ON PRODUCT-ONE SEQUENCES OVER DIHEDRAL GROUPS

ALFRED GEROLDINGER AND DAVID J. GRYNKIEWICZ AND JUN SEOK OH AND QINGHAI ZHONG

Abstract. Let G be a finite group. A sequence over G means a finite sequence of terms from G, where repetition is allowed and the order is disregarded. A product-one sequence is a sequence whose elements can be ordered such that their product equals the identity element of the group. The set of all product-one sequences over G (with concatenation of sequences as the operation) is a finitely generated C-monoid. Product-one sequences over dihedral groups have a variety of extremal properties. This article provides a detailed investigation, with methods from arithmetic combinatorics, of the arithmetic of the monoid of product-one sequences over dihedral groups.

1. Introduction

Let G be a finite group. A sequence over G means a finite sequence of terms from G, where repetition of terms is allowed and their order is disregarded. A sequence is called product-one free if no subproduct of terms (in any order) equals the identity of the group, and it is called a product-one sequence if its terms can be ordered such that their product equals the identity of G. The small Davenport constant $\mathsf d(G)$ is the maximal length of a product-one free sequence and the large Davenport constant $\mathsf D(G)$ is the maximal length of a minimal product-one sequence (a minimal product-one sequence is a product-one sequence that cannot be factorized, or say partitioned, into two nontrivial product-one sequences). The study of sequences, their sequence subproducts, and their structure under extremal properties is a classical topic in additive combinatorics.

If G is additively written and abelian, then we speak of zero-sum free sequences, zero-sum sequences, and of sequence subsums. Their study is a main objective of zero-sum theory, which has intimate connections to various areas of combinatorics, graph theory, finite geometry, factorization theory, and invariant theory. Although, for a long time, the focus of study was on the abelian setting, the study of combinatorial invariants in the general setting dates back at least to the 1970s when Olson gave an upper bound for $\mathsf d(G)$ ([35]). There are recent studies on (small and large) Davenport constants, on the Erdős-Ginzburg-Ziv constant $\mathsf s(G)$, and on the constant $\mathsf E(G)$, which asks for the smallest integer ℓ such that every sequence over G of length at least ℓ has a product-one subsequence of length $|G|$ (e.g., [3, 11, 28, 4, 29, 34, 33]). These investigations were pushed forward by new applications to invariant theory and to factorization theory. To begin with invariant theory, let $\boldsymbol\beta(G)$ denote the Noether number of G. If G is abelian, then B. Schmid [38] observed that $\mathsf d(G) + 1 = \boldsymbol\beta(G) = \mathsf D(G)$. If G has a cyclic subgroup of index two, then it was shown by Cziszter, Domokos, and by two of the present authors that $\mathsf d(G) + 1 \le \boldsymbol\beta(G) \le \mathsf D(G)$ ([12, 7]). For general groups the relationship between the Davenport constants and the Noether number is open, but in all cases studied so far we have $\mathsf d(G) + 1 \le \boldsymbol\beta(G)$ ([8, 9, 6]).

To discuss the connection with factorization theory, we first observe that the set $\mathcal B(G)$ of product-one sequences over G is a finitely generated (commutative and cancellative) monoid with concatenation of sequences as its operation. The atoms (i.e., the irreducible elements) of $\mathcal B(G)$ are precisely the minimal product-one sequences over G. First, let G be abelian and, for simplicity, suppose that $|G| \ge 3$. Then $\mathcal B(G)$ is a Krull monoid with class group (isomorphic to) G and every class contains precisely one prime

2010 *Mathematics Subject Classification.* 11B30, 11B50, 11B75, 20M13, 20M14.

Key words and phrases. product-one sequences, Davenport constant, finite groups, partition theorem, sets of lengths, sets of distances, sets of catenary degrees.

This work was supported by the Austrian Science Fund FWF, Projects W1230.

divisor. If H is any Krull monoid with class group G and prime divisors in each class, then there is a transfer homomorphism $\theta\colon H \to \mathcal{B}(G)$ implying that arithmetical invariants (such as sets of lengths, catenary degrees, and more) of H and of $\mathcal{B}(G)$ coincide. The arithmetic of $\mathcal{B}(G)$ is studied with methods of additive combinatorics and the long-term goal is to determine the precise value of arithmetical invariants in terms of the group invariants of G and/or in terms of classical combinatorial invariants such as the Davenport constant. We refer to [15] for the interplay of the arithmetic of Krull monoids and additive combinatorics, and to the survey [40] for a discussion of the state of the art.

Monoids of product-one sequences over finite groups are C-monoids. C-domains and C-monoids are submonoids of factorial monoids with finite class semigroup. They include Krull monoids with finite class group (and in that case the class semigroup coincides with the usual class group) but also classes of non-integrally closed noetherian domains (such as orders in number fields). The finiteness of the class semigroup yields abstract finiteness results for arithmetical invariants, but so far no combinatorial description of invariants in terms of the class semigroup are available (as is the case for Krull monoids) let alone any sort of precise results.

In the present paper, we study the arithmetic of the monoid of product-one sequences over dihedral groups G of order $2n$ for odd $n \ge 3$, and we obtain precise results. These dihedral groups were chosen because their arithmetic shows extremal behavior among all finite groups (see Proposition 2.3 and Theorem 6.7), such as cyclic groups and elementary 2-groups do among all finite abelian groups. We do not involve algebraic considerations (structural results on the class semigroup of monoids of product-one sequences were recently established in [31, Section 3]) but work with methods from additive combinatorics. We use substantially the recent characterization of minimal product-one sequences of maximal length (Proposition 2.4) and a recent refinement ([23]) of the Partition Theorem ([26, Chapters 14 and 15]). Let G be a dihedral group of order $2n$ for some odd $n \ge 3$. In the short Section 3, we do some necessary algebraic clarifications. Theorem 4.1 states that $\omega(G) = 2n$. Theorem 5.1 states that the set of distances $\Delta(G)$ is equal to $[1, 2n-2]$, and the set of catenary degrees $\mathsf{Ca}(G)$ equals $[2, 2n]$. Theorems 6.7 and 6.8 give detailed information on crucial subsets of $\Delta(G)$ which describe the structure of sets of lengths. Our results are strong enough to characterize $\mathcal{B}(G)$ arithmetically with respect to some other classes of monoids (Corollary 6.12).

2. Background on the arithmetic of monoids

Our notation and terminology are consistent with [13, 26]. We briefly gather some key notions and fix notation. We denote by $\mathbb{N}$ the set of positive integers. For rational numbers $a, b \in \mathbb{Q}$, $[a, b] = \{x \in \mathbb{Z}\colon a \le x \le b\}$ means the discrete interval between a and b. For an additive group G and subsets $A, B \subset G$, $A + B = \{a + b\colon a \in A, b \in B\}$ denotes their sumset. For $A \subseteq \mathbb{Z}$, the set of distances $\Delta(A)$ is the set of all $d \in \mathbb{N}$ for which there is $a \in A$ such that $A \cap [a, a + d] = \{a, a + d\}$. If $A \subset \mathbb{N}_0$, then $\rho(A) = \sup(A \cap \mathbb{N})/\min(A \cap \mathbb{N}) \in \mathbb{Q}_{\ge 1} \cup \{\infty\}$ denotes the elasticity of A with the convention that $\rho(A) = 1$ if $A \cap \mathbb{N} = \emptyset$.

2.1. **Monoids.** Throughout this paper, a *monoid* means a commutative, cancellative semigroup with identity. Let H be a monoid. Then $H^\times$ denotes the group of invertible elements, $\mathcal{A}(H)$ the set of atoms of H, $\mathsf{q}(H)$ the quotient group of H, and $H_{\rm red} = \{aH^\times\colon a \in H\}$ the associated reduced monoid of H. A submonoid $S \subset H$ is said to be *divisor-closed* if $a \in H, b \in S$ and $a \mid b$ implies that $a \in S$. For a subset $E \subset H$ we denote by

- $[E] \subset H$ the smallest submonoid of H containing E, and by
- $[\![E]\!] \subset H$ the smallest divisor-closed submonoid of H containing E.

Clearly, $[\![E]\!]$ is the set of all $a \in H$ dividing some element $b \in [E]$. If $E = \{a_1, \ldots, a_m\}$, then we write $[a_1, \ldots, a_m] = [E]$ and $[\![a_1, \ldots, a_m]\!] = [\![E]\!]$. We denote by

- $H' = \{x \in \mathsf{q}(H)\colon$ there is $N \in \mathbb{N}$ such that $x^n \in H$ for all $n \ge N\}$ the *seminormal closure* of H,
- $\widetilde{H} = \{x \in \mathsf{q}(H)\colon\ x^n \in H$ for some $n \in \mathbb{N}\}$ the *root closure* of H, and by

- $\widehat{H} = \{x \in \mathsf q(H)\colon \text{there is } c \in H \text{ such that } cx^n \in H \text{ for all } n \in \mathbb N\}$ the *complete integral closure* of H.

Then $H \subset H' \subset \widetilde{H} \subset \widehat{H} \subset \mathsf q(H)$, and H is called seminormal (root closed, resp. completely integrally closed) if $H = H'$ ($H = \widetilde{H}$, resp. $H = \widehat{H}$). For a set P, we denote by $\mathcal F(P)$ the free abelian monoid with basis P whose elements are written as

$$a = \prod_{p \in P} p^{\mathsf v_p(a)} \in \mathcal F(P)\,,$$

where $\mathsf v_p\colon H \to \mathbb N_0$ is the p-adic valuation of a. We call $|a| = \sum_{p \in P} \mathsf v_p(a) \in \mathbb N_0$ the *length* of a and $\mathrm{supp}(a) = \{p \in P\colon \mathsf v_p(a) > 0\} \subset P$ the *support* of a.

The monoid $\mathsf Z(H) = \mathcal F(\mathcal A(H_{\red}))$ is the factorization monoid of H and the unique epimorphism $\pi\colon \mathsf Z(H) \to H_{\red}$, satisfying $\pi(u) = u$ for all $u \in \mathcal A(H_{\red})$, denotes the factorization homomorphism. For $a \in H$, we denote by

- $\mathsf Z(a) = \pi^{-1}(aH^\times)$ the *set of factorizations* of a,
- $\mathsf L(a) = \{|z| \mid z : z \in \mathsf Z(a)\} \subset \mathbb N_0$ the *set of lengths* of a, and
- $\mathcal L(H) = \{\mathsf L(a)\colon a \in H\}$ the *system of sets of lengths of* H.

Note that $\mathsf L(a) = \{0\}$ if and only if $a \in H^\times$ and that $\mathsf L(a) = \{1\}$ if and only if $a \in \mathcal A(H)$. The monoid H is called *atomic* if $\mathsf Z(a) \ne \emptyset$ for all $a \in H$ (equivalently, if every $a \in H \setminus H^\times$ has a factorization into atoms), and H is called *half-factorial* if $|L(a)| = 1$ for all $a \in H$. We denote by

$$\Delta(H) = \bigcup_{L \in \mathcal L(H)} \Delta(L) \ \subset \mathbb N \tag{2.1}$$

the *set of distances* of H. If $\Delta(H) \ne \emptyset$, then

$$\min \Delta(H) = \gcd \Delta(H)\,. \tag{2.2}$$

For an atomic monoid H with $H \ne H^\times$ and every $k \in \mathbb N$, let

$$\mathcal U_k(H) = \bigcup_{k \in L \in \mathcal L(H)} L \quad \subset \mathbb N \tag{2.3}$$

denote the *union of sets of lengths* containing k. Then $\rho_k(H) = \sup \mathcal U_k(H)$ is the k-th *elasticity* of H and (see [13, Proposition 1.4.2])

$$\rho(H) = \sup\{\rho(L)\colon L \in \mathcal L(H)\} = \lim_{k \to \infty} \frac{\rho_k(H)}{k} \tag{2.4}$$

is the *elasticity* of H. We define a distance function $\mathsf d$ on $\mathsf Z(H)$. If $z, z' \in \mathsf Z(H)$, then z and z' can be written uniquely in the form

$$z = u_1 \cdot \ldots \cdot u_\ell v_1 \cdot \ldots \cdot v_m \quad \text{and} \quad z' = u_1 \cdot \ldots \cdot u_\ell w_1 \cdot \ldots \cdot w_n\,,$$

where $\ell, m, n \in \mathbb N_0$, all $u_i, v_j, w_k \in \mathcal A(H_{\red})$, and $\{v_1, \ldots, v_m\} \cap \{w_1, \ldots, w_n\} = \emptyset$, and we define $\mathsf d(z, z') = \max\{m, n\} \in \mathbb N_0$.

2.2. **Product-one sequences over finite groups.** Let G be a multiplicatively written finite group with identity $1_G \in G$ and let $G_0 \subset G$ be a subset. Then $\langle G_0 \rangle \subset G$ is the subgroup generated by G_0 and $G' = \langle g^{-1}h^{-1}gh\colon g, h \in G\rangle \subset G$ is commutator subgroup of G. If G is (additively written) abelian, then $\mathsf H(G_0) = \{g \in G\colon g + G_0 = G_0\}$ denotes the *stabilizer* of G_0. We say that a subset $A \subseteq G$ is H-periodic if $H \le \mathsf H(A)$, which is equivalent to A being a union of H-cosets, and that A is *aperiodic* if $\mathsf H(A)$ is trivial. We use $\phi_H : G \to G/H$ to denote the natural homomorphism. For every $n \in \mathbb N$, C_n denotes a cyclic group of order n and D_{2n} denotes a dihedral group of order $2n$.

Elements of $\mathcal F(G_0)$ are called *sequences* over G_0. Thus, in combinatorial language, a sequence means a finite sequence of terms from G_0 which is unordered with the repetition of terms allowed. In order to

distinguish between the group operation in G and the operation in $\mathcal{F}(G_0)$, we use the symbol $\boldsymbol{\cdot}$ for the multiplication in $\mathcal{F}(G_0)$ and we denote multiplication in G by juxtaposition of elements. Let

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell = \prod\nolimits^{\bullet}_{g \in G_0} g^{[\mathsf{v}_g(S)]}$$

be a sequence over G_0. Then

- $\mathsf{h}(S) = \max\{\mathsf{v}_g(S) \colon g \in G_0\}$ is the *maximum multiplicity* of a term of S,
- $\mathsf{k}(S) = \sum_{i=1}^{\ell} \frac{1}{\mathrm{ord}(g_i)} \in \mathbb{Q}$ is the *cross number* of S, and
- $\pi(S) = \{g_{\tau(1)} \ldots g_{\tau(\ell)} \in G \colon \tau \text{ is a permutation of } [1, \ell]\} \subset G$ is the *set of products* of S,

and it is readily seen that $\pi(S)$ is contained in a G'-coset. If $|S| = 0$, then we use the convention that $\pi(S) = \{1_G\}$. 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. For $n \in \mathbb{N}_0$, the *n-sums* and *n-products* of S are respectfully denoted by

$$\Sigma_n(S) = \{\sigma(T) \colon T \mid S \text{ and } |T| = n\} \subset G \quad \text{and} \quad \Pi_n(S) = \bigcup_{T \mid S, |T| = n} \pi(T) \subset G\,.$$

The *sequence subsums* and *sequence subproducts* of S are respectively denoted by

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

A 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 the multiplication by some $m \in \mathbb{N}$, then we set $mS = (mg_1) \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} (mg_\ell)$. Furthermore, we set $S^{-1} = g_1^{-1} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell^{-1}$. For a subset $X \subset G_0$, we let

$$S_X = \prod\nolimits^{\bullet}_{g \in X} g^{[\mathsf{v}_g(S)]}$$

denote the subsequence of S consisting of all terms from X. The sequence S is called

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

The set

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \colon 1_G \in \pi(S)\} \subset \mathcal{F}(G_0)$$

is a finitely generated submonoid of $\mathcal{F}(G_0)$, called the *monoid of product-one sequences* over G_0. For all arithmetical invariants $*(H)$ defined for a monoid H, we write $*(G_0)$ instead of $*(\mathcal{B}(G_0))$ (although being an abuse of notation this is a usual convention that will not lead to confusion). Similarly, we say that G_0 is (non-)half-factorial if $\mathcal{B}(G_0)$ is (non-)half-factorial. The atoms of $\mathcal{B}(G_0)$ are also called *minimal product-one sequences*. Since $\mathcal{B}(G_0)$ is finitely generated, $\mathcal{A}(G_0)$ is finite,

- $\mathsf{K}(G_0) = \max\{\mathsf{k}(S) \colon S \in \mathcal{A}(G_0)\} \in \mathbb{Q}_{\ge 0}$ is the *cross number* of G_0,
- $\mathsf{D}(G_0) = \max\{|S| \colon S \in \mathcal{A}(G_0)\} \in \mathbb{N}_0$ is the *large Davenport constant* of G_0, and
- $\mathsf{d}(G_0) = \max\{|S| \colon S \in \mathcal{F}(G_0) \text{ is product-one free}\} \in \mathbb{N}_0$ is the *small Davenport constant* of G_0.

It is easy to verify that

$$\mathsf{d}(G) + 1 \le \mathsf{D}(G) \le |G| \quad \text{and} \quad \mathsf{K}(G) \le \max\Big\{1, \frac{\mathsf{D}(G)}{2}\Big\}\,. \tag{2.5}$$

Let G be a finite group and $G_0 < G$ a proper subgroup. Then $\mathsf{d}(G_0) < \mathsf{d}(G)$ and $\mathsf{D}(G_0) \le \mathsf{D}(G)$. If G is abelian, then $\mathsf{D}(G_0) = 1 + \mathsf{d}(G_0) < 1 + \mathsf{d}(G) = \mathsf{D}(G)$. If G is not abelian, then we might have $\mathsf{D}(G_0) = \mathsf{D}(G)$, as it is outlined in the next example.

Example 2.1. We consider the semidirect product

$$G = C_5 \rtimes_2 C_4 = \langle a, b \colon a^5 = b^4 = 1, bab^{-1} = a^2 \rangle\,.$$

Thus G is a group with 20 elements and Table 1 in [9] shows that $\mathsf{D}(G) = 10$. Let $G_0 = \langle a, b^2 \rangle \subset G$. Then G_0 is a dihedral group with 10 elements, whence $\mathsf{D}(G_0) = 10 = \mathsf{D}(G)$.

Thus the example shows that the subgroup G_0 (with $G_0 < G$ proper and $\mathsf{D}(G_0) = \mathsf{D}(G)$) can be dihedral (for some consequences, see Proposition 2.3), but the next lemma shows that G_0 cannot be abelian.

Lemma 2.2. *Let G be a finite group and $G_0 < G$ a subgroup with $\mathsf{D}(G_0) = \mathsf{D}(G)$.*

1. *If $\mathsf{D}(G_0) = 1 + \mathsf{d}(G_0)$, then $G_0 = G$.*
2. *If G is nilpotent but not a 2-group, then G_0 is not generated by elements of order two.*

Proof. 1. Let $S \in \mathcal{F}(G_0)$ be product-one free with $|S| = \mathsf{d}(G_0)$. Assume to the contrary that there is an element $g \in G \setminus G_0$. Then $S \boldsymbol{\cdot} g$ is product-one free, whence

$$\mathsf{D}(G) = \mathsf{D}(G_0) = 1 + \mathsf{d}(G_0) < 1 + |S \boldsymbol{\cdot} g| \le 1 + \mathsf{d}(G) \le \mathsf{D}(G)\,,$$

a contradiction.

2. Let $G_1 \subset G$ be a subgroup that is generated by elements of order two. It suffices to show that $\mathsf{D}(G_1) < \mathsf{D}(G)$. Since finite nilpotent groups that are generated by elements of order p are p-groups ([30, Corollary 2.4]), it follows that G_1 is a 2-group, thus contained in the Sylow 2-group. As a finite nilpotent group is the direct product of its Sylow subgroups (which are each normal for nilpotent groups), there is a non-trivial group $G_2 < G$ (any nontrivial Sylow p-group with $p \ne 2$) such that $G_1 \times G_2$ is a subgroup of G, which implies that $\mathsf{D}(G_1) < \mathsf{D}(G_1 \times G_2) \le \mathsf{D}(G)$. □

Proposition 2.3. *Let G be a finite group with $|G| > 1$.*

1. $$\mathsf{D}(G) \begin{cases} = |G| & G \text{ is either cyclic or a dihedral group of order } 2n \text{ for some odd } n \ge 3\,, \\ \le \dfrac{3|G|}{4} & \text{otherwise}\,. \end{cases}$$
2. *Consider the following two conditions:*
   (a) *G is either an elementary 2-group or has a subgroup $G_0 < G$ which is a dihedral group of order $2n$ for some odd $n \ge 3$ with $\mathsf{D}(G_0) = \mathsf{D}(G)$.*
   (b) $\mathsf{K}(G) = \frac{\mathsf{D}(G)}{2}$.

   Then (a) implies (b). If G is nilpotent and (b) holds, then G is a 2-group, and it is an elementary 2-group in the abelian case.

Proof. 1. See [25, Theorem 7.2].

2. (a) ⇒ (b) If G is elementary 2-group, then by [13, Corollaries 5.1.9 and 5.1.13], we obtain that

$$\mathsf{K}(G) = \frac{1}{2} + \mathsf{k}(G) = \frac{1 + \mathsf{d}(G)}{2} = \frac{\mathsf{D}(G)}{2}\,.$$

Suppose that $G_0 = \langle \alpha, \tau \,|\, \alpha^n = \tau^2 = 1_G \text{ and } \tau\alpha = \alpha^{-1}\tau \rangle < G$ is a dihedral group of order $2n$ for some odd $n \ge 3$ with $\mathsf{D}(G_0) = \mathsf{D}(G)$. Then Equation (2.5) shows that $\mathsf{K}(G) \le \frac{\mathsf{D}(G)}{2}$. On the other hand, it is easy to verify (or use Proposition 2.4) that $S = (\alpha\tau)^{[n]} \boldsymbol{\cdot} \tau^{[n]}$ is a minimal product-one sequence with

$$|S| = 2n = \mathsf{D}(G_0) = \mathsf{D}(G) \quad \text{and} \quad \mathsf{k}(S) = \frac{2n}{2} = \frac{\mathsf{D}(G)}{2}\,.$$

Now suppose that G is nilpotent and (b) holds. Suppose that $\mathsf{K}(G) = \frac{\mathsf{D}(G)}{2}$ and note that $\mathsf{K}(G) \ge 1$ since $|G| > 1$. Then there exists $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{A}(G)$ such that $\mathsf{k}(S) = \frac{\mathsf{D}(G)}{2}$. Then $\mathrm{ord}(g_i) \ge 2$ for all $i \in [1, \ell]$, whence

$$\frac{\mathsf{D}(G)}{2} = \mathsf{k}(S) = \sum_{i=1}^{|S|} \frac{1}{\mathrm{ord}(g_i)} \le \frac{|S|}{2}\,.$$

Therefore $|S| = \mathsf D(G)$ and $\mathrm{ord}(g_i) = 2$ for all $i \in [1, \ell]$. Thus $G_0 = \langle g_1, \ldots, g_\ell \rangle$ is generated by elements of order two and $\mathsf D(G_0) = \mathsf D(G)$. If G_0 is abelian, then G_0 is an elementary 2-group and since $\mathsf D(G_0) = 1 + \mathsf d(G_0)$, Lemma 2.2.1 implies that $G = G_0$ is an elementary 2-group. If G is nilpotent, then Lemma 2.2.2 implies that G is a 2-group. □

The associated inverse problem with respect to the Davenport constant asks for the structure of minimal product-one sequences of length $\mathsf D(G)$. Even for abelian groups, the inverse problem is settled only for a small number of cases, namely for cyclic groups and elementary 2-groups (for them the problem has a trivial answer), for groups of rank two, and for groups of the form $C_2 \oplus C_2 \oplus C_{2n}$ ([39]). Dihedral and dicyclic groups are the only non-abelian groups for which a characterization of product-one sequences of length $\mathsf D(G)$ is available. We cite the result for dihedral groups of order $2n$, where $n \ge 3$ is odd (see [34, Theorem 4.1]).

Proposition 2.4. *Let G be a dihedral group of order $2n$, where $n \ge 3$ is odd. A sequence S over G of length $\mathsf D(G)$ is a minimal product-one sequence if and only if it has one of the following two forms*:

(a) *There exist $\alpha, \tau \in G$ such that $G = \langle \alpha, \tau \mid \alpha^n = \tau^2 = 1_G$ and $\tau\alpha = \alpha^{-1}\tau \rangle$ and $S = \alpha^{[2n-2]} \cdot \tau^{[2]}$.*

(b) *There exist $\alpha, \tau \in G$ and $i, j \in [0, n-1]$ with $\gcd(i-j, n) = 1$ such that $G = \langle \alpha, \tau \mid \alpha^n = \tau^2 = 1_G$ and $\tau\alpha = \alpha^{-1}\tau \rangle$ and $S = (\alpha^i\tau)^{[n]} \cdot (\alpha^j\tau)^{[n]}$.*

Finally, we will make ample use of Kneser's Theorem [26, Chapter 6].

Theorem 2.5 (Kneser's Theorem)**.** *Let G be an abelian group, let $A_1, \ldots, A_n \subseteq G$ be finite, nonempty subsets, and let $H = \mathsf H(\sum_{i=1}^n A_i)$. Then $|\sum_{i=1}^n A_i| \ge \sum_{i=1}^n |A_i + H| - (n-1)|H|$.*

3. Algebraic Properties

In this section, we study ideal theoretic properties of monoids of product-one sequences. Our references for ideal theory are [27, 13]. Let H be a monoid. We denote by $s\text{-spec}(H)$ the set of prime s-ideals of H and by $\mathfrak X(H) \subset s\text{-spec}(H)$ the set of minimal nonempty prime s-ideals of H. For a prime ideal $\mathfrak p \in s\text{-spec}(H)$, we denote by $H_{\mathfrak p} = (H \setminus \mathfrak p)^{-1}H \subset \mathsf q(H)$ the localization at $\mathfrak p$. The monoid H is said to be *weakly Krull* if

$$H = \bigcap_{\mathfrak p \in \mathfrak X(H)} H_{\mathfrak p} \quad \text{and} \quad \{\mathfrak p \in \mathfrak X(H) \colon a \in \mathfrak p\} \quad \text{is finite for all } a \in H\,.$$

The localizations $H_{\mathfrak p}$ are primary, and all primary monoids are weakly Krull. If all localizations $H_{\mathfrak p}$ are discrete valuation monoids, then H is a Krull monoid. A domain R is weakly Krull if and only if its multiplicative monoid $R^\bullet$ of nonzero elements is weakly Krull. Atomic domains having only finitely many non-associated atoms (i.e., $R^\bullet_{\mathrm{red}}$ is a finitely generated monoid) are called Cohen-Kaplansky domains ([2, Theorem 4.3]), and they are weakly Krull ([1, Corollary 5]). However, in contrast to the ring setting, finitely generated monoids are not weakly Krull in general. Root-closed finitely generated monoids are Krull and hence weakly Krull. In this section, we show that the monoid of product-one sequences over a finite group is weakly Krull if and only if the group is abelian (Theorem 3.3).

Proposition 3.1. *Let G be a finite group.*

1. $\mathfrak X\big(\mathcal B(G)\big) = \{\mathfrak p_g \colon g \in G\}$, *where $\mathfrak p_g = \{A \in \mathcal B(G) \colon \mathsf v_g(A) \ge 1\}$ for each $g \in G$.*
2. $$\widehat{\mathcal B(G)} = \{S \in \mathcal F(G) \colon \pi(S) \subset G'\} = \bigcap_{\mathfrak p \in \mathfrak X(\mathcal B(G))} \mathcal B(G)_{\mathfrak p}\,.$$

Proof. We set $H = \mathcal B(G)$, $F = \mathcal F(G)$, and $n = \mathrm{lcm}\{\mathrm{ord}(g) \mid g \in G\}$.

1. Let $g \in G$. Clearly, $\mathfrak p_g$ is a prime s-ideal of H. Since $g^{[\mathrm{ord}(g)]} \in \mathfrak p_g \setminus \mathfrak p_h$ for all $h \in G \setminus \{g\}$, it follows that $\mathfrak p_g \ne \mathfrak p_h$ and $\mathfrak p_g \subsetneq \mathfrak p_h$ for all $h \in G \setminus \{g\}$. Thus it remains to show the following claim.

