ are abelian. Assuming we knew the theorem held for minimal non-abelian p-groups, we could apply the result to H and then invoke Theorem 2.11, yielding the bound

$$\mathsf{D}(G) \le \mathsf{D}(H)|G:H| \le \frac{p^2+2p-2}{p^3}|H||G:H| = \frac{p^2+2p-2}{p^3}|G|,$$

as desired. Therefore, we see that it suffices to prove the theorem when G is a minimal non-abelian group, which we now assume.

Miller and Moreno characterized all finite minimal non-abelian groups back in 1903 [10]. A summary of their result for finite p-groups can be found in the more modern text [2, pp. 179], with some of the details for the p-group case also given in [9]. We do not need the full characterization, only the following easily derived consequences:

$$G' \cong C_p \qquad \text{and} \qquad G/\mathsf{Z}(G) \cong C_p^2,$$

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

Since $G' \cong C_p$ and all proper subgroups of G are abelian (in view of G being a *minimal* non-abelian group), it follows from Corollary 3.4 that

$$\mathsf{D}(G) \le \mathsf{d}(G) + |G'| = \mathsf{d}(G) + p. \tag{36}$$

Since $G/\mathsf{Z}(G) \cong C_p^2$, Lemma 4.2 implies $\mathsf{d}(G) \le \frac{1}{p}|G| + p - 2$. Combining with (36), it follows that

$$\mathsf{D}(G) \le \frac{1}{p}|G| + 2p - 2 = \left(\frac{1}{p} + \frac{2p-2}{|G|}\right)|G|. \tag{37}$$

Since G is a non-abelian p-group, we have $|G| \ge p^3$ [14, Theorem 1.6.15], which combined with (37) yields the desired bound

$$\mathsf{D}(G) \le \left(\frac{1}{p} + \frac{2p-2}{p^3}\right)|G| = \frac{p^2+2p-2}{p^3}|G|,$$

completing the proof. □

We remark that the constant $\frac{p^2+2p-2}{p^3}$ from Theorem 4.1 is close to optimal. The group

$$M_{p^n} = \langle \alpha, \tau : \ \alpha^{p^{n-1}} = 1, \tau^p = 1, \alpha\tau = \tau\alpha^{1+p^{n-2}} \rangle$$

is a well-known minimal non-abelian group of order p^n for $n \ge 3$, and considering the sequence

$$\tau^{p-1}\alpha \cdot \alpha^{[p-1]} \cdot \tau\alpha^{1-p} \cdot \alpha^{[p^{n-1}-1]} \in \mathcal{F}(M_{p^n})$$

shows that $\mathsf{D}(M_{p^n}) \ge p^{n-1} + p$. When $n = 3$, this gives $\mathsf{D}(M_{p^3}) \ge p^2 + p = \frac{p^2+p}{p^3}|M_{p^3}|$, showing that the constant $\frac{p^2+2p-2}{p^3}$ is only off by at most $\frac{p-2}{p^3}$.

As simple consequences of Theorem 4.1, we get the following corollaries.

Corollary 4.3. *Let G be a finite p-group with $p \ge 2$ prime. If G is non-cyclic, then*

$$\mathsf{D}(G) \le \frac{2p-1}{p^2}|G|.$$

Proof. If G is abelian, then, since G is a non-cyclic p-group, there must be a subgroup $H \le G$ with $H \cong C_p^2$. Then, from Theorem 2.11 and (6), we obtain

$$\mathsf{D}(G) \le \mathsf{D}(H)|G/H| = \mathsf{D}(C_p^2)|G/H| = (2p-1)\frac{1}{p^2}|G|,$$

as desired. On the other hand, if G is non-abelian, then Theorem 4.1 yields

$$\mathsf{D}(G) \le \frac{p^2+2p-2}{p^3}|G| \le \frac{2p-1}{p^2}|G|,$$

completing the proof. □

Corollary 4.4. *Let G be a finite nilpotent group. If G is non-abelian, then*

$$\mathsf{D}(G) \le \frac{p^2+2p-2}{p^3}|G|,$$

where p is the smallest prime divisor of $|G|$.

Proof. A finite nilpotent group is a direct product of its Sylow subgroups [14, Theorem 5.2.4]. Thus, if every Sylow subgroup were abelian, then G would be abelian, contrary to hypothesis. As result, we conclude that G has a non-abelian Sylow q-group $P \le G$ for some prime $q \mid |G|$. But then Theorem 2.11 and Theorem 4.1 give

$$\mathsf{D}(G) \le \mathsf{D}(P)|G/P| \le \frac{q^2+2q-2}{q^3}|P||G/P| = \frac{q^2+2q-2}{q^3}|G| \le \frac{p^2+2p-2}{p^3}|G|,$$

as desired. □

5. The Non-Abelian group of Order pq

All groups of order p^2, where p is prime, are abelian [14, Theorem 1.6.15]. A non-abelian group of order pq, where p and q are distinct primes with $p < q$, exists precisely when $p \mid q-1$ and, in such case, is unique (up to isomorphism), being given by the presentation [8, Theorem 3.4.4]

$$F_{pq} := \langle \alpha, \tau : \ \alpha^q = 1, \quad \tau^p = 1, \quad \alpha\tau = \tau\alpha^r \rangle,$$

where $r \in \mathbb{Z}$ is an integer such that

$$r^p \equiv 1 \mod q \quad \text{but} \quad r \not\equiv 1 \mod q. \tag{38}$$

Note this means that the multiplicative order of r modulo q is equal to p. Since all proper subgroups of F_{pq} are of prime order, they are cyclic, which makes F_{pq} an example of a non-abelian group having all proper subgroups cyclic.

In Section 7, we will be able to reduce the question of bounding $\mathsf{D}(G)$, for more arbitrary G, to the case of $G = F_{pq}$ and one other group (treated in Section 6). This makes determining $\mathsf{D}(F_{pq})$ fairly important, which will be accomplished in the main result of this section, Theorem 5.1. The proof of Theorem 5.1 will be divided into several lemmas.

Theorem 5.1. *Let p and q be primes with $p \mid q-1$. Then*

$$\mathsf{D}(F_{pq}) = 2q.$$

Let us begin first with the lower bound.

Lemma 5.2. *Let p and q be primes with $p \mid q-1$. Then*

$$\mathsf{D}(F_{pq}) \ge 2q.$$

Proof. Let $G = F_{pq}$. Consider the sequence

$$S = \tau^{p-1} \cdot \alpha^{[q-1]} \cdot \tau\alpha^{r+1} \cdot \alpha^{[q-1]} \in \mathcal{F}(G).$$

Since

$$\tau^{p-1}\alpha^{q-1}\tau\alpha^{r+1}\alpha^{q-1} = \tau^{p-1}\tau\alpha^{-r}\alpha^{r+1}\alpha^{q-1} = \tau^p\alpha^q = 1,$$

we see that S is a product-one sequence. We claim that S is an atom, which will show $\mathsf{D}(G) \ge |S| = 2q$, as desired. Assuming to the contrary that S is not an atom, we obtain a factorization $S = T_1 \cdot T_2$ with $T_1, T_2 \in \mathcal{F}(G)$ both nontrivial, product-one sequences. Clearly, either $T_1 = \alpha^{[q]}$ or $T_2 = \alpha^{[q]}$, say T_1, and then $T_2 = \tau^{p-1} \cdot \tau\alpha^{r+1} \cdot \alpha^{[q-2]}$. Since T_2 has product-one, it follows in view of Lemma 2.5 that

$$1 = \tau^{p-1}\alpha^x(\tau\alpha^{r+1})\alpha^{q-2-x} = \alpha^{(x+1)(r-1)}, \quad \text{for some } x \in [0, q-2].$$

Since $\mathrm{ord}(\alpha) = q$ is prime, this means $x + 1 \equiv 0 \mod q$ or $r - 1 \equiv 0 \mod q$. The latter is ruled out by (38) while the former is impossible in view of $x \in [0, q-2]$, yielding the desired contradiction. □

For the proof of Theorem 5.1, we will need to adapt the ideas from Section 3 using very specific knowledge about the conjugacy structure of F_{pq}. To this end, we summarize some easily verified group theoretic properties for $G = F_{pq}$:

$$G' = [G, G] = \langle \alpha \rangle \cong C_q \quad \text{and} \quad \mathsf{Z}(G) = \{1\}; \tag{39}$$

$$\mathsf{C}_G(g) = \langle g \rangle \quad \text{for every } g \in G \setminus \{1\}; \tag{40}$$

$$\mathrm{ord}(g) = q \quad \text{for every } g \in G' \setminus \{1\} \quad \text{and} \quad \mathrm{ord}(g) = p \quad \text{for every } g \in G \setminus G'; \tag{41}$$

and the conjugacy classes of G are given by

$$\{1\}, \quad \{\alpha^x, \alpha^{xr}, \alpha^{xr^2}, \ldots, \alpha^{xr^{p-1}}\} \quad \text{for } x \in X, \quad \text{and} \quad \tau^y\langle \alpha \rangle \quad \text{for } y = 1, 2, \ldots, p-1, \tag{42}$$

where $X \subseteq [1, q-1]$ is some subset of size $|X| = \frac{q-1}{p}$. We continue with a simple lemma.

Lemma 5.3. *Let p and q be primes with $p \mid q-1$, let $G = F_{pq}$, let $S \in \mathcal{F}(G' \setminus \{1\})$ and let $x \in G \setminus G'$. Then*

$$|\pi(x \cdot S)| \geq \min\{q, |x \cdot S|\}.$$

Proof. We may w.l.o.g. assume $|S| \leq q-1$, for if $|S| \geq q$, then applying the lemma to any length $q-1$ subsequence of S completes the proof. We need to show

$$|\pi(x \cdot S)| \geq |x \cdot S|. \tag{43}$$

If S is the empty sequence, then (43) is trivial, so we assume $|S| \geq 1$ and proceed by induction on $|S| \leq q-1$. Let $y \in \mathrm{supp}(S)$ and set $S' = y^{[-1]} \cdot S$. Since $S \in \mathcal{F}(G' \setminus \{1\})$, we have

$$\langle y \rangle = G' \cong C_q. \tag{44}$$

Since $x \in G \setminus G'$ and $\mathrm{supp}(S') \subseteq \mathrm{supp}(S) \subseteq G'$, it follows that

$$\pi(x \cdot S') \subseteq xG' \neq G'. \tag{45}$$

Note that

$$\pi(x \cdot S')y \cup y\pi(x \cdot S') \subseteq \pi(x \cdot S' \cdot y) = \pi(x \cdot S). \tag{46}$$

By induction hypothesis, $|\pi(x \cdot S')| \geq |x \cdot S'| = |x \cdot S| - 1$. Thus $|\pi(x \cdot S)| \geq |x \cdot S|$ follows from (46), completing the proof, unless $\pi(x \cdot S')y = y\pi(x \cdot S')$. However, this is equivalent to saying

$$y^{-1}\pi(x \cdot S')y = \pi(x \cdot S').$$

Thus the set $\pi(x \cdot S')$ must be a union of orbits under the action of conjugation by elements from $\langle y \rangle = G'$ (in view of (44)). In particular, the G'-orbit of z is contained in $\pi(x \cdot S')$ for any $z \in \pi(x \cdot S')$. By (45), we have $z \in G \setminus G'$ for any such $z \in \pi(x \cdot S')$. But since $\mathsf{C}_G(z) \cap G' = \langle z \rangle \cap G' = \{1\}$, and since the size of the G'-orbit containing z is $|G'|/(\mathsf{C}_G(z) \cap G') = |G'| = q$ (by (2)), it follows that

$$|\pi(x \cdot S)| \geq |\pi(x \cdot S')| \geq q \geq |x \cdot S|,$$

completing the proof. □

The next lemma improves the *bound* from Lemma 5.3 under some mild restrictions and requires a more technical argument (and slightly different hypotheses).

Lemma 5.4. *Let p and q be primes with $p \mid q-1$, let $G = F_{pq}$, let $S \in \mathcal{F}(G' \setminus \{1\})$ and let $g_1, g_2 \in G \setminus G'$. Suppose $g_1 g_2 \notin G'$. Then*

$$|\pi(g_1 \cdot g_2 \cdot S)| \geq \min\{q, 2|S| + 1\}.$$

Proof. Let $g_1 = \tau^{x_1}\alpha^{a_1}$, let $g_2 = \tau^{x_2}\alpha^{a_2}$, and let $S = \alpha^{y_1} \cdot \ldots \cdot \alpha^{y_\ell}$, where $\ell = |S|$. Since $S \in \mathcal{F}(G' \setminus \{1\})$, we have

$$y_i \not\equiv 0 \mod q \quad \text{for all } i \in [1, \ell], \tag{47}$$

since $g_1, g_2 \in G \setminus G'$, we have

$$x_1 \not\equiv 0 \mod p \qquad \text{and} \qquad x_2 \not\equiv 0 \mod p, \tag{48}$$

and since $g_1 g_2 \notin G'$, we have

$$x_1 + x_2 \not\equiv 0 \mod p. \tag{49}$$

Since the multiplicative order of r modulo q is p (care of (38)), we deduce from (48) and (49) that

$$\{1, r^{x_2}, r^{x_1+x_2}\}$$

is a set of 3 distinct non-zero residue classes modulo q.

Now

$$\pi(g_1 \cdot g_2 \cdot S) = \{\pi(T^*) : T^* \in \mathcal{F}^*(G) \qquad \text{and} \qquad [T^*] = g_1 \cdot g_2 \cdot S\}.$$

Every $T^* \in \mathcal{F}^*(G)$ with $[T^*] = g_1 \cdot g_2 \cdot S$ has the term equal to g_1 either preceding or following the term equal to g_2. Consider only those $T^* \in \mathcal{F}^*(G)$ with $[T^*] = g_1 \cdot g_2 \cdot S$ such that g_1 precedes g_2. Then each term α^{y_i} of S can either occur before g_1 in T^*, between g_1 and g_2, or after g_2. Furthermore,

$$\pi(T^*) = \tau^{x_1+x_2}\alpha^{a_1 r^{x_2} + a_2 + \sum_{i=1}^{\ell} y_i w_i},$$

where $w_i \in \{r^{x_1+x_2}, r^{x_2}, 1\}$ is dependent on whether the term α^{y_i} of S occurs before g_1 in T^*, between g_1 and g_2, or after g_2. Combining these thoughts, we find that

$$|\pi(g_1 \cdot g_2 \cdot S)| \geq \left| \left\{ \phi_{q\mathbb{Z}}(y) : y \in \sum_{i=1}^{\ell} y_i \{r^{x_1+x_2}, r^{x_2}, 1\} \right\} \right|. \tag{50}$$

The right hand side of (50) is just the number of distinct residue classes modulo q contained in the integer sumset from (50). We showed above that $\{r^{x_1+x_2}, r^{x_2}, 1\}$ is a set of 3 distinct residue classes modulo q, and since (47) ensures that each $y_i \not\equiv 0 \mod q$, it follows that each summand $y_i\{r^{x_1+x_2}, r^{x_2}, 1\}$ in the sumset from (50) has size 3 modulo the prime q. Thus, applying the Cauchy-Davenport Theorem to (50) yields

$$|\pi(g_1 \cdot g_2 \cdot S)| \geq \min\{q, 2\ell + 1\}.$$

Since $\ell = |S|$, the proof is now complete. □

The following lemma will be quite helpful.

Lemma 5.5. *Let p and q be primes with $p \mid q-1$, let $G = F_{pq}$, and let $S \in \mathcal{F}(G \setminus \{1\})$. If $\langle \mathrm{supp}(S)\rangle = G$, then*

$$|\pi(S)| \ge \min\{p, |S|\}.$$

Proof. We may w.l.o.g. assume $|S| \le p$, for if $|S| > p$, then applying the lemma to any length p subsequence of S that generates G completes the proof (note any 2 non-commuting terms generate G). We need to show $|\pi(S)| \ge |S|$. Factor $S = S_{G'} \cdot S_{G\setminus G'}$ with $S_{G'} \mid S$ the subsequence consisting of all terms from G'. Note, since $S \in \mathcal{F}(G \setminus \{1\})$, that no term of S is equal to 1. In view of $\langle \mathrm{supp}(S)\rangle = G$, there must be some $g_0 \in \mathrm{supp}(S)$ with $g_0 \notin G'$. From Lemma 5.3, we have

$$|\pi(g_0 \cdot S_{G'})| \ge |g_0 \cdot S_{G'}|. \tag{51}$$

Let $R \mid S$ be a maximal length subsequence such that $g_0 \cdot S_{G'} \mid R$ and $|\pi(R)| \ge |R|$. Note that R exists in view of (51). If $R = S$, then the proof is complete, so assume otherwise and let $x \in \mathrm{supp}(S \cdot R^{[-1]})$. Since $S_{G'} \mid R$, we have

$$x \in G \setminus G'. \tag{52}$$

Since $g_0 \cdot S_{G'} \mid R$, we could only have $|R| = 1$ if $|S_{G'}| = 0$ and $\mathrm{supp}(S) \subseteq \mathsf{C}_G(g_0) = \langle g_0\rangle$ (in view of (40)). However, $\mathrm{supp}(S) \subseteq \langle g_0\rangle$ would contradict the hypothesis $\langle \mathrm{supp}(S)\rangle = G$. Therefore we conclude that $|R| \ge 2$. Hence

$$|\pi(R)| \ge |R| \ge 2. \tag{53}$$

We have $\pi(R)x \cup x\pi(R) \subseteq \pi(R \cdot x)$. Thus $|\pi(R \cdot x)| \ge |R \cdot x|$ will follow, contradicting the maximality of R, unless $\pi(R)x = x\pi(R)$, which is equivalent to saying

$$x^{-1}\pi(R)x = \pi(R).$$

In consequence, $\pi(R)$ must be a union of orbits under the action of conjugation by elements from $\langle x\rangle$.

Let $g \in G$ be an arbitrary element. Then g is contained in a $\langle x\rangle$-orbit of size $|\langle x\rangle|/|\mathsf{C}_G(g) \cap \langle x\rangle|$ (cf. (2)). In particular, in view of (40), (41) and (52), we see that the size of the $\langle x\rangle$-orbit containing g is either 1 (if $g \in \langle x\rangle$) or p (otherwise). Thus, if $\pi(R)$ contains some element from $G \setminus \langle x\rangle$, then (as noted above) it will contain the full $\langle x\rangle$-orbit containing this element, implying that $|\pi(R \cdot x)| \ge |\pi(R)| \ge p \ge |S| \ge |R \cdot x|$, which would contradict the maximality of R. So we instead conclude that

$$\pi(R) \subseteq \langle x\rangle. \tag{54}$$

Since $x \in G \setminus G'$ (in view of (52)), it is readily seen that each element of $\langle x\rangle$ is from a separate G'-coset. However, as noted in Section 2, the set $\pi(R)$ is contained in a single G'-coset. Thus (54) ensures that $|\pi(R)| \le |G' \cap \langle x\rangle| = 1$, contradicting (53) to complete the proof. □

The following lemma shows that a sufficiently long sequence having a product in G' must actually have a product-one subsequence.

Lemma 5.6. *Let p and q be primes with $p \mid q-1$, let $G = F_{pq}$, and let $S \in \mathcal{F}(G)$. If $\pi(S) \subseteq G'$ and $|S| \ge q$, then $1 \in \Pi(S)$.*

Proof. By hypothesis, $\phi_{G'}(S) \in \mathcal{F}(G/G') \cong \mathcal{F}(C_p)$ is a product-one sequence. Let $S = T_1 \cdot \ldots \cdot T_\ell$ be a factorization of S with $\phi_{G'}(T_i) \in \mathcal{A}(G/G')$ for $i = 1, \ldots, \ell$. Note (in view of Lemma 2.6) that

$$1 \le |T_i| \le \mathsf{D}(G/G') = \mathsf{D}(C_p) = p \quad \text{for } i \in [1, \ell]. \tag{55}$$

If $1 \in \pi(T_i)$, then the lemma is complete in view of $\pi(T_i) \subseteq \Pi(S)$. Therefore we may assume $1 \notin \pi(T_i)$ for every $i \in [1, \ell]$.