A. Let $\mathfrak{p} \in s\text{-spec}(H)$. Then there is a $g \in G$ such that $\mathfrak{p}_g \subset \mathfrak{p}$.

Proof of **A**. Let $A = g_1 \cdot \ldots \cdot g_k \in \mathfrak{p}$. Then

$$A^{[n]} = \Big(g_1^{[\mathrm{ord}(g_1)]}\Big)^{[n/\,\mathrm{ord}(g_1)]} \cdot \ldots \cdot \Big(g_k^{[\mathrm{ord}(g_k)]}\Big)^{[n/\,\mathrm{ord}(g_k)]} \in \mathfrak{p}\,,$$

whence there is some $g \in \{g_1, \ldots, g_k\}$ such that $g^{[\mathrm{ord}(g)]} \in \mathfrak{p}$. We assert that $\mathfrak{p}_g \subset \mathfrak{p}$. Assume to the contrary that there is some $B \in \mathfrak{p}_g \setminus \mathfrak{p}$, say $B = g \cdot h_2 \cdot \ldots \cdot h_\ell$. Since $g^{[\mathrm{ord}(g)]} \in \mathfrak{p}$, it follows that

$$B^{[n]} = \Big(g^{[\mathrm{ord}(g)]}\Big)^{[n/\,\mathrm{ord}(g)]} \cdot \Big(h_2^{[\mathrm{ord}(h_2)]}\Big)^{[n/\,\mathrm{ord}(h_2)]} \cdot \ldots \cdot \Big(h_\ell^{[\mathrm{ord}(h_\ell)]}\Big)^{[n/\,\mathrm{ord}(h_\ell)]} \in \mathfrak{p}\,,$$

whence $B \in \mathfrak{p}$, a contradiction. □[**Proof of A.**]

2. We proceed in three steps.

(i) Let $a = \frac{s_1}{s_2} \in \widehat{H}$, where $s_1, s_2 \in H$. Then there exists $c \in H$ such that $ca^n \in H \subset F$ for all $n \in \mathbb{N}$. Since F is completely integrally closed, we have $a \in F$ and $\pi(a) \subset \{xy^{-1} \mid x \in \pi(s_1) \text{ and } y \in \pi(s_2)\} \subset G'$. Thus we have $\widehat{H} \subset \{a \in F \mid \pi(a) \subset G'\}$.

(ii) In order to prove that $\{a \in F \mid \pi(a) \subset G'\} \subset \bigcap_{\mathfrak{p} \in \mathfrak{X}(H)} H_\mathfrak{p}$ it suffices to verify that $f \in \bigcap_{\mathfrak{p} \in \mathfrak{X}(H)} H_\mathfrak{p}$ for every $f \in G'$. Since $G' = \langle ghg^{-1}h^{-1} \mid g, h \in G\rangle$, it is sufficient to show that $ghg^{-1}h^{-1} \in \bigcap_{\mathfrak{p} \in \mathfrak{X}(H)} H_\mathfrak{p}$ for all $g, h \in G$. Let $g, h \in G$ and $f = ghg^{-1}h^{-1}$. If $f = 1$, then $f \in \bigcap_{\mathfrak{p} \in \mathfrak{X}(H)} H_\mathfrak{p}$. Suppose $f \ne 1$. Since

$$f = \frac{f \cdot h^{[n]} \cdot g \cdot g^{-1}}{h^{[n]} \cdot g \cdot g^{-1}} = \frac{f \cdot h \cdot h^{-1} \cdot g^{[n]}}{h \cdot h^{-1} \cdot g^{[n]}} = \frac{f \cdot h \cdot h^{-1} \cdot (hg)^{[n]}}{h \cdot h^{-1} \cdot (hg)^{[n]}} = \frac{f \cdot g \cdot g^{-1} \cdot (hg)^{[n]}}{g \cdot g^{-1} \cdot (hg)^{[n]}} \in \mathfrak{q}(H)\,,$$

$$\text{and} \quad f \cdot h^{[n]} \cdot g \cdot g^{-1}, \quad f \cdot h \cdot h^{-1} \cdot g^{[n]}, \quad f \cdot h \cdot h^{-1} \cdot (hg)^{[n]}, \quad f \cdot g \cdot g^{-1} \cdot (hg)^{[n]} \in H\,,$$

we have $f \in H_{\mathfrak{p}_x}$ for all $x \in G \setminus \big(\{g, g^{-1}, h\} \cap \{h, h^{-1}, g\} \cap \{h, h^{-1}, hg\} \cap \{g, g^{-1}, hg\}\big) = G$. Thus the assertion follows from 1.

(iii) Let $a = \frac{s_1}{s_2} \in \bigcap_{\mathfrak{p} \in \mathfrak{X}(H)} H_\mathfrak{p}$, where $s_1, s_2 \in H$. Then for every $g \in G$, $a \in H_{\mathfrak{p}_g}$ implies that $\mathsf{v}_g(s_1) \ge \mathsf{v}_g(s_2)$. Therefore $s_2 \mid_F s_1$ and hence $a \in F$. By the definition of n, we know that $a^n \in H$. Let $c = s_2^n \in H$. Then, for every $k \in \mathbb{N}$ and every $r \in [0, n-1]$, we have $ca^{kn+r} = a^{kn} s_1^r s_2^{n-r} \in H$ whence $a \in \widehat{H}$. □

Lemma 3.2. *Let G be a finite group and $G_0 \subset G$ a subset. Consider the following conditions*:

(a) $1 + \mathsf{d}(G_0) < \mathsf{D}(G_0)$.

(b) *There exist distinct $U, V \in \mathcal{A}(G_0)$, $1 \ne W \in \mathcal{B}(G_0)$ and $m \in \mathbb{N}$ such that $\mathsf{Z}(V^{[m]})\mathsf{Z}(W) \subset \mathsf{Z}(U^{[m]})$.*

(c) *G is not abelian.*

Then (a) $\Rightarrow$ (b) $\Leftrightarrow$ (c).

Proof. (a) $\Rightarrow$ (b) Let $U = g_0 \cdot \ldots \cdot g_\ell \in \mathcal{A}(G_0)$ with $|U| = \mathsf{D}(G_0)$. Since $1 + \mathsf{d}(G_0) < \mathsf{D}(G_0) = 1 + \ell$, it follows that $g_1 \cdot \ldots \cdot g_\ell$ is not product-one free. Thus there is $V \in \mathcal{A}(G_0)$ such that $U = V \cdot S$ for some $1 \ne S \in \mathcal{F}(G_0)$. There is some $m \in \mathbb{N}_{\ge 2}$ such that $W = S^{[m]} \in \mathcal{B}(G_0)$, whence $U^{[m]} = V^{[m]} \cdot W$ and $\mathsf{Z}(V^{[m]})\mathsf{Z}(W) \subset \mathsf{Z}(U^{[m]})$.

(b) $\Rightarrow$ (c) Let $U, V \in \mathcal{A}(G_0)$ and $1 \ne W \in \mathcal{B}(G_0)$ with $U^{[m]} = V^{[m]} \cdot W$ and assume to the contrary that G is abelian. Then $(V^{[-1]} \cdot U)^{[m]} \in \mathcal{B}(G)$ and since $\mathcal{B}(G)$ is root-closed, it follows that $V^{[-1]} \cdot U \in \mathcal{B}(G)$ whence $V = U$, a contradiction to $W \ne 1$.

(c) $\Rightarrow$ (b) There exist $g, h \in G$ such that $gh \ne hg$. We consider the sequence

$$U = g \cdot h \cdot g^{-1} \cdot (gh^{-1}g^{-1}) \in \mathcal{A}(G)$$

and set $m = \mathrm{ord}(hgh^{-1}g^{-1}) \in \mathbb{N}$. Then $V = (g \cdot g^{-1}) \in \mathcal{A}(G)$, $W = (h \cdot (gh^{-1}g^{-1}))^{[m]} \in \mathcal{B}(G) \setminus \{1\}$, and

$$U^{[m]} = V^{[m]} \cdot W\,.$$

□

Theorem 3.3. *Let G be a finite group.*

1. *The following statements are equivalent:*
   (a) *G is abelian.*
   (b) *$\mathcal{B}(G)$ is Krull.*
   (c) *$\mathcal{B}(G)$ is transfer Krull.*
   (d) *$\mathcal{B}(G)$ is weakly Krull.*
   (e) *If $U, V \in \mathcal{A}(G)$, $W \in \mathcal{B}(G)$, and $m \in \mathbb{N}$ such that $\mathsf{Z}(V^{[m]})\mathsf{Z}(W) \subset \mathsf{Z}(U^{[m]})$, then $U = V$ and $W = 1$.*
2. *$\mathcal{B}(G)$ is seminormal if and only if $|G'| \le 2$. In particular, a dihedral group of order $2n$, where $n \ge 3$ is odd, is not seminormal.*

Proof. 1. (a) $\Rightarrow$ (b) $\Rightarrow$ (c) This is obvious.

(c) $\Rightarrow$ (a) See [31, Proposition 3.4].

(d) $\Leftrightarrow$ (b) Every Krull monoid is weakly Krull. If $\mathcal{B}(G)$ is weakly Krull, then Proposition 3.1 implies that

$$\mathcal{B}(G) = \bigcap_{\mathfrak{p} \in \mathfrak{X}\left(\mathcal{B}(G)\right)} \mathcal{B}(G)_{\mathfrak{p}} = \widehat{\mathcal{B}(G)}\,,$$

whence $\mathcal{B}(G)$ is completely integrally closed and so $\mathcal{B}(G)$ is Krull.

(e) $\Leftrightarrow$ (a) This follows from Lemma 3.2 (with $G_0 = G$).

2. See [32, Corollary 3.12]. □

4. On the omega invariant

Let H be an atomic monoid. For an element $a \in H$, let $\omega(H, a)$ be the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

> If $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in H$ with $a \mid a_1 \cdot \ldots \cdot a_n$, then there exists a subset $\Omega \subset [1, n]$ such that $|\Omega| \le N$ and $a \mid \prod_{\nu \in \Omega} a_\nu$.

Furthermore, we set

$$\omega(H) = \sup\{\omega(H, a) \colon a \in \mathcal{A}(H)\}\,.$$

Thus $\omega(H, a) = 1$ if and only if $a \in H$ is a prime element, and for an atomic monoid H that is not a group we have $\omega(H) = 1$ if and only if H is factorial. If H satisfies the ascending chain condition on divisorial ideals or if H is strongly primary, then $\omega(H, a) < \infty$ for all $a \in H$. Furthermore, $\omega(H) < \infty$ if and only if H is globally tame ([14, Proposition 3.6]) whence $\omega(H) < \infty$ for all finitely generated monoids. If G is a finite group, then we set $\omega(G) := \omega(\mathcal{B}(G))$ and since $\mathcal{B}(G)$ is finitely generated, we have $\omega(G) < \infty$. If G is abelian with $|G| \ge 3$, then it is easy to see that $\omega(G) = \mathsf{D}(G)$. But so far the precise value of $\omega(G)$ has not been determined yet for any non-abelian group. We formulate the main result of this section.

Theorem 4.1. *Let G be a dihedral group of order $2n$, where $n \ge 3$ is odd. Then $\omega(G) = \mathsf{D}(G) = 2n$.*

The goal of this section is to prove Theorem 4.1. To do so, we make use of the following recent strengthenings of the Partition Theorem, formulated as Propositions 4.2 and 4.3, as well as a basic lemma from [23]. Their proofs are given in [23, Theorem 3.2, Theorem 3.3, Lemma 2.4] (for simplicity, we state here only the cyclic case in Proposition 4.2). A setpartition $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n$ is a sequence of finite and nonempty subsets $A_i \subseteq G$. Then $\mathsf{S}(\mathcal{A}) = \prod_{i \in [1,n]}^{\bullet} \prod_{g \in A}^{\bullet} g \in \mathcal{F}(G)$ is the corresponding sequence of terms from G partitioned by the sets A_i in $\mathcal{A}$. Clearly, $\sum_{i=1}^{n} A_i \subset \Sigma_n(S)$, where $S = \mathsf{S}(\mathcal{A})$.

Proposition 4.2. *Let G be a cyclic group, let $n \ge 1$, let $X \subset G$ be a finite, nonempty subset, let $L \le \mathsf{H}(X)$, let $S \in \mathcal{F}(G)$ be a sequence, and let $S' \mid S$ be a subsequence with $\mathsf{h}(\phi_L(S')) \le n \le |S'|$. Suppose $|S'| \le 2n$. Then there exists a setpartition $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n$ with $\mathsf{S}(\mathcal{A}) \mid S$, $|\mathsf{S}(\mathcal{A})| = |S'|$ and $|\phi_L(A_i)| = |A_i| \le 2$ for all i such that either*

1. $|X + \Sigma_n(S)| \ge |X + \sum_{i=1}^{n} A_i| \ge (|S'| - n)|L| + |X|$, *or*
2. *there is a subgroup* $K \le H = \mathsf{H}(X + \Sigma_n(S))$ *with* $L < K$ *proper and* $\alpha \in G$ *such that*
   (a) $X + \Sigma_n(S) = X + \sum_{i=1}^{n} A_i$,
   (b) $\operatorname{supp}(\mathsf{S}(\mathcal{A})^{[-1]} \cdot S) \subset \alpha + K = \bigcap_{i=1}^{n}(A_i + K)$ *and* $|A_i \setminus (\alpha + K)| \le 1$ *for all* i,
   (c) $|X + \Sigma_n(S)| \ge |X + H| + |S_{G\setminus(\alpha+H)}| \cdot |H|$ *and* $|X + \Sigma_n(S)| \ge |X + K| + |S_{G\setminus(\alpha+K)}| \cdot |K|$,
   (d) $L + \sum_{i \in I_K} A_i = \alpha|I_K| + K$, *where* $I_K \subset [1, n]$ *is the nonempty subset of all* $i \in [1, n]$ *with* $A_i \subset \alpha + K$.

Proposition 4.3. *Let* G *be an abelian group, let* $n \ge 1$, *and let* $S \in \mathcal{F}(G)$ *be a sequence with* $|S| > n$. *Suppose* $|\Sigma_n(S)| \le m + 1$, *where* $m = \min\{n, |S| - n, |S| - \mathsf{h}(S)\}$. *Then one of the following holds, with Items 1–4 only possible if* $|\Sigma_n(S)| = m + 1$ *or* $|\operatorname{supp}(S)| = 1$.

1. $n = 2$, $|S| = |\operatorname{supp}(S)|$, *and* $\operatorname{supp}(S) = x + K$ *for some* $K \le G$ *and* $x \in G$ *with* $K \cong (\mathbb{Z}/2\mathbb{Z})^2$.
2. $m = 2$ *and* $\operatorname{supp}(S) = x + K$ *for some* $K \le G$ *and* $x \in G$ *with* $K \cong \mathbb{Z}/3\mathbb{Z}$.
3. $|\operatorname{supp}(S)| \le 2$.
4. $\operatorname{supp}(S) \subset \{x - d, x, x + d\}$ *for some* x, $d \in G$ *with* $\mathsf{v}_x(S) = \mathsf{h}(S) \ge |S| - m$.
5. *There exists* $x \in G$ *and a setpartition* $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n$ *with* $\mathsf{S}(\mathcal{A}) \mid S$, $|\mathsf{S}(\mathcal{A})| = n+m$, $\sum_{i=1}^{n} A_i = \Sigma_n(S)$, $\operatorname{supp}(\mathsf{S}(\mathcal{A})^{[-1]} \cdot S) \subset x + H$, $|A_i| \le 2$ *and* $(x + H) \cap A_i \ne \emptyset$ *for all* $i \in [1, n]$, *and* $|\sum_{i=1}^{n} A_i| = |\sum_{\substack{i=1 \\ i \ne j}}^{n} A_i|$ *for some* $j \in [1, n]$, *where* $H = \mathsf{H}(\Sigma_n(S))$ *is nontrivial.*

Lemma 4.4. *Let* G *be an abelian group, let* $n \ge 0$, *let* $X \subset G$ *be a finite, nonempty subset, let* $S \in \mathcal{F}(G)$ *be a sequence, let* $H \le G$, *and let* $x \in G$. *Suppose* $\mathcal{A} = A_1 \cdot \ldots \cdot A_n$ *is a setpartition with* $\mathsf{S}(\mathcal{A}) \mid S$, $\operatorname{supp}(\mathsf{S}(\mathcal{A})^{[-1]} \cdot S) \subset x + H \subset \bigcap_{i=1}^{n}(A_i + H)$, $|A_i \setminus (x + H)| \le 1$ *for all* i, *and* $H \le \mathsf{H}(X + \sum_{i=1}^{n} A_i)$. *Then* $X + \Sigma_\ell(S) = X + \sum_{i=1}^{n} A_i + (\ell - n)x$ *for any* $\ell \in [n, n + |\mathsf{S}(\mathcal{A})^{[-1]} \cdot S|]$.

Let G be a dihedral group of order $2n$ with $n \ge 3$, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$. Then $\langle \alpha \rangle$ is a cyclic subgroup of index 2. The commutator subgroup $G' = \langle \alpha^2 \rangle$ is a cyclic group of order n (when n is odd) or order $\frac{n}{2}$ (when n is even). Let $S \in \mathcal{F}(G)$ be a sequence of terms from G. We have a natural partition $S = S_{\langle\alpha\rangle} \cdot S_{\tau\langle\alpha\rangle}$, where $S_{\langle\alpha\rangle}$ consists of all terms $\alpha^x \in \langle \alpha \rangle$ and $S_{\tau\langle\alpha\rangle}$ consists of all terms $\tau\alpha^y \in \tau\langle\alpha\rangle$, where x, $y \in \mathbb{Z}$. For $x \in \mathbb{Z}/n\mathbb{Z}$, let α^x be α^{x_0}, where x_0 is any integer representative for x modulo n. The additive cyclic group $\mathbb{Z}/n\mathbb{Z}$ and the multiplicative cyclic group $\langle \alpha \rangle$ can be identified via the isomorphism $\cdot^* : \mathbb{Z}/n\mathbb{Z} \to \langle \alpha \rangle$ defined by $x^* = \alpha^x$. The inverse isomorphism $\cdot^+ : \langle \alpha \rangle \to \mathbb{Z}/n\mathbb{Z}$ is defined by $(\alpha^x)^+ = x \mod n$. The notation is chosen so that x^* lives in the multiplicative cyclic group $\langle \alpha \rangle$, while g^+ lies in the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$. We extend the definition of $\cdot^+$ to all of G by setting $(\tau\alpha^y)^+ = y \mod n$. The definitions of $\cdot^*$ and $\cdot^+$ depend on the fixed generating set $\{\alpha, \tau\}$ for G, with the map $\cdot^*$ only depending on α. If we exchange $\{\alpha, \tau\}$ for an alternative generating set, then the definitions of $\cdot^*$ and $\cdot^+$ are implicitly altered as well. The maps $\cdot^*$ and $\cdot^+$ are extended to sequences/sets in the usual fashion of applying the corresponding map to each term/element. The effect of replacing the generator τ by $\tau\alpha^y$ is to translate all terms of $(\tau\langle\alpha\rangle)^+$ by $-y$. To avoid confusion, when dealing with the dihedral group G, all subgroups of $\mathbb{Z}/n\mathbb{Z}$ will be notated in the form K^+ for the appropriate isomorphic subgroup $K \le \langle \alpha \rangle$. This will allow immediate visual recognition of whether a subgroup lies in the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$ or in the multiplicative cyclic group $\langle \alpha \rangle$, and provides a strong visual connection between the linked subgroups K and K^+. Additionally, the map $\cdot^+$ provides a one-to-one correspondence between the subgroups $H \le G$ with $H \not\le \langle \alpha \rangle$ and all subgroup-coset pairs $(K^+, y + K^+)$, where $K^+ \le \mathbb{Z}/n\mathbb{Z}$ and

$y \in \mathbb{Z}/n\mathbb{Z}$, as follows. For a subgroup $K \le \langle \alpha \rangle$ and $y \in \mathbb{Z}/n\mathbb{Z}$, we let $K_y = \langle K, \tau\alpha^y \rangle$. Note every $H \le G$ with $H \not\le \langle \alpha \rangle$ has some $\tau\alpha^y \in H$, where $y \in \mathbb{Z}/n\mathbb{Z}$, and then $H = \langle H \cap \langle \alpha \rangle, \tau\alpha^y \rangle$, ensuring that $H = K_y$ with $K = H \cap \langle \alpha \rangle$. The subgroup $K = H \cap \langle \alpha \rangle = K_y \cap \langle \alpha \rangle$ is uniquely defined. Since all $\tau\alpha^z \in H$ with $z \in \mathbb{Z}/n\mathbb{Z}$ have $z \in y + (H \cap \langle \alpha \rangle)^+ = y + K^+$, the element $y \in \mathbb{Z}/n\mathbb{Z}$ is uniquely defined modulo K^+. Thus the map $H \mapsto ((H \cap \langle \alpha \rangle)^+, y + (H \cap \langle \alpha \rangle)^+)$ is well-defined, and clearly bijective as its inverse is the map $(K^+, y + K^+) \mapsto K_y$. In light of this, we will often denote subgroups of G not contained in $\langle \alpha \rangle$ in the form K_y for some $K \le \langle \alpha \rangle$ and $y \in \mathbb{Z}/n\mathbb{Z}$. Moreover, when this is the case, we note that

$$K_y^+ = K^+ \cup (K_y \setminus K)^+ = K^+ \cup (y + K^+)$$

with $K_y' = K_y \cap \langle \alpha \rangle = K$ (if n is odd), and $K_y' = K^2 = (2K^+)^*$ (if n is even). When $y = 0$ (equivalently, if we choose our generating set to be $\{\alpha, \tau\alpha^y\}$), then

$$K_0 \setminus K = \tau K \qquad \text{and} \qquad K_0^+ = K^+.$$

To help lighten the notation, we also use $\phi_K : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})/K^+$ to denote the natural homomorphism modulo K^+.

The following proposition shows how the computation of $\pi(S)$ reduces to an additive question in $\mathbb{Z}/n\mathbb{Z}$ combining $\pm$ weighted subsums alongside ordinary $\lfloor \ell/2 \rfloor$-term subsums.

Proposition 4.5. *Let G be a dihedral group of order $2n$ where $n \ge 3$, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$, and let $S \in \mathcal{F}(G)$ with $S_{\langle \alpha \rangle} = \alpha^{x_1} \cdot \ldots \cdot \alpha^{x_s}$, where $x_1, \ldots, x_s \in \mathbb{Z}/n\mathbb{Z}$.*

1. *If $S \in \mathcal{F}(\langle \alpha \rangle)$, then $\pi(S) = \{\sigma(S^+)^*\}$.*
2. *If $S \notin \mathcal{F}(\langle \alpha \rangle)$, then*

$$\pi(S) = \tau^\ell \Big(\{x_1, -x_1\} + \ldots + \{x_s, -x_s\} + (-1)^\ell \Sigma_{\lfloor \ell/2 \rfloor}(2S^+_{\tau\langle \alpha \rangle}) - (-1)^\ell \sigma(S^+_{\tau\langle \alpha \rangle}) \Big)^*,$$

where $\ell = |S_{\tau\langle \alpha \rangle}| \ge 1$.

Proof. Item 1 is clear as $\langle \alpha \rangle$ is abelian. For Item 2, consider an arbitrary ordered product of all $s+\ell$ terms of S, say $g_1 \cdot \ldots \cdot g_{s+\ell} \in \pi(S)$. By the defining relations for the dihedral group, we have $g_1 \cdot \ldots \cdot g_{s+\ell} = \tau^\ell(\pm g_1^+ \pm \ldots \pm g_{s+\ell}^+)^*$, where the sign of each g_i depends upon the number of terms from $S_{\tau\langle \alpha \rangle}$ contained in $g_1 \cdot \ldots \cdot g_i$: if the number of terms from $\tau\langle \alpha \rangle$ contained in $g_1 \cdot \ldots \cdot g_i$ is congruent to ℓ modulo 2, then it is positive, while if it congruent to $\ell + 1$, then it is negative. Since $\ell \ge 1$ (in view of the hypothesis $S \notin \mathcal{F}(\langle \alpha \rangle)$), each term α^{x_j} from $S_{\langle \alpha \rangle}$ can be placed either in an even or odd slot relative to the fixed ordering of the sequence $S_{\tau\langle \alpha \rangle}$ in the product, the even slots being those places $i \in [1, s+\ell]$ where there are an even number of terms from $\tau\langle \alpha \rangle$ contain in $g_1 \cdot \ldots \cdot g_i$, and the odd slots $i \in [1, s+\ell]$ being those for which the number of such terms is odd. The effect of moving α^{x_j} between an even and odd slot is to simply change its sign in the sum. There must be exactly $\lceil \ell/2 \rceil$ terms from $S_{\tau\langle \alpha \rangle}$ placed in odd slots, and exactly $\lfloor \ell/2 \rfloor$ placed in even slots. Thus the elements of $\pi(S)$ are those from the sets

$$\tau^\ell \Big((-1)^\ell \big(\sigma(T^+_{even}) - \sigma(T^+_{odd}) \big) + \{x_1, -x_1\} + \ldots + \{x_s, -x_s\} \Big)^*$$

as we range over all partitions $S_{\tau\langle \alpha \rangle} = T_{odd} \cdot T_{even}$ with $|T_{even}| = \lfloor \ell/2 \rfloor$. Observing that $\sigma(T^+_{odd}) = \sigma(S^+_{\tau\langle \alpha \rangle}) - \sigma(T^+_{even})$, we find that the elements of $\pi(S)$ are those from the sets

$$\tau^\ell \Big((-1)^\ell \big(\sigma(2T^+_{even}) - \sigma(S^+_{\tau\langle \alpha \rangle}) \big) + \{x_1, -x_1\} + \ldots + \{x_s, -x_s\} \Big)^*$$

as we range over all subsequences $T^+_{even} \mid S^+_{\tau\langle \alpha \rangle}$ with $|T^+_{even}| = \lfloor \ell/2 \rfloor$, which yields the desired result. □

Corollary 4.6. *Let G be a dihedral group of order $2n$ where $n \ge 3$, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$, and let $S \in \mathcal{F}(G)$ with $S_{\langle \alpha \rangle} = \alpha^{x_1} \cdot \ldots \cdot \alpha^{x_s}$, where $x_1, \ldots, x_s \in \mathbb{Z}/n\mathbb{Z}$. Suppose $S \notin \mathcal{F}(\langle \alpha \rangle)$. Then $S \in \mathcal{B}(G)$ if and only if $|S_{\tau\langle \alpha \rangle}| = 2\ell$ is even and*

$$0 \in \{x_1, -x_1\} + \ldots + \{x_s, -x_s\} + \Sigma_\ell(2S^+_{\tau\langle \alpha \rangle}) - \sigma(S^+_{\tau\langle \alpha \rangle}).$$

Proof. This follows immediately from Proposition 4.5. □

Lemma 4.7. *Let G be a dihedral group of order $2n$ where $n \ge 3$, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$. If $U \in \mathcal{A}(G)$ with $|U_{\tau\langle\alpha\rangle}| > 2$, then $\mathsf{h}(U_{\tau\langle\alpha\rangle}) \le \frac{1}{2}|U_{\tau\langle\alpha\rangle}|$.*

Proof. Since $U \in \mathcal{A}(G)$ is product-one and $|U_{\tau\langle\alpha\rangle}| > 2$, we have $|U_{\tau\langle\alpha\rangle}| = 2\ell$ even with $\ell \ge 2$. Assume by contradiction that $\mathsf{h}(U_{\tau\langle\alpha\rangle}) \ge \frac{1}{2}|U_{\tau\langle\alpha\rangle}| + 1 = \ell + 1$. By replacing the generator τ by an appropriate alternative generator $\tau\alpha^x$, we can w.l.o.g. assume that $\mathsf{v}_\tau(U) = \mathsf{h}(U_{\tau\langle\alpha\rangle}) \ge \ell + 1$. Then $\tau^{[2]} \mid U$ is a product-one subsequence. Since $|U| \ge |U_{\tau\langle\alpha\rangle}| = 2\ell \ge 4$, it follows that $V := U \cdot \tau^{[-2]}$ is a nontrivial sequence. Since $\mathsf{v}_\tau(U) \ge \ell+1 = \frac{1}{2}|U_{\tau\langle\alpha\rangle}|+1$, every ℓ-term subsequence of $2U^+_{\tau\langle\alpha\rangle}$ must contain at least one term equal to 0, and $\mathsf{v}_\tau(V) \ge \ell - 1$. It follows that $\Sigma_\ell(2U^+_{\tau\langle\alpha\rangle}) = \Sigma_{\ell-1}(2V^+_{\tau\langle\alpha\rangle})$ and $\sigma(U^+_{\tau\langle\alpha\rangle}) = \sigma(V^+_{\tau\langle\alpha\rangle})$. Thus $U \in \mathcal{A}(G)$ combined with Corollary 4.6 applied to U and V (possible as $U, V \notin \mathcal{F}(\langle\alpha\rangle)$ follows from $\ell \ge 2$) shows that $V \in \mathcal{B}(G)$, and now $U = (\tau^{[2]}) \cdot V$ is a factorization of U into two nontrivial product-one subsequences, contradicting that $U \in \mathcal{A}(G)$ is an atom. □

Lemma 4.8. *Let G be an abelian group, let $X, Y \subset G$ be finite subsets with $H = \mathsf{H}(X)$, $K = \mathsf{H}(Y)$ and $X + H = Y + H$. Then $K \le H$.*

Proof. We have $X+H+K = Y+H+K = Y+K+H = Y+H = X+H = X$. Thus $H+K \le \mathsf{H}(X) = H$, implying $K \le H$. □

Lemma 4.9. *Let G be a dihedral group of order $2n$ where $n \ge 3$, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$. If $H \le \langle\alpha\rangle$ is a subgroup and $U \in \mathcal{A}(G)$ with $|U| > 1$, then $|U_H| \le 2|H| - 2$.*

Proof. As $|U| > 1$, we see that U is not the atom consisting of a single term equal to 1, which ensures $1 \notin \mathrm{supp}(U)$. Thus the lemma holds for H trivial, and we may assume $|H| > 1$. If $U \in \mathcal{F}(\langle\alpha\rangle)$, then $\langle \mathrm{supp}(U)\rangle$ is abelian, whence $|U_H| \le \mathsf{D}(H) = |H| \le 2|H| - 2$, as desired. Therefore, we may assume $|U_{\tau\langle\alpha\rangle}| > 0$, allowing us to use Proposition 4.5.2. Then $|U_{\tau\langle\alpha\rangle}| \ge 2$ is even and there exists an ordering of the terms of U whose product is one, say w.l.o.g. (as $\tau\alpha^{z_i}\tau\alpha^{z_{i+1}} \in \langle\alpha\rangle$ commutes with all terms $g, h \in \langle\alpha\rangle$)

$$U = g_1 \cdot \ldots \cdot g_r \cdot \tau\alpha^{z_1} \cdot h_1 \cdot \ldots \cdot h_s \cdot \tau\alpha^{z_2} \cdot \ldots \cdot \tau\alpha^{z_\ell},$$

where $\ell = |U_{\tau\langle\alpha\rangle}|$ and $U_{\langle\alpha\rangle} = g_1 \cdot \ldots \cdot g_r \cdot h_1 \cdot \ldots \cdot h_s$ with $r, s \ge 0$. If $|U_H| \ge 2|H| - 1$, then the pigeonhole principle ensures either $g_1 \cdot \ldots \cdot g_r$ or $h_1 \cdot \ldots \cdot h_s$ contains at least $|H| = \mathsf{D}(H)$ terms from H. Thus, re-ordering the terms of $g_1 \cdot \ldots \cdot g_r$ or $h_1 \cdot \ldots \cdot h_s$ appropriately, we find a consecutive nontrivial product-one sequence in $g_1 \cdot \ldots \cdot g_r$ or $h_1 \cdot \ldots \cdot h_s$, forcing the complement of this sequence in U to also have product-one, which contradicts that U is an atom in view of $\ell = |U_{\tau\langle\alpha\rangle}| > 0$. Therefore $|U_H| \le 2|H| - 2$, as desired. □

Lemma 4.10. *Let G be an abelian group, let $S \in \mathcal{F}(G)$ be a sequence, let $X \subset G$ be a finite, nonempty set, let $H \le G$, and let $U \cdot V \mid S$. Suppose $\mathrm{supp}(S \cdot (U \cdot V)^{[-1]}) \subset H$, $|U_H| \ge |U|/2$, $|V_H| \ge |V|/2$, and $X + \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V)$ is H-periodic. Then*

$$X + \Sigma_{\lfloor |S'|/2 \rfloor}(S') = X + \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V) = X + (\Sigma(S) \cup \{0\})$$

for any subsequence $S' \mid S$ with $U \cdot V \mid S'$ and either $|U|$ even, $|V|$ even or $|U \cdot V| < |S'|$.

Proof. Let us begin by showing

$$X + \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V) = X + (\Sigma(S) \cup \{0\}). \tag{4.1}$$

The inclusion $X + \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V) \subset X + (\Sigma(S) \cup \{0\})$ is trivial in view of $U \cdot V \mid S$. Since $X + \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V)$ is H-periodic, it suffices to prove $\Sigma(S) \cup \{0\} \subset \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V)$ holds modulo H. Let $T \mid S$ be an arbitrary (possibly trivial) subsequence such that all terms of T are nonzero modulo H. In view of the hypotheses $\mathrm{supp}(S \cdot (U \cdot V)^{[-1]}) \subset H$, $|U_H| \ge |U|/2$, and $|V_H| \ge |V|/2$, we have $T = T_U \cdot T_V$ for some $T_U \mid U$ and $T_V \mid V$ with $|T_U| \le |U|/2$ and $|T_V| \le |V|/2$. Moreover,

$|U_H| \ge |U|/2$ and $|V_H| \ge |V|/2$ ensure there are at least $|U|/2$ terms in U which are zero modulo H, and at least $|V|/2$ terms in V which are zero modulo H. It follows that we can extend the sequence $T_U \mid U$ to a subsequence $T'_U \mid U$ of length $|T'_U| = \lfloor |U|/2 \rfloor$ by concatenating an additional $\lfloor |U|/2 \rfloor - |T_U|$ terms from $U \cdot T_U^{[-1]}$, each zero modulo H. Likewise, we can extend the sequence $T_V \mid V$ to a subsequence $T'_V \mid V$ of length $|T'_V| = \lfloor |V|/2 \rfloor$ by concatenating an additional $\lfloor |V|/2 \rfloor - |T_V|$ terms from V, each zero modulo H. Let $T' = T'_U \cdot T'_V$. As we have only extended the sequences by terms zero modulo H, it follows that $\sigma(T) \equiv \sigma(T') \mod H$. By construction, $\sigma(T') \in \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V)$. Consequently, since $T \mid S$ was an arbitrary subsequence of terms nonzero modulo H, we conclude that the inclusion $\Sigma(S) \cup \{0\} \subset \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V)$ holds modulo H, which establishes (4.1) as noted earlier.

For any subsequence $S' \mid S$, the inclusion $\Sigma_{\lfloor |S'|/2 \rfloor}(S') \subset \Sigma(S) \cup \{0\}$ holds trivially. For any subsequence $S' \mid S$ with $U \cdot V \mid S'$ and either $|U|$ even, $|V|$ even or $|U \cdot V| < |S'|$, we have $|S'| - |U| - |V| \ge \lfloor \frac{|S'|}{2} \rfloor - \lfloor \frac{|U|}{2} \rfloor - \lfloor \frac{|V|}{2} \rfloor \ge 0$, ensuring that the set $\Sigma_{\lfloor |S'|/2 \rfloor}(S')$ contains a translate of $\Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V)$. Hence (4.1) implies

$$X + \Sigma_{\lfloor |S'|/2 \rfloor}(S') = X + \Sigma_{\lfloor |U|/2 \rfloor}(U) + \Sigma_{\lfloor |V|/2 \rfloor}(V) = X + (\Sigma(S) \cup \{0\})$$

for any sequence $S' \mid S$ with $U \cdot V \mid S'$ and either $|U|$ even, $|V|$ even or $|U \cdot V| < |S'|$, completing the proof. □

Proposition 4.11. *Let G be a dihedral group of order $2n$ where $n \ge 3$, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$, and let $H_x = \langle H, \tau\alpha^x \rangle \le G$ be a subgroup with $H \le \langle \alpha \rangle$ and $x \in \mathbb{Z}/n\mathbb{Z}$.*

1. *Suppose $V \in \mathcal{F}(G)$ has a decomposition $V^+_{\tau\langle\alpha\rangle} = T_1 \cdot \ldots \cdot T_\ell$ such that $\ell \ge 1$, $|T_i| = 2$ for all i, $X + \sum_{i=1}^{\ell} A_i$ is H^+-periodic, and $A_i \cap (2x + H^+) \ne \emptyset$ for all i, where $A_i = \mathrm{supp}(2T_i)$ for all i, $2\ell = |V_{\tau\langle\alpha\rangle}|$, $V^+_{\langle\alpha\rangle} = x_1 \cdot \ldots \cdot x_s$ and $X = \{x_1, -x_1\} + \ldots + \{x_s, -x_s\}$. Then*

$$\pi(V)^+ = X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) - \sigma(V^+_{\tau\langle\alpha\rangle}) = X + \sum_{i=1}^{\ell} A_i - \sigma(V^+_{\tau\langle\alpha\rangle})$$

   is H^+-periodic and $|V_{H_x \setminus H}| \ge \frac{1}{2}|V_{\tau\langle\alpha\rangle}| = \ell$.
2. *Suppose $U, V \in \mathcal{F}(G)$ with $\pi(V)^+$ H^+-periodic, $|V_{H_x \setminus H}| \ge \frac{1}{2}|V_{\tau\langle\alpha\rangle}| > 0$ and $\mathrm{supp}(U) \subset H_x$. Then $\pi(U \cdot V)$ is a translate of $\pi(V)$. In particular, if U is product-one, then $\pi(U \cdot V) = \pi(V)$.*

Proof. 1. The hypotheses $|T_i| = 2$ and $A_i \cap (2x + H^+) \ne \emptyset$ for all i ensure $|V_{H_x \setminus H}| \ge \frac{1}{2}|V_{\tau\langle\alpha\rangle}|$. Applying Lemma 4.4 to the sub-sumset of $\sum_{i=1}^{\ell} A_i$ consisting of all cardinality two summands yields $X + \sum_{i=1}^{\ell} A_i = X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})$. Since $\ell \ge 1$, Item 1 now follows by Proposition 4.5.

2. By replacing the generating set $\{\alpha, \tau\}$ by $\{\alpha, \tau\alpha^x\}$, we can w.l.o.g. assume $x = 0$. We can also assume U is nontrivial, else the item holds trivially. Let $\ell = |V_{\tau\langle\alpha\rangle}|$. It follows in view of Proposition 4.5 and the hypothesis $\ell > 0$ that $\pi(V)^+ = (-1)^\ell \Big(X + \Sigma_{\lfloor \ell/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle}) - \sigma(V^+_{\tau\langle\alpha\rangle}) \Big)$, where $V^+_{\langle\alpha\rangle} = x_1 \cdot \ldots \cdot x_s$ and $X = \{x_1, -x_1\} + \ldots + \{x_s, -x_s\}$. Thus $X + \Sigma_{\lfloor \ell/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle})$ is H^+-periodic by hypothesis. Since $x = 0$, we have $|(2V^+_{\tau\langle\alpha\rangle})_{H^+}| = |V_{H_0 \setminus H}| \ge \frac{1}{2}|V_{\tau\langle\alpha\rangle}| = \frac{1}{2}\ell > 0$ by hypothesis. The hypothesis $\mathrm{supp}(U) \subset H_x = H_0$ ensures $\mathrm{supp}(U^+) \subset H^+$. Thus Lemma 4.10 (applied with V taken to be $2V^+_{\tau\langle\alpha\rangle}$, U taken to be the trivial sequence, and $S' = S = 2(U \cdot V)^+_{\tau\langle\alpha\rangle}$) yields

$$X + \Sigma_{\lfloor \ell/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle}) = X + \Sigma_{\lfloor \ell'/2 \rfloor}(2(U \cdot V)^+_{\tau\langle\alpha\rangle}), \tag{4.2}$$

where $\ell' = |(U \cdot V)_{\tau\langle\alpha\rangle}|$. Note the set in (4.2) is H^+-periodic by hypothesis. Let $U^+_{\langle\alpha\rangle} = y_1 \cdot \ldots \cdot y_r$ and $Y = \{y_1, -y_1\} + \ldots + \{y_r, -y_r\}$. Since $\mathrm{supp}(U^+) \subset H^+$, we have $Y \subset H^+$, whence it follows that $X + \Sigma_{\lfloor \ell'/2 \rfloor}(2(U \cdot V)^+_{\tau\langle\alpha\rangle}) = Y + X + \Sigma_{\lfloor \ell'/2 \rfloor}(2(U \cdot V)^+_{\tau\langle\alpha\rangle})$ as this set is H^+-periodic. As a result, in

view of (4.2), $\ell > 0$ and Proposition 4.5, it follows that $\pi(V)$ and $\pi(U \cdot V)$ are translates of each other, as desired. □

Lemma 4.12. *Let G be a dihedral group of order $2n$ where $n \ge 3$ is odd, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$, and let $U \in \mathcal{F}(G)$. Let $K_y = \langle K, \tau\alpha^y \rangle \le G$ be a subgroup with $K \le \langle \alpha \rangle$, let $V \mid U$ be a subsequence, let $\ell_V = |V_{\tau\langle\alpha\rangle}|$, and let $Z = X_V + \Sigma_{\lfloor \ell_V/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle})$, where $V^+_{\langle\alpha\rangle} = x_1 \cdot \ldots \cdot x_s$ and $X_V = \{x_1, -x_1\} + \ldots + \{x_s, -x_s\}$. Suppose $|V_{K_y \setminus K}| \ge \frac{1}{2}|V_{\tau\langle\alpha\rangle}|$, Z is K^+-periodic,*

$$|(U \cdot V^{[-1]})_{K_y}| \ge |K| + 1 + |G'/K| - |\phi_K(Z)| \quad \text{and} \quad |(U \cdot V^{[-1]})_{K_y \setminus K}| \ge |G'/K| - |\phi_K(Z)|$$

with both above inequalities strict when $K = G'$. Then U is not an atom.

Proof. Let $\epsilon = 1$ if $K = G'$ and $\epsilon = 0$ otherwise. Assume by contradiction $U \in \mathcal{A}(G)$. By exchanging the generating τ for $\tau\alpha^y$, we can w.l.o.g. assume $y = 0$, so that $K_0 = \tau K \cup K$ and $K_0^+ = K^+$. Note $|\phi_K(Z)| \le |G'/K| - 1 + \epsilon$, so

$$\ell := |G'/K| - |\phi_K(Z)| + \epsilon > 0.$$

By hypothesis (note $\mathsf{d}(K_0) = |K|$ as K_0 is dihedral [12]),

$$|(U \cdot V^{[-1]})_{K_0}| \ge \mathsf{d}(K_0) + 1 + \ell \quad \text{and} \quad |(U \cdot V^{[-1]})_{\tau K}| \ge \ell > 0. \tag{4.3}$$

In particular, $U \notin \mathcal{F}(\langle\alpha\rangle)$, ensuring that U is not the atom consisting of a single term equal to 1, whence $1 \notin \mathrm{supp}(U)$. For a subsequence $T \mid U$, let

$$\ell_T = |T_{\tau\langle\alpha\rangle}| \quad \text{and} \quad X_T = \{x_1, -x_1\} + \ldots + \{x_t, -x_t\}, \quad \text{where } T^+_{\langle\alpha\rangle} = x_1 \cdot \ldots \cdot x_t,$$

and set $X_T = \{0\}$ if $T_{\langle\alpha\rangle}$ is the trivial sequence.

CASE 1. $|(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}| \le \ell$.

If $\ell_V = 0$ and $|(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}| = 0$, then $U \notin \mathcal{F}(\langle\alpha\rangle)$ ensures $|(U \cdot V^{[-1]})_{\tau K}| = |U_{\tau\langle\alpha\rangle}| \ge 2$ is even ($|U_{\tau\langle\alpha\rangle}|$ must be even as U is product-one). In this case, it follows in view of (4.3) that there exists a nontrivial product-one subsequence $W_0 \mid U \cdot V^{[-1]}$ with $|W_0| \le \mathsf{d}(K_0) + 1$ and $W_0 \in \mathcal{F}(K_0)$ such that W_0 does not contain all terms from τK. This ensures that $U \cdot (V \cdot W_0)^{[-1]}$ contains an even positive number of terms from τK (as $\ell_V = 0$ and U and W_0 are product-one), and we define $W \in \mathcal{F}(\tau K)$ to be any length two subsequence of $(U \cdot (V \cdot W_0)^{[-1]})_{\tau K}$. In all other cases, we let $W \in \mathcal{F}(\tau\langle\alpha\rangle)$ be a sequence of length $2|(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}|$ consisting of the terms from $(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}$ together with $|(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}| \le \ell \le |(U \cdot V^{[-1]})_{\tau K}|$ additional terms from $(U \cdot V^{[-1]})_{\tau K}$, which is possible in view of (4.3) and the case hypothesis. Since all terms from $(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}$ lie outside K_0, the first bound in (4.3) ensures there is a nontrivial product-one subsequence $W_0 \mid U \cdot (V \cdot W)^{[-1]}$ with $W_0 \in \mathcal{F}(K_0)$ and $|W_0| \le \mathsf{d}(K_0) + 1$. In both cases, $W \in \mathcal{F}(\tau\langle\alpha\rangle)$ is a sequence of even length $\ell_W \le 2\ell$ with $|W_{\tau K}| \ge \frac{1}{2}\ell_W$ and $V \cdot W \cdot W_0 \mid U$, where W_0 is a nontrivial product-one sequence. Moreover, $|(V \cdot W)_{\tau\langle\alpha\rangle}| \ge 1$ and $\mathrm{supp}\left((U \cdot (V \cdot W)^{[-1]})_{\tau\langle\alpha\rangle}\right) \subset \tau K$.

By hypothesis, $|V_{\tau K}| = |V_{K_0 \setminus K}| \ge \frac{1}{2}|V_{\tau\langle\alpha\rangle}| = \frac{1}{2}\ell_V$. We also have $|W_{\tau K}| \ge \frac{1}{2}\ell_W = \frac{1}{2}|W|$ and $\mathrm{supp}\left((U \cdot (V \cdot W)^{[-1]})_{\tau\langle\alpha\rangle}\right) \subset \tau K$ by definition of W, while $Z = X_V + \Sigma_{\lfloor \ell_V/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle})$ is K^+-periodic by hypothesis. Thus Lemma 4.10 (applied with U taken to be $2V^+_{\tau\langle\alpha\rangle}$, V taken to be $2W^+$, H taken to be K^+, S taken to be $2U^+_{\tau\langle\alpha\rangle}$, and X taken to be X_V) implies

$$X_V + \Sigma_{\lfloor \ell_V/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle}) + \Sigma_{\ell_W/2}(2W^+) = X_V + \Sigma_{\lfloor \ell_S/2 \rfloor}(2S^+) \tag{4.4}$$

for any sequence $S \mid U_{\tau\langle\alpha\rangle}$ with $V_{\tau\langle\alpha\rangle} \cdot W \mid S$, with this set being K^+-periodic by hypothesis. Since $X_V + X_{U \cdot (V \cdot W_0)^{[-1]}} = X_{U \cdot W_0^{[-1]}}$, we derive from (4.4) that

$$X_{U \cdot W_0^{[-1]}} + \Sigma_{\lfloor \ell_V/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle}) + \Sigma_{\ell_W/2}(2W^+) = X_{U \cdot W_0^{[-1]}} + \Sigma_{\lfloor \ell_S/2 \rfloor}(2S^+)$$

for any sequence $S \mid U_{\tau\langle\alpha\rangle}$ with $V_{\tau\langle\alpha\rangle} \cdot W \mid S$, with this set being K^+-periodic by hypothesis. Considering the cases $S = (U \cdot W_0^{[-1]})_{\tau\langle\alpha\rangle}$ and $S = U_{\tau\langle\alpha\rangle}$, we find

$$X_{U\cdot W_0^{[-1]}} + \Sigma_{\lfloor (\ell_{U\cdot W_0^{[-1]}})/2 \rfloor}(2(U \cdot W_0^{[-1]})^+_{\tau\langle\alpha\rangle}) = X_{U\cdot W_0^{[-1]}} + \Sigma_{\lfloor \ell_U/2 \rfloor}(2U^+_{\tau\langle\alpha\rangle}), \tag{4.5}$$

with this being a K^+-periodic set. By construction, the set X_{W_0} consists of a sumset of sets $\{x_i, -x_i\}$ with $x_i \in \mathrm{supp}(W_0^+) \subset K^+$. Thus, since the quantity in (4.5) is K^+-periodic, we obtain

$$X_{U\cdot W_0^{[-1]}} + \Sigma_{\lfloor \frac{1}{2}\ell_{U\cdot W_0^{[-1]}} \rfloor}(2(U \cdot W_0^{[-1]})^+_{\tau\langle\alpha\rangle}) = X_U + \Sigma_{\lfloor \ell_U/2 \rfloor}(2U^+_{\tau\langle\alpha\rangle}). \tag{4.6}$$

Since $V \cdot W \mid U \cdot W_0^{[-1]}$ and $|(V \cdot W)_{\tau\langle\alpha\rangle}| \ge 1$, (4.6) and Proposition 4.5 imply that $\pi(U)$ is a translate of the set $\pi(U \cdot W_0^{[-1]})$. However, since W_0 is product-one, this forces them to be equal, in which case $1 \in \pi(U) = \pi(U \cdot W_0^{[-1]})$. Thus the factorization $U = W_0 \cdot (U \cdot W_0^{[-1]})$ contradicts that U is an atom (as W_0 is nontrivial) unless $U = W_0$. However, $|W_0| \le \mathsf{d}(K_0) + 1$ by construction, while (4.3) ensures that $|U| \ge |U \cdot V^{[-1]}| \ge \mathsf{d}(K_0) + 1 + \ell > \mathsf{d}(K_0) + 1$, ensuring that $W_0 \ne U$, which completes CASE 1.

CASE 2. $|(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}| \ge \ell$.

Since $\ell > 0$, the case hypothesis ensures that $K < \langle\alpha\rangle = G'$ is a proper subgroup, forcing $\epsilon = 0$. Let $W \in \mathcal{F}(\tau\langle\alpha\rangle)$ be a sequence of length 2ℓ consisting of $\ell > 0$ terms from $(U \cdot V^{[-1]})_{\tau\langle\alpha\rangle\setminus\tau K}$ together with $\ell > 0$ terms from $(U \cdot V^{[-1]})_{\tau K}$, which exists in view of the case hypothesis and (4.3). Let

$$V' = V \cdot (U \cdot V^{[-1]})_{\langle\alpha\rangle\setminus K}.$$

Since $Z = X_V + \Sigma_{\lfloor \ell_V/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle})$ is K^+-periodic by hypothesis, it follows that

$$X := X_{V'} + \Sigma_{\lfloor \ell_V/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle})$$

is also K^+-periodic with $|X| \ge |Z|$.

Apply Proposition 4.2 to $X + \Sigma_\ell\Big(2(U \cdot V^{[-1]})^+_{\tau\langle\alpha\rangle}\Big)$ taking L to be K^+ and using $2W^+ \mid 2(U \cdot V^{[-1]})^+_{\tau\langle\alpha\rangle}$ (which has precisely ℓ terms equal to 0 modulo K^+, and ℓ terms which are non-zero modulo K^+). Let

$$H^+ = \mathsf{H}\Big(X + \Sigma_\ell(2(U \cdot V^{[-1]})^+_{\tau\langle\alpha\rangle})\Big).$$

Note $K^+ \le H^+$ follows as X is K^+-periodic. Since $|X| + \ell|K| \ge |Z| + (|G'/K| - |\phi_K(Z)|)|K| = |G'|$, Proposition 4.2 ensures that H/K is nontrivial (it it were trivial, then Proposition 4.2.1 must hold, in which case the previous calculation combined with the bound in Proposition 4.2.1 forces $H = G'$, in which case $H/K = G'/K$ is nontrivial as $K < G'$ is a proper subgroup). Regardless of whether Item 1 or 2 holds in Proposition 4.2, it follows that there is an H^+-coset that contains all but at most $\ell - 1$ of the terms of $2(U \cdot V^{[-1]})^+_{\tau\langle\alpha\rangle}$: in case Item 1 holds, then $H^+ = \mathbb{Z}/n\mathbb{Z}$, while if Item 2 holds, then this conclusion follows from Proposition 4.2.2(b)(d) with the desired coset equal to the coset $\alpha + H$ given by 2(b), which fully contains all elements from some A_i by 2(d). Since there are at least ℓ terms from $K^+ \le H^+$ lying in $2(U \cdot V^{[-1]})^+_{\tau\langle\alpha\rangle}$ by (4.3), this H^+-coset must equal the subgroup H^+. Thus Proposition 4.2 ensures that we can find a subsequence $W_1 \mid (U \cdot V^{[-1]})_{\tau\langle\alpha\rangle}$ with $|W_1| = |W| = 2\ell$, $\mathsf{h}\big(\phi_K(2W_1^+)\big) \le \ell$, $|(2W_1^+)_{H^+}| \ge \ell = \frac{1}{2}|W_1|$ and $\mathrm{supp}\left(2\Big(U_{\tau\langle\alpha\rangle} \cdot (V_{\tau\langle\alpha\rangle} \cdot W_1)^{[-1]}\Big)^+\right) \subset H^+$ such that

$$X + \Sigma_\ell\big(2(U \cdot V^{[-1]})^+_{\tau\langle\alpha\rangle}\big) = X + \Sigma_\ell(2W_1^+) = X_{V'} + \Sigma_{\lfloor \ell_V/2 \rfloor}(2V^+_{\tau\langle\alpha\rangle}) + \Sigma_\ell(2W_1^+)$$

is H^+-periodic. Since $\mathsf{h}\big(\phi_K(2W_1^+)\big) \le \ell$, it follows that at most ℓ terms of W_1 lie in K_0, while no terms in $V' \cdot V^{[-1]}$ lie in K_0 by its definition. Thus (4.3) ensures that $U \cdot (V' \cdot W_1)^{[-1]}$ contains at least $\mathsf{d}(K_0) + 1$ terms from K_0, meaning there exists a nontrivial product-one subsequence $W_0 \mid U \cdot (V' \cdot W_1)^{[-1]}$ with $|W_0| \le \mathsf{d}(K_0) + 1$ and $W_0 \in \mathcal{F}(K_0)$. By hypothesis, $|V_{\tau K}| = |V_{K_0\setminus K}| \ge \frac{1}{2}|V_{\tau\langle\alpha\rangle}|$, meaning at least half the terms of $2V^+_{\tau\langle\alpha\rangle}$ lie in $(\tau K)^+ = K^+ \le H^+$. As a result, we can apply Lemma 4.10 (taking U to be

$2V^+_{\tau\langle\alpha\rangle}$, taking V to be $2W_1^+$, taking H to be H^+, taking S to be $2U^+_{\tau\langle\alpha\rangle}$, taking X to be $X_{V'}$, and taking S' to be $2U^+_{\tau\langle\alpha\rangle}$ as well as $2(U\cdot W_0^{[-1]})^+_{\tau\langle\alpha\rangle}$) to conclude

$$X_{V'} + \Sigma_{\lfloor \frac{1}{2}\ell_{U\cdot W_0^{[-1]}}\rfloor}\big(2(U\cdot W_0^{[-1]})^+_{\tau\langle\alpha\rangle}\big) = X_{V'} + \Sigma_{\lfloor \ell_U/2\rfloor}(2U^+_{\tau\langle\alpha\rangle}) = X + \Sigma_\ell(2W_1^+) \tag{4.7}$$

is H^+-periodic. By definition of V', all $g \in \operatorname{supp}(U\cdot (V')^{[-1]}) \cap \langle\alpha\rangle$ lie in K, ensuring $g^+ \in K^+ \le H^+$. As a result, since the quantity in (4.7) is H^+-periodic, it follows that

$$X_{U\cdot W_0^{[-1]}} + \Sigma_{\lfloor \frac{1}{2}\ell_{U\cdot W_0^{[-1]}}\rfloor}\big(2(U\cdot W_0^{[-1]})_{\tau\langle\alpha\rangle}\big) = X_U + \Sigma_{\lfloor \ell_U/2\rfloor}(2U^+_{\tau\langle\alpha\rangle}),$$

whence $|\pi(U\cdot W_0^{[-1]})| = |\pi(U)|$ by Proposition 4.5, forcing $1 \in \pi(U) = \pi(U\cdot W_0^{[-1]})$ since both U and W_0 are product-one. It follows that $U = W_0\cdot(U\cdot W_0^{[-1]})$ is a factorization of U into product-one sequences, with W_0 nontrivial by definition. Since U is an atom, this forces $W_0 = U$. However, $|W_0| \le \mathsf{d}(K_0)+1$ by definition, while $|U| \ge |U\cdot V^{[-1]}| \ge \mathsf{d}(K_0)+1+\ell > \mathsf{d}(K_0)+1 \ge |W_0|$ by (4.3), whence $W_0 = U$ is impossible, completing the proof. □

Lemma 4.13. *Let G be an abelian group, let $A_1,\dots,A_\ell \subset G$ be cardinality two subsets, let $X = \sum_{i=1}^{\ell} A_i$, and let $H = \mathsf{H}(X)$. Let $I_H \subset [1,\ell]$ be all those $i \in [1,\ell]$ with $|\phi_H(A_i)| = 1$. Then there exists a subset $J \subset [1,\ell]$ with $|\sum_{i\in J} A_i| = |X|$, $J \setminus I_H = [1,\ell]\setminus I_H$, $|J\cap I_H| \le |H|-1$, $|J\setminus I_H| \le |\phi_H(X)|-1$ and $|J| \le |H| + |\phi_H(X)| - 2$.*

Proof. Note $\phi_H(A_i)$ has cardinality one or two depending on whether $i \in I_H$ or $i \in [1,\ell]\setminus I_H$. Thus Kneser's Theorem implies $|[1,\ell]\setminus I_H| \le |\phi_H(X)|-1$, while [24, Proposition 2.2] applied to $\sum_{i\in I_H} A_i$ ensures there is a subset $I'_H \subset I_H$ with $|\sum_{i\in I'_H} A_i| = |\sum_{i\in I_H} A_i|$ and $|I'_H| \le |\sum_{i\in I_H} A_i| - 1 \le |H|-1$. Setting $J = I'_H \cup ([1,\ell]\setminus I_H)$ now yields the desired index set. □

Proposition 4.14. *Let G be a dihedral group of order $2n$ where $n \ge 3$ is odd, say $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1,\ \tau\alpha = \alpha^{-1}\tau\rangle$. If $H_z = \langle H, \tau\alpha^z\rangle < G$ is a proper subgroup with $H \le \langle\alpha\rangle$, and $U \in \mathcal{A}(G)$, then $|U_{H_z}| \le n + |H| - 1$, with equality only possible if H is trivial.*

Proof. By replacing the generator τ by $\tau\alpha^z$, we can w.l.o.g. assume $z = 0$. Assume by contradiction $U \in \mathcal{A}(G)$ with

$$|U_{H_0}| = |U_H| + |U_{\tau H}| \ge n + |H| - 1 + \epsilon, \tag{4.8}$$

where $\epsilon = 1$ if H is trivial and otherwise $\epsilon = 0$. Since $H_0 < G$ is proper, it follows that $H < G'$ is proper. By (4.8), we have $|U| \ge n+1 \ge 4$, ensuring that the atom $U \in \mathcal{A}(G)$ does not consist of a single term equal to 1, forcing $1 \notin \operatorname{supp}(U)$. If $U \in \mathcal{F}(\langle\alpha\rangle)$, then $\langle\operatorname{supp}(U)\rangle$ is abelian and $U_{H_0} = U_H$. Thus $|U_{H_0}| = |U_H| \le \mathsf{D}(H) = |H|$, again contradicting (4.8). Therefore $|U_{\tau\langle\alpha\rangle}| > 0$.