Observe that

$$\pi(T_1)\Big(\{1\} \cup \pi(T_2)\Big) \dots \Big(\{1\} \cup \pi(T_\ell)\Big) \subseteq \Pi(S). \tag{56}$$

Since $1 \notin \pi(T_i)$ for each i, we have

$$|\{1\} \cup \pi(T_i)| = |\pi(T_i)| + 1 \quad \text{for } i \in [1, \ell] \tag{57}$$

As remarked in Section 2, each $\pi(T_i)$ is contained in a single G'-coset, which must be G' itself in view of $\phi_{G'}(T_i) \in \mathcal{A}(G/G')$. Thus

$$\{1\} \cup \pi(T_i) \subseteq G' \quad \text{for } i \in [1, \ell]. \tag{58}$$

Next, we proceed to show that

$$|\pi(T_i)| \ge |T_i| \quad \text{for } i \in [1, \ell]. \tag{59}$$

Let $i \in [1, \ell]$ be arbitrary. If $\operatorname{supp}(T_i) \cap G' \neq \emptyset$, then $\phi_{G'}(T_i) \in \mathcal{A}(G/G')$ forces $|T_i| = 1$, in which case (59) is clear. If $\operatorname{supp}(T_i) \subseteq G \setminus G'$ but $\operatorname{supp}(T_i) \nsubseteq H$ for every $H \le G$ with $|H| = p$, then $\langle \operatorname{supp}(T_i) \rangle = G$. In this case, since (55) ensures $|T_i| \le p$, Lemma 5.5 gives (59). Finally, consider the case when $\operatorname{supp}(T_i) \subseteq H$ for some $H \le G$ with $|H| = p$. In this case, $\pi(T_i) \subseteq H$, which combined with (58) gives $\pi(T_i) \subseteq H \cap G' = \{1\}$. Hence $\pi(T_i) = \{1\}$, contrary to (57). Thus (59) is established in all cases.

In view of (58) and $G' = \langle \alpha \rangle \cong C_q$, we can apply the Cauchy-Davenport Theorem to the product-set from (56), yielding

$$\begin{aligned} |\Pi(S) \cap G'| &\ge \min\{q, |\pi(T_1)| + \sum_{i=2}^{\ell} |\{1\} \cup \pi(T_i)| - \ell + 1\} \\ &= \min\{q, \sum_{i=1}^{\ell} |\pi(T_i)|\} \ge \min\{q, \sum_{i=1}^{\ell} |T_i|\} = \min\{q, |S|\} = q, \end{aligned} \tag{60}$$

where the first equality is from (57), the second inequality is from (59), the second equality is from $S = T_1 \cdot \ldots \cdot T_\ell$ being a a factorization of S, and the final equality is in view of the hypothesis $|S| \ge q$. In view of (60) and $|G'| = q$, it follows that $1 \in G' = \Pi(S') \cap G'$, completing the proof. □

It is now a simple corollary to determine the small Davenport constant of F_{pq}, which was first achieved by Bass [1].

Corollary 5.7. *Let p and q be primes with $p \mid q - 1$. Then*

$$\mathsf{d}(F_{pq}) = q + p - 2.$$

Proof. The sequence $\alpha^{[q-1]} \cdot \tau^{[p-1]} \in \mathcal{F}(F_{pq})$ is readily seen to have no nontrivial, product-one subsequence. Thus $\mathsf{d}(F_{pq}) \ge p + q - 2$. To show $\mathsf{d}(F_{pq}) \le p + q - 2$, let $S \in \mathcal{F}(F_{pq})$ be a sequence with $|S| \ge q + p - 1$. We need to show $1 \in \Pi(S)$. In view of Lemma 5.6, to show $1 \in \Pi(S)$, it suffices to show S has a subsequence $T \mid S$ with $|T| \ge q$ and $\pi(T) \subseteq G'$. However, this is equivalent to finding a product-one subsequence of $\phi_{G'}(S)$ having length at least q. Repeated application of the definition of $\mathsf{D}(G/G') = \mathsf{D}(C_p) = p$ (in view of Lemma 2.6) to $\phi_{G'}(S)$ gives a product-one subsequence of $\phi_{G'}(S)$ with length at least $|S| - \mathsf{D}(G/G') + 1 = |S| - p + 1 \ge q$, with the final inequality in view of the hypothesis $|S| \ge q + p - 1$. Thus the proof is complete. □

If $|S| \ge \mathsf d(F_{pq}) + 1$, then we are guaranteed a nontrivial, product-one subsequence $T \mid S$ but know nothing about its length apart from the trivial bound $|T| \le \mathsf d(F_{pq}) + 1$. Lemma 5.8 shows that when $|S|$ is slightly larger than $\mathsf d(F_{pq}) + 1$, then we can be assured of finding a nontrivial, product-one subsequence of length at most q.

Lemma 5.8. *Let p and q be primes with $p \mid q-1$, let $G = F_{pq}$, and let $S \in \mathcal F(G)$. If $|S| \ge q+2p-3$, then there is a nontrivial, product-one subsequence $T \mid S$ with $|T| \le q$. In other words, $\eta(F_{pq}) \le q + 2p - 3$.*

Proof. We handle two cases.

Case 1: $\mathsf h\big(\phi_{G'}(S)\big) \le |S| - p + 1$.

We aim to show that there exists a subsequence $T' \mid S$ with

$$|T'| = q \qquad \text{and} \qquad \pi(T') \subseteq G'. \tag{61}$$

Once (61) is established, we can apply Lemma 5.6 to T' to find a nontrivial, product-one subsequence $T \mid T'$ with $|T| \le |T'| = q$, as desired. Thus it remains to establish (61) to complete Case 1. If $\Pi_q\big(\phi_{G'}(S)\big) = G/G'$, then (61) readily follows, completing the case. Therefore, we can assume otherwise:

$$\Pi_q\big(\phi_{G'}(S)\big) \ne G/G'. \tag{62}$$

Thus, since $G/G' \cong C_p$ with p prime, it follows that $\mathsf H\Big(\Pi_q\big(\phi_{G'}(S)\big)\Big) = \{1\}$. Consequently, applying Theorem 2.9 to $\Pi_q\big(\phi_{G'}(S)\big)$ yields

$$|\Pi_q\big(\phi_{G'}(S)\big)| \ge \sum_{g \in G/G'} \min\{q, \mathsf v_g\big(\phi_{G'}(S)\big)\} - q + 1, \tag{63}$$

If $\mathsf v_g\big(\phi_{G'}(S)\big) \le q$ for all $g \in G/G'$, then (63) together with the hypothesis $|S| \ge q + 2p - 3$ yields $|\Pi_q\big(\phi_{G'}(S)\big)| \ge |S| - q + 1 \ge 2p - 2 \ge p$. If $\mathsf v_g\big(\phi_{G'}(S)\big) > q$ holds for precisely one $g \in G/G'$, then (63) together with the case hypothesis yields $|\Pi_q\big(\phi_{G'}(S)\big)| \ge (q+p-1) - q + 1 = p$. Finally, if $\mathsf v_g\big(\phi_{G'}(S)\big) > q$ holds for more than one $g \in G/G'$, then (63) yields $|\Pi_q\big(\phi_{G'}(S)\big)| \ge 2q - q + 1 = q + 1 \ge p$. In all cases, we find that $|\Pi_q\big(\phi_{G'}(S)\big)| \ge p = |G/G'|$, which contradicts (62), completing Case 1.

Case 2: $\mathsf h\big(\phi_{G'}(S)\big) \ge |S| - p + 2$.

If there were at least q terms of S from $G' \cong C_q$, then there would be a nontrivial, product-one sequence of length at most $\mathsf d(G') + 1 = q$ (care of Lemma 2.6.4), as desired. Therefore we may assume there are at most $q - 1$ terms of S from G'. Thus, since $|S| - p + 2 \ge q + p - 1 \ge q$, we see that the case hypothesis implies that there exists a G'-coset $\tau^x G'$ with $x \in [1, p-1]$ such that $\mathsf v_{\tau^x G'}(S) \ge |S| - p + 2$. Let $S_{\tau^x G'} \mid S$ be the subsequence of all terms from $\tau^x G'$, so

$$|S_{\tau^x G'}| = \mathsf v_{\tau^x G'}(S) \ge |S| - p + 2 \ge q + p - 1. \tag{64}$$

Since $x \in [1, p-1]$, each element $g \in \tau^x G'$ has $\mathrm{ord}(g) = p$ (care of (41)). In consequence, we have

$$\mathsf h(S_{\tau^x G'}) \le p - 1, \tag{65}$$

as otherwise a subsequence of $S_{\tau^x G'}$ consisting of the same term repeated $p \le q$ times would give the desired product-one subsequence. Since $|S_{\tau^x G'}| \ge q + p - 1 \ge p$, it follows from Lemma 2.8 and (65) that there exist nonempty subsets $A_1, \ldots, A_p \subseteq G'$ with $(\tau^x A_1) \cdot \ldots \cdot (\tau^x A_p)$ a setpartition of $S_{\tau^x G}$. In

particular, if $1 \in (\tau^x A_1) \ldots (\tau^x A_p)$, then $S_{\tau^x G'}$ will have a product-one subsequence of length $p \le q$, completing the proof. Thus it remains to show $1 \in (\tau^x A_1) \ldots (\tau^x A_p)$ to complete the proof.

Since each $A_i \subseteq G'$ with the commutator subgroup G' normal in G, it follows that

$$(\tau^x A_1) \ldots (\tau^x A_p) = (\tau^x)^p A_1' \ldots A_p' = A_1' \ldots A_p' \subseteq G' \tag{66}$$

for some subsets $A_i' \subseteq G'$ with $|A_i| = |A_i'|$ for all $i \in [1, p]$. Thus, since $G' \cong C_q$ with q prime, we can invoke the Cauchy-Davenport Theorem, recall that $(\tau^x A_1) \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} (\tau^x A_p)$ a setpartition of $S_{\tau^x G}$, and then use (64) to obtain

$$\begin{aligned} |A_1' \ldots A_p'| &\ge \min\{q, \sum_{i=1}^{p} |A_i'| - p + 1\} = \min\{q, \sum_{i=1}^{p} |\tau^x A_i| - p + 1\} \\ &= \min\{q, |S_{\tau^x G'}| - p + 1\} = q = |G'|. \end{aligned}$$

As a result, the inclusion in (66) must be an equality, which implies $1 \in G' = (\tau^x A_1) \ldots (\tau^x A_p)$, completing the proof as mentioned above. □

Next, we show that a counter-example to Theorem 5.1 cannot have many terms from $G' = \langle \alpha \rangle$.

Lemma 5.9. *Let p and q be odd primes with $p \mid q-1$, let $G = F_{pq}$, and let $S \in \mathcal{A}(G)$. If $|S| \ge 2q+1$, then*

$$\mathsf{v}_{G'}(S) = \sum_{g \in G'} \mathsf{v}_g(S) \le \frac{q-3}{2}.$$

Proof. Since S has product-one, let $S^* \in \mathcal{F}^*(G)$ be an ordering of S, so $[S^*] = S$, with $\pi(S^*) = 1$. If $\mathrm{supp}(S) \subseteq G'$, then $|S| \le \mathsf{D}(G') = \mathsf{D}(\langle \alpha \rangle) = q$ (in view of $S \in \mathcal{A}(G)$ and Lemma 2.6.4), contradicting that $|S| \ge 2q+1$. Thus S must have a term from $G \setminus G'$, and in view of Lemma 2.5, we can assume the first term of S^* is from $G \setminus G'$.