Let $K \le \langle\alpha\rangle$ be arbitrary. Lemma 4.9 implies

$$|U_K| \le 2|K| - 2 \quad \text{for every } K \le \langle\alpha\rangle, \ \text{ and } \ \ell := |U_{\tau H}| \ge n - |H| + 1 + \epsilon \ge |G'/H| + 1 \ge 4, \tag{4.9}$$

with the latter inequality following from the former (taking $K = H$) combined with (4.8) (and recalling that $H < G'$ is proper). Since $n \ge 3$ is odd and $\frac{1}{2}|U_{\tau\langle\alpha\rangle}| \ge \frac{1}{2}\ell \ge 2$, Lemma 4.7 gives

$$\mathsf{h}(2U^+_{\tau\langle\alpha\rangle}) = \mathsf{h}(U_{\tau\langle\alpha\rangle}) \le \frac{1}{2}|U_{\tau\langle\alpha\rangle}| \le n, \tag{4.10}$$

with the latter inequality in view of $|U_{\tau\langle\alpha\rangle}| \le |U| \le \mathsf{D}(G) = 2n$. If H is trivial, then $H = \{1\}$ and $H_0 = \langle\tau\rangle = \{1,\tau\}$, so U_H is the trivial sequence (as $1 \notin \operatorname{supp}(U)$) and $\operatorname{supp}(U_{H_0}) = \{\tau\}$. In such case, (4.8) implies $\mathsf{v}_\tau(U) = |U_{H_0}| \ge n+1$, contradicting (4.10). Therefore we may now assume H is nontrivial, and thus $\epsilon = 0$.

For a subsequence $T \mid U$, let $\ell_T = |T_{\tau\langle\alpha\rangle}|$ and $X_T = \{y_1, -y_1\}+\ldots+\{y_t, -y_t\}$, where $T^+_{\langle\alpha\rangle} = y_1\cdot\ldots\cdot y_t$. Let $X = X_{U_H}$, $\ell = \ell_{U_{H_0}}$ and

$$L^+ = \mathsf{H}(X) \le H^+.$$

Since $\ell > 0$, Proposition 4.5.2 implies that $\pi(U_{H_0})^+$ is a translate of the set $X + \Sigma_{\lfloor \ell/2\rfloor}(2U^+_{\tau H})$. Let

$$m_X = \mathsf{h}\big(\phi_L(2U^+_{\tau H})\big) = \mathsf{h}\big(\phi_L(U^+_{\tau H})\big)$$

and let $U'_{\tau H} \mid U_{\tau H}$ be a maximal length subsequence with $\mathsf{h}\big(\phi_L(2(U'_{\tau H})^+)\big) \le \lceil \ell/2\rceil$. Note $\phi_L(X)$ is aperiodic as L^+ is the stabilizer of X. As a result, applying Kneser's Theorem to the aperiodic sumset $\phi_L(X)$, which is a sumset of $|U_{H\setminus L}|$ cardinality two sets and $|U_L|$ cardinality one sets, yields

$$|\phi_L(X)| \ge |U_{H\setminus L}| + 1. \tag{4.11}$$

Combining the above bound with (4.9), we obtain

$$|U_H| = |U_L| + |U_{H\setminus L}| \le 2|L| + |\phi_L(X)| - 3. \tag{4.12}$$

In view of (4.8), (4.12), $|\phi_L(X)| \le |H/L|$ (as $X \subset H^+$) and $H < G'$ proper, we have

$$\ell = |U_{\tau H}| = |U_{H_0}| - |U_H| \ge n + |H| + 2 - 2|L| - |\phi_L(X)| \ge n - |H| + 1 \ge 2|H| + 1. \tag{4.13}$$

Lemma 4.12 and the following claim will complete the proof by contradicting that U is an atom.

Claim A. There is a subgroup $K_y = \langle K, \tau\alpha^y\rangle \le H_0$ with $K \le \langle\alpha\rangle$ and a subsequence $V \mid U_{H_0}$ such that $|V_{K_y\setminus K}| \ge \frac{1}{2}|V_{\tau H}|$, Z is K^+-periodic, $|(U\cdot V^{[-1]})_{K_y}| \ge |K| + 1 + |G'/K| - |\phi_K(Z)|$ and $|(U\cdot V^{[-1]})_{K_y\setminus K}| \ge |G'/K| - |\phi_K(Z)|$, where $Z = X_V + \Sigma_{\lfloor \ell_V/2\rfloor}(2V^+_{\tau H})$.

CASE 1. $m_X \ge |U_{\tau H}| - |H/L| + 2$.

Let $y \in \mathrm{supp}(U^+_{\tau H})$ be an element which modulo L^+ has multiplicity m_X in $\phi_L(U^+_{\tau H})$, and set $L_y = \langle L, \tau\alpha^y\rangle$. Lemma 4.13 applied to the sumset X finds a subsequence $V \mid U_H$ with $V_{H\setminus L} = U_{H\setminus L}$, $|V_L| \le |L| - 1$, $|V| \le |L| + |\phi_L(X)| - 2$, and $X_V = X_{U_H} = X$. Note

$$\begin{aligned}
|(U\cdot V^{[-1]})_{L_y}| &\ge m_X + |U_L| - |V_L| \ge |U_{H_0}| - |U_{H\setminus L}| - |H/L| + 2 - |V_L| \\
&\ge |U_{H_0}| - |\phi_L(X)| - |L| - |H/L| + 4 \ge |U_{H_0}| - |\phi_L(X)| - |H| + 3 \\
&\ge n - |\phi_L(X)| + 2 \ge |L| + |G'/L| - |\phi_L(X)| + 1,
\end{aligned}$$

with the first inequality as $V \mid U_H$, with the second inequality by case hypothesis, the third in view of $|V_L| \le |L| - 1$ and (4.11), and the fifth in view of (4.8). The case hypothesis ensures there are at most $|H/L| - 2$ terms of $U_{\tau H}$ lying outside $L_y = \langle L, \tau\alpha^y\rangle$. Consequently, if $|(U\cdot V^{[-1]})_{L_y\setminus L}| = |U_{L_y\setminus L}| \le |G'/L| - 1 - |\phi_L(X)|$, then $|U_{\tau H}| \le (|G'/L| - 1 - |\phi_L(X)|) + (|H/L| - 2)$, which combined with (4.12) yields $|U_{H_0}| = |U_H| + |U_{\tau H}| \le 2|L| + \frac{n+|H|}{|L|} - 6 \le n + |H| - 4$, contrary to (4.8). Therefore $|(U\cdot V^{[-1]})_{L_y\setminus L}| = |U_{L_y\setminus L}| \ge |G'/L| - |\phi_L(X)|$, meaning Claim A holds with K_y taken to be L_y and Z taken to be X, contradicting that U is an atom.

CASE 2. $|X + \Sigma_{\lceil \ell/2\rceil}(2U^+_{\tau H})| \ge \min\{|H|, (|U'_{\tau H}| - \lceil \ell/2\rceil)|L| + |X|\}$ and $m_X \le |U_{\tau H}| - |H/L| + 1$.

Apply Proposition 4.2 to $X+\Sigma_{\lceil \ell/2\rceil}(2U^+_{\tau H})$ taking L to be L^+ and using $2(U'_{\tau H})^+ \mid 2U^+_{\tau H}$. First suppose that $|X + \Sigma_{\lceil \ell/2\rceil}(2U^+_{\tau H})| \ge (|U'_{\tau H}| - \lceil \ell/2\rceil)|L| + |X|$, so that Proposition 4.2.1 holds. Consequently, if $m_X = \mathsf{h}(2\phi_L(U^+_{\tau H})) \le \lceil \ell/2\rceil$, then $U'_{\tau H} = U_{\tau H}$, in which case Proposition 4.5 implies that $|\pi(U_{H_0})| \ge (|U_{\tau H}| - \lceil \frac{\ell}{2}\rceil)|L| + |X| = \lfloor \ell/2\rfloor\,|L| + |X| \ge \lfloor \ell/2\rfloor \ge |H|$, with the final inequality by (4.13). On the other hand, if $m_X = \mathsf{h}(2\phi_L(U^+_{\tau H})) > \lceil \ell/2\rceil$, then there is a unique term with multiplicity greater than $\lceil \ell/2\rceil$ in $\phi_L(2U^+_{\tau H})$, and Proposition 4.5 instead implies $|\pi(U_{H_0})| \ge (|U'_{\tau H}| - \lceil \frac{\ell}{2}\rceil)|L| + |X| \ge (|U'_{\tau H}| - \lceil \frac{\ell}{2}\rceil + 1)|L| = (|U_{\tau H}| - m_X + 1)|L| \ge |H|$, with the final inequality holding by the upper bound $m_X \le |U_{\tau H}| - |H/L| + 1$ in the hypothesis of CASE 2. In either case, we conclude that $|\pi(U_{H_0})| = |H|$ (note $|\pi(U_{H_0})| \le |H|$ holds trivially as $\mathrm{supp}(U^+_{H_0}) \subseteq H^+_0 = H$, ensuring the inequality in Proposition 4.2.1 must hold with equality), and so Proposition 4.2 ensures there is a setpartition of cardinality two sets realizing $X + \Sigma_{\lceil \ell/2\rceil}(2U^+_{\tau H})$

as a sumset. If instead $|X + \Sigma_{\lceil \ell/2 \rceil}(2U_{\tau H}^+)| < (|U'_{\tau H}| - \lceil \ell/2 \rceil)|L| + |X|$ and $|\pi(U_{H_0})| = |H|$, then Proposition 4.2.2 yields these same conclusions. Thus in both cases, Lemma 4.13 applied to the sumset $X = X_{U_H}$ and [24, Proposition 2.2] applied to $\phi_L(2U_{\tau H}^+)$ (via the setpartition realizing $X + \Sigma_{\lceil \ell/2 \rceil}(2U_{\tau H}^+)$ considered modulo L^+) give us a subsequence $V \mid U_{H_0}$ with $|V| = |V_H| + |V_{\tau H}| \le (|L| + |\phi_L(X)| - 2) + \max\{2,\, 2(|H/L| - |\phi_L(X)|)\} \le 2|H| - 2$ such that $|\pi(V)| = |\pi(U_{H_0})| = |H|$. Indeed, [24, Proposition 2.2] (which is simply the greedy algorithm) ensures we need keep at most one cardinality two set for each element of $\phi_L\big(X + \Sigma_{\lceil \ell/2 \rceil}(2U_{\tau H}^+)\big)$ in excess of the original $|\phi_L(X)|$ elements from $\phi_L(X)$, and thus $|V_{\tau H}| \le 2\Big(|\phi_L\big(X + \Sigma_{\lceil \ell/2 \rceil}(2U_{\tau H}^+)\big)| - |\phi_L(X)|\Big) \le 2(|H/L| - |\phi_L(X)|)$. However, in order to ensure $V_{\tau\langle\alpha\rangle}$ is nonempty when $|X| = |H|$ (so that we can apply Proposition 4.5 to conclude the resulting sumset has the same cardinality as $|\pi(V)|$), we always include at least $2 \le \ell$ terms from some cardinality two set, resulting in $|V_{\tau H}| \le \max\{2,\, 2(|H/L| - |\phi_L(X)|)\}$. But now (4.8) yields $|(U \cdot V^{[-1]})_{H_0}| \ge n - |H| + 1 \ge |H| + |G'/H|$, with the latter inequality following as H is a proper, nontrivial subgroup of the odd order group G' (forcing $|G'| \ge 9$), while (4.13) then implies $|(U \cdot V^{[-1]})_{\tau H}| \ge \ell - 2(|H/L| - |\phi_L(X)| + 1) \ge n + |H| + 1 - 2|L| - 2|H/L| \ge n - |H| - 1 \ge |G'/H| - 1$. So Claim A holds with $K_y = H_0$, contradicting that U is an atom.

CASE 3. $|X + \Sigma_{\lceil \ell/2 \rceil}(2U_{\tau H}^+)| < \min\{|H|,\, (|U'_{\tau H}| - \lceil \ell/2 \rceil)|L| + |X|\}$.

In view of the case hypothesis, we can apply Proposition 4.2.2 to $X + \Sigma_{\lceil \ell/2 \rceil}(2U_{\tau H}^+)$ taking L to be L^+ and using $2(U'_{\tau H})^+ \mid 2U_{\tau H}^+$. Let $y + K^+$ be the resulting coset with $K/L < H/L$ proper and nontrivial (so $y + K^+$ is the coset $\alpha + H$ from Proposition 4.2.2; note K/L is proper in view of the case hypothesis $|X + \Sigma_{\lceil \ell/2 \rceil}(2U_{\tau H}^+)| < |H|$), and set $K_y = \langle K, \tau\alpha^y \rangle \le H_0$. In particular, K is nontrivial and $|G'| \ge 3^3 = 27$. In this case, Lemma 4.13 along with [24, Proposition 2.2] applied to the sumset given by Proposition 4.2.2(d) yields a subsequence $V \mid U_{H_0}$ with

$$|V| = |V_H| + |V_{\tau H}| \le (|L| + |\phi_L(X)| - 2) + 2(|K/L| - 1) = |L| + 2|K/L| - 4 + |\phi_L(X)| \tag{4.14}$$

and $\pi(V)^+$ being K^+-periodic. Moreover, as the subsequence $V_{\tau H}$ is that partitioned by a sub-setpartition of the one given by Proposition 4.2 (cf. [24, Proposition 2.2]), we have $|V_{K_y \setminus K}| \ge \frac{1}{2}|V_{\tau H}|$, for each cardinality two subset must contain at least one term from $y + K^+ = (K_y \setminus K)^+$ by Proposition 4.2.2(b). Proposition 4.2.2(c) ensures that at most $|H/K| - 2$ of the terms of $U_{\tau H}$ are not in K_y (as $(K_y \setminus K)^+ = y + K^+$). Thus

$$\begin{aligned} |(U \cdot V^{[-1]})_{K_y \setminus K}| &\ge |U_{\tau H}| - (|H/K| - 2) - 2(|K/L| - 1) \ge n - |H| + 5 - 2|K/L| - |H/K| \\ &\ge n - |H| + 5 - 2|K| - |H/K| \ge \frac{2}{3}|G'| + 5 - 2|K| - \frac{1}{3}|G'/K| \ge |G'/K| - 1, \end{aligned}$$

with the second inequality above in view of (4.13). By construction (cf. Lemma 4.13), V_H contains all terms of U_H lying outside L, so all terms in $U_H \cdot V_H^{[-1]}$ lie in $L \le K \le K_y$. Combining this with (4.14), (4.8) and the already observed fact that there are at most $|H/K| - 2$ terms from $U_{\tau H}$ lying outside K_y implies

$$\begin{aligned} |(U \cdot V^{[-1]})_{K_y}| &\ge |U_{H_0}| - |H/K| + 2 - |V| \ge |U_{H_0}| - |H/K| - |L| - 2|K/L| + 6 - |H/L| \\ &\ge n + |H| - |H/K| - |L| - 2|K/L| - |H/L| + 5 \\ &\ge n + |H| - |H/K| - 2|K| - |H| + 4 \ge |G'| - \frac{1}{3}|G'/K| - 2|K| + 4 \\ &\ge |K| + |G'/K|, \end{aligned}$$

where the final inequality follows as K is nontrivial with $K < H < G'$. Therefore Claim A holds with K_y as defined above, contradicting that U is an atom. This completes CASE 3 and the proof. □

Proof of Theorem 4.1. Let G be a dihedral group of order $2n$ where $n \ge 3$ is odd, say $G = \langle \alpha, \tau :\ \alpha^n = \tau^2 = 1,\ \tau\alpha = \alpha^{-1}\tau \rangle$.

To see $\omega(G) \ge 2n$, let $U = ((\tau\alpha)\cdot\tau)^{[n]} \in \mathcal{A}(G)$. Then $U \cdot U = (\tau\cdot\tau)^{[n]} \cdot (\tau\alpha\cdot\tau\alpha)^{[n]}$ is a factorization into $2n$ length two atoms. Suppose U divides (in $\mathcal{B}(G)$) a sub-product $S \in \mathcal{B}(G)$ of these length two atoms. Then S must have an even number of copies of both $\tau\alpha$ and τ, ensuring that $S \cdot U^{[-1]} \in \mathcal{B}(G)$ contains an odd number of both $\tau\alpha$ and τ (as n is odd). However, it is readily seen (cf. Lemma 4.7) that $\tau^{[2]}$, $(\tau\alpha)^{[2]}$ and U are the only atoms with support contained in $\{\tau\alpha, \tau\}$. In particular, U is the only atom with support contained in $\{\tau\alpha, \tau\}$ having an odd number of copies of τ and $\tau\alpha$. Thus $S\cdot U^{[-1]} = U$, ensuring S must be the sub-product of all $2n$ length two atoms, which shows $\omega(G) \ge 2n$.

It remains to show $\omega(G) \le 2n$. To this end, suppose $U, U_1, \ldots, U_w \in \mathcal{A}(G)$ are atoms with $U \mid_{\mathcal{B}(G)} U_1\cdot\ldots\cdot U_w$, i.e., $U \mid U_1\cdot\ldots\cdot U_w$ and $(U_1\cdot\ldots\cdot U_w)\cdot U^{[-1]} \in \mathcal{B}(G)$. We need to show there exists a subset $J \subset [1,w]$ with $U \mid_{\mathcal{B}(G)} \prod_{i\in J}^{\bullet} U_i$ and $|J| \le 2n$.

Since $U \mid U_1\cdot\ldots\cdot U_w$, let $I_\varnothing \subset [1,w]$ be a minimal cardinality subset with $U \mid \prod_{\in I_\varnothing}^{\bullet} U_i$. In view of the minimality of $|I_\varnothing|$, we have $|I_\varnothing| \le |U| \le \mathsf{D}(G) = 2n$. Thus, if $V_\varnothing := U^{[-1]}\cdot\prod_{i\in I_\varnothing}^{\bullet} U_i$ is product-one, then the proof is complete taking J to be $I_\varnothing$. Therefore we may assume

$$1 \notin \pi(V_\varnothing).$$

Since both U and $\prod_{i\in I_\varnothing}^{\bullet} U_i$ are product-one sequences, it follows that $2\ell_\varnothing := |(V_\varnothing)_{\tau\langle\alpha\rangle}|$ must be even with $\pi(V_\varnothing) \subset G'$. Since $U \mid_{\mathcal{B}(G)} \prod_{i\in[1,w]}^{\bullet} U_i$, we have $1 \in \pi(U^{[-1]}\cdot\prod_{i\in[1,w]}^{\bullet} U_i) = \pi(V_\varnothing\cdot\prod_{i\in[1,w]\setminus I_\varnothing}^{\bullet} U_i)$. In consequence, if $\operatorname{supp}(V_\varnothing\cdot\prod_{i\in[1,w]\setminus I_\varnothing}^{\bullet} U_i) \subseteq \langle\alpha\rangle$, then $1 \in \pi(V_\varnothing)$ (as $\langle\alpha\rangle$ is abelian), contrary to assumption. As a result, if $\ell_\varnothing > 0$, then set $I_\emptyset = I_\varnothing$, and otherwise set $I_\emptyset = I_\varnothing \cup \{i_\emptyset\}$, where $i_\emptyset \in [1,w]\setminus I_\varnothing$ is an index with $\operatorname{supp}(U_{i_\emptyset}) \cap \tau\langle\alpha\rangle$ nonempty.

Let $I \subset [1,w]$ be an arbitrary subset with $I_\emptyset \subset I$. Set $V_\emptyset = U^{[-1]}\cdot\prod_{\in I_\emptyset}^{\bullet} U_i \in \mathcal{F}(G)$ and $V = U^{[-1]}\cdot\prod_{\in I}^{\bullet} U_i \in \mathcal{F}(G)$. Since U, $\prod_{i\in I}^{\bullet} U_i$ and $\prod_{i\in I_0}^{\bullet} U_i$ are product-one sequences, $2\ell := |V_{\tau\langle\alpha\rangle}|$ and $2\ell_\emptyset = |(V_\emptyset)_{\tau\langle\alpha\rangle}|$ must both be even with $\pi(V) \subset G'$. Let

$$X = \{x_1, -x_1\} + \ldots + \{x_s, -x_s\},$$

where $V^+_{\langle\alpha\rangle} = x_1\cdot\ldots\cdot x_s$. By construction, $\ell \ge \ell_\emptyset > 0$. Thus Proposition 4.5 ensures that

$$\pi(V)^+ = X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) - \sigma(V^+_{\tau\langle\alpha\rangle}).$$

Let $H^+ = \mathsf{H}(\pi(V)^+)$ and $L^+ = \mathsf{H}(X)$ (set $L^+ = X = \{0\}$ if $s = 0$). Note $L \le H$. If $\mathsf{h}(V_{\tau\langle\alpha\rangle}) \le \ell$, let $\ell' = \ell$. Otherwise, let $\ell' = 2\ell - \mathsf{h}(V_{\tau\langle\alpha\rangle})$. Note $\ell' \ge 0$ is the maximal integer for which there is a decomposition $V^+_{\tau\langle\alpha\rangle} = T_1\cdot\ldots\cdot T_\ell$ with $|T_i| = 2$ for all $i \in [1,\ell]$ and $|\operatorname{supp}(T_i)| = 2$ for all $i \le \ell'$. Likewise, if $\mathsf{h}(\phi_L(V^+_{\tau\langle\alpha\rangle})) \le \ell$, let $\ell_L = \ell$. Otherwise, let $\ell_L = 2\ell - \mathsf{h}(\phi_L(V^+_{\tau\langle\alpha\rangle}))$. Since $U \mid \prod_{\in I_\varnothing}^{\bullet} U_i$, we have decompositions $U_i = W_i\cdot W_i^U$, for $i \in I_\varnothing$, with $\prod_{i\in I_\varnothing}^{\bullet} W_i = V_\varnothing$ and $\prod_{i\in I_\varnothing}^{\bullet} W_i^U = U$. Note $|W_i^U| > 0$ for all $i \in I_\varnothing$ in view of the minimality of $|I_\varnothing|$. Let W_i^U be the trivial sequence with $W_i = U_i$ for $i \in I\setminus I_\varnothing$. Partition $I = I^2_\varnothing \cup I^\alpha \cup I^{\alpha\tau} \cup I^\tau$, where $I^2_\varnothing \subset I_\varnothing$ consist of all $i \in I_\varnothing$ with $|W_i^U| \ge 2$, where $I^\alpha \subset I$ consists of all $i \in I\setminus I^2_\varnothing$ with $\operatorname{supp}(W_i) \subset \langle\alpha\rangle$, where $I^\tau \subset I$ consists of all $i \in I\setminus I^2_\varnothing$ with $\operatorname{supp}(W_i) \subset \tau\langle\alpha\rangle$, and where $I^{\alpha\tau} \subset I$ consists of all $i \in I\setminus I^2_\varnothing$ with $\operatorname{supp}(W_i) \cap \langle\alpha\rangle$ and $\operatorname{supp}(W_i) \cap \tau\langle\alpha\rangle$ both nonempty. Let $I^1_\varnothing = I_\varnothing \setminus I^2_\varnothing$. Let $I_\varnothing = I^2_\varnothing \cup I^\alpha_\varnothing \cup I^{\alpha\tau}_\varnothing \cup I^\tau_\varnothing$ and $I_\emptyset = I^2_\varnothing \cup I^\alpha_\emptyset \cup I^{\alpha\tau}_\emptyset \cup I^\tau_\emptyset$ be the analogous partitions for $I_\varnothing$ and $I_\emptyset$. To simplify notation, we have suppressed the dependency on I of V, ℓ, X, s, H, L, and ℓ' from the notation. In the case when $I = I_\emptyset$, we denote these parameters by $V_\emptyset$, $\ell_\emptyset$, $X_\emptyset$, $s_\emptyset$, $H_\emptyset$, $L_\emptyset$ and $\ell'_\emptyset$.

Since $U \mid \prod_{i\in I_\varnothing}^{\bullet} U_i$ and $1 \notin \pi(V_\varnothing)$, it follows that $\operatorname{supp}(\prod_{i\in I_\varnothing}^{\bullet} U_i) \cap \tau\langle\alpha\rangle$ is nonempty. In particular, if $I_\varnothing \ne I_\emptyset$, then there must be some U_i with $\operatorname{supp}(U_i) \cap \tau\langle\alpha\rangle$ nonempty and $i \in I_\varnothing$. Moreover, as U_i is product-one, it must then have an even number of terms from $\tau\langle\alpha\rangle$, all of which are not contained in $V_\varnothing$ as $I_\varnothing \ne I_\emptyset$, whence $i \in I^2_\varnothing$, ensuring $I^2_\varnothing$ is nonempty. In summary, $I^2_\varnothing \ne \varnothing$ when $I_\varnothing \ne I_\emptyset$. In particular, if $I_\varnothing \ne I_\emptyset$, then $|I_\emptyset| = |I_\varnothing| + 1 \le (|U| - |I^2_\varnothing|) + 1 \le |U| \le 2n$. Thus we can also assume

$$1 \notin \pi(V_\emptyset), \tag{4.15}$$

for otherwise the proof is complete taking $J = I_\emptyset$.

Claim A. $\ell'_\varnothing \ge \min\{\ell_\varnothing, |I^\tau_\varnothing|\} \ge \frac{1}{2}|I^\tau_\varnothing|$.

Proof. If $I_\emptyset \neq I_\varnothing$, then $\ell_\varnothing = \ell'_\varnothing = |I^\tau_\varnothing| = 0$, and the claim is true. Therefore we now assume $I_\emptyset = I_\varnothing$. Let $j \in I^\tau_\varnothing$ be arbitrary. Then $|W^U_j| = 1$ and $\mathrm{supp}(W_j) \subset \tau\langle\alpha\rangle$. Let us consider the various possibilities that can occur for W_j. If $|W_j| = 1$, then U_j is a length two atom, forcing $U_j = w_j^{[2]}$ for some $w_j \in \tau\langle\alpha\rangle$. However, in such case, we must have $\mathsf{v}_{w_j}(V_\varnothing) = 1$, for if $w_j \in \mathrm{supp}(W_{j'})$ for some $j' \in I_\varnothing \setminus \{j\}$, then, since $W^U_j = \{w_j\}$, this means $U \mid \prod^\bullet_{i\in I_\varnothing\setminus\{j\}} U_i$, contradicting the minimality of $|I_\varnothing|$. If $|W_j| = 2$, then $|U_j| = 3$. Consequently, since the number of terms from $\tau\langle\alpha\rangle$ in a product-one sequence must be even, we conclude that $U_j = g_j \cdot h_j \cdot \alpha^z$ for some $g_j = \tau\alpha^x, h_j = \tau\alpha^y \in \tau\langle\alpha\rangle$ and $z \in \mathbb{Z}/n\mathbb{Z}$. Since U_j is an atom, we cannot have $\alpha^z = 1$ while either $x + z = y$ or $y + z = x$. Thus $g_j \neq h_j$. If $|W_j| \ge 3$, then Lemma 4.7 ensures that there are distinct $g_j, h_j \in \mathrm{supp}(W_j)$. Partition $I^\tau_\varnothing = J_1 \cup J_2$, with $J_1 \subset I^\tau_\varnothing$ consisting of all $j \in I^\tau_\varnothing$ with $|W_j| = 1$, and $J_2 \subset I^\tau_\varnothing$ consisting of all $j \in I^\tau_\varnothing$ with $|W_j| \ge 2$. By the above work, $\prod^\bullet_{j\in J_1} w_j \cdot \prod^\bullet_{j\in J_2}(g_j \cdot h_j) \mid (V_\varnothing)_{\tau\langle\alpha\rangle}$ with $g_j \neq h_j$ for all $j \in J_2$, and the w_j for $j \in J_1$ all distinct. Suppose $\ell'_\varnothing < \ell_\varnothing$. Then there is a unique $g \in \tau\langle\alpha\rangle$ with $\mathsf{v}_g(V_\varnothing) \ge \ell_\varnothing + 1 = \ell_\emptyset + 1 \ge 2$ (the equality follows from the assumption $I_\emptyset = I_\varnothing$). Since $\mathsf{v}_{w_j}(V_\varnothing) = 1$ for all $j \in J_1$, we have $g \neq w_j$ for all $j \in J_1$. Since $g_j \neq h_j$, each $j \in J_2$ has $g \neq g_j$ or $g \neq h_j$. Thus, swapping the roles of each g_j and h_j as need by, we may w.l.o.g. assume $\prod^\bullet_{j\in J_1} w_j \cdot \prod^\bullet_{j\in J_2} g_j \mid (V_\varnothing)_{\tau\langle\alpha\rangle}$ is a sequence of $|J_1|+|J_2| = |I^\tau_\varnothing|$ terms all distinct from g. Since $\mathsf{v}_g(V_\varnothing) \ge \ell_\varnothing + 1 > \frac{1}{2}|(V_\varnothing)_{\tau\langle\alpha\rangle}|$, each of these terms can be paired up with a distinct term equal to g, showing $\ell'_\varnothing \ge |I^\tau_\varnothing|$. So $\ell'_\varnothing \ge \min\{\ell_\varnothing, |I^\tau_\varnothing|\}$. Since each W_i with $i \in I^\tau_\varnothing$ contains at least one term from $\tau\langle\alpha\rangle$, we have $2\ell_\varnothing = |(V_\varnothing)_{\tau\langle\alpha\rangle}| \ge |I^\tau_\varnothing|$, and the claim follows. □

We say the set $I \subset [1, w]$ (containing $I_\emptyset$) is *ample* if the following hold:

A1. $|\pi(V)| \ge \left\lfloor \frac{1}{2}|I^1_\varnothing| \right\rfloor + 1 + |I \setminus I_\varnothing|$.
A2. $|X| \ge |X_\varnothing| + |I^\alpha \setminus I^\alpha_\varnothing|$.