Suppose $\mathsf{v}_{G \setminus G'}(S) \le 2$. Then there will be at least $|S| - 2 \ge 2q - 1$ terms of S from G'. But now, since the first term of S^* is from $G \setminus G'$, the pigeonhole principle guarantees that there is a consecutive subsequence $T^* \mid S^*$ with $|T^*| \ge q = |G'|$ and $\mathrm{supp}(T^*) \subseteq G'$. Applying Lemma 2.6.1 to $T^* \in \mathcal{F}(G')$, we obtain a nontrivial, product-one consecutive subsequence in S^* of length at most $q < |S|$, which contradicts Lemma 2.3. So we instead conclude that

$$\mathsf{v}_{G \setminus G'}(S) \ge 3. \tag{67}$$

We claim that (67) implies there is a subsequence $g_1 \boldsymbol{\cdot} g_2 \mid S$ with

$$g_1,\, g_2 \in G \setminus G' \qquad \text{and} \qquad g_1 g_2 \notin G'. \tag{68}$$

To see this, in view of (67), let $x, y, z \in \mathrm{supp}(S)$ be terms with $x,\, y,\, z \in G \setminus G'$ and $x \boldsymbol{\cdot} y \boldsymbol{\cdot} z \mid S$ and assume by contradiction that $xy,\, xz,\, yz \in G'$. Then $\phi_{G'}(x)\phi_{G'}(y) = \phi_{G'}(x)\phi_{G'}(z) = 1$, implying $\phi_{G'}(y) = \phi_{G'}(z)$. But now $yz \in G'$ implies $1 = \phi_{G'}(y)\phi_{G'}(z) = \phi_{G'}(y)^2$, so that $\mathrm{ord}(\phi_{G'}(y)) \mid 2$. However, since $G/G' \cong C_p$ with p odd by hypothesis, $\mathrm{ord}(\phi_{G'}(y))$ cannot be even, forcing $\mathrm{ord}(\phi_{G'}(y)) = 1$. Thus $y \in G'$, contrary to its definition. This establishes (68), as claimed.

Assume by contradiction that

$$\mathsf{v}_{G'}(S) = \sum_{g \in G'} \mathsf{v}_g(S) \ge \frac{q-1}{2}$$

and let $T \mid S$ be a subsequence with $\mathrm{supp}(T) \subseteq G'$ and $|T| = \frac{q-1}{2}$. Since S is an atom of length $|S| \geq 2q+1 \geq 2$, we have $\mathrm{supp}(T) \subseteq \mathrm{supp}(S) \subseteq G \setminus \{1\}$. Thus we can apply Lemma 5.4 using the sequence $g_1 \cdot g_2 \cdot T$ and thereby find that

$$|\pi(g_1 \cdot g_2 \cdot T)| \geq \min\{q, 2|T|+1\} = q, \tag{69}$$

where the final inequality follows in view of $|T| = \frac{q-1}{2}$.

Since $|S| \geq 2q+1$ and $|T| = \frac{q-1}{2}$, it follows that

$$|S \cdot (T \cdot g_1 \cdot g_2)^{[-1]}| = |S| - |T| - 2 \geq \frac{3q-1}{2}. \tag{70}$$

Since $p \mid q-1$ with p and q odd, we have $q \geq 2p+1$. Combining this with (70) yields

$$|S \cdot (T \cdot g_1 \cdot g_2)^{[-1]}| \geq q + \frac{q-1}{2} \geq q + p = \mathsf{d}(G) + 2,$$

where the final inequality follows from Corollary 5.7. Thus applying the definition of $\mathsf{d}(G)$ to the sequence $S \cdot (T \cdot g_1 \cdot g_2)^{[-1]}$, we find a nontrivial, product-one subsequence $R \mid S$ such that $T \cdot g_1 \cdot g_2 \mid R^{[-1]} \cdot S$. As noted in Section 2, $\pi(R^{[-1]} \cdot S)$ is contained in a G'-coset. By Lemma 2.3, this G'-coset is actually the subgroup G' itself. Moreover, in view of $T \cdot g_1 \cdot g_2 \mid R^{[-1]} \cdot S$ and (69), we see that, in fact, $\pi(R^{[-1]} \cdot S) = G'$. In particular, $1 \in G' \in \pi(R^{[-1]} \cdot S)$. As a result, $S = R \cdot (R^{[-1]} \cdot S)$ is a factorization of S into 2 nontrivial, product-one subsequences, contradicting that $S \in \mathcal{A}(G)$ is an atom and completing the proof. □

As we will see in the proof, the following lemma is essentially just a consequence of the fact that a set in $\mathbb{F}_q$ having multiplicative stabilizer of size at least 3 cannot be an arithmetic progression apart from trivial extremes for its cardinality. Note, since $A \setminus \{0\}$ is a disjoint union of sets of size $p \geq 3$ (in view of the sets from Lemma 5.10 being orbits under the multiplication by r action), that the hypothesis $2 \leq |A| \leq q-2$ in Lemma 5.10 actually implies $3 \leq p \leq |A| \leq q-p \leq q-3$.

Lemma 5.10. *Let p and q be odd primes with $p \mid q-1$, let $r \in \mathbb{F}_q^\times$ be an element of multiplicative order p, and let $A \subseteq \mathbb{F}_q$ be a subset which is a union of sets of the form*

$$\{0\} \quad \text{and} \quad g\{1, r, r^2, \ldots, r^{p-1}\} \quad \text{for } g \in \mathbb{F}_q \setminus \{0\}. \tag{71}$$

If $2 \leq |A| \leq q-2$, then A is not an arithmetic progression.

Proof. Since p and q are odd primes, we have $p, q \geq 3$. Thus, since $r \in \mathbb{F}_q^\times$ has multiplicative order $p \geq 3$, we see that

$$r \notin \{-1, 0, 1\} \quad \text{with} \quad r^p = 1. \tag{72}$$

Let $P = \{1, r, r^2, \ldots, r^{p-1}\}$ and note that $rP = P$ in view of $r^p = 1$. Now $r\{0\} = \{0\}$ and $rgP = grP = gP$ for all $g \in \mathbb{F}_q \setminus \{0\}$. Thus A is a union of sets which are stable under multiplication by r, which implies that A is stable under multiplication by r:

$$A = rA.$$

Assume by contradiction that A is an arithmetic progression, so $A = \{a, a+d, \ldots, a+\ell d\}$ for some $a \in \mathbb{F}_q$ and $d \in \mathbb{F}_q^\times$, where $\ell = |A| - 1$. Then $A = rA = \{ra, ra+rd, \ldots, ra+\ell rd\}$ is also an arithmetic progression with difference $rd \in \mathbb{F}_q^\times$. However, since $2 \leq |A| \leq q-2$, it is well-known (and easily shown) that the difference d of the arithmetic progression A is unique up to sign. Hence $rd = \pm d$, implying $r \in \{-1, 1\}$, contrary to (72). □

The following lemma will be used in conjunction with Lemma 3.3.

Lemma 5.11. *Let p and q be odd primes with $p \mid q-1$, let $G = F_{pq}$, and let $T_1, \dots, T_r \in \mathcal{F}(G)$ be sequences for which* (10) *holds. Then the following hold.*

(i) $|\pi(T_1)\dots\pi(T_r)| \ge \min\{q-1, \sum_{i=1}^{r}|\pi(T_i)|\} \ge \min\{q-1, \sum_{i=1}^{r}|T_i|\}$.

(ii) *If* $\sum_{i=1}^{r}|T_i| \ge q+1$, *then* $|\pi(T_1)\dots\pi(T_r)| = q$.

Proof. Note, since $\pi(T)$ is contained in a G'-coset for any sequence $T \in \mathcal{F}(G)$, that we trivially have $|\pi(T)| \le |G'| = q$. In particular, since G' is normal, we have $|\pi(T_1)\dots\pi(T_r)| \le q$ (per the discussion after (4)). Consider an arbitrary $j \in [1, r-1]$. Then $\pi(T_i)^G = \pi(T_i)$ for all $i \in [1, j]$, which means that each $\pi(T_i)$, for $i \in [1, j]$, is a union of G-orbits. It easily seen that this property is preserved by taking product-sets: Indeed, given any x, y, $g \in G$, we have $g^{-1}xyg = g^{-1}xgy' = x'y'$ for some $y' \in y^G$ and $x' \in x^G$, which shows that the product-set of two orbits is stable under conjugation. Consequently,

$$(\pi(T_1)\dots\pi(T_j))^G = \pi(T_1)\dots\pi(T_j).$$

Thus the product-set $\pi(T_1)\dots\pi(T_j)$, for $j \in [1, r-1]$, is also a union of G-orbits. Since $\mathsf{Z}(G) = \{1\}$ and $|\pi(T_j)| \ge |T_j| \ge 2$, there can be at most one orbit of size 1 contained in $\pi(T_j)$, and so there is at least one orbit of size greater than 1 in $\pi(T_j)$, which must have size either p or q. If size q occurs, then we trivially have $|\pi(T_1)\dots\pi(T_r)| \ge |\pi(T_j)| \ge q$, as desired. So we instead conclude that each $\pi(T_j)$, for $j \in [1, r-1]$, is a union of G-orbits of size p possibly union $\{1\}$. Likewise, $\pi(T_1)\dots\pi(T_j)$, for $j \in [1, r-1]$, is also a union of G-orbits of size p possibly union $\{1\}$. In particular, we have

$$\pi(T_i) \subseteq G' \cong C_q \quad \text{for all } i \in [1, r-1].$$

Thus, since $\pi(T_r)$ is contained in a G'-coset (as remarked in Section 2), the Cauchy-Davenport Theorem and Vosper's Theorem can be used to estimate the product-set $\pi(T_1)\dots\pi(T_r)$.

Let us next deduce (ii) from (i). To this end, suppose $\sum_{i=1}^{r}|T_i| \ge q+1$. If $r = 1$, then we have $|\pi(T_1)\dots\pi(T_r)| = |\pi(T_1)| \ge |T_1| = \sum_{i=1}^{r}|T_i| \ge q+1 = |G'|+1$, which is impossible. Thus $r \ge 2$. Applying (i) to $\pi(T_1)\dots\pi(T_{r-1})$, we find that

$$|\pi(T_1)\dots\pi(T_{r-1})| \ge \min\{q-1, \sum_{i=1}^{r-1}|T_i|\}.$$

If $|\pi(T_1)\dots\pi(T_{r-1})| \ge q-1$, then the Cauchy-Davenport Theorem implies $|\pi(T_1)\dots\pi(T_{r-1})\pi(T_r)| = q$ in view of $|\pi(T_r)| \ge |T_r| \ge 2$, as desired. Thus $|\pi(T_1)\dots\pi(T_{r-1})| \ge \sum_{i=1}^{r-1}|T_i|$, and now the Cauchy-Davenport Theorem instead implies

$$|\pi(T_1)\dots\pi(T_{r-1})\pi(T_r)| \ge \min\{q, \sum_{i=1}^{r-1}|T_i| + |T_r| - 1\} = q,$$

with the final equality in view of the hypothesis $\sum_{i=1}^{r}|T_i| \ge q+1$. Thus we see that (ii) follows from (i).

It remains to prove (i). Translating between the multiplicative notation of (42) and the additive notation of Lemma 5.10, we see that the sets described in (71) correspond to the G-orbits contained

in G' as described by (42). In particular, we see that a set X which is a union of G-orbits of size p possibly union $\{1\}$ cannot be a (multiplicative) arithmetic progression unless $|X| \le 1$ or $|X| \ge q-1$. Thus, in view of the conclusion of the first paragraph (and since $|\pi(T_1)| \ge |T_1| \ge 2$ by (10)), we may assume each $\pi(T_1)\ldots\pi(T_j)$, for $j \in [1, r-1]$, is not a (multiplicative) arithmetic progression, else $|\pi(T_1)\ldots\pi(T_r)| \ge q-1$ follows, as desired. But that means we can apply Vosper's Theorem to the product-sets $\Big(\pi(T_1)\ldots\pi(T_j)\Big)\Big(\pi(T_{j+1})\Big)$, for $j \in [1, r-1]$, to obtain the estimate

$$|\pi(T_1)\ldots\pi(T_r)| \ge \min\{q-1, \sum_{i=1}^{r}|\pi(T_i)|\} \ge \min\{q-1, \sum_{i=1}^{r}|T_i|\},$$

with the second inequality in view of (10), as desired. □

Lemma 5.12 is the counterpart to Lemma 5.9, showing that a counter-example to Theorem 5.1 cannot have too many terms from the same order p subgroup $H \le G$.

Lemma 5.12. *Let p and q be odd primes with $p \mid q-1$, let $G = F_{pq}$, and let $S \in \mathcal{A}(G)$. If $|S| \ge 2q+1$, then*

$$\mathsf{v}_H(S) = \sum_{g\in H}\mathsf{v}_g(S) \le q \quad \text{for every subgroup } H \le G \text{ with } |H| = p.$$

Proof. Since $S \in \mathcal{A}(G)$, let $S^* \in \mathcal{F}(G)$ be an ordering of S, so $[S^*] = S$, with $\pi(S^*) = 1$. Since S is an atom of size $|S| > 1$, we have $1 \notin \mathrm{supp}(S)$. Assume by contradiction that there is an order p subgroup $H \le G$ with

$$\mathsf{v}_H(S) \ge q+1. \tag{73}$$

Consequently, since $q+1 \ge p+1$, we can apply Lemma 3.3 to S^* using H with $\omega = q+1$, $\omega_H = p+1$ and $\omega_0 = 0$. Let $S'^* = T_1^* \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T_r^* \boldsymbol{\cdot} R^*$ be the resulting factorization with all notation as given by Lemma 3.3. Since $\pi(S^*) = 1$, (8) ensures that

$$\pi(S'^*) = 1. \tag{74}$$

There are three cases depending on whether (i), (ii) or (iii) holds in Lemma 3.3.

Case 1: Lemma 3.3(i) holds. Then $\sum_{i=1}^{r}|T_i| \le \omega - 1 = q$ with $\langle \mathrm{supp}(R)\rangle$ a proper subgroup. In view of (73) and $\sum_{i=1}^{r}|T_i| \le \omega - 1 = q$, we see that $\langle \mathrm{supp}(R)\rangle$ must contain a term from H. Moreover, since $S \in \mathcal{A}(G)$ with $|S| \ge 2q+1 \ge 2$ ensures that no term of S is equal to 1, it follows that $\mathrm{supp}(R)$ contains a generating element from H, in which case $\langle \mathrm{supp}(R)\rangle < G$ being proper forces $\langle \mathrm{supp}(R)\rangle = H$. But now we have $|R| \ge |S| - \sum_{i=1}^{r}|T_i| \ge 2q+1-q = q+1 > p = |H|$, in which case we can apply Lemma 2.6.1 to find a product-one consecutive subsequence of R^* that is nontrivial and proper, which contradicts Lemma 2.3 in view of $[S'^*] = S \in \mathcal{A}(G)$ and (74).

Case 2: Lemma 3.3(ii) holds. Then $\sum_{i=1}^{r}|T_i| \ge \omega = q+1$ and there are at least $p+1 = |H|+1$ terms of R from H, in which case Lemma 2.6.1 ensures that R contains a nontrivial, product-one subsequence $R' \mid R$. Since $R' \mid R$, we have $T_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T_r \mid S \boldsymbol{\cdot} R'^{[-1]}$. In consequence, since lemma 5.11(ii) and $\sum_{i=1}^{r}|T_i| \ge q+1$ show that $\pi(T_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T_r)$ is a full G'-coset, it follows that $\pi(S \boldsymbol{\cdot} R'^{[-1]})$ is also a full G'-coset. Hence, since Lemma

2.4 implies $\pi(S \cdot R'^{[-1]}) \subseteq G'$, we conclude that $\pi(S \cdot R'^{[-1]}) = G'$, in which case $S = (S \cdot R'^{[-1]}) \cdot R'$ is a nontrivial factorization of S, contradicting that $S \in \mathcal{A}(G)$ is an atom.

Case 3: Lemma 3.3(iii) holds. Then $\sum_{i=1}^{r} |T_i| \le \omega - 1 = q$ and $\mathsf{v}_H(R) = p + 1$. Thus (73) ensures that

$$\mathsf{v}_H(T_1 \cdot \ldots \cdot T_r) = \mathsf{v}_H(S) - p - 1 \ge q - p. \tag{75}$$

Since H is an abelian subgroup, we see that $|\pi(T_i)| \ge |T_i| \ge 2$ (from (10)) ensures that each T_i contains some term from $G \setminus H$. Combined with (75), this implies

$$|T_1 \cdot \ldots \cdot T_r| \ge q - p + r \ge q - p + 1, \tag{76}$$

where $r \ge 1$ (which is equivalent to $R \ne S$) follow in view of of $\mathsf{v}_H(R) = p + 1 < q + 1 \le \mathsf{v}_H(S)$.

Since $\sum_{i=1}^{r} |T_i| \le \omega - 1 = q$ and $\mathsf{v}_H(R) = p + 1$, there are at least

$$|S| - q - p - 1 \ge 2q + 1 - q - p - 1 = q - p \ge p - 1$$

terms of R from $G \setminus H$ (recall that $p \mid q-1$ with p odd implies $q \ge 2p+1$). Thus we can find a subsequence $R_\alpha \mid R$ with

$$|R_\alpha| = p - 1 \qquad \text{and} \qquad \operatorname{supp}(R_\alpha) \cap H = \emptyset. \tag{77}$$

Let $g_0 \in \operatorname{supp}(R) \cap H$. Then $\langle \operatorname{supp}(g_0 \cdot R_\alpha) \rangle = G$ (in view of (77)), in which case Lemma 5.5 implies that

$$|\pi(g_0 \cdot R_\alpha)| \ge \min\{p, |\pi(g_0 \cdot R_\alpha)|\} = p. \tag{78}$$

Since $\pi(g_0 \cdot R_\alpha)$ is contained inside a G'-coset with $G' \trianglelefteq G$ a normal subgroup of prime order q, we can apply the Cauchy-Davenport Theorem and then make use of Lemma 5.11, (78) and (76) to conclude that

$$\begin{aligned} |\pi(T_1 \cdot \ldots \cdot T_r)\pi(g_0 \cdot R_\alpha)| &\ge \min\{q, |\pi(T_1 \cdot \ldots \cdot T_r)| + |\pi(g_0 \cdot R_\alpha)| - 1\} \\ &\ge \min\Big\{q, \min\{q-1, \sum_{i=1}^{r} |T_i|\} + |\pi(g_0 \cdot R_\alpha)| - 1\Big\} \\ &\ge \min\Big\{q, \min\{q-1, q-p+1\} + p - 1\Big\} = q. \end{aligned} \tag{79}$$

Since $\mathsf{v}_H(R) = p+1$ and $\mathsf{v}_H(g_0 \cdot R_\alpha) = 1$, we still have $p = |H|$ terms of $R \cdot (g_0 \cdot R_\alpha)^{[-1]}$ from H. Thus Lemma 2.6.1 ensures that we have a nontrivial, product-one subsequence $R' \mid R \cdot (g_0 \cdot R_\alpha)^{[-1]}$. In view of (74) and Lemma 2.4, we see that $\pi(S \cdot R'^{-1}) \subseteq G'$. However, since $S \cdot R'^{-1}$ contains the subsequence $T_1 \cdot \ldots \cdot T_r \cdot g_0 \cdot R_\alpha$, it follows from (79) that $\pi(S \cdot R'^{-1}) = G'$. Thus $S = (S \cdot R'^{-1}) \cdot R'$ is a nontrivial factorization of S, contradicting that $S \in \mathcal{A}(G)$ is an atom. This completes the proof. □

With the above work complete, we are now ready to begin the main portion of the proof of Theorem 5.1.

Proof of Theorem 5.1. Let $G = F_{pq}$. In view of Lemma 5.2, it suffice to prove the upper bound $\mathsf{D}(G) \le 2q$. If $p = 2$, then Lemma 2.6.1 implies $\mathsf{D}(G) \le |G| = 2q$, as desired. Therefore we may assume p is odd, and thus also q in view of $p \mid q - 1$. Note that this implies

$$q \ge 2p + 1.$$

Let $S \in \mathcal{A}(G)$ be an atom with $|S| = \mathsf{D}(G)$ and suppose by contradiction that $|S| \ge 2q+1$. Since $S \in \mathcal{A}(G)$ is an atom with $|S| \ge 2$, we have $1 \notin \mathrm{supp}(S)$. Let $S^* \in \mathcal{F}^*(G)$ be an ordering of S with $\pi(S^*) = 1$. By Lemma 5.9, we have

$$\mathsf{v}_{G'}(S) \le \frac{q-3}{2}. \tag{80}$$

We divide the proof into 2 main cases.