We will say the set I (containing $I_\emptyset$) is *constrained* or (more specifically) H_x*-constrained* if there exists a subgroup $H_x = \langle H, \tau\alpha^x\rangle \le G$, as well as a decomposition $V^+_{\tau\langle\alpha\rangle} = T_1 \cdot \ldots \cdot T_\ell$ with $|T_i| = 2$ for all $i \in [1, \ell]$ such that, letting $A_i = \mathrm{supp}(2T_i)$ for $i \in [1, \ell]$, the following hold:

C1. $X + \sum_{i=1}^{\ell} A_i$ is H^+-periodic.
C2. $A_i \cap (2x + H^+) \neq \emptyset$ for all $i \in [1, \ell]$.
C3. There is a $j \in [1, \ell]$ with $|X + \sum_{\substack{i=1\\ i\neq j}}^{\ell} A_i| = |X + \sum_{i=1}^{\ell} A_i|$.
C4. $|X| \ge |X_\varnothing| + |I^\alpha \setminus I^\alpha_\varnothing|$.

Conditions C1 and C2 allow us to apply Proposition 4.11.1 to conclude $X + \sum_{i=1}^{\ell} A_i = X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = \pi(V)^+ + \sigma(V^+_{\tau\langle\alpha\rangle})$, in which case $H^+ = \mathsf{H}(X + \sum_{i=1}^{\ell} A_i) = \mathsf{H}(\pi(V)^+)$ by definition of H. Note that $\phi_H(X + \sum_{i=1}^{\ell} A_i) = \phi_H(\{x_1, -x_1\}) + \ldots + \phi_H(\{x_s, -x_s\}) + \sum_{i=1}^{\ell} \phi_H(A_i)$ is a sumset of cardinality at most two sets. Since n is odd, the set $\{x_i, -x_i\}$ considered modulo H^+ has cardinality two precisely when $x_i \notin H^+$, while the set $\phi_H(A_i)$ has cardinality two (in view of C2) precisely when T_i consists of one term from $x + H^+$ with its other term lying outside $x + H^+$. As a result, $|V_{G\setminus H_x}|$ equals the number of cardinality two summands in the sumset $\phi_H(\{x_1, -x_1\}) + \ldots + \phi_H(\{x_s, -x_s\}) + \sum_{i=1}^{\ell} \phi_H(A_i)$, in which case

Kneser's Theorem implies $|X + \sum_{i=1}^{\ell} A_i| \ge (|V_{G\setminus H_x}| + 1)|H|$. In summary, Conditions C1 and C2 imply

$$X + \sum_{i=1}^{\ell} A_i = X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = \pi(V)^+ + \sigma(V^+_{\tau\langle\alpha\rangle}) \quad \text{and} \quad |X + \sum_{i=1}^{\ell} A_i| \ge (|V_{G\setminus H_x}| + 1)|H|. \tag{4.16}$$

Kneser's Theorem (applied modulo H^+) ensures that $A_j \subset 2x + H^+$ for any $j \in [1, \ell]$ satisfying C3. As we trivially have $|X + \sum_{i=1}^{\ell} A_i| \le n$, with equality only possible when $H^+ = \mathbb{Z}/n\mathbb{Z}$, (4.16) implies

$$|V_{G\setminus H_x}| \le |G'/H| - 2 + \epsilon, \tag{4.17}$$

where $\epsilon = 0$ if $H^+ < \mathbb{Z}/n\mathbb{Z}$ is proper, and $\epsilon = 1$ if $H^+ = \mathbb{Z}/n\mathbb{Z}$.

Claim B. If $|\pi(V)| \le \lfloor \frac{1}{2}|I^1_\varnothing| \rfloor + 1 + |I \setminus I_\varnothing|$ and C4 holds but I is not constrained, then $\ell = \ell'$, $|I^1_\varnothing|$ is even, $|\pi(V)| = \frac{1}{2}|I^1_\varnothing| + 1 + |I \setminus I_\varnothing| = \ell + 1$, L is trivial, $|I^{\alpha\tau}| = |I^\alpha| = 0$, $X = \{0\}$, and $|U_i| = 2$ for every $i \in I^\tau$. Moreover, $\mathrm{supp}(V^+_{\tau\langle\alpha\rangle}) \subset \{x - d, x, x + d\}$ with $\mathsf{v}_x(V^+_{\tau\langle\alpha\rangle}) = \mathsf{h}(V^+_{\tau\langle\alpha\rangle}) = \ell \le \mathrm{ord}(d) - 1$, for some $x, d \in \mathbb{Z}/n\mathbb{Z}$.

Proof. By definition of ℓ_L and ℓ', there is a decomposition $V^+_{\tau\langle\alpha\rangle} = T_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T_\ell$ with $|T_i| = 2$ for all $i \in [1, \ell]$, $|A_i| = 2$ for all $i \le \ell'$, $|\phi_L(A_i)| = 2$ for all $i \le \ell_L$, and $|\phi_L(A_i)| = 1$ for all $i > \ell_L$, where $A_i = \mathrm{supp}(2T_i)$ for $i \in [1, \ell]$.

Suppose $\ell_L < \ell$, i.e., $\mathsf{h}(\phi_L(V^+_{\tau\langle\alpha\rangle})) \ge \ell + 1$, and let $x \in \mathbb{Z}/n\mathbb{Z}$ be an element with $\phi_L(x)$ a maximum multiplicity term in $\phi_L(V^+_{\tau\langle\alpha\rangle})$. Since $\ell_L < \ell$, we have $A_i \cap (2x + L^+) \ne \emptyset$ and $|A_i \setminus (2x + L^+)| \le 1$ for all i. Hence, since $L^+ = \mathsf{H}(X)$, Proposition 4.11.1 implies that $X + \sum_{i=1}^{\ell} A_i = X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = \pi(V)^+ + \sigma(V^+_{\tau\langle\alpha\rangle})$, which is H^+-periodic by definition. Thus C1 holds. Additionally, since $L \le H$, it follows that C2 holds (in view of $A_i \cap (2x + L^+) \ne \emptyset$ for all i), while C3 holds for any $j > \ell_L$ as these sets are subsets of the same L^+-coset with $\mathsf{H}(X) = L^+$. As C4 holds by hypothesis, we conclude that I is constrained, which is contrary to hypothesis. So we instead assume $\ell_L = \ell$, i.e., $\mathsf{h}(\phi_L(V^+_{\tau\langle\alpha\rangle})) \le \ell$, which also forces $\ell' = \ell$.

Suppose $|X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| < \ell|L| + |X| = (|V_{\tau\langle\alpha\rangle}| - \ell)|L| + |X|$. Then, in view of $\ell_L = \ell$ (which is equivalent to $\mathsf{h}(\phi_L(V^+_{\tau\langle\alpha\rangle})) \le \ell$), we can apply Proposition 4.2.2 to $X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})$ taking L to be L^+ and using $2V^+_{\tau\langle\alpha\rangle} \mid 2V^+_{\tau\langle\alpha\rangle}$. But now C1–C2 all hold for the resulting setpartition $B_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} B_\ell$ given by Proposition 4.2.2, and C4 holds by hypothesis. Moreover, if C3 fails, then $|X + \sum_{i=1}^{j} B_i| \ge |X + \sum_{i=1}^{j-1} B_i| + |L|$ for all $j \in [1, \ell]$, which implies $|X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| \ge \ell|L| + |X|$, contrary to assumption. Thus C3 also holds, meaning I is constrained, which is contrary to hypothesis. So we now instead assume

$$|X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| \ge \ell|L| + |X| \ge |X| + \ell + |L| - 1. \tag{4.18}$$

Let $e_\alpha \ge 0$ be the number of indices $i \in I^\alpha_\varnothing$ for which W_i contains some term lying outside $L_\varnothing$. Kneser's Theorem implies $|X_\varnothing| \ge (e_\alpha + 1)|L_\varnothing|$. Combined with C4, we find that

$$|X| \ge (e_\alpha + 1)|L_\varnothing| + |I^\alpha| - |I^\alpha_\varnothing|. \tag{4.19}$$

For each of the $|I^\alpha_\varnothing| - e_\alpha$ indices $i \in I^\alpha_\varnothing$ not counted by e_α, we have $\mathrm{supp}(W_i) \subset L_\varnothing$. Thus, since U_i is an atom with $W_i^U = U_i \boldsymbol{\cdot} W_i^{[-1]}$ a single term, it follows that the unique term from W_i^U must also lie in $L_\varnothing$. It follows that $|U_{L_\varnothing}| \ge |I^\alpha_\varnothing| - e_\alpha$. Hence Lemma 4.9 applied to U implies $|I^\alpha_\varnothing| \le 2|L_\varnothing| - 2 + e_\alpha$. Combined with (4.19), we obtain

$$|X| \ge |I^\alpha| + (e_\alpha - 1)(|L_\varnothing| - 1) + 1 \ge |I^\alpha| - |L_\varnothing| + 2, \tag{4.20}$$

with equality only possible if $|I^\alpha_\varnothing| = 2|L_\varnothing| - 2 + e_\alpha$. Since each W_i with $i \in I^1_\varnothing \setminus I^\alpha_\varnothing$ contains at least one term from $\tau\langle\alpha\rangle$, and since each $W_i = U_i$ with $i \in I \setminus (I^\alpha \cup I_\varnothing) = (I \setminus I_\varnothing) \setminus (I^\alpha \setminus I^\alpha_\varnothing)$ contains at least two terms from $\tau\langle\alpha\rangle$, we have

$$\ell \ge (|I \setminus I_\varnothing| - |I^\alpha| + |I^\alpha_\varnothing|) + \left\lceil \frac{1}{2}(|I^1_\varnothing| - |I^\alpha_\varnothing|) \right\rceil = |I \setminus I_\varnothing| - |I^\alpha| + \left\lceil \frac{1}{2}|I^1_\varnothing| + \frac{1}{2}|I^\alpha_\varnothing| \right\rceil, \tag{4.21}$$

with equality only possible if $|(U_i)_{\tau\langle\alpha\rangle}| = 2$ for all $i \in I^{\alpha\tau}$ and $|U_i| = 2$ for all $i \in I^\tau$ (since each $|(U_i)_{\tau\langle\alpha\rangle}|$ must be even). Combining (4.18), (4.20) and (4.21), we obtain

$$|X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| \ge \left\lceil \frac{1}{2}|I^1_\varnothing| + \frac{1}{2}|I^\alpha_\varnothing| \right\rceil + |I \setminus I_\varnothing| + 1 + |L| - |L_\varnothing| \ge \left\lceil \frac{1}{2}|I^1_\varnothing| \right\rceil + |I \setminus I_\varnothing| + 1. \tag{4.22}$$

Since $|X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| \le \lfloor \frac{1}{2}|I^1_\varnothing| \rfloor + |I \setminus I_\varnothing| + 1$ holds by hypothesis, we are left to conclude equality holds in (4.22) as well as in the estimates (4.18), (4.20) and (4.21) used to derive (4.22), and that $|I^1_\varnothing|$ is even, $|I^\alpha_\varnothing| = 0$ and $L = L_\varnothing$ (lest the second inequality in (4.22) be strict). Equality in (4.20) implies $|I^\alpha_\varnothing| = 2|L_\varnothing| - 2 + e_\alpha$, which combined with $|I^\alpha_\varnothing| = 0$ forces $|L_\varnothing| = 1$ and $e_\alpha = 0$. Since $L = L_\varnothing$ is trivial, Kneser's Theorem implies $|X| \ge |V_{\langle\alpha\rangle}| + 1 \ge 2|I^\alpha \setminus I^\alpha_\varnothing| + |I^\alpha_\varnothing| + |I^{\alpha\tau}| + 1 = 2|I^\alpha| - |I^\alpha_\varnothing| + |I^{\alpha\tau}| + 1 = 2|I^\alpha| + |I^{\alpha\tau}| + 1$. As a result, since equality holds in (4.20), we are left to conclude $|V_{\langle\alpha\rangle}| = |I^\alpha| = |I^{\alpha\tau}| = 0$. Thus $\operatorname{supp}(V) \subset \tau\langle\alpha\rangle$ and $X = \{0\}$. As equality holds in (4.21), we have $|U_i| = 2$ for all $i \in I^\tau$. It remains to show $\operatorname{supp}(V^+_{\tau\langle\alpha\rangle}) \subset \{x - d, x, x + d\}$ with $\mathsf{v}_x(V^+_{\tau\langle\alpha\rangle}) = \mathsf{h}(V^+_{\tau\langle\alpha\rangle}) = \ell \le \operatorname{ord}(d) - 1$, for some $x, d \in \mathbb{Z}/n\mathbb{Z}$.

Since equality holds in (4.22) and (4.21) with $X = \{0\}$, $|I^\alpha_\varnothing| \le |I^\alpha| = 0$ and $|I^1_\varnothing|$ even, we have $|\pi(V)| = |\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| = \frac{1}{2}|I^1_\varnothing| + |I \setminus I_\varnothing| + 1 = \ell + 1 = \ell' + 1$, allowing us to apply Proposition 4.3 (with $m = n = \ell$) to $\Sigma_\ell(2V^+_\tau\langle\alpha\rangle)$. If Proposition 4.3.5 holds, then I is constrained in view of C4 holding by hypothesis, which is contrary to hypothesis. If Proposition 4.3.4 holds, then $\operatorname{supp}(V^+_{\tau\langle\alpha\rangle}) \subset \{x - d, x, x + d\}$ with $\mathsf{v}_x(V^+_{\tau\langle\alpha\rangle}) = \mathsf{h}(V^+_{\tau\langle\alpha\rangle}) = \ell$, for some $x, d \in \mathbb{Z}/n\mathbb{Z}$. Thus the claim is complete unless $\ell \ge \operatorname{ord}(d)$. However, in this case, each A_i is an arithmetic progression with difference $2d$, so that $|\sum_{i=1}^{j} A_i| = \min\{\operatorname{ord}(d), j + 1\}$ for all $j \in [1, \ell]$. Thus $\ell \ge \operatorname{ord}(d)$ implies that $|\sum_{i=1}^{\ell-1} A_i| = |\sum_{i=1}^{\ell} A_i| = \operatorname{ord}(d)$, whence C3 holds as well as C1 with $H^+ = \langle d\rangle$. Since there is some term $2x \in 2V^+_{\tau\langle\alpha\rangle}$ with multiplicity ℓ, we obtain $2x \in A_i$ for all i, whence C2 holds. Hence I is constrained as C4 holds by hypothesis, a contradiction. If Proposition 4.3.3 holds, then each $A_i = \{2x, 2x + 2d\}$ for some $x, x + d \in \mathbb{Z}/n\mathbb{Z}$. If $\ell \le \operatorname{ord}(d) - 1$, the claim is complete. Otherwise, arguing as in the previous case, we conclude that I is constrained, contrary to hypothesis. If Proposition 4.3.2 holds, then $\ell = 2$ and $\operatorname{supp}(V^+_{\tau\langle\alpha\rangle}) = x + \langle d\rangle$ for some $x, d \in \mathbb{Z}/n\mathbb{Z}$ with $\operatorname{ord}(d) = 3$. In this case, the pigeonhole principle ensures there is some $y \in x + \langle d\rangle$ with $\mathsf{v}_y(V^+_{\tau\langle\alpha\rangle}) = 2$, so the claim follows as $\langle d\rangle$ is trivially an arithmetic progression with difference d and length $\operatorname{ord}(d) = 3$. Finally, we note that Proposition 4.3.1 cannot hold since this requires $\mathbb{Z}/n\mathbb{Z}$ to contain a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. As this exhausts all possibilities, the claim is complete. □

CASE 1. There exists an ample subset $I \subset [1, w]$.

We may w.l.o.g. assume $|I|$ is maximal among all ample subsets. By definition of $I^2_\varnothing$, we have $2n \ge |U| \ge 2|I^2_\varnothing| + |I^1_\varnothing|$. Hence, by A1, we have $n \ge |\pi(V)| \ge \frac{1}{2}|I^1_\varnothing| + \frac{1}{2} + |I \setminus I_\varnothing| = |I| + \frac{1}{2} - \frac{1}{2}|I^1_\varnothing| - |I^2_\varnothing| \ge |I| + \frac{1}{2} - n$, implying $|I| \le 2n - 1$. If $|\pi(V)| = n$, then $\pi(V) = G'$ follows. In particular, $1 \in \pi(V)$, ensuring that $U \mid_{\mathcal{B}(G)} \prod^\bullet_{i \in I} U_i$ with $|I| \le 2n - 1$, and the proof is complete. Therefore we may assume $|\pi(V)| \le n - 1$, in which case the above estimates improve to $|I| \le 2n - 2$. We must have $I \subset [1, w]$ proper; otherwise $U \mid_{\mathcal{B}(G)} \prod^\bullet_{i \in [1,w]} U_i = \prod^\bullet_{i \in I} U_i$ with $|I| \le 2n - 2$, and the proof is again complete.

Let $j \in [1, w] \setminus I$ be arbitrary. The maximality of $|I|$ ensures that $I_j = I \cup \{j\}$ is not ample, meaning either A1 or A2 fails. Let V_j, ℓ_j, X_j and I^α_j be the respective quantities V, ℓ, X and I^α for the set I_j.

Suppose there is some $j \in [1,w] \setminus I$ and $g \in \supp(U_j) \cap \langle \alpha \rangle$ with $g \notin H$. Since $H^+ = \mathsf H(X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}))$, it follows that $\phi_H(X)$ and $\phi_H(X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}))$ are both aperiodic. Thus Kneser's Theorem implies that $|X_j| \ge |\{g^+, -g^+\} + X| > |X|$ and $|\pi(V_j)| \ge |\{g^+, -g^+\} + X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| > |X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| = |\pi(V)|$, so that A1 and A2 holding for I ensures they hold for I_j, contradicting the maximality of $|I|$. So we instead conclude that

$$\supp\big(\prod\nolimits^\bullet_{i\in[1,w]\setminus I} U_i\big) \cap \langle\alpha\rangle \subset H. \tag{4.23}$$

As a result, if $\supp(U_i) \subset \langle\alpha\rangle$ for all $i \in [1,w] \setminus I$, then $\pi(U^{[-1]} \cdot \prod_{i\in[1,w]} U_i)^+ = \pi(V \cdot \prod^\bullet_{i\in[1,w]\setminus I} U_i)^+ = \pi(V)^+$ follows from Proposition 4.5.2. Thus, since $1 \in \pi(U^{[-1]} \cdot \prod_{i\in[1,w]} U_i)$ in view of the hypothesis that $U \mid_{\mathcal B(G)} \prod_{i\in[1,w]} U_i$, we conclude that $1 \in \pi(V)$, so that $U \mid_{\mathcal B(G)} \prod_{i\in I} U_i$ with $|I| \le 2n-2$, and then the proof is complete taking $J = I$. Therefore let $J_\tau \subset [1,w] \setminus I$ be the nonempty set of all $i \in [1,w] \setminus I$ with $\supp(U_i) \cap \tau\langle\alpha\rangle \ne \emptyset$. Note that $I^\alpha_j = I^\alpha$ for all $j \in J_\tau$, so that A2 holds for any I_j with $j \in J_\tau$ since it holds for I. This means A1 fails for every I_j with $j \in J_\tau$, which in view of A1 holding for I implies

$$|\pi(V)| = \Big\lfloor \frac{1}{2}|I^1_\varnothing| \Big\rfloor + 1 + |I \setminus I_\varnothing|. \tag{4.24}$$

CASE 1.1. I is not constrained.

In this case, (4.24) and A2 holding for I allow us to apply Claim B yielding $\ell = \ell'$, $|I^1_\varnothing|$ is even, L is trivial, $|I^{\alpha\tau}| = |I^\alpha| = 0$, $X = \{0\}$, $|U_i| = 2$ for every $i \in I^\tau$, $|\pi(V)| = \ell + 1$ and $\supp(V^+_{\tau\langle\alpha\rangle}) \subset \{x-d, x, x+d\}$ for some $x, d \in \mathbb Z/n\mathbb Z$ with $\ell \le \ord(d) - 1$ and $\mathsf v_{2x}(2V^+_{\tau\langle\alpha\rangle}) = \mathsf h(2V^+_{\tau\langle\alpha\rangle}) = \ell$. Thus we have a decomposition $V^+_{\tau\langle\alpha\rangle} = T_1 \cdot \ldots \cdot T_\ell$ with $|A_i| = |T_i| = 2$ for all i, where each $A_i = \supp(2T_i)$ is an arithmetic progression with difference $2d$ containing $2x$, for all $i \in [1,\ell]$, in which case Lemma 4.4 (with H taken to be trivial) ensures $\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = \sum_{i=1}^{\ell} A_i \subset 2\ell x + \langle d\rangle$ is an arithmetic progression of length $\ell+1$. In particular, either $\ell < \ord(d) - 1$ and H is trivial, or $\ell = \ord(d) - 1$ and $H^+ = \langle d\rangle$.

Consider an arbitrary index $j \in J_\tau$, in which case $\ell_j > \ell$. Since $V_j = V \cdot U_j$, we have $\Sigma_{\ell_j-\ell}(2(U_j)^+_{\tau\langle\alpha\rangle}) + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) \subset \Sigma_{\ell_j}(2(V_j)^+_{\tau\langle\alpha\rangle})$. Consequently, since A1 fails for I_j (as $j \in J_\tau$), it then follows from (4.24) that $|\pi(V)| = |\pi(V_j)| = \lfloor \frac12 |I^1_\varnothing| \rfloor + 1 + |I \setminus I_\varnothing|$, and hence $|\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| = |\pi(V)| = |\pi(V_j)| = |\Sigma_{\ell_j}(2(V_j)^+_{\tau\langle\alpha\rangle})|$ and

$$\Sigma_{\ell_j-\ell}(2(U_j)^+_{\tau\langle\alpha\rangle}) + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = \Sigma_{\ell_j}(2(V_j)^+_{\tau\langle\alpha\rangle}) = \beta + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}), \tag{4.25}$$

for any $\beta \in \Sigma_{\ell_j-\ell}(2(U_j)^+_{\tau\langle\alpha\rangle})$. In particular, since $|(U_j)_{\tau\langle\alpha\rangle}| = 2(\ell_j - \ell) \ge 2$, we conclude that all terms of $2(U_j)^+_{\tau\langle\alpha\rangle}$ are congruent to each other modulo the stabilizer $H^+ = \mathsf H(\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}))$.

Suppose H^+ is nontrivial. Then $H^+ = \langle d\rangle$ with $\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = \sum_{i=1}^{\ell} A_i = 2\ell x + H^+$, in which case $\Sigma_{\ell_j}(2(V_j)^+_{\tau\langle\alpha\rangle}) = \beta + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = \beta + 2\ell x + H^+$ is also an H^+-coset. However, as $\ell_j < |(V_j)_{\tau\langle\alpha\rangle}|$, this is only possible if all terms of $(V_j)^+_{\tau\langle\alpha\rangle}$ lie in the same H^+-coset, ensuring that $\supp((V_j)^+_{\tau\langle\alpha\rangle}) \subset x + H^+ = x + \langle d\rangle$. This must be true for any $j \in J_\tau$, so $\supp\Big((\prod^\bullet_{i\in[1,w]\setminus I} U_i)^+_{\tau\langle\alpha\rangle}\Big) \subset x + H^+$. Combined with (4.23), we conclude $\supp\big(\prod^\bullet_{i\in[1,w]\setminus I} U_i\big) \subset H_x$, and now Proposition 4.11.2 implies that $\pi(V)$ is a translate of $\pi\Big(U^{[-1]} \cdot \prod^\bullet_{i\in[1,w]} U_i\Big) = \pi(V \cdot \prod^\bullet_{i\in[1,w]\setminus I} U_i)$. However, since $\prod^\bullet_{i\in[1,w]\setminus I} U_i$ is product-one, we have $1 \in \pi\Big(U^{[-1]} \cdot \prod^\bullet_{i\in[1,w]} U_i\Big) = \pi(V)$. Thus $U \mid_{\mathcal B(G)} \prod^\bullet_{i\in I} U_i$ with $|I| \le 2n-2$, and the proof is complete taking $J = I$. So we now instead assume H is trivial and $\ell < \ord(d) - 1$.

Combining H trivial with (4.23) implies $\supp(U_i) \subset \tau\langle\alpha\rangle$ for all $i \in [1,w] \setminus I$ (as we can assume no U_i is the atom consisting of a single term equal to 1). We showed above that all terms of $U_j = (U_j)_{\tau\langle\alpha\rangle}$

are equal (as H is trivial), for any $j \in J_\tau = [1,w] \setminus I$. Thus Lemma 4.7 ensures each $U_j = g_j^{[2]}$ for some $g_j \in \tau\langle\alpha\rangle$. Suppose, for some $j \in [1,w] \setminus I$, that $\mathrm{supp}(U_j^+) = \{y\}$ with $2y \notin A_{j'}$ for some $j' \in [1,\ell]$, say w.l.o.g. $2y \notin A_\ell$. Observe that $(\ell_j - \ell)2y + \sum_{i=1}^{\ell-1} A_i + (A_\ell \cup \{2y\}) \subset \Sigma_{\ell_j}(2(V_j)^+_{\tau\langle\alpha\rangle})$. Since $\sum_{i=1}^{\ell} A_i$ is aperiodic (as H^+ is trivial and $X = \{0\}$) and $2y \notin A_\ell$, Kneser's Theorem and [23, Lemma 2.6] imply $|\sum_{i=1}^{\ell-1} A_i + (A_\ell \cup \{2y\})| > \sum_{i=1}^{\ell} |A_i| - \ell + 1 = \ell + 1 = |\sum_{i=1}^{\ell} A_i|$. Thus $|\Sigma_{\ell_j}(2(V_j)^+_{\tau\langle\alpha\rangle})| > |\sum_{i=1}^{\ell} A_i| = |\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})|$, contrary to (4.25). So we are left to conclude that, for any $j \in [1,w]\setminus I$, all terms of U_j are equal to some multiplicity ℓ term in $V_{\tau\langle\alpha\rangle}$. If it always the same multiplicity ℓ term for each U_j with $j \in [1,w]\setminus I$, then Proposition 4.11 (taking H to be trivial) implies $\pi(V) = \pi(V \cdot \prod^\bullet_{i\in[1,w]\setminus I} U_i) = \pi\Big(U^{[-1]} \cdot \prod^\bullet_{i\in[1,w]} U_i\Big)$, and the proof is complete as before.

It remains to consider the case when there are two multiplicity ℓ terms in $V^+_{\tau\langle\alpha\rangle}$, so w.l.o.g. $A_i = \{x, x+d\}$ for all $i \in [1,\ell]$, and $(V_j)^+_{\tau\langle\alpha\rangle} = x^{[2]}$ and $(V_{j'})^+_{\tau\langle\alpha\rangle} = (x+d)^{[2]}$ for some $j, j' \in [1,w]\setminus I$. Set $A_{\ell+1} = A_{\ell+2} = \{2x, 2x+d\}$. Define $J = I \cup \{j, j'\}$ and let V_J, ℓ_J, I^α_J and ℓ'_J be the corresponding quantities V, ℓ, I^α and ℓ' for the set J. Then $\ell'_J = \ell' + 2 = \ell + 2 = \ell_J$ and $I^\alpha = I^\alpha_J$, ensuring that A2 holds for J since it held for I. Observe (in view of (4.23) and Proposition 4.5) that

$$\pi(V_J)^+ + \sigma(V^+_{\tau\langle\alpha\rangle}) = \sum_{i=1}^{\ell+2} A_i = \underbrace{\{2x, 2x+2d\} + \ldots + \{2x, 2x+2d\}}_{\ell+2}.$$

If $|X + \sum_{i=1}^{\ell+2} A_i| \ge |X + \sum_{i=1}^{\ell} A_i| + 2$, then A1 holding for I will imply it holds for J, in which case $|J|$ contradicts the maximality of $|I|$. Therefore $|X + \sum_{i=1}^{\ell+2} A_i| \le |X + \sum_{i=1}^{\ell} A_i| + 1$, which is only possible if $2d \in H^+_J := \mathsf{H}(\sum_{i=1}^{\ell+1} A_i) = \mathsf{H}(\sum_{i=1}^{\ell+2} A_i) = \mathsf{H}(\Sigma_{\ell+2}(V_J)) = \langle d\rangle$. As a result, since $\mathrm{supp}((U_j)^+_{\tau\langle\alpha\rangle}) \subset \{x, x+d\} \subset x + H^+_J$ for all $j \in J_\tau$, we conclude via Proposition 4.11 that $1 \in \pi(U^{[-1]} \cdot \prod^\bullet_{i\in[1,w]} U_i) = \pi(V_J \cdot \prod^\bullet_{i\in[1,w]\setminus J} U_i) = \pi(V_J)$. Thus $U \mid_{\mathcal{B}(G)} \prod^\bullet_{i\in J} U_i$ with $|J| = |I| + 2 \le 2n$, completing the proof and subcase.