Case 1: $1 \in \Pi_{\le q-p}(S)$.

In view of the case hypothesis, let $U \mid S$ be a nontrivial, product-one subsequence with $|U| \le q-p$. Let $W = S \cdot U^{[-1]}$.

We first show that we can assume $|\langle \mathrm{supp}(U)\rangle| = p$ with $|U| \le p$. If $\mathsf{v}_{G'}(W) = 0$, then set W_0 to be the trivial sequence. Otherwise, in view of $|W| = |S| - |U| \ge q+p+1$ and (80), we can find a subsequence $W_0 \mid W$ containing all terms from G' and exactly 1 term from $G \setminus G'$. In view of Lemma 5.3, we have $|\pi(W_0)| \ge |W_0|$; moreover, if W_0 is nontrivial, then $|\pi(W_0)| \ge |W_0| \ge 2$, which together with $\mathsf{Z}(G) = \{1\}$ ensures that $\pi(W_0) \cap \Big(G \setminus \mathsf{Z}(G)\Big) \neq \emptyset$. Thus, letting $W^* \in \mathcal{F}^*(G)$ be any ordering of W such that $[W^*(1, |W_0|)] = W_0$, we can apply Lemma 3.3 to W^* taking H trivial, $\omega = q+1$, $\omega_H = -1$, and $\omega_0 = |W_0| \le \frac{q-1}{2}$. Let $W'^* = T_1^* \cdot \ldots \cdot T_r^* \cdot R^*$ be the resulting factorization with all notation as given by Lemma 3.3. Since ω_H is negative, Lemma 3.3(iii) cannot hold. If Lemma 3.3(ii) holds, then Lemma 5.11(ii) implies that $\pi(W) = \pi(S \cdot U^{[-1]})$ is a full G'-coset. However, since U is a nontrivial, product-one subsequence, Lemma 2.4 then implies that this full G'-coset must be G' itself, whence $S = (S \cdot U^{[-1]}) \cdot U$ is a nontrivial factorization of S, contradicting that $S \in \mathcal{A}(G)$ is an atom. Therefore, we see that Lemma 3.3(i) must hold, in which case $|R| = |W| - \sum_{i=1}^{r} |T_i| \ge 2q+1-(q-p)-q = p+1$ with $H := \langle \mathrm{supp}(R)\rangle < G$ proper. Hence, since all terms of W from G' were included in $W_0 \mid T_1$, it follows that $|H| = p$. But now we have $p+1$ terms from a group of order p, in which case Lemma 2.6.1 yields a nontrivial, product-one subsequence with all terms from H having length at most $p \le q-p$. Exchanging this product-one sequence for U, we can now assume that

$$|\langle \mathrm{supp}(U)\rangle| = p \qquad \text{and} \qquad |U| \le p \le q-p. \tag{81}$$

Let $W = S \cdot U^{[-1]}$, define $W_0 \mid W$ and W^* as before, and once more apply Lemma 3.3 to W^* taking H trivial, $\omega = q+1$, $\omega_H = -1$, and $\omega_0 = |W_0| \le \frac{q-1}{2}$. Let $W'^* = T_1^* \cdot \ldots \cdot T_r^* \cdot R^*$ be the resulting factorization with all notation as given by Lemma 3.3. Repeating the above arguments using the new U, we again find that Lemma 3.3(i) holds with

$$|R| \ge |S| - |U| - \omega + 1 \ge 2q+1-p-q = q-p+1 \ge p+1$$

and $H' = \langle \mathrm{supp}(R)\rangle < G$ an order p subgroup. If $H' = H = \langle \mathrm{supp}(U)\rangle$, then all terms from $R \cdot U$ will be from the same order p subgroup. However, since $|R \cdot U| \ge |S| - \omega + 1 \ge 2q+1-q = q+1$, this would contradict Lemma 5.12. Therefore, we must have $H' \neq H$. Applying Lemma 2.6.1 to R, we can find another nontrivial, product-one subsequence U' satisfying (81) with $\langle \mathrm{supp}(U')\rangle = H'$.

Let $V = W \cdot U'^{-1} \cdot U$. Trading W for $V = W \cdot U'^{-1} \cdot U$ amounts to swapping the product-one sequences U' and U. Since $|R| \ge p+1$ with all terms from H', we see that $R \cdot U'^{[-1]} \cdot U$ contains terms from both H and H'. Since no term of S is equal to 1, this means that that there is a pair of non-commuting terms

$g_0, h_0 \in \mathrm{supp}(R \cdot U'^{[-1]} \cdot U)$. Consequently, if $\sum_{i=1}^{r} |T_i| \ge q-1$, then Lemma 5.11(i) and the Cauchy-Davenport Theorem together imply that $|\pi(T_1)\ldots\pi(T_r)\pi(g_0 \cdot h_0)| \ge q$, in which case $\pi(S \cdot U'^{[-1]})$ is a full G'-coset. But then, as before, since U' is a product-one subsequence, Lemma 2.4 ensures that this G'-coset is G' itself, so that $S = (S \cdot U'^{[-1]}) \cdot U'$ is a nontrivial factorization of S, contradicting that $S \in \mathcal{A}(G)$ is an atom. Therefore, we must have $\sum_{i=1}^{r} |T_i| \le q-2$.

Let $V_0 = T_1 \cdot \ldots \cdot T_r$ and let V^* be an ordering of $V = W \cdot U'^{-1} \cdot U$ with $[V^*(1, |V_0|)] = V_0$. In view of Lemma 5.11 and $|V_0| = \sum_{i=1}^{r} |T_i| \le q-2$, we have $|\pi(V_0)| \ge |V_0|$. Thus we can once more apply Lemma 3.3 to V^* taking taking H trivial, $\omega = q+1$, $\omega_H = -1$, and $\omega_0 = |V_0| \le q-2$. Let $V'^* = T_1' \cdot \ldots \cdot T_{r'}' \cdot R'$ be the resulting factorization. Since $V_0 \mid T_1'$ with $V_0 = T_1 \cdot \ldots \cdot T_r$, it follows that $R' \mid R \cdot U'^{[-1]} \cdot U$. Now $\mathrm{supp}(R \cdot U'^{[-1]} \cdot U) \subseteq H \cup H'$ with $\mathsf{v}_H(R \cdot U'^{[-1]} \cdot U) = \mathsf{v}_H(U) = |U| \le p$. Consequently, at most p terms of R' are from H with all other terms from H'. However, as argued above, Lemma 3.3(i) must hold with all of the at least $p+1$ terms of R' from the same order p subgroup. Since there are only at most p terms of R' from H, this order p subgroup cannot be H, and thus all terms of R' are from H' (in view of $\mathrm{supp}(R') \subseteq H \cup H'$). But now $\mathrm{supp}(R' \cdot U') \subseteq H'$ with $|R' \cdot U'| = |S| - \sum_{i=1}^{r'} |T_i'| \ge |S| - \omega + 1 \ge 2q+1-q = q+1$ (with the first inequality from Lemma 3.3(i) and the second by hypothesis), which is contrary to Lemma 5.12. This completes Case 1.

Case 2: $1 \notin \Pi_{\le q-p}(S)$.

If there were p terms of S from the same order p subgroup, then we could apply Lemma 2.6.1 to find a nontrivial, product-one subsequence with length at most $p \le q-p$, which is contrary to case hypothesis. Therefore

$$\mathsf{v}_H(S) \le p-1 \quad \text{for every } \ H \le G \ \text{ with } \ |H| = p. \tag{82}$$

From Lemma 5.8, we can find a nontrivial, product-one subsequence $U \mid S$ with $|U| \le q$. In view of $|S| - |U| \ge 2q+1-q = q+1 \ge \frac{q-3}{2} + p$, (80) and (82), we can find two non-commuting terms $g_0, h_0 \in \mathrm{supp}(S \cdot U^{[-1]}) \cap G \setminus G'$. Since any 2 non-commuting terms generate G, we have

$$\langle g_0, h_0 \rangle = G \quad \text{with} \quad g_0, h_0 \in G \setminus G'. \tag{83}$$

Let $W = (U \cdot g_0 \cdot h_0)^{[-1]} \cdot S$.

If $\mathsf{v}_{G'}(W) = 0$, then set W_0 to be the trivial sequence. Otherwise, in view of $|W| = |S| - |U| - 2 \ge 2q+1-q-2 = q-1$ and (80), we can find a subsequence $W_0 \mid W$ containing all terms from G' and exactly 1 term from $G \setminus G'$. In view of (80) and Lemma 5.3, we have $|\pi(W_0)| \ge |W_0|$; moreover, if W_0 is nontrivial, then $|\pi(W_0)| \ge |W_0| \ge 2$, which together with $\mathsf{Z}(G) = \{1\}$ ensures that $\pi(W_0) \cap \Big(G \setminus \mathsf{Z}(G)\Big) \ne \emptyset$. Thus, letting $W^* \in \mathcal{F}^*(G)$ be any ordering of W such that $[W^*(1, |W_0|)] = W_0$, we can apply Lemma 3.3 to W^* taking H trivial, $\omega = q-p+1$, $\omega_H = -1$, and $\omega_0 = |W_0| \le \frac{q-1}{2} \le q-p+1$. Let $W'^* = T_1^* \cdot \ldots \cdot T_r^* \cdot R^*$ be the resulting factorization with all notation as given by Lemma 3.3. Since ω_H is negative, Lemma 3.3(iii) cannot hold. This gives two subcases based on whether (i) or (ii) from Lemma 3.3 holds.

Case 2.1: Lemma 3.3(ii) holds.

In this case, we have $q-p+1=\omega \le \sum_{i=1}^{r}|T_i| \le \omega+1=q-p+2 \le q-1$. Thus Lemma 5.11 implies that

$$|\pi(T_1)\ldots\pi(T_r)| \ge \sum_{i=1}^{r}|T_i| = q-p+1+\epsilon, \tag{84}$$

where $\epsilon \in \{0,1\}$. In view of (83), we have $\langle \mathrm{supp}(R\cdot g_0\cdot h_0)\rangle = G$. Since $|W|+2=|S|-|U| \ge q+1$, we have $|R|+2 \ge q+1-\sum_{i=1}^{r}|T_i| = p-\epsilon$. Consequently, Lemma 5.5 implies that $|\pi(R\cdot g_0\cdot h_0)| \ge p-\epsilon$. But now the Cauchy-Davenport Theorem together with (84) implies that

$$\begin{aligned}\Big|\Big(\pi(T_1)\ldots\pi(T_r)\Big)\Big(\pi(R\cdot g_0\cdot h_0)\Big)\Big| &\ge \min\{q,\, |\pi(T_1)\ldots\pi(T_r)|+|\pi(R\cdot g_0\cdot h_0)|-1\}\\ &\ge \min\{q,\, (q-p+1+\epsilon)+(p-\epsilon)-1\}=q.\end{aligned}$$

As a result, we see that $\pi(S\cdot U^{[-1]}) = \pi(T_1\cdot\ldots\cdot T_r\cdot R\cdot g_0\cdot h_0)$ is a full G'-coset. However, since U is a product-one subsequence, Lemma 2.4 ensures that this G'-coset is G' itself, whence $S=(S\cdot U^{[-1]})\cdot U$ is a nontrivial factorization of S, contradicting that $S\in\mathcal{A}(G)$ is an atom.

Case 2.2: Lemma 3.3(i) holds.

In this case, we have $\sum_{i=1}^{r}|T_i| \le \omega-1=q-p$, so that

$$|R| \ge |S|-|U|-2-(q-p) \ge 2q+1-q-2-q+p=p-1, \tag{85}$$

with $H:=\langle \mathrm{supp}(R)\rangle < G$ proper. As all terms of W from G' were included in $W_0 \mid T_1$, it follows that H must have order p. Thus (82) ensures that $|R|=p-1$ with $g_0,\, h_0 \in G\setminus H$. Since $|R|=p-1$, all estimates used in (85) must be equalities. In particular, $\sum_{i=1}^{r}|T_i|=\omega-1=q-p$.

Let $g_0' \in \mathrm{supp}(R)$. Since $h_0\notin H$ but $g_0'\in H$, it follows that g_0' and h_0 are non-commuting terms from $G\setminus G'$. In particular, (83) holds with g_0' in place of g_0. Let $V=W\cdot {g'}_0^{[-1]}\cdot g_0$. Trading W for $V=W\cdot {g'}_0^{[-1]}\cdot g_0$ amounts to swapping the terms g_0 and ${g'}_0$. Since $\sum_{i=1}^{r}|T_i|=\omega-1=q-p\le q-1$, Lemma 5.11(i) implies that $|\pi(V_0)|\ge|V_0|$, where $V_0=T_1\cdot\ldots\cdot T_r$. Thus, letting V^* be any ordering of V such that $[V^*(1,|V_0|)]=V_0$, we can once more apply Lemma 3.3 to V^* taking taking H trivial, $\omega=q-p+1$, $\omega_H=-1$, and $\omega_0=|V_0|=q-p\le\omega-1$. Let $V'^*=T'^*_1\cdot\ldots\cdot T'^*_{r'}\cdot R'^*$ be the resulting factorization. As before, Lemma 3.3(iii) cannot hold, while if Lemma 3.3(ii) holds, then Case 2.1 completes the proof. Therefore, Lemma 3.3(i) must hold, in which case $\sum_{i=1}^{r'}|T_i'|\le\omega-1=q-p=|V_0|$. Since $V_0\mid T_1'$, this is only possible if $r'=1$ with $T_1'=V_0=T_1\cdot\ldots\cdot T_r$, in which case $R'=R\cdot {g'}_0^{[-1]}\cdot g_0$. However, since $R\cdot {g'}_0^{[-1]}\cdot g_0$ contains exactly $p-2>0$ terms from H along with the term $g_0\notin H$, it follows that $\langle\mathrm{supp}(R')\rangle=\langle\mathrm{supp}(R\cdot {g'}_0^{[-1]}\cdot g_0)\rangle=G$, which is contrary to Lemma 3.3(i). This completes the proof. □

6. The Near Dihedral Group

The goal of this section is to prove the following theorem, which will be needed for the proof of Theorem 7.2. The proof uses the same strategy as for Corollary 5.7, though more technical care must be taken. Note, since q is an odd prime possessing a square root of -1, that $q\equiv 1 \mod 4$.

Theorem 6.1. *Let q be an odd prime, let $r \in [1, q-1]$ be an integer such that $r^2 \equiv -1 \mod q$, and let*

$$G = \langle \alpha, \tau : \ \alpha^q = 1, \quad \tau^4 = 1, \quad \alpha\tau = \tau\alpha^r \rangle.$$

Then $\mathsf{d}(G) = q + 2$.

We begin first with the following analogue of Lemma 5.6.

Lemma 6.2. *Let q be an odd prime, let $r \in [1, q-1]$ be an integer such that $r^2 \equiv -1 \mod q$, let*

$$G = \langle \alpha, \tau : \ \alpha^q = 1, \quad \tau^4 = 1, \quad \alpha\tau = \tau\alpha^r \rangle,$$

and let $S \in \mathcal{F}(G)$ be a sequence such that $\phi_{G'}(S) \in \mathcal{A}(G/G')$, where $G' = \langle \alpha \rangle = [G, G] \le G$ is the commutator subgroup. Then either $1 \in \pi(S)$ or $|\pi(S)| \ge |S|$.

Proof. We begin by describing some routinely verified properties of the group G. First, we have

$$G' = \langle \alpha \rangle \quad \text{and} \quad \mathsf{Z}(G) = \{1\}.$$

Apart from the subgroup $G' \le G$, there are q subgroups $H_i = \langle \tau\alpha^i \rangle \le G$, for $i = 0, 1, \ldots, q-1$, of order 4, which have trivial intersection with each other as well as G'. Each contains a single element $\tau^2\alpha^{(r+1)i}$ of order 2, naturally generating an order 2 subgroup contained in H_i. Any of the order 2 elements along with G' generates the subgroup $K = \langle \alpha, \tau^2 \rangle$, which is dihedral of order $2q$. There are no other subgroups apart from $\{1\}$ and G. In particular, any two non-identity elements from distinct H_i generate either K (if both have order 2) or G (otherwise). With this information in hand, we can continue with the proof.

Since $\mathsf{D}(G/G') = \mathsf{D}(C_4) = 4$ (care of Lemma 2.6.1) and $\phi_{G'}(S) \in \mathcal{A}(G/G')$, we have $1 \le |S| \le 4$. If $|S| = 1$, then $|\pi(S)| \ge |S|$ is trivial. Therefore we may assume $\ell := |S| \ge 2$, in which case $\mathrm{supp}(S) \subseteq G \setminus G'$ follows from $\phi_{G'}(S) \in \mathcal{A}(G/G')$. Let $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$ with $g_i \in G \setminus G'$.

If $|S| = 2$, then $|\pi(S)| \ge 2 = |S|$ follows, as desired, unless both terms of S commute. However, the only way two terms from $G \setminus G'$ can commute with each other is if they are from the same order 4 subgroup H_j. However, since $H_j \cap G' = \{1\}$ for every $j \in [0, q-1]$, we see that $\pi(S) \subseteq G' \cap H_j = \{1\}$ then forces S to be a product-one sequence, as desired. Therefore we may assume $|S| \ge 3$.

Observing that any two order 2 elements have product one modulo G', we see that $|S| \ge 3$ together with $\phi_{G'}(S) \in \mathcal{A}(G/G')$ ensures that S contains at most one order 2 element. Thus w.l.o.g. we may assume $\mathrm{ord}(g_i) = 4$ for $i \in [2, \ell]$, while $\mathrm{ord}(g_1) = 2$ or 4. Let H_{j_i} be the order 4 subgroup containing g_i, for $i \in [1, \ell]$. If $\mathrm{supp}(S) \subseteq H_{j_1}$, then, since $\pi(S') \subseteq G'$ follows in view of $\phi_{G'}(S) \in \mathcal{A}(G/G')$ and $\pi(S)$ being contained in a G'-coset (as noted in Section 2), it follows that $\pi(S) \subseteq H_{j_1} \cap G' = \{1\}$, yielding the desired conclusion $1 \in \pi(S)$. Therefore we assume there is some g_i from a different order 4 subgroup $H_{j_i} \ne H_{j_1}$, say w.l.o.g. g_2. But then $g_1g_2 \ne g_2g_1$, so that $|\pi(g_1 \boldsymbol{\cdot} g_2)| = 2$.

Let us show that $|\pi(g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} g_3)| \ge 3$. Let $X = \pi(g_1 \boldsymbol{\cdot} g_2)$. Note that $g_3X \cup Xg_3 \subseteq \pi(g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} g_3)$. If $g_3X \ne Xg_3$, then $|\pi(g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} g_3)| \ge |X| + 1 = 3$ follows, as claimed. Otherwise, $g_3X = Xg_3$ implies $g_3^{-1}Xg_3 = X$, whence X is stable under conjugation by elements from the order 4 subgroup $H_{j_3} = \langle g_3 \rangle$. Thus $|X| \ge |x^{H_{j_3}}|$ for each $x \in X$. Since $\phi_{G'}(S) \in \mathcal{A}(G/G')$ is an atom with $G/G' \cong C_4$ abelian, we have $X \subseteq G \setminus G'$. By (2), we have $|x^{H_{j_3}}| = |H_{j_3}|/|\mathsf{C}_G(x) \cap H_{j_3}|$. Now $\mathsf{C}_G(x)$, for $x \in G \setminus G'$, is simply equal to the order 4 subgroup that contains x. Since distinct order 4 groups intersect trivially, it follows that $|x^{H_{j_3}}| = 4$ (if $\mathsf{C}_G(x) \ne H_{j_3}$) or $|x^{H_{j_3}}| = 1$ (if $\mathsf{C}_G(x) = H_{j_3}$). If $|x^{H_{j_3}}| = 4$, then $|\pi(S)| \ge |\pi(X)| \ge 4 \ge |S|$, as desired. Therefore we may assume $|x^{H_{j_3}}| = 1$ for every $x \in X$, which is only possible if $X \subseteq H_{j_3}$.

As noted in Section 2, we also have $\pi(g_1 \cdot g_2) = X$ contained in a G'-coset. Hence, since $X \subseteq H_{j_3}$ and $|H_{j_3} \cap G'| = 1$, it follows that $|X| \le 1$, which is contrary to what has already been shown. Thus $|\pi(g_1 \cdot g_2 \cdot g_3)| \ge 3$, as claimed.