CASE 1.2. I is H_x-constrained.

Let $2x + H^+$ and $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_\ell$ be the coset and setpartition showing I is constrained, and let w.l.o.g. $j = \ell$ be the index from C3. Consider an arbitrary index $k \in J_\tau$. Then A1 fails for I_k, which in view of (4.24) implies that $|\pi(V)| = |\pi(V_k)|$. Indeed, since $|\pi(V)| = |X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| \le |X + \Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle})| \le |X_k + \Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle})| = |\pi(V_k)|$, we obtain that $|X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})| = |X + \Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle})|$. Moreover, arguing as we did when establishing (4.25), we conclude that

$$X + \Sigma_{\ell_k-\ell}(2(U_k)^+_{\tau\langle\alpha\rangle}) + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = X + \Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle}) = \beta + X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}), \tag{4.26}$$

for any $\beta \in \Sigma_{\ell_k-\ell}(2(U_k)^+_{\tau\langle\alpha\rangle})$, and that all terms of $(U_k)^+_{\tau\langle\alpha\rangle}$ are congruent to each other modulo the stabilizer $H^+ = \mathsf{H}(X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}))$. We claim that they are, in fact, all congruent to x modulo H^+. If this fails, then there is some $z \in \mathrm{supp}((U_k)^+_{\tau\langle\alpha\rangle})$ with $z \notin x + H^+$, whence (4.26) yields

$$X + \Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle}) = (\ell_k - \ell)2z + X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}). \tag{4.27}$$

Recall that $j = \ell$ is the index given by C3 and define a new setpartition $\mathcal{B} = B_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} B_\ell$ by setting $B_\ell = \{2y, 2z\}$, where $2y \in A_\ell = A_j \subset 2x + H^+$ is any element, and setting $B_i = A_i$ for $i < \ell$. In view of C3 and (4.16), we have $(\ell_k - \ell)2z + X + \Sigma_\ell(2V^+_{\tau\langle\alpha\rangle}) = (\ell_k - \ell)2z + X + \sum_{i=1}^{\ell} A_i \subset (\ell_k -$

$\ell)2z + X + \sum_{i=1}^{\ell} B_i \subset X + \Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle})$, whence $X + \sum_{i=1}^{\ell} A_i = X + \sum_{i=1}^{\ell} B_i$ follows in view of (4.27). In particular, since $X + \sum_{i=1}^{\ell-1} A_i$ is a translate of $X + \sum_{i=1}^{\ell} A_i$ by C3, and thus has stabilizer H^+, Kneser's Theorem implies that all terms of $B_\ell = \{2y, 2z\}$ are congruent modulo H^+, contradicting the assumption $z \notin x + H^+ = y + H^+$. So we conclude that $\mathrm{supp}((U_k)^+_{\tau\langle\alpha\rangle}) \subset x + H^+$, as claimed. However, as $j \in J_\tau$ was arbitrary, combining this with (4.23) and Proposition 4.11 (as V is H_x-constrained) once more yields $1 \in \pi(U^{[-1]} \cdot \prod^{\bullet}_{i\in[1,w]} U_i) = \pi(V \cdot \prod^{\bullet}_{i\in[1,w]\setminus I} U_i) = \pi(V)$, showing that $U \mid_{\mathcal{B}(G)} \prod^{\bullet}_{i\in I} U_i$ with $|I| \le 2n-2$. Thus the proof is complete taking $J = I$, which completes CASE 1.

CASE 2. There is no ample subset $I \subset [1, w]$.

As a particular instance of the case hypothesis, $I_\emptyset$ is not ample. Since A2/C4 holds trivially for $I_\emptyset$ (as $i_\emptyset \in I^\tau \cup I^{\alpha\tau}$ when $I_\varnothing \ne I_\emptyset$), this means A1 must fail:

$$|X_\emptyset + \Sigma_{\ell_\emptyset}(2(V_\emptyset)^+_{\tau\langle\alpha\rangle})| = |\pi(V_\emptyset)| \le \frac{1}{2}|I^1_\varnothing| + |I_\emptyset \setminus I_\varnothing|. \tag{4.28}$$

Thus Claim B ensures that $I_\emptyset$ is $(H_\emptyset)_{x_0}$-constrained for some $x_0 \in \mathbb{Z}/n\mathbb{Z}$, and we use the abbreviation $\tilde{H}_\emptyset = (H_\emptyset)_{x_0}$.

Suppose $H_\emptyset$ is trivial. Then $X_\emptyset + \Sigma_{\ell_\emptyset}(2(V_\emptyset)^+_{\tau\langle\alpha\rangle})$ is aperiodic. Moreover, from the definitions involved, $X_\emptyset$ is a sumset of $|(V_\emptyset)_{\langle\alpha\rangle}| \ge |I^\alpha_\emptyset| + |I^{\alpha\tau}_\emptyset|$ cardinality two sets, while in view of (4.16), C2 and the definition of $\ell'_\emptyset$, it follows that $\Sigma_{\ell_\emptyset}(2(V_\emptyset)^+_{\tau\langle\alpha\rangle})$ is a sumset of $\ell'_\emptyset$ cardinality two sets (as well as several cardinality one sets). Hence it follows from Kneser's Theorem that

$$|X_\emptyset + \Sigma_{\ell_\emptyset}(2(V_\emptyset)^+_{\tau\langle\alpha\rangle})| \ge |(V_\emptyset)_{\langle\alpha\rangle}| + 1 + \ell'_\emptyset \ge |I^\alpha_\emptyset| + |I^{\alpha\tau}_\emptyset| + 1 + \ell'_\emptyset. \tag{4.29}$$

If $I_\varnothing \ne I_\emptyset$, then $|I_\emptyset \setminus I_\varnothing| = 1$, $\ell'_\emptyset \ge 0$, $(V_\varnothing)_{\langle\alpha\rangle} = V_\varnothing$, and $|(V_\emptyset)_{\langle\alpha\rangle}| \ge |(V_\varnothing)_{\langle\alpha\rangle}| = |V_\varnothing| \ge \max\{1, |I^1_\varnothing|\}$, in which case (4.29) contradicts (4.28). On the other hand, if $I_\varnothing = I_\emptyset$, then $|I_\emptyset \setminus I_\varnothing| = 0$, and (4.29) implies $|X_\emptyset + \Sigma_{\ell_\emptyset}(2(V_\emptyset)^+_{\tau\langle\alpha\rangle})| \ge |I^\alpha_\varnothing| + |I^{\alpha\tau}_\varnothing| + 1 + \ell'_\varnothing \ge |I^\alpha_\varnothing| + |I^{\alpha\tau}_\varnothing| + 1 + \frac{1}{2}|I^\tau_\varnothing| \ge \frac{1}{2}|I^1_\varnothing| + 1$, with the second inequality in view of Claim A. However, this also contradicts (4.28). So we instead conclude that $H_\emptyset$ is nontrivial. We must also have $H_\emptyset$ proper, else $1 \in \pi(V_\emptyset)$, contradicting (4.15). Since $n = |G'|$ is odd, this forces $3 \le |H_\emptyset| \le \frac{n}{3}$.

Let $I^e_\emptyset \subset I_\emptyset$ consist of all indices $i \in I_\emptyset$ such that W_i contains some term from $|G \setminus \tilde{H}_\emptyset|$. Then $\mathrm{supp}(W_i) \subset \tilde{H}_\emptyset$ for all $i \in I_\emptyset \setminus I^e_\emptyset$, while $U_i \cdot W_i^{[-1]} = W_i^U$ is a single term if we additionally have $i \in I^1_\varnothing$. It follows that the remaining term from W_i^U in the product-one sequence U_i must also be from $\tilde{H}_\emptyset$ for $i \in I^1_\varnothing \setminus I^e_\emptyset$. As a result, the atom U contains at least $|I^1_\varnothing \setminus I^e_\emptyset|$ terms from the subgroup $\tilde{H}_\emptyset$, in which case Proposition 4.14 ensures that

$$|I^1_\varnothing \setminus I^e_\emptyset| \le n + |H_\emptyset| - 2. \tag{4.30}$$

In view of (4.17), we have $|(V_\emptyset)_{G\setminus\tilde{H}_\emptyset}| \le |G'/H_\emptyset| - 2$, in which case

$$|I^e_\emptyset| \le |(V_\emptyset)_{G\setminus\tilde{H}_\emptyset}| \le |G'/H_\emptyset| - 2. \tag{4.31}$$

Thus $|I^1_\varnothing| \le n + |H_\emptyset| - 2 + |(V_\emptyset)_{G\setminus\tilde{H}_\emptyset}|$. Averaged with the inequality $2|I^2_\varnothing| + |I^1_\varnothing| \le |U| \le 2n$, we obtain

$$|I_\emptyset| \le |I_\varnothing| + 1 \le \frac{1}{2}\Big(3n - 2 + |H_\emptyset| + |(V_\emptyset)_{G\setminus\tilde{H}_\emptyset}|\Big) + 1 < 2n - \Big(|G'/H_\emptyset| - 1 - |(V_\emptyset)_{G\setminus\tilde{H}_\emptyset}|\Big), \tag{4.32}$$

with the final inequality making use of $3 \le |H_\emptyset| \le \frac{n}{3}$.

Let $I \subset [1, w]$ be a subset containing $I_\emptyset$ with $|I|$ maximal subject to A2 holding,

$$H_\emptyset \le H \quad \text{and} \quad |\pi(V)| \ge |\pi(V_\emptyset)| + |I \setminus I_\emptyset||H_\emptyset|. \tag{4.33}$$

Thus our case hypothesis ensures that A1 fails, allowing us to apply Claim B to conclude I is H_x-constrained. Let $2x+H^+$ and $\mathcal{A} = A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_\ell$ be the coset and setpartition exhibiting that I is constrained,

so $X+\sum_{i=1}^{\ell} A_i = X+\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})$ by (4.16). In view of the second condition in (4.33) and (4.16) (applied to $I_\emptyset$), we have $n \ge |\pi(V)| \ge (|(V_\emptyset)_{G\setminus \tilde{H}_\emptyset}|+1)|H_\emptyset|+|I\setminus I_\emptyset||H_\emptyset|$, and thus $|I\setminus I_\emptyset| \le |G'/H_\emptyset|-1-|(V_\emptyset)_{G\setminus\tilde{H}_\emptyset}|$, with equality only possible if $H^+=\mathbb{Z}/n\mathbb{Z}$. Thus (4.32) implies $|I|=|I_\emptyset|+|I\setminus I_\emptyset|\le 2n-1$. Consequently, if $1\in\pi(V)$, then taking $J=I$ completes the proof as $|I|\le 2n-1$. Therefore we may assume $1\notin\pi(V)$. In particular, H is proper, in which case the previous estimate improves by one: $|I|\le 2n-2$.

If $\mathrm{supp}(U_k)\subset H_x$ for all $i\in[1,w]\setminus I$, then Proposition 4.11 again ensures $1\in\pi(U^{[-1]}\cdot\prod^\bullet_{i\in[1,w]}U_i) = \pi(V\cdot\prod^\bullet_{i\in[1,w]\setminus I}U_i)=\pi(V)$ (as V is H_x-constrained), contrary to assumption. Therefore there must be some $k\in[1,w]\setminus I$ with $\mathrm{supp}(U_k)\not\subseteq H_x$. Let $I_k=I\cup\{k\}$, and let V_k, ℓ_k, X_k, H_k, and I_k^α be the respective quantities V, ℓ, X, H, and I^α for I_k. If $\mathrm{supp}((U_k)^+_{\tau\langle\alpha\rangle})\subset x+H^+$, then (4.16) and Lemma 4.4 imply that $X+\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})$ is a translate of $X+\Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle})$. In particular, $H_\emptyset\le H\le H_k$ (the first inclusion follows from (4.33)). Moreover, there must be be some $g\in\mathrm{supp}((U_k)_{\langle\alpha\rangle})$ with $g\notin H$, and now Kneser's Theorem ensures that $X_k+\Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle})$ is strictly larger in size than $X+\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})$. Since both these sets are $H_\emptyset$-periodic in view of $H_\emptyset\le H\le H_k$, it follows from Proposition 4.5 that $|\pi(V_k)|=|X_k+\Sigma_{\ell_k}(2(V_k)^+_{\tau\langle\alpha\rangle})|\ge|X+\Sigma_\ell(2V^+_{\tau\langle\alpha\rangle})|+|H_\emptyset| = |\pi(V)|+|H_\emptyset|\ge|\pi(V_\emptyset)|+|I_k\setminus I_\emptyset|\,|H_\emptyset|$, with the final inequality from (4.33). Since $g\notin H$, we also have $g\notin L\le H$, so that Kneser's Theorem implies $|X_k|>|X|$, ensuring A2 holds for I_k (as it holds for I). It follows that I_k satisfies (4.33), contradicting the maximality of $|I|$. Therefore we instead conclude that

$$\mathrm{supp}((U_k)^+_{\tau\langle\alpha\rangle})\not\subseteq x+H^+. \tag{4.34}$$

In particular, $(U_k)^+_{\tau\langle\alpha\rangle}$ is not trivial, and hence $\mathrm{supp}(U_k)\not\subset\langle\alpha\rangle$. Thus $I^\alpha=I_k^\alpha$, ensuring that A2 holds for I_k (as it holds for I).

Let $S\mid(V_k)_{\tau\langle\alpha\rangle}$ be a subsequence with $V_{\tau\langle\alpha\rangle}\mid S$, so $S=V_{\tau\langle\alpha\rangle}\cdot T'$ for some $T'\mid(U_k)_{\tau\langle\alpha\rangle}$, for which $|S|=2r$ is maximal subject to there existing a decomposition $S^+=S_1\cdot\ldots\cdot S_r$ with $|S_i|=2$ for all $i\in[1,r]$ and the following holding, where $B_i=\mathrm{supp}(2S_i)$ for $i\in[1,r]$:

D1. $H\le H_S$, where $H_S^+=\mathsf{H}(X+\sum_{i=1}^r B_i)$.

D2. $B_i\cap(2x+H_S^+)\ne\emptyset$ for $i\in[1,r]$.

D3. There is a $j\in[1,r]$ with $|X+\sum_{\substack{i=1\\ i\ne j}}^r B_i| = |X+\sum_{i=1}^r B_i|$.

D4. $\phi_{H_S}(A_i)=\phi_{H_S}(B_i)$ for all $i\in I_S$, where $I_S\subset[1,\ell]$ is the subset of all $i\in[1,\ell]$ with $|\phi_{H_S}(A_i)|=2$.

Note $S=V_{\tau\langle\alpha\rangle}$ satisfies the above conditions with $A_i=B_i$ for all i in view of I being H_x-constrained, so S exists.

Claim C. $S=(V_k)_{\tau\langle\alpha\rangle}$

Proof. Assume by contradiction that $T:=S^{[-1]}\cdot(V_k)_{\tau\langle\alpha\rangle}=(T')^{[-1]}\cdot(U_k)_{\tau\langle\alpha\rangle}$ is nontrivial. Let $H_S^+=\mathsf{H}(X+\sum_{i=1}^r B_i)$. Since $|(V_k)_{\tau\langle\alpha\rangle}|=2\ell_k$ and $|S|=2r$ are both even, it follows that $|T|$ is even, so $|T|\ge 2$. If there is some $y\in\mathrm{supp}(T^+)\cap(x+H_S^+)$, then setting $S_{r+1}=y\cdot z$ and $B_{r+1}=\mathrm{supp}(2S_{r+1})$, where z is any other term from T, we find that D1–D4 hold for $S\cdot y\cdot z$, contradicting the maximality of $|S|$. Therefore we instead conclude that $\mathrm{supp}(T^+)$ is disjoint from $x+H_S^+$. As a result, there is a two-term subsequence $z_1\cdot z_2\mid T^+$ with $z_1,\,z_2\notin x+H_S^+$. Let $j\in[1,r]$ be an index given by D3. Let $y\in\mathrm{supp}(S_j)$ be any element, and define a decomposition $S^+\cdot z_1\cdot z_2=S_1'\cdot\ldots\cdot S_{r+1}'$ and sets $B_i'=\mathrm{supp}(2S_i')$ as follows: $S_j'=S_j\cdot y^{[-1]}\cdot z_1$, $S_{r+1}'=z_2\cdot y$, and $S_i'=S_i$ for $i\ne j,r+1$. In view of D1 and D3 holding for the original decomposition, it follows that $H\le H_S\le H_{S'}$, where $H_{S'}^+=\mathsf{H}(X+\sum_{i=1}^{r+1}B_i')$, so D1 holds for the

new decomposition. Since $|B_i| \le 2$ for all i, Kneser's Theorem and D3 imply that $|\phi_{H_S}(B_j)| = 1$, which combined with D2 ensures $\mathrm{supp}(S_j) \subset x + H_S^+$. Thus D4 holds for the new decomposition as it held for the original decomposition (in view of $H_S \le H_{S'}$), and both terms from S_j lie in $x + H_S^+ \subset x + H_{S'}^+$, ensuring that D2 also holds for the new decomposition. In order not to contradict the maximality of $|S|$, we are left to conclude that D3 fails for the new decomposition. As a result, $|X + \sum_{i=1}^{m} B_i'| > |X + \sum_{i=1}^{m-1} B_i'|$ for all m, ensuring that

$$|X + \sum_{i=1}^{r+1} B_i'| \ge |X| + r + 1 \ge |X| + \ell + 1 \ge |X| + \frac{1}{2}|I_\varnothing^\tau| + |I^\tau \setminus I_\varnothing^\tau| + \frac{1}{2}|I_\varnothing^{\alpha\tau}| + |I^{\alpha\tau} \setminus I_\varnothing^{\alpha\tau}| + 1. \tag{4.35}$$

Let $e_\alpha \ge 0$ be the number of indices $i \in I_\varnothing^\alpha$ for which W_i contains some term lying outside $L_\varnothing$. Since A2/C4 holds for I, arguing as in Claim B when establishing (4.20), we conclude that $|X| \ge |I^\alpha| + (e_\alpha - 1)(|L_\varnothing| - 1) + 1 \ge |I^\alpha| - |L_\varnothing| + 2$. In view of A2/C4 and $X_\varnothing$ being $L_\varnothing$-periodic, we trivially have $|X| \ge |X_\varnothing| + |I^\alpha \setminus I_\varnothing^\alpha| \ge |L_\varnothing| + |I^\alpha \setminus I_\varnothing^\alpha|$, which averaged with the previous bound implies $|X| \ge \frac{1}{2}|I_\varnothing^\alpha| + |I^\alpha \setminus I_\varnothing^\alpha| + 1$. Combined with (4.35), we find

$$|X + \sum_{i=1}^{r+1} B_i'| \ge \frac{1}{2}|I_\varnothing^1| + |I \setminus I_\varnothing| + 2 = \frac{1}{2}|I_\varnothing^1| + |I_k \setminus I_\varnothing| + 1.$$

Since a translate of $X + \sum_{i=1}^{r+1} B_i'$ lies contained in $X + \Sigma_{\ell_k}(2(V_k)^+_{\tau(\alpha)})$, it follows from Proposition 4.5 that $|\pi(V_k)| \ge |X + \Sigma_{\ell_k}(2(V_k)^+_{\tau(\alpha)})| \ge \frac{1}{2}|I_\varnothing^1| + |I_k \setminus I_\varnothing| + 1$, ensuring that A1 holds for I_k. However, since A2/C4 holds for I with $I^\alpha = I_k^\alpha$, it follows that A2 holds for I_k, implying that I_k is ample, contrary to case hypothesis. This completes Claim C. □

In view of Claim C, we have $S = (V_k)_{\tau(\alpha)}$. In particular, $r = \ell_k$. In view of D1 and D2, we can apply Proposition 4.11.1 (with H taken to be H_S^+) to conclude

$$X + \sum_{i=1}^{\ell_k} B_i = X + \Sigma_{\ell_k}(2(V_k)^+_{\tau(\alpha)}). \tag{4.36}$$

In particular, $H_S \le H_k$. In view of (4.36), D1 and D4, we see that $X + \sum_{i=1}^{\ell_k} B_i = X + \Sigma_{\ell_k}(2(V_k)^+_{\tau(\alpha)})$, and thus also $X_k + \Sigma_{\ell_k}(2(V_k)^+_{\tau(\alpha)})$, is H^+-periodic and contains a translate of the H^+-periodic set $X + \sum_{i=1}^{\ell} A_i = X + \Sigma_\ell(2V^+_{\tau(\alpha)})$. If this translate is a proper subset, then

$$|\pi(V_k)| = |X_k + \Sigma_{\ell_k}(2(V_k)^+_{\tau(\alpha)})| \ge |X + \Sigma_\ell(2V^+_{\tau(\alpha)})| + |H| = |\pi(V)| + |H|.$$

Thus (4.33) holds for $I_k = I \cup \{k\}$ as it held for I, with $H_\emptyset \le H \le H_S \le H_k$ following from D1. We already noted above D1–D4 that A2 holds for I_k, so $|I_k|$ contradicts the maximality of $|I|$ in such case. Therefore we instead conclude that $X_k + \sum_{i=1}^{\ell_k} B_i$ is equal to a translate of $X + \sum_{i=1}^{\ell} A_i$. Consequently, since a translate of $X + \Sigma_\ell(2V^+_{\tau(\alpha)}) = X + \sum_{i=1}^{\ell} A_i$ is trivially contained in $X + \Sigma_{\ell_k}(2(V_k)^+_{\tau(\alpha)}) = X + \sum_{i=1}^{\ell_k} B_i \subset X_k + \sum_{i=1}^{\ell_k} B_i$ (the equalities follows from (4.16) and (4.36)), it follows that $X + \sum_{i=1}^{\ell_k} B_i$ is also equal to a translate of $X + \sum_{i=1}^{\ell} A_i$, whence $H_S = H$.

Since $S = (V_k)_{\tau\langle\alpha\rangle}$, we have $S = V_{\tau\langle\alpha\rangle} \cdot (U_k)_{\tau\langle\alpha\rangle}$. Since $H = H_S$ is the stabilizer of both $X + \sum_{i=1}^{\ell_k} B_i$ and $X + \sum_{i=1}^{\ell} A_i$, which are simply translates of each other, Kneser's Theorem combined with D4 ensures this is only possible if the cardinality two sets among $\phi_H(B_1), \ldots, \phi_H(B_{\ell_k})$ are the same as the cardinality two sets among $\phi_H(A_1), \ldots, \phi_H(A_\ell)$. Combined with D2, we conclude that $\phi_H(B_1), \ldots, \phi_H(B_{\ell_k})$ consists of the cardinality two sets from $\phi_H(A_1), \ldots, \phi_H(A_\ell)$ with all other sets equal to $\{\phi_H(2x)\}$. Recall that $A_1 \cdot \ldots \cdot A_\ell$ partitions the terms from $2V^+_{\tau\langle\alpha\rangle}$ by its definition, meaning the terms in sets B_i with $|\phi_H(B_i)| \ge 2$ form a subsequence of $2V^+_{\tau\langle\alpha\rangle}$. Thus $\mathrm{supp}((U_k)^+_{\tau\langle\alpha\rangle}) = \mathrm{supp}((S \cdot V^{[-1]}_{\tau\langle\alpha\rangle})^+) \subset x + H^+$, contradicting (4.34), which completes the case and proof. □

5. On the set of distances and the set of catenary degrees

In this section, we study the set of distances and the set of catenary degrees. Our main result is Theorem 5.1, which substantially uses Theorem 4.1. We recall the definition of catenary degrees and summarize some basic properties of distances and catenary degrees.

Let H be an atomic monoid. For an element $a \in H$, let $\mathsf{c}(a)$ be the smallest $N \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:

> If $z, z' \in \mathsf{Z}(a)$ are two factorizations of a, then there exist factorizations $z = z_0, z_1, \ldots, z_k = z' \in \mathsf{Z}(a)$ such that $\mathsf{d}(z_{i-1}, z_i) \le N$ for each $i \in [1, k]$.

Then $\mathsf{c}(a) = 0$ if and only if $|\mathsf{Z}(a)| = 1$ (i.e., a has unique factorization) and if $|\mathsf{Z}(a)| > 1$, then $2 \le \mathsf{c}(a) \le \sup \mathsf{L}(a)$. Then

$$\mathsf{Ca}(H) = \{\mathsf{c}(a) \mid a \in H \text{ with } \mathsf{c}(a) > 0\} \subset \mathbb{N}_0$$

denotes the *set of (positive) catenary degrees*, and its supremum $\mathsf{c}(H) = \sup \mathsf{Ca}(H)$ is called the *catenary degree* of H (we use the convention that $\sup \emptyset = 0$). It is easy to see that ([14, Proposition 3.6])

$$2 + \max \Delta(H) \le \mathsf{c}(H) \le \omega(H)\,. \tag{5.1}$$

Each of the inequalities can be strict, and the structure of the sets $\Delta(H)$ and $\mathsf{Ca}(H)$ can be quite arbitrary. We mention a couple of results. For every finite set $\Delta \subset \mathbb{N}$ with $\min \Delta = \gcd \Delta$ (recall property (2.2)) there is a finitely generated Krull monoid H with $\Delta(H) = \Delta$ ([16]). For every finite set $C \subset \mathbb{N}_{\ge 2}$, there is a finitely generated Krull monoid H_1 and, if $\max C \ge 3$, a numerical monoid H_2 such that $\mathsf{Ca}(H_1) = \mathsf{Ca}(H_2) = C$ ([36, 10]). On the other hand, sets of distances and sets of catenary degrees are intervals for transfer Krull monoids over finite groups and for classes of seminormal weakly Krull monoids ([21, 18]).

The main result (Theorem 5.1) of the present section states that the set of distances and the set of catenary degrees of $\mathcal{B}(D_{2n})$ are intervals. By Theorem 3.3, $\mathcal{B}(D_{2n})$ is neither transfer Krull nor weakly Krull nor seminormal nor does it have the property studied in [31, Theorem 5.5] enforcing that sets of distances are intervals.

Theorem 5.1. *Let G be a dihedral group of order $2n$, where $n \ge 3$ is odd. Then $\Delta(D_{2n}) = [1, 2n-2]$ and $\mathsf{Ca}(G) = [2, 2n]$.*

We start with a simple lemma.

Lemma 5.2. *Let $n \in \mathbb{N}_{\ge 3}$ be an odd, and $G = \langle \alpha, \tau : \alpha^n = \tau^2 = 1_G \text{ and } \tau\alpha = \alpha^{-1}\tau \rangle$. Then*

$$\begin{aligned}\mathcal{A}\big(\{\alpha, \tau, \alpha\tau\}\big) = &\Big\{\alpha^{[j]} \cdot \tau^{[n-j]} \cdot (\alpha\tau)^{[n-j]} : j \in [0, n]\Big\} \bigcup \\ &\Big\{\alpha^{[2j-1]} \cdot \tau \cdot \alpha\tau : j \in [1, n-1]\Big\} \bigcup \Big\{\alpha^{[2j]} \cdot \tau^{[2]}, \quad \alpha^{[2j]} \cdot (\alpha\tau)^{[2]} : j \in [0, n-1]\Big\}\,.\end{aligned}$$

Proof. First, it is easy to check that the product-one sequences on the right hand side are indeed atoms. Let $S = \alpha^{[k_1]} \boldsymbol{\cdot} \tau^{[k_2]} \boldsymbol{\cdot} (\alpha\tau)^{[k_3]} \in \mathcal{A}\big(\{\alpha, \tau, \alpha\tau\}\big)$, where $k_1, k_2, k_3 \in \mathbbm{N}_0$. It is easily checked that S must have one of the listed forms if $k_2 + k_3 \le 2$. For $k_2 + k_3 > 2$, Lemma 4.7 implies $k_2 = k_3$, say $k_2 = k_3 = n - j$ with $j \in [0, n-2]$. Then w.l.o.g. $S = \alpha^{[k_1-x]} \boldsymbol{\cdot} \alpha\tau \boldsymbol{\cdot} \alpha^{[x]} \boldsymbol{\cdot} \tau \boldsymbol{\cdot} (\alpha\tau \boldsymbol{\cdot} \tau)^{[n-j-1]}$ with $1 = \alpha^{k_1-x} \cdot \alpha\tau \cdot \alpha^x \cdot \tau \cdot (\alpha\tau \cdot \tau)^{n-j-1}$, $0 \le x \le \min\{n-1, k_1\}$ and $k_1 - x \le n - 1$. Since $1 = \alpha^{k_1-x} \cdot \alpha\tau \cdot \alpha^x \cdot \tau \cdot (\alpha\tau \cdot \tau)^{n-j-1} = \alpha^{k_1-2x-j}$, we must have $k_1 - 2x - j \equiv 0 \mod n$. If $x \ge 1$, then $\alpha^{[k_1-x]} \boldsymbol{\cdot} \alpha\tau \boldsymbol{\cdot} \alpha^{[x-1]} \boldsymbol{\cdot} \tau \boldsymbol{\cdot} (\alpha\tau \boldsymbol{\cdot} \tau)^{[n-j-2]}$ and $\alpha \boldsymbol{\cdot} \tau \boldsymbol{\cdot} \alpha\tau$ are both product-one, contradicting that S is an atom. If $x = 0$, then $k_1 - 2x - j \equiv 0 \mod n$ forces $k_1 \equiv j \mod n$. However, as $0 \le k_1 = k_1 - x \le n - 1$ and $j \in [0, n-2]$, this implies $k_1 = j$, and now S has the desired form. □

Proof of Theorem 5.1. Let $n \in \mathbbm{N}_{\ge 3}$ be odd and let $G = \langle \alpha, \tau \,|\, \alpha^n = \tau^2 = 1_G \text{ and } \tau\alpha = \alpha^{-1}\tau \rangle$ be a dihedral group of order $2n$. Clearly, we have that $[1, n-2] = \Delta(C_n) \subset \Delta(G)$ ([13, Theorem 6.7.1]) and $[2, n] \subset \mathsf{Ca}(G)$. We assert that

$$[n-2, 2n-2] \subset \Delta(G) \quad \text{and} \quad [n, 2n] \subset \mathsf{Ca}(G)\,. \tag{5.2}$$

Then Equation (5.1) and Theorem 4.1 imply that

$$2n \le 2 + \max \Delta(G) \le \mathsf{c}(G) \le \omega(G) = 2n\,.$$

Thus it remains to verify the inclusions (5.2).