If $|S| = 3$, the proof is complete. If $|S| = 4$, repeating the above arguments using $Y = \pi(g_1 \cdot g_2 \cdot g_3)$ and g_4 in place of X and g_3 shows that $|\pi(S)| \ge 4$, completing the proof in the final remaining case. □

Proof of Theorem 6.1. The lower bound is easily verified by considering the sequence $\alpha^{[q-1]} \cdot \tau^{[3]} \in \mathcal{F}(G)$. It remains to prove $\mathsf{d}(G) \le q + 2$. Let $S \in \mathcal{F}(G)$ be a sequence with $|S| \ge q + 3$. We need to show $1 \in \Pi(S)$. Since $\mathsf{d}(G/G') + 1 = \mathsf{D}(G/G') = \mathsf{D}(C_4) = 4$ (care of Lemma 2.6), repeated application of the definition of $\mathsf{d}(G/G')$ to $\phi_{G'}(S)$ yields a factorization $S = T_1 \cdot \ldots \cdot T_\ell \cdot R$, where $\phi_{G'}(T_i) \in \mathcal{A}(G/G')$ for $i \in [1, \ell]$ and $|R| \le 3$. Since $\phi_{G'}(T_i) \in \mathcal{A}(G/G')$, it follows that

$$\pi(T_i) \subseteq G' \quad \text{for all } i \in [1, \ell]. \tag{86}$$

We may assume $1 \notin \pi(T_i)$ for $i \in [1, \ell]$, else the proof is complete. But then Lemma 6.2 implies that

$$|\{1\} \cup \pi(T_i)| \ge |T_i| + 1 \quad \text{for } i \in [1, \ell].$$

Thus, since $G' \cong C_q$ is cyclic of prime order, repeated application of the Cauchy-Davenport Theorem yields

$$\Big|\pi(T_\ell) \prod_{i=1}^{\ell-1} (\{1\} \cup \pi(T_i))\Big| \ge \min\{q, \sum_{i=1}^{\ell} |T_i|\} = \min\{q, |S| - |R|\} = q = |G'|,$$

where the penultimate equality follows in view of $|R| \le 3$ and $|S| \ge q + 3$. Thus, together with (86), we see that $1 \in G' = \Pi(T_1 \cdot \ldots \cdot T_\ell) \cap G' \subseteq \Pi(S) \cap G' \subseteq \Pi(S)$, as desired. □

7. General Upper Bounds

The goal of this section is to give two general upper bounds for the large Davenport constant of a non-cyclic group. We begin with the first one.

Theorem 7.1. *Let G be a finite, non-cyclic group and let p be the smallest prime divisor of $|G|$. Then*

$$\mathsf{D}(G) \le \frac{2}{p}|G|.$$

Proof. In view of Theorem 2.11, we see that it suffices to prove $\mathsf{D}(H) \le \frac{2}{p}|H|$ for any nontrivial subgroup $H \le G$. If G is abelian, then since G is non-cyclic, there must be a subgroup $H \le G$ with $H \cong C_q^2$ for some prime $q \ge p$. However, (6) gives $\mathsf{D}(H) = \mathsf{D}(C_q^2) = 2q - 1 = \frac{2q-1}{q^2}|H| < \frac{2}{p}|H|$, as desired. Therefore we may assume G is non-abelian, in which case G contains a minimal non-abelian subgroup. Thus it suffices to prove the theorem for all finite minimal non-abelian groups, so we now assume G is a minimal non-abelian group (all proper subgroups are abelian).

If G is a p-group, then Theorem 4.1 gives $\mathsf{D}(G) \le \frac{p^2+2p-2}{p^3}|G| \le \frac{2}{p}|G|$, also as desired. Therefore, we may assume G is a minimal non-abelian group which is not a p–group. The finite minimal non-abelian subgroups were classified by Miller and Moreno [10]. When such a group is not a p–group, its commutator subgroup G' is an elementary abelian group of prime power order. Thus $G' \cong C_q^r$ for some prime q and $r \ge 1$. However, if $r \ge 2$, then G contains a subgroup $H \cong C_q^2$, and the desired bound $\mathsf{D}(H) = \mathsf{D}(C_q^2) = 2q - 1 \le \frac{2}{p}|H|$ follows as before. Therefore we may assume G' is cyclic of prime order q. But then the classification result of Miller and Moreno tells us that $|G| = p^n q$ for some $n \ge 1$ with

$p \mid q-1$. Moreover, there is exactly one such non-abelian group of order $p^n q$ (up to isomorphism), which is given by the presentation

$$G = \langle \alpha, \tau : \ \alpha^q = 1, \quad \tau^{p^n} = 1, \quad \alpha\tau = \tau\alpha^r \rangle,$$

where $r^p \equiv 1 \mod q$ but $r \not\equiv 1 \mod q$. It is now routine to calculate

$$\mathsf{Z}(G) = \langle \tau^p \rangle \quad \text{and} \quad G' = \langle \alpha \rangle.$$

In particular, $G' \cap \mathsf{Z}(G) = \{1\}$. Moreover, $G/\mathsf{Z}(G)$ is a non-abelian group of order pq. Thus Theorem 2.12, Theorem 5.1 and Lemma 2.6.1 yield

$$\mathsf{D}(G) \le \mathsf{D}(G/\mathsf{Z}(G))\mathsf{D}(\mathsf{Z}(G)) \le \frac{2}{p}|G/\mathsf{Z}(G)||\mathsf{Z}(G)| = \frac{2}{p}|G|,$$

completing the proof. □

We conclude with the following result, which improves Theorem 7.1 for even order groups.

Theorem 7.2. *Let G be a finite group which is neither cyclic nor isomorphic to a dihedral group of order $2n$ with n odd. Then*

$$\mathsf{D}(G) \le \frac{3}{4}|G|$$

Proof. If $|G|$ is odd, then Theorem 7.1 gives $\mathsf{D}(G) \le \frac{2}{p}|G| \le \frac{2}{3}|G| < \frac{3}{4}|G|$, as desired. Therefore we may assume $|G|$ is even. As in the proof of Theorem 7.1, it suffices to prove $\mathsf{D}(H) \le \frac{3}{4}|H|$ for any subgroup $H \le G$. If G is abelian, then, since G is not cyclic, there must be a subgroup $H \cong C_q^2$ for some prime $q \ge 2$, whence $\mathsf{D}(H) = \mathsf{D}(C_q^2) = 2q-1 \le \frac{3}{4}|H|$ follows from (6). Therefore, we may assume G is non-abelian. If G contains a non-cyclic Sylow subgroup $H \le G$, then applying Theorem 4.3 gives $\mathsf{D}(H) \le \frac{3}{4}|G|$, as desired. Therefore we may assume all Sylow subgroups are cyclic. It is well-known (see [14, Theorem 10.1.10]) that a finite group G having all its Sylow subgroups cyclic must have a presentation of the form

$$G = \langle \alpha, \tau : \ \alpha^n = 1, \quad \tau^m = 1, \quad \alpha\tau = \tau\alpha^r \rangle, \tag{87}$$

where $\gcd(r-1, n) = \gcd(m, n) = 1$, $r^m \equiv 1 \mod n$, and n is odd. As $|G| = mn$ is even, we have m even.

It is routine to calculate

$$G' = \langle \alpha \rangle.$$

Consequently, $|G'| = \frac{1}{m}|G|$, so that if $m \ge 8$, then Theorem 3.1 and Theorem 2.10 give the desired bound. Therefore, recalling that m is even, we find that $m \in \{2, 4, 6\}$. If $m = 2$, then G has a cyclic, index 2 subgroup, in which case [5, Theorem 1.1, Section 5] gives the desired bound. It remains to consider $m \in \{4, 6\}$.

If $m = 6$, then $H = \langle \alpha, \tau^2 \rangle$ is a subgroup of odd order $3n$. If it is cyclic, then H is a cyclic, index 2 subgroup, which is a case that has already been handled. On the other hand, if it is non-cyclic, then applying Theorem 7.1 to H yields the desired bound. Therefore it remains to consider the case $m = 4$.

Let $q \mid n$ be a prime and observe that $H = \langle \alpha^{n/q}, \tau \rangle \le G$ is a non-abelian subgroup of order $mq = 4q$ having a presentation of the form (87) with $n = q$. Since H is neither cyclic nor dihedral of order $2n'$ with n' odd, we see that it suffices to show the theorem holds for H. Thus we may w.l.o.g. $H = G$ with $n = q$ prime in (87).

Since G is non-abelian and $r^m = r^4 \equiv 1 \mod q$, we see that the multiplicative order of r modulo q is either 2 or 4. If it is 2, then $r^2 \equiv 1 \mod q$, in which case $\langle \tau^2 \alpha \rangle$ is a cyclic, index 2 subgroup, which is a case that has already been handled. Thus it remains to consider the case when $r^2 \not\equiv 1 \mod q$ but $r^4 \equiv 1 \mod q$, which is easily seen to imply, as q is prime and $r^4 - 1 = (r^2 - 1)(r^2 + 1)$, that

$$r^2 \equiv -1 \mod q.$$

But now Theorems 6.1 and 3.1 yield the desired bound $\mathsf{D}(G) \le \mathsf{d}(G) + 2|G'| - 2 = q + 2 + 2q - 2 = \frac{3}{4}|G|$, completing the proof. □

References

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

[2] Y. Berkovich and Z. Janko, *Groups of Prime Power Order, Vol. 3*, Expositions in Mathematics 56, Walter de Gruyter GmbH & Co., Germany (2011).

[3] A. Bialostocki, P. Dierker, D. Grynkiewicz, and M. Lotspeich, *On some developments of the Erdős-Ginzburg-Ziv Theorem II*, Acta Arith. **110** (2003), 173 – 184.

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

[5] A. Geroldinger and D. J. Grynkiewicz, The Large Davenport Constant I: Groups with a Cyclcic, Index 2 Subgroup, *J. Pure and Appl. Alg.*, to appear.

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

[7] D.J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics, Springer, to appear.

[8] G.A. Jones, Jinho Kwak, and Mingyao Xu, *Finite Group Theory for Combinatorists*, Chapman & Hall/CRC, to appear.

[9] M. Mastnak, and H. Radjavi, Structure of finite, minimal nonabelian groups and triangularization, *Linear Algebra Appl.*, 430 (2009), no. 7, 1838-1848.

[10] G. A. Miller and H. C. Moreno, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.*, 4 (1903), no. 4, 398-404.

[11] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, Harrisonburg, VA (1996).

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

[13] 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.

[14] 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.

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

E-mail address: diambri@hotmail.com