Let $U = \tau^{[n]} \cdot (\alpha\tau)^{[n]} \in \mathcal{A}(G)$. For every $k \in [0, n]$, we let $U_k = \alpha^{[k]} \cdot \tau^{[n-k]} \cdot (\alpha\tau)^{[n-k]}$. We claim that $\mathsf{L}(U \cdot U_k) = \{2, 2n-k\}$ for all $k \in [0, n]$, and the assertions then follow by definition.

Let $k \in [0, n]$. Since $U \boldsymbol{\cdot} U_k = (\alpha \boldsymbol{\cdot} \tau \boldsymbol{\cdot} \alpha\tau)^{[k]} \boldsymbol{\cdot} (\tau^{[2]})^{[n-k]} \boldsymbol{\cdot} ((\alpha\tau)^{[2]})^{[n-k]}$, we obtain that $\{2, 2n-k\} \subset \mathsf{L}(U \boldsymbol{\cdot} U_k)$. Suppose

$$U \cdot U_k \;=\; \big(\tau^{[n]} \cdot (\alpha\tau)^{[n]}\big) \cdot \big(\alpha^{[k]} \cdot \tau^{[n-k]} \cdot (\alpha\tau)^{[n-k]}\big) \;=\; V_1 \cdot \ldots \cdot V_\ell\,,$$

where $\ell \ge 3$ and $V_1, \ldots, V_\ell \in \mathcal{A}(G)$. If there exists $i \in [1, \ell]$ such that $V_i = \alpha^{[j]} \cdot \tau^{[n-j]} \cdot (\alpha\tau)^{[n-j]}$ for some $j \in [1, k]$, then the remaining sequence is $\alpha^{[k-j]} \boldsymbol{\cdot} \tau^{[n-k+j]} \boldsymbol{\cdot} (\alpha\tau)^{[n-k+j]}$, which is an atom, and hence $\ell = 2$, a contradiction. Thus we may assume by Lemma 5.2 that, for every $i \in [1, \ell]$, $\mathsf{v}_\tau(V_i) + \mathsf{v}_{\alpha\tau}(V_i) = 2$. Therefore $\ell = \frac{n+n+n-k+n-k}{2} = 2n - k$, and hence $\mathsf{L}(U \cdot U_k) = \{2, 2n-k\}$. □

6. On the structure of sets of lengths

For an atomic monoid H, unions of sets of lengths $\mathcal{U}_k(H)$, where $k \in \mathbbm{N}$, and sets of elasticities $\mathcal{R}(H) = \{\rho(L) \colon L \in \mathcal{R}(H)\}$ are well-studied invariants. Under very mild conditions, unions of sets of lengths are almost arithmetical progressions (e.g., [41]). For monoids of product-one sequences, both invariants, unions and sets of elasticities, are as simple as possible, and this is not difficult to obtain. Recall that $\rho_k(H) = \sup \mathcal{U}_k(H)$ and set $\lambda_k(H) = \min \mathcal{U}_k(H)$. If G is a finite group with $|G| \le 2$, then $\mathcal{B}(G)$ is half-factorial, whence

$$\mathcal{L}(G) = \big\{\{k\} \colon k \in \mathbbm{N}_0\big\}\,.$$

Thus, whenever convenient, we will assume that $|G| \ge 3$.

Proposition 6.1. *Let G be a finite group with $|G| \ge 3$.*

1. *For every $k \in \mathbbm{N}$, $\mathcal{U}_k(G)$ is an interval, $\rho_{2k}(G) = k\mathsf{D}(G)$, $k\mathsf{D}(G) + 1 \le \rho_{2k+1}(G) \le (2k+1)\mathsf{D}(G)/2$, and if $|G| > 1$, then $\rho(G) = \mathsf{D}(G)/2$. If G is dihedral of order $2n$ for some odd $n \ge 3$, then, for every $k \ge 2$ and every $\ell \in \mathbbm{N}_0$, $\rho_k(G) = kn$ and*

$$\lambda_{2\ell n + j}(G) = \begin{cases} 2\ell + j & \text{for } j \in [0, 1]\,, \\ 2\ell + 2 & \text{for } j \ge 2 \text{ and } \ell = 0\,, \\ 2\ell + 1 & \text{for } j \in [2, n] \text{ and } l \ge 1\,, \\ 2\ell + 2 & \text{for } j \in [n+1, 2n-1] \text{ and } \ell \ge 1\,, \end{cases}$$

provided that $2\ell n + j \ge 1$.

2. $\{\rho(L)\colon L \in \mathcal{L}(G)\} = \{q \in \mathbb{Q}\colon 1 \le q \le \mathsf{D}(G)/2\}$.

Proof. 1. See [31, Theorem 5.5 and Proposition 5.6] and [34, Theorem 5.4].

2. By 1., we have $\rho(G) = \mathsf{D}(G)/2$. By definition of the elasticity $\rho(G)$ (see Equation (2.4)), we have

$$\{\rho(L)\colon L \in \mathcal{L}(G)\} \subset \{q \in \mathbb{Q}\colon 1 \le q \le \rho(G)\}\,.$$

In order to show that equality holds, we use [43, Theorem 1.2]. By that result, it is sufficient to verify that

$$\inf\{\overline{\rho}(A)\colon 1 \ne A \in \mathcal{B}(G)\} = 1\,, \quad \text{where} \quad \overline{\rho}(A) = \lim_{n\to\infty} \rho(\mathsf{L}(A^{[n]}))\,.$$

If $g \in G$ and $A = g^{[\mathrm{ord}(g)]}$, then $\mathsf{L}(A^{[n]}) = \{n\}$ for every $n \in \mathbb{N}$ whence $\overline{\rho}(A) = 1$ and $\inf\{\overline{\rho}(B)\colon 1 \ne B \in \mathcal{B}(G)\} = 1$. □

In this section, we study the structure of sets of lengths over dihedral groups G. In order to do so, we consider two distinguished subsets of $\Delta(G)$, namely $\Delta^*(G)$ and $\Delta^*_\rho(G)$, which play a crucial role in all structural descriptions of sets of lengths. We start with the definitions of generalizations of arithmetic progressions.

Let $d \in \mathbb{N}$, ℓ, $M \in \mathbb{N}_0$, and $\{0, d\} \subset \mathcal{D} \subset [0, d]$. A subset $L \subset \mathbb{Z}$ is called an

- *almost arithmetical multiprogression* (AAMP) with *difference* d, *period* $\mathcal{D}$, *length* l, and *bound* M, if
$$L = y + (L' \cup L^* \cup L'') \subset y + \mathcal{D} + d\mathbb{Z} \quad \text{where}$$
  - $\min L^* = 0$, $L^* = (\mathcal{D} + d\mathbb{Z}) \cap [0, \max L^*]$, and ℓ is maximal such that $\ell d \in L^*$,
  - $L' \subset [-M, -1]$, $L'' \subset \max L^* + [1, M]$, and
  - $y \in \mathbb{Z}$.
- *almost arithmetical progression* (AAP) with *difference* d, *bound* M, and *length* ℓ, if it is an AAMP with difference d, period $\{0, d\}$, bound M, and length ℓ.

Let H be an atomic monoid. Following [13, Definition 4.3.12], we define

- $\Delta_1(H)$ to be the set of all $d \in \mathbb{N}$ having the following property:
  For every $k \in \mathbb{N}$, there is some $L_k \in \mathcal{L}(H)$ that is an AAP with difference d and length at least k.
- $\Delta^*(H)$ to be the set of all $\min \Delta(S)$ for some divisor-closed submonoid $S \subset H$ with $\Delta(S) \ne \emptyset$.

If H is finitely generated, then by [13, Corollary 4.3.16]

$$\Delta^*(H) \subset \Delta_1(H) \subset \{d_1 \in \Delta(H)\colon d_1 \text{ divides some } d \in \Delta^*(H)\} \subset \Delta(H)\,. \tag{6.1}$$

The significance of the sets $\Delta^*(H)$ and $\Delta_1(H)$ stem from the following result ([13, Theorem 4.4.11]).

Lemma 6.2. *Let H be a finitely generated monoid. Then there is a constant $M \in \mathbb{N}_0$ such that every $L \in \mathcal{L}(H)$ is an* AAMP *with difference $d \in \Delta^*(H)$ and bound M.*

Let G be a finite group. By [31, Lemma 3.3], a submonoid $S \subset \mathcal{B}(G)$ is divisor-closed if and only if $S = \mathcal{B}(G_0)$ for some subset $G_0 \subset G$. As usual, we set $\Delta^*(G) := \Delta^*(\mathcal{B}(G))$. Thus it follows that

$$\Delta^*(G) = \{\min \Delta(G_0)\colon G_0 \subset G \text{ such that } \Delta(G_0) \ne \emptyset\}\,.$$

If $G_1 \subset G_0$ with $\Delta(G_1) \ne \emptyset$, then $\Delta(G_1) \subset \Delta(G_0)$ whence

$$\min \Delta(G_0) = \gcd \Delta(G_0) \mid \gcd \Delta(G_1) = \min \Delta(G_1)\,.$$

Thus there exists a minimal non-half-factorial subset $G_0 \subset G$ with $\max \Delta^*(G) = \min \Delta(G_0)$. The set of minimal distances $\Delta^*(G)$ has found much attention in the literature. If G is finite abelian with $|G| > 2$, then (by [19])

$$\max \Delta^*(G) = \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}\,, \tag{6.2}$$

and $[1, \mathsf{r}(G) - 1] \subset \Delta^*(G)$ (here $\mathsf{r}(G)$ denotes the rank of G). In contrast to $\Delta(G)$, the set $\Delta^*(G)$ is not an interval in general, but there is a characterization when this is the case ([42, Theorem 1.1]). Cross

numbers are a crucial tool in the study of half-factorial and minimal non-half-factorial sets. We start with a simple lemma whose proof runs along the same lines as the proof in the abelian case.

Lemma 6.3. *Let G be a finite group and $G_0 \subset G$ a subset. Then the following statements are equivalent*:
(a) *G_0 is half-factorial.*
(b) *$\mathsf k(U) = 1$ for every $U \in \mathcal A(G_0)$.*
(c) *$\mathsf L(A) = \{\mathsf k(A)\}$ for every $A \in \mathcal B(G_0)$.*

Proof. (a) $\Longrightarrow$ (b) Let $U = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal A(G_0)$ and suppose that $\mathrm{ord}(g_i) = m_i$ for every $i \in [1, \ell]$. For every $i \in [1, \ell]$, we have $U_i = g_i^{[m_i]} \in \mathcal A(G_0)$. We set $m = \mathrm{lcm}(m_1, \ldots, m_\ell)$ and $m = m_i m_i'$ for every $i \in [1, \ell]$. Then $U^{[m]} = U_1^{[m_1']} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} U_\ell^{[m_\ell']}$ and $\mathsf L(U^{[m]}) = \{m\}$ imply that

$$m = m_1' + \ldots + m_\ell' = m\mathsf k(U), \quad \text{whence} \quad \mathsf k(U) = 1\,.$$

(b) $\Longrightarrow$ (c) If $A = U_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} U_m \in \mathcal B(G_0)$, where $m \in \mathbb N$ and $U_1, \ldots, U_m \in \mathcal A(G_0)$, then $m = \mathsf k(U_1) + \ldots + \mathsf k(U_m) = \mathsf k(A)$, whence $\mathsf L(A) = \{\mathsf k(A)\}$.
(c) $\Longrightarrow$ (a) Obvious. □

A subset $G_0 \subset G$ is called an LCN-set if $\mathsf k(U) \ge 1$ for each $U \in \mathcal A(G_0)$. We define

$$\mathsf m(G) = \max\{\min \Delta(G_0) \colon G_0 \subset G \text{ is a non-half-factorial LCN-set}\}\,.$$

Let G be a finite cyclic group and let $g \in G$ with $\mathrm{ord}(g) = |G| \ge 2$. For every product-one sequence $S = g^{[n_1]} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g^{[n_\ell]} \in \mathcal F(G)$, where $\ell \in \mathbb N$ and $n_1, \ldots, n_\ell \in [1, |G|]$, we define its g-norm

$$\|S\|_g = \frac{n_1 + \ldots + n_\ell}{|G|} \in \mathbb N\,.$$

Lemma 6.4. *Let G be a finite group, $G_0 \subset G$ a non-half-factorial subset, and $e \in \mathbb N$ such that $\mathrm{ord}(g) \mid e$ for all $g \in G_0$.*

1. $$\min \Delta(G_0) \mid \gcd\big(e(\mathsf k(U) - 1) \colon U \in \mathcal A(G_0)\big)\,.$$
   In particular, if there is some $U \in \mathcal A(G_0)$ with $\mathsf k(U) < 1$, then $\min \Delta(G_0) \le e - 2$.
2. $\min \Delta(G_0) \le \max\{e - 2, \mathsf m(G)\}$.
3. *If $\langle G_0 \rangle = \langle g \rangle$ for some $g \in G_0$, then $\min \Delta(G_0) = \gcd\big\{\|V\|_g - 1 \colon V \in \mathcal A(G_0)\big\}$.*
4. *Let $g \in G$ with $\mathrm{ord}(g) = n > 3$ and let $a \in [2, n-1]$. If $[a_0, \ldots, a_m]$ is the continued fraction expansion of n/a with odd length (i.e. m is even), then $\min \Delta(\{g, ag\}) = \gcd(a_1, a_3, \ldots, a_{m-1})$.*

Proof. 1. We set $d = \min \Delta(G_0) = \gcd(\Delta(G_0))$ and choose some $U \in \mathcal A(G_0)$. It is sufficient to show that $d \mid e(\mathsf k(U) - 1)$. We set $U = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$. Then $U_i = g_i^{[\mathrm{ord}(g_i)]} \in \mathcal A(G_0)$ for all $i \in [1, \ell]$ and

$$U^{[e]} = \prod\nolimits_{i \in [1,\ell]}^{\bullet} U_i^{[e/\,\mathrm{ord}(g_i)]} \quad \text{implies that} \quad e\mathsf k(U) = \sum_{i=1}^{\ell} \frac{e}{\mathrm{ord}(g_i)} \in \mathsf L(U^{[e]})\,.$$

Since $e \in \mathsf L(U^{[e]})$, we infer that d divides $e\mathsf k(U) - e$.
If $\mathsf k(U) < 1$, then $e\mathsf k(U) \in [2, e-1]$ whence $e - e\mathsf k(U) \in [1, e-2]$ and thus $d \le e - 2$.
2. This follows immediately from 1.
3. follows from [13, Lemma 6.8.5] and 4. from [5, Theorem 2.1]. □

Lemma 6.5. *Let G be a dihedral group of order $2n$ where $n \ge 3$ is odd, say $G = \langle \alpha, \tau \colon \alpha^n = \tau^2 = 1$ and $\alpha\tau = \tau\alpha^{-1} \rangle$. For $U \in \mathcal F(\langle \alpha \rangle)$, define*

$$\phi(U) = \prod\nolimits_{g \in \langle \alpha \rangle}^{\bullet} (g\tau \boldsymbol{\cdot} \tau)^{[\mathsf v_g(U)]}.$$

Then U is an atom if and only if $\phi(U)$ is an atom.

Proof. If U is not an atom, then there is a factorization $U = U_1 \cdot U_2$ with $U_1, U_2 \in \mathcal{B}(G)$ nontrivial product-one sequences. But then $\phi(U) = \phi(U_1) \cdot \phi(U_2)$ is also a factorization of $\phi(U)$ into nontrivial product-one sequences, showing that $\phi(U)$ is not an atom.

For the other direction, assume U is an atom and let $\mathsf{v}_{\alpha^x}(U) = s_x$ for $x \in [1, n]$. Then

$$\sum_{x=1}^{n} s_x x \equiv 0 \mod n \quad \text{and} \quad \sum_{x=1}^{n} s'_x x \not\equiv 0 \mod n$$

for any $s'_x \in [0, s_x]$ with $0 < \sum_{x=1}^{n} s'_x < \sum_{i=1}^{n} s_x$. If we take an arbitrary ordering of the terms of $\phi(U)$, then its product equals α^z with $z \equiv \sum_{x=1}^{n} \big((s_x - s'_x)x - s'_x x\big) \mod n$, where $s'_x \in [0, s_x]$ is the number of terms equal to $\alpha^x\tau$ occurring as the j-th term in the ordering with j even (making $s_x - s'_x$ the number of terms occurring as the j-th term in the ordering with j odd). Thus, in any ordering whose product is one, we must have $0 \equiv \sum_{x=1}^{n} s_x x - 2\sum_{x=1}^{n} s'_x x \equiv -2\sum_{x=1}^{n} s'_x x \mod n$. Since n is odd, this forces $\sum_{x=1}^{n} s'_x x \equiv 0 \mod n$, which is only possible if $s'_x = 0$ for all x, or if $s'_x = s_x$ for all x (as U is an atom). We are left to conclude that, in any ordering of the terms of $\phi(U)$ having product-one, either all terms equal to $g\tau$ with $g \in \operatorname{supp}(U)$ occur at odd places in the ordering, or all occur at even places. From this conclusion, it is now rather immediate that $\phi(U)$ is an atom, completing the proof. □

Proposition 6.6. *Let G be a dihedral group of order $2n$ where $n \ge 3$ is odd, say $G = \langle \alpha, \tau \colon \alpha^n = \tau^2 = 1$ and $\alpha\tau = \tau\alpha^{-1}\rangle$, and let $G_0 = \{\tau, \alpha\tau, \alpha^i\tau\}$, where $i \in [2, n-1]$. Then $\min \Delta^*(G_0)$ divides $\gcd\big(\min \Delta(\{\alpha, \alpha^i\}), \min \Delta(\{\alpha, \alpha^{1-i}\}), \min \Delta(\{\alpha^i, \alpha^{i-1}\})\big)$.*

Proof. We set $d = \min \Delta(G_0)$. Clearly, it is sufficient to show $d \mid \min \Delta(\{\alpha, \alpha^i\})$, $d \mid \min \Delta(\{\alpha, \alpha^{1-i}\})$ and $d \mid \min \Delta(\{\alpha^i, \alpha^{i-1}\})$. Let $d_1 = \min \Delta(\{\alpha, \alpha^i\})$ and let $U_1, \ldots, U_k, V_1, \ldots, V_{k+d_1} \in \mathcal{A}(\{\alpha, \alpha^i\})$ be atoms with $U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_{k+d_1}$. Letting ϕ be as in Lemma 6.5, we have

$$\phi(U_1) \cdot \ldots \cdot \phi(U_k) = \phi(V_1) \cdot \ldots \cdot \phi(V_{k+d_1}) \,,$$

with each of the $\phi(U_j)$ and $\phi(V_j)$ atoms over $\{\tau, \alpha\tau, \alpha^i\tau\}$ (by Lemma 6.5). Since $d = \gcd\big(\Delta(\{\tau, \alpha\tau, \alpha^i\tau\})\big)$, this shows $d \mid d_1$. Using the generating sets $\{\alpha^{-1}, \alpha\tau\}$ and $\{\alpha^{-1}, \alpha^i\tau\}$ in place of $\{\alpha, \tau\}$, we obtain that $\min \Delta(G_0) = \min \Delta(\{\alpha, \alpha\tau, \alpha^i\tau\}) = \min \Delta(\{\alpha\tau, \tau, \alpha^{1-i}\tau\}) = \min \Delta(\{\alpha^i\tau, \alpha^{i-1}\tau, \tau\})$, and now repeating the above arguments likewise shows $d \mid \min \Delta(\{\alpha, \alpha^{1-i}\}))$ and $d \mid \min \Delta(\{\alpha^i, \alpha^{i-1}\})$, completing the proof. □

Theorem 6.7. *Let G be a finite group with $|G| \ge 3$.*

1. *$1 \in \Delta^*(G)$ and $\{\operatorname{ord}(g) - 2 \colon g \in G$ with $\operatorname{ord}(g) \ge 3\} \subset \Delta^*(G)$.*
2. *$\max \Delta^*(G) \le \mathsf{D}(G) - 2$.*
3. *$\max \Delta^*(G) = |G| - 2$ if and only if G is cyclic or a dihedral group of order $2n$ for some odd $n \ge 3$.*
4. *If G is a dihedral group of order $2n$ for some odd $n \ge 3$, then $\{1, 2, n-2, 2n-2\} \subset \Delta^*(G)$ and $\max \Delta^*(G) \setminus \{2n-2\} = \max\{2, n-2\}$.*
5. *If $\max \Delta^*(G) = \mathsf{D}(G) - 2$, then G is cyclic or there is a subgroup $G_1 \subset G$ such that $\mathsf{D}(G_1) = \mathsf{D}(G)$ and G_1 is generated by elements of order two.*

Proof. 1. Suppose there is $g \in G$ with $\operatorname{ord}(g) = n \ge 3$. Since $1 \in \Delta^*(C_n)$ by [13, Proposition 6.8.2], it follows that $1 \in \Delta^*(G)$. Since $\Delta(\{g, g^{-1}\}) = \{\operatorname{ord}(g) - 2\}$, we infer that $\operatorname{ord}(g) - 2 = \min \Delta(\{g, g^{-1}\}) \in \Delta^*(G)$. Suppose that all elements of G have order two. Then G is an elementary 2-group and since $|G| \ge 3$, G has a subgroup isomorphic to $C_2 \oplus C_2$. Then, again by [13, Proposition 6.8.2], we obtain that $1 \in \Delta^*(C_2 \oplus C_2) \subset \Delta^*(G)$.

2. Let $G_0 \subset G$ be a non half-factorial subset. Suppose there exists an atom $A \in \mathcal{A}(G_0)$ such that $\mathsf{k}(A) < 1$. We assume that $\mathsf{k}(A)$ is minimal. Let $A = g_1 \cdot \ldots \cdot g_\ell$, where $\ell \in \mathbb{N}_{\ge 2}$ and $g_1, \ldots, g_\ell \in G_0$.

Since A is product-one, we can index the terms of A such that $g_1 \cdot \ldots \cdot g_\ell = 1$ (and cyclically permuting such an ordering allows $g_1 \in \supp(A)$ to be arbitrary), meaning $(g_2 \cdot \ldots \cdot g_\ell) = g_1^{-1}$, which ensures that $(g_2 \cdot \ldots \cdot g_\ell)^{[\ord(g_1)]}$ is product-one. Hence $g_1^{[\ord(g_1)]}$ divides $A^{[\ord(g_1)]}$, so $A^{[\ord(g_1)]} = U_1 \cdot U_2 \cdot \ldots \cdot U_{\ell_0}$ for some $U_i \in \mathcal{A}(G_0)$ with $U_1 = g_1^{[\ord(g_1)]}$. But then $\mathsf k(U_1) = 1$ and $\mathsf k(U_i) \ge \mathsf k(A)$ (in view of the minimality of $\mathsf k(A)$), whence $\ord(g_1)\mathsf k(A) = \mathsf k(A^{[\ord(g_1)]}) \ge 1 + (\ell_0 - 1)\mathsf k(A) > \ell_0 \mathsf k(A)$, implying $\ell_0 < \ord(g_1)$. It follows that there exists $\ell_0 \in \mathbb N$ with $2 \le \ell_0 < \ord(g_1)$ such that $\{\ord(g_1), \ell_0\} \subset \mathsf L(A^{[\ord(g_1)]})$, which implies that

$$\min \Delta(G_0) \le \ord(g_1) - \ell_0 \le \ord(g_1) - 2 \le \mathsf D(G) - 2\,. \tag{6.3}$$

Suppose $\mathsf k(A) \ge 1$ for all $A \in \mathcal{A}(G_0)$. Since G_0 is not half-factorial, Lemma 6.3 implies there exists $A \in \mathcal{A}(G_0)$ with $\mathsf k(A) > 1$. Let $A = g_1 \cdot \ldots \cdot g_\ell$, where $\ell \in \mathbb N_{\ge 2}$ and $g_1, \ldots, g_\ell \in G_0$, and let $B = g_1^{[\ord(g_1)]} \cdot \ldots \cdot g_\ell^{[\ord(g_\ell)]}$. Then $B \in \mathcal{B}(G_0)$ and A divides B in $\mathcal{B}(G_0)$, so $B = A \cdot U_2 \cdot \ldots \cdot U_{\ell_0}$ for some $U_i \in \mathcal{A}(G_0)$. But now $\ell = \mathsf k(B) = \mathsf k(A) + \mathsf k(U_2) + \ldots + \mathsf k(U_{\ell_0}) > \ell_0$. Therefore there exists $\ell_0 \in [2, \ell - 1]$ such that $\{\ell, \ell_0\} \subset \mathsf L(B)$, which implies that

$$\min \Delta(G_0) \le \ell - \ell_0 \le |A| - 2 \le \mathsf D(G) - 2\,. \tag{6.4}$$

Since G_0 is arbitrary, we obtain $\max \Delta^*(G) \le \mathsf D(G) - 2$.

3.(a). If G is a cyclic group, then $\max \Delta^*(G) = |G| - 2$ by (6.2). Let G be a dihedral group of order $2n$ where $n \ge 3$ is odd, say $G = \langle \alpha, \tau \mid \alpha^n = \tau^2 = 1 \text{ and } \alpha\tau = \tau\alpha^{-1} \rangle$, and set $G_0 = \{\alpha\tau, \tau\}$. Then $\min \Delta(G_0) = 2n - 2 = |G| - 2$ which, together with 2., implies that $\max \Delta^*(G) = |G| - 2$.

3.(b). Suppose $\max \Delta^*(G) = |G| - 2$. Then Item 2. implies that $|G| \le \mathsf D(G)$ whence the assertion follows from Proposition 2.3.

4. Let G be a dihedral group of order $2n$, where $n \ge 3$ is odd, say say $G = \langle \alpha, \tau \,|\, \alpha^n = \tau^2 = 1_G \text{ and } \tau\alpha = \alpha^{-1}\tau \rangle$.

4.(a). Items 1 implies that $\{1, n-2\} \subset \Delta^*(C_n) \subset \Delta^*(G)$ and Item 3 implies that $2n - 2 = |G| - 2 \in \Delta^*(G)$. We assert that $2 = \min \Delta(\{\alpha, \tau\})$. Note that $\mathcal{A}(\{\tau, \alpha\}) = \{\alpha^{[n]}\} \cup \{\alpha^{[2i]} \cdot \tau^{[2]} \colon i \in [0, n-1]\}$. Since $(\alpha^{[n]})^{[2]} \cdot (\tau^{[2]})^{[2]} = (\alpha^{[2n-2]} \cdot \tau^{[2]}) \cdot (\alpha^{[2]} \cdot \tau^{[2]})$, we obtain that $\min \Delta(\{\tau, \alpha\}) \le 4 - 2 = 2$. Suppose $U_1, \ldots, U_k, V_1, \ldots, V_\ell \in \mathcal{A}(\{\tau, \alpha\})$, where $k, \ell \in \mathbb N$ with $k < \ell$, such that $U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_\ell$ and $\{U_1, \ldots, U_k\} \cap \{V_1, \ldots, V_\ell\} = \emptyset$. If $\alpha^{[n]} \notin \{U_1, \ldots, U_k, V_1, \ldots, V_\ell\}$, then $k = \ell = \frac{\mathsf v_\tau(U_1 \cdot \ldots \cdot U_k)}{2}$, a contradiction. Thus $\alpha^{[n]} \in \{U_1, \ldots, U_k, V_1, \ldots, V_\ell\}$. Since $\ell > k$, we obtain $\alpha^{[n]} \in \{V_1, \ldots, V_\ell\}$ and

$$k = \mathsf v_\tau(U_1 \cdot \ldots \cdot U_k)/2 \quad \text{and} \quad \ell = |\{j \in [1, \ell] \colon V_j = \alpha^{[n]}\}| + \mathsf v_\tau(V_1 \cdot \ldots \cdot V_\ell)/2\,.$$

Since $\mathsf v_\alpha(U_1 \cdot \ldots \cdot U_k)$ is even, we infer that $\ell - k = |\{j \in [1, \ell] \colon V_j = \alpha^{[n]}\}|$ is even whence $\min \Delta(\{\alpha, \tau\}) \ge 2$.

4.(b) By 4.(a), it remains to verify $\max \Delta^*(G) \setminus \{2n-2\} \le \max\{2, n-2\}$. Let $G_0 \subset G \setminus \{1\}$ with $|G_0| \ge 2$. If $G_0 \subset \langle \alpha \rangle$, then $\min \Delta(G_0) \le \max \Delta^*(C_n) = n - 2$ by Item 3. Suppose there exists $i \in [0, n-1]$ such that $\alpha^i\tau \in G_0$. If there exists $j \in [1, n-1]$ such that $\alpha^j \in G_0$, then

$$((\alpha^j)^{[n/\gcd(j,n)]})^{[2]} \cdot ((\alpha^i\tau)^{[2]})^{[2]} = \big((\alpha^j)^{[2n/\gcd(j,n)-2]} \cdot (\alpha^i\tau)^{[2]}\big) \cdot \big((\alpha^j)^{[2]} \cdot (\alpha^i\tau)^{[2]}\big)$$

implies that $\min \Delta(G_0) \le 2$. Suppose $G_0 \cap \langle \alpha \rangle = \emptyset$ and hence there exist distinct $i, j \in [0, n-1]$ such that $\{\alpha^i\tau, \alpha^j\tau\} \subset G_0$. If $\gcd(i-j, n) > 1$, then $\min \Delta(G_0) \le \min \Delta(\{\alpha^i\tau, \alpha^j\tau\}) \le \frac{2n}{\gcd(i-j,n)} - 2 < n - 2$. If $\gcd(i-j, n) = 1$, then choosing a different basis if necessary, we may assume that $\tau, \alpha\tau \in G_0$. If $G_0 = \{\tau, \alpha\tau\}$, then $\min \Delta(G_0) = 2n - 2$. Suppose there exists $r \in [2, n-1]$ such that $\alpha^r\tau \in G_0$. By Proposition 6.6 and Lemma 6.4.3, we obtain that $\min \Delta(G_0) \le \|(\alpha^r)^{[n]}\|_\alpha - 1 = r - 1 \le n - 2$.

5. Let $G_0 \subset G$ be a non half-factorial subset such that $\min \Delta(G_0) = \mathsf D(G) - 2$. If there exists an atom $A \in \mathcal{A}(G_0)$ such that $\mathsf k(A) < 1$, then (6.3) implies that there is $g \in G_0$ with $\ord(g) = \mathsf D(G)$ and hence G is cyclic.

Suppose $\mathsf k(A) \ge 1$ for all $A \in \mathcal{A}(G_0)$. Then (6.4) implies that there exists $A = g_1 \cdot \ldots \cdot g_{\mathsf D(G)} \in \mathcal{A}(G_0)$ such that $B = g_1^{[\ord(g_1)-1]} \cdot \ldots \cdot g_{\mathsf D(G)}^{[\ord(g_{\mathsf D(G)})-1]}$ is an atom. Hence $\ord(g_i) = 2$ for all $i \in [1, \mathsf D(G)]$, else $|B| > \mathsf D(G)$. Then $G_1 = \langle g_1, \ldots, g_{\mathsf D(G)} \rangle$ is a subgroup satisfying the assertion. □

If G is a dihedral group of order $2n$, then G has a cyclic subgroup of order n whence $\Delta^*(C_n) \subset \Delta^*(G)$. The set $\Delta^*(G)$ for finite cyclic groups is studied in detail in [37]. If G is finite cyclic, then, by Theorem 6.7, we have $\max \Delta^*(G) = |G| - 2$. The second largest value of $\Delta^*(G)$ equals $\lfloor |G|/2 \rfloor - 1$.

Next we look at the structure of (long) sets of lengths having maximal elasticity. To do so, we define two further subsets of the set of distances. Let H be an atomic monoid. Following ([20, Definition 2.1 and Lemma 2.2], we define

- $\Delta_\rho(H)$ to be the set of all $d \in \mathbb{N}$ having the following property:
  For every $k \in \mathbb{N}$, there is some $L_k \in \mathcal{L}(H)$ that is an AAP with difference d and length at least k.
- $\Delta^*_\rho(H) = \{\min \Delta(\mathsf{L}(a)) \colon a \in H \text{ with } \rho(\mathsf{L}(a)) = \rho(H)\}$.

If H is finitely generated and $\Delta(H) \neq \emptyset$, then by [20, Lemma 2.4]

$$\Delta^*_\rho(H) \subset \Delta_\rho(H) \subset \{d_1 \in \Delta(H) \colon d_1 \text{ divides some } d \in \Delta^*_\rho(H)\}\,. \tag{6.5}$$

Let G be a finite group. Every divisor-closed submonoid of $\mathcal{B}(G)$ is generated by one element and all divisor-closed submonoids $S \subset \mathcal{B}(G)$ are of the form $S = \mathcal{B}(G_0)$ for a subset $G_0 \subset G$. Consistent with our conventions, we set $\Delta_\rho(G) := \Delta_\rho(\mathcal{B}(G))$ and $\Delta^*_\rho(G) := \Delta^*_\rho(\mathcal{B}(G))$, and we have (by using [20, Lemma 2.2.3] and that $\rho(G) = \mathsf{D}(G)/2$)

$$\Delta^*_\rho(G) = \{\min \Delta(G_0) \colon G_0 \subset G \text{ with } \rho(G_0) = \mathsf{D}(G)/2\} \subset \Delta^*(G)\,.$$

Before we formulate our main result on $\Delta^*_\rho(G)$ for dihedral groups G, we briefly summarize what is known on $\Delta^*_\rho(G)$ for abelian groups. Let G be a finite abelian group with $|G| \ge 3$. If G is an elementary 2-group of rank r, then $\Delta^*_\rho(G) = \Delta_\rho(G) = \{1, r-1\}$. If G is neither cyclic nor an elementary 2-group, then the standing conjecture states that $\Delta_\rho(G) = \{1\}$. If G is cyclic with $|G| > 10$, then $\{1, |G|-2\} \subset \Delta^*_\rho(G) = \Delta_\rho(G)$ and the precise form of $\Delta_\rho(G)$ depends on number theoretic properties of the group order $|G|$ ([20]). Thus it is no surprise that the similar phenomena occur for dihedral groups.

Theorem 6.8. *Let G be a dihedral group of order $2n$, where $n \ge 3$ is odd, say $G = \langle \alpha, \tau \colon \alpha^n = \tau^2 = 1 \text{ and } \alpha\tau = \tau\alpha^{-1} \rangle$.*

1. $\{1, 2n-2\} \subset \Delta^*_\rho(G)$ *and* $\max \Delta^*_\rho(G) \setminus \{2n-2\} \le \max\{1, \frac{n-1}{4}\}$.
2. *If there exists $i \in [2, n-1]$ with $\gcd(i, n) = 1$ such that*

$$\gcd\big(\min \Delta(\{\alpha, \alpha^i\}),\ \min \Delta(\{\alpha, \alpha^{1-i}\}),\ \min \Delta(\{\alpha^i, \alpha^{i-1}\})\big) \quad \text{is even,} \qquad (*)$$

then $\Delta^*_\rho(G) \supsetneq \{1, 2n-2\}$, and $(*)$ holds, for example, if $n = m^2 - m + 1$ for some odd $m \ge 3$.

Proof. 1.(i) Let $U_1 = \alpha^{[2n-2]} \cdot \tau^{[2]}$, $U_2 = (\alpha\tau)^{[n]} \cdot \tau^{[n]}$. Then $U_1, U_2 \in \mathcal{A}(G)$ with $|U_1| = |U_2| = 2n = \mathsf{D}(G)$. Since $\rho(\mathsf{L}(U_1 \cdot U_1^{-1})) = \rho(\mathsf{L}(U_2^{[2]})) = \rho(G)$, we obtain $\min \Delta(\mathrm{supp}(U_1 \cdot U_1^{-1})) = \min \Delta(\{\alpha, \alpha^{-1}, \tau\}) \in \Delta^*_\rho(G)$ and $\min \Delta(\mathrm{supp}(U_2^{[2]})) = \min \Delta(\{\alpha\tau, \tau\}) = 2n - 2 \in \Delta^*_\rho(G)$

Since $\alpha^{[n]} \cdot (\alpha^{-1})^{[n]} = (\alpha \cdot \alpha^{-1})^{[n]}$ and $\alpha^{[n]} \cdot \alpha^{[n]} \cdot \tau^{[2]} \cdot \tau^{[2]} = (\alpha^{[2n-2]} \cdot \tau^{[2]}) \cdot (\alpha^{[2]} \cdot \tau^{[2]})$, we obtain that $\min \Delta(\{\alpha, \alpha^{-1}, \tau\}) \mid \gcd(n-2, 2) = 1$ which implies that $\min \Delta(\{\alpha, \alpha^{-1}, \tau\}) = 1 \in \Delta^*_\rho(G)$.

1.(ii) Let $d = \max \Delta^*_\rho(G) \setminus \{2n-2\}$. Then there exist $G_0 \subset G$ and $W \in \mathcal{B}(G_0)$ with $d = \min \Delta(G_0)$ and $G_0 = \mathrm{supp}(W)$ such that $\rho(\mathsf{L}(W)) = \frac{\mathsf{D}(G)}{2} = n$. Therefore there are atoms $U_1, \ldots, U_k$ of length $2n$ and atoms $V_1, \ldots, V_{kn}$ of length 2 such that $W = U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_{kn}$. Thus if $a \in \mathrm{supp}(W)$, then $a^{-1} \in \mathrm{supp}(W)$.

If there exists $i \in [1, k]$ such that $U_i = (\alpha^{k_1})^{[2n-2]} \cdot (\alpha^{k_2}\tau)^{[2]}$, where $\gcd(k_1, n) = 1$, then $\{\alpha^{k_1}, \alpha^{-k_1}, \alpha^{k_2}\tau\} \subset G_0$ and hence $d \mid \min \Delta(\{\alpha^{k_1}, \alpha^{-k_1}, \alpha^{k_2}\tau\}) = \min \Delta(\{\alpha, \alpha^{-1}, \tau\}) = 1$. By Proposition 2.4, we may assume that for all $i \in [1, k]$, there are $k_i, t_i \in [0, n-1]$ with $\gcd(k_i - t_i, n) = 1$ such that $U_i = (\alpha^{k_i}\tau)^{[n]} \cdot (\alpha^{t_i}\tau)^{[n]}$. Changing a different basis if necessary, we may assume that $U_1 = \tau^{[n]} \cdot (\alpha\tau)^{[n]}$. If $U_i = U_1$ for all $i \in [2, k]$, then $G_0 = \{\tau, \alpha\tau\}$ and $d = 2n - 2$, a contradiction. Otherwise there is $r \in [2, n-1]$ such that $\{\tau, \alpha\tau, \alpha^r\tau\} \subset G_0$. By Proposition 6.6 and Lemma 6.4.3, we obtain that

$d \mid \gcd(\|(\alpha^r)^{[n]}\|_\alpha - 1, \|(\alpha^{n+1-r})^{[n]}\|_\alpha - 1) = \gcd(r-1, n-r)$ and hence $d < n-1$. If $d = \frac{n-1}{2} \ge 2$, then $r - 1 = n - r = \frac{n-1}{2}$. Since the continued fraction of n/r is $[1; 1, r-1]$, it follows by Lemma 6.4.4 that $\min \Delta(\{\alpha, \alpha^r\}) = 1$ and hence $d = 1$, a contradiction. Suppose $d = \frac{n-1}{3} \ge 2$. Then $r-1 = 2(n-r) = 2\frac{n-1}{3}$ or $n - r = 2(r-1) = 2\frac{n-1}{3}$.

If $r - 1 = 2(n-r)$, then $2n = 3r - 1$ and hence the continued fraction of $n/(n+1-r)$ is $[2; 1, \frac{r-3}{4}]$ or $[2; 1, \frac{r-5}{4}, 1, 1]$. It follows by Lemma 6.4.4 that $\min \Delta(\{\alpha, \alpha^{1-r}\}) = 1$ and hence $d = 1$, a contradiction.

If $n - r = 2(r-1)$, then $n = 3r - 2$ and hence the continued fraction of n/r is $[2; 1, \frac{r-3}{2}, 1, 1]$. It follows by Lemma 6.4.4 that $\min \Delta(\{\alpha, \alpha^r\}) = 1$ and hence $d = 1$, a contradiction.

Therefore, we obtain that $d \le \frac{n-1}{4}$.

2.(i) Let $i \in [2, i-1]$ with $\gcd(i, n) = 1$ such that

$$\gcd\big(\min \Delta(\{\alpha, \alpha^i\}),\ \min \Delta(\{\alpha, \alpha^{1-i}\}),\ \min \Delta(\{\alpha^i, \alpha^{i-1}\})\big)$$

is even. Since $U = (\alpha\tau \cdot \tau)^{[n]}$ and $V = (\alpha^i\tau \cdot \tau)^{[n]}$ are atoms of length $\mathsf D(G)$, then $\rho(\mathsf L(U^{[2]} \cdot V^{[2]})) = \rho(G)$ and hence $d = \min \Delta(\{\tau, \alpha\tau, \alpha^i\tau\}) \in \Delta^*_\rho(G)$. By 1., it suffices to show $d \ne 1$ and $d \ne 2n-2$.

Let $W = (\alpha\tau \cdot \tau^{[n-i]}) \cdot \alpha^i\tau \cdot \tau$. Then W is an atom of Type III. Since $W^{[n]} = ((\alpha\tau \cdot \tau)^{[n]})^{[n-i]} \cdot (\alpha^i\tau \cdot \tau)^{[n]}$, we obtain that $d \mid n - (n-i+1) = i - 1$ which implies that $i < 2n - 2$.

Assume to the contrary that $d = 1$. Then there are atoms $U_1, \ldots, U_k, V_1, \ldots, V_{k+1}$ over $\{\tau, \alpha\tau, \alpha^i\tau\}$ such that

$$U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_{k+1}\,.$$

We assert that if $A \in \mathcal A(\{\tau, \alpha\tau, \alpha^i\tau\})$, then $|A| \equiv 2 \pmod 4$. Suppose this holds. Then $2k \equiv 2(k+2) \pmod 4$, a contradiction. Thus we only need to show the assertion. Note that $(\alpha^i)^{[n]}$ is an atom. Since $\min \Delta(\{\alpha, \alpha^i\})$ is even, it follows by Lemma 6.4.3 that $i = \|(\alpha^i)^{[n]}\|_\alpha$ is odd. If A is of Type I or Type II, the assertion follows by n is odd. If A is of Type III, say $A = (\alpha\tau \cdot \tau)^{[x]} \cdot (\alpha^i\tau \cdot \tau)^{[y]}$, then $\alpha^{[x]} \cdot (\alpha^{1-i})^{[y]}$ is an atom and by Lemma 6.4.3 that $\|\alpha^{[x]} \cdot (\alpha^{1-i})^{[y]}\|_\alpha = \frac{x+iy}{n}$ is odd. Therefore $x + y \equiv 1 \pmod 2$ and $|A| = 2x + 2y \equiv 2 \pmod 4$. If A is of Type IV, say $A = (\alpha\tau \cdot \tau)^{[x]} \cdot (\alpha\tau \cdot \alpha^i\tau)^{[y]}$, then $\alpha^{[x]} \cdot (\alpha^{1-i})^{[y]}$ is an atom. Since $\min \Delta(\{1, 1-i\})$ is even, it follows by Lemma 6.4.3 that $\|\alpha^{[x]} \cdot (\alpha^{1-i})^{[y]}\|_\alpha = \frac{x+(n+1-i)y}{n}$ is odd. Therefore $x + y \equiv 1 \pmod 2$ and $|A| = 2x + 2y \equiv 2 \pmod 4$. If A is of Type V, say $A = (\alpha^i\tau \cdot \alpha\tau)^{[x]} \cdot (\alpha^i\tau \cdot \tau)^{[y]}$, then $(\alpha^{i-1})^{[x]} \cdot (\alpha^{1-i})^{[y]}$ is an atom. Let $j \in [1, n-1]$ such that $ij \equiv 1 \pmod n$. Then j is odd, $\min \Delta(\{\alpha^i, \alpha^{i-1}\}) = \min \Delta(\{\alpha, \alpha^{n+1-j}\})$ is even, and $\alpha^{[x]} \cdot (\alpha^{1-j})^{[y]}$, $(\alpha^{1-j})^{[n/\gcd(1-j,n)]}$ are both atoms. Thus Lemma 6.4.3 implies that $\|\alpha^{[x]} \cdot (\alpha^{n+1-j})^{[y]}\|_\alpha = \frac{x+(n+1-j)y}{n}$ and $\|(\alpha^{1-j})^{[n/\gcd(1-j,n)]}\|_\alpha = n(n+1-j)/\gcd(1-j, n)$ are odd. Therefore $x + y \equiv 1 \pmod 2$ and $|A| = 2x + 2y \equiv 2 \pmod 4$.

2.(ii) For the "in particular" part, let $n = x^2 - x + 1$ for some odd $x \in \mathbb N$. Then $\gcd(n, x) = 1$. Since $\alpha^{x-1} = (\alpha^x)^x$, we have $\min \Delta(\{\alpha^x, \alpha^{x-1}\}) = \min \Delta(\{\alpha, \alpha^x\})$. Since the continued fraction of n/x with odd length is $[x-1; x-1, 1]$ and the continued fraction of $n/(n+1-x)$ with odd length is $[1; x-1, x-1]$, it follows by Lemma 6.4.4 that $\gcd(\min \Delta(\{\alpha, \alpha^x\}), \min \Delta(\{\alpha, \alpha^{1-x}\})) = x - 1$ is even. Therefore $\Delta^*_\rho(G_0) \supsetneq \{1, 2n-2\}$. □

Remark 6.9. Let G be a dihedral group of order $2n$, where $n \ge 3$ is odd, say $G = \langle \alpha, \tau \colon \alpha^n = \tau^2 = 1 \text{ and } \alpha\tau = \tau\alpha^{-1} \rangle$. If, for all $i \in [2, n-1]$, we have

$$\gcd(\min \Delta(\{\alpha, \alpha^i\}), \min \Delta(\{\alpha, \alpha^{1-i}\}), \min \Delta(\{\alpha^{i-1}, \alpha^i\})) = 1\,, \tag{6.6}$$

then a similar proof as that of Theorem 6.8.1 shows that $\max \Delta^*_\rho(G) \setminus \{2n-2\} = 1$ and hence $\Delta^*_\rho(G) = \{1, 2n-2\}$. By Lemma 6.4, we can use continued fraction expansions to check Condition 6.6 and (within a few minutes of computer calculations) one gets the list of all $n \in [5, 10000]$ with $\Delta^*_\rho(G) = \{1, 2n-2\}$.

Corollary 6.10. *Let G be a dihedral group of order $2n$ where $n \ge 3$ is odd. Then*

$$2 + \max \Delta^*_\rho(G) = 2 + \max \Delta^*(G) = 2 + \max \Delta(G) = \mathsf c(G) = \omega(G) = 2n = \mathsf D(G) = |G|\,.$$

Proof. We have $\Delta^*_\rho(G) \subset \Delta^*(G) \subset \Delta(G)$. Proposition 6.8 implies that $2n \le 2 + \max \Delta^*_\rho(G)$. Thus the assertion follows from Theorems 4.1 and 5.1. □

Consider a class $\mathcal{C}$ of atomic monoids or domains (say orders in algebraic number fields, Krull monoids, or monoids of product-one sequences). Arithmetical investigations of objects from $\mathcal{C}$ are always done with respect to the following aims and questions.

- Are the arithmetical invariants of two objects H_1 and H_2 in $\mathcal{C}$ characteristic for H_1 and H_2? To pick a prominent question of this type, let G_1 and G_2 be two finite abelian groups, say with $|G_1| > 4$. The standing conjecture states that $\mathcal{L}(G_1) = \mathcal{L}(G_2)$ implies that G_1 and G_2 are isomorphic (see [22] for an overwiew).
- To what extent is the arithmetic of an object H in $\mathcal{C}$ distinct from the arithmetic of objects of a further class $\mathcal{C}'$?

In our final result (Corollary 6.12) we demonstrate that our results on the arithmetic of $\mathcal{B}(D_{2n})$, where $n \ge 3$ is odd, are strong enough to settle questions of the above type. We start with a lemma.

Lemma 6.11. *Let G_1 and G_2 be finite groups such that $\mathcal{L}(G_1) = \mathcal{L}(G_2)$.*

1. *$\Delta(G_1) = \Delta(G_2)$, $\mathcal{U}_k(G_1) = \mathcal{U}_k(G_2)$ for all $k \in \mathbb{N}$.*
2. *For every $k \in \mathbb{N}$ we have $\rho_k(G_1) = \rho_k(G_2)$ and $\mathsf{D}(G_1) = \mathsf{D}(G_2)$.*
3. *$\max \Delta^*(G_1) = \max \Delta^*(G_2)$ and $\max \Delta^*_\rho(G_1) = \max \Delta^*_\rho(G_2)$.*

Proof. 1. Since $\mathcal{L}(G_1) = \mathcal{L}(G_2)$, this follows from Equations (2.1) and (2.3).

2. This follows from 1. and from Proposition 6.1.1.

3. Since $\mathcal{L}(G_1) = \mathcal{L}(G_2)$, it follows that $\Delta_1(G_1) = \Delta_2(G_2)$ and $\Delta_\rho(G_1) = \Delta_\rho(G_2)$. Thus (6.1) and (6.5) imply that

$$\max \Delta^*(G_1) = \max \Delta_1(G_1) = \max \Delta_1(G_2) = \max \Delta^*(G_2) \quad \text{and}$$
$$\max \Delta^*_\rho(G_1) = \max \Delta_\rho(G_1) = \max \Delta_\rho(G_2) = \max \Delta^*_\rho(G_2)\,. \quad \square$$

A monoid H is said to be strongly primary if $H \neq H^\times$ and, for each $a \in H \setminus H^\times$, there is some $n \in \mathbb{N}$ such that $(H \setminus H^\times)^n \subset aH$. Numerical monoids and the multiplicative monoids of nonzero elements of local one-dimensional noetherian domains are strongly primary. Every strongly primary monoid is weakly Krull, whence $\mathcal{B}(D_{2n})$ is not strongly primary by Theorem 3.3.

Corollary 6.12. *Let $n \ge 3$ be odd.*

1. *If $m \in \mathbb{N}_{\ge 3}$ with $m \neq n$, then $\mathcal{L}(D_{2n}) \neq \mathcal{L}(D_{2m})$.*
2. *If G is a finite nilpotent group but not a non-abelian 2-group, then $\mathcal{L}(D_{2n}) \neq \mathcal{L}(G)$.*
3. *If H is a strongly primary monoid, then $\mathcal{L}(D_{2n}) \neq \mathcal{L}(H)$.*

Proof. 1. Let $m \in \mathbb{N}_{\ge 3}$ with $m \neq n$ and assume to the contrary that $\mathcal{L}(D_{2n}) = \mathcal{L}(D_{2m})$. Then Lemma 6.11 and Corollary 6.10 imply that $2n = \mathsf{D}(D_{2n}) = \mathsf{D}(D_{2m})$ and $2n-2 = \max \Delta^*_\rho(D_{2n}) = \max \Delta^*_\rho(D_{2m})$. If m is odd, then $2n = \mathsf{D}(D_{2m}) = 2m$, a contradiction. Thus $m \ge 4$ is even. Let $G = D_{2m}$ and let U be an atom of length $\mathsf{D}(G)$ over G. By [34, Theorem 4.2], there exist $\alpha, \tau \in G$ with $G = \langle \alpha, \tau \colon \alpha^m = \tau^2 = 1, \tau\alpha = \alpha^{-1}\tau \rangle$ such that $U = \alpha^{[3m/2-2]} \cdot \tau \cdot \alpha^{m/2}\tau$. It follows by the definition of $\Delta^*_\rho(G)$ that

$$\max \Delta^*_\rho(G) = \min \Delta(\{\mathrm{supp}(U \cdot U^{-1})\}) \le \min \Delta(\{\alpha, \alpha^{-1}\}) = m - 2 < \mathsf{D}(G) - 2 = \max \Delta^*_\rho(D_{2n})\,,$$

a contradiction.

2. Let G be a finite nilpotent group such that $\mathcal{L}(G) = \mathcal{L}(D_{2n})$. Then G is not abelian by [32, Theorem 4.4]. Thus Theorem 6.7 implies $\max \Delta^*(G) = \max \Delta^*(D_{2n}) = \mathsf{D}(D_{2n}) - 2 = \mathsf{D}(G) - 2$, and hence G has a subgroup G_1 with $\mathsf{D}(G_1) = \mathsf{D}(G)$ such that G_1 is generated by elements of order 2. Since G_1 is also a nilpotent group, it follows that G_1 is a 2-group by [30, Corollary 2.4]. Thus Lemma 2.2.2 implies that G is a 2-group.

3. Let H be a strongly primary monoid. Then Proposition 6.2 and [17, Theorem 5.5] show that the set of elasticities $\{\rho(L) \colon L \in \mathcal{L}(H)\}$ and $\{\rho(L) \colon L \in \mathcal{L}(G)\}$ are distinct, whence $\mathcal{L}(H) \neq \mathcal{L}(G)$. □

References

[1] D.D. Anderson, D.F. Anderson, and M. Zafrullah, *Atomic domains in which almost all atoms are prime*, Commun. Algebra **20** (1992), 1447 – 1462.

[2] D.D. Anderson and J.L. Mott, *Cohen-Kaplansky domains: integral domains with a finite number of irreducible elements*, J. Algebra **148** (1992), 17 – 41.

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

[4] F.E. Brochero Martínez and S. Ribas, *Extremal product-one free sequences in Dihedral and Dicyclic Groups*, Discrete Math. **341** (2018), 570 – 578.

[5] S. Chang, S.T. Chapman, and W.W. Smith, *On minimum delta set values in block monoids over cyclic groups*, Ramanujan J. **14** (2007), 155 – 171.

[6] K. Cziszter, *The Noether number of p-groups*, J. Algebra Appl. **18** (2019), no. 4, 1950066, 14.

[7] K. Cziszter and M. Domokos, *The Noether number for the groups with a cyclic subgroup of index two*, J. Algebra **399** (2014), 546 – 560.

[8] K. Cziszter, M. Domokos, and A. Geroldinger, *The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics*, in Multiplicative Ideal Theory and Factorization Theory, Springer, 2016, pp. 43 – 95.

[9] K. Cziszter, M. Domokos, and I. Szöllősi, *The Noether number and the Davenport constants of the groups of order less than* 32, J. Algebra **510** (2018), 513 – 541.

[10] Y. Fan and A. Geroldinger, *Minimal relations and catenary degrees in Krull monoids*, J. Commut. Algebra **11** (2019), 29 – 47.

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

[12] A. Geroldinger and D.J. Grynkiewicz, *The large Davenport constant I: Groups with a cyclic index* 2 *subgroup*, J. Pure Appl. Algebra **217** (2013), 863 – 885.

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

[14] A. Geroldinger and F. Kainrath, *On the arithmetic of tame monoids with applications to Krull monoids and Mori domains*, J. Pure Appl. Algebra **214** (2010), 2199 – 2218.

[15] A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics - CRM Barcelona, Birkhäuser, 2009.

[16] A. Geroldinger and W.A. Schmid, *A realization theorem for sets of distances*, J. Algebra **481** (2017), 188 – 198.

[17] A. Geroldinger and W.A. Schmid and Q. Zhong, *Systems of sets of lengths: transfer Krull monoids versus weakly Krull monoids*, in Rings, Polynomials, and Modules, 191 – 235, Springer, 2017.

[18] A. Geroldinger and Q. Zhong, *The set of distances in seminormal weakly Krull monoids*, J. Pure Appl. Algebra **220** (2016), 3713 – 3732.

[19] ———, *The set of minimal distances in Krull monoids*, Acta Arith. **173** (2016), 97 – 120.

[20] ———, *Long sets of lengths with maximal elasticity*, Can. J. Math. **70** (2018), 1284 – 1318.

[21] ———, *Sets of arithmetical invariants in transfer Krull monoids*, J. Pure Appl. Algebra **223** (2019), 3889 – 3918.

[22] ———, *Factorization theory in commutative monoids*, https://arxiv.org/abs/1907.09869.

[23] D.J. Grynkiewicz, *Representing sequence subsums as sumsets of near equal sized sets*, https://arxiv.org/abs/1910.11807.

[24] ———, *On an extension of the Erdős-Ginzburg-Ziv Theorem to hypergraphs*, Eur. J. Comb. **26** (2005), 1154 – 1176.

[25] ———, *The large Davenport constant II: General upper bounds*, J. Pure Appl. Algebra **217** (2013), 2221 – 2246.

[26] ———, *Structural Additive Theory*, Developments in Mathematics 30, Springer, Cham, 2013.

[27] F. Halter-Koch, *Ideal Systems. An Introduction to Multiplicative Ideal Theory*, Marcel Dekker, 1998.

[28] Dongchun Han, *The Erdős-Ginzburg-Ziv Theorem for finite nilpotent groups*, Archiv Math. **104** (2015), 325 – 332.

[29] Dongchun Han and Hanbin Zhang, *The Erdős-Ginzburg-Ziv Theorem and Noether number for* $C_m \ltimes C_{mn}$, J. Number Theory **198** (2019), 159 – 175.

[30] L. L. Grunenfelder, T. Košir, M. Omladič, and H. Radjavi, *On groups generated by elements of prime order*, Geom. Dedicata **75** (1999), no. 3, 317–332.

[31] J.S. Oh, *On the algebraic and arithmetic structure of the monoid of product-one sequences*, J. Commut. Algebra, to appear, https://projecteuclid.org/euclid.jca/1523433705.

[32] ———, *On the algebraic and arithmetic structure of the monoid of product-one sequences II*, Periodica Math. Hungarica **78** (2019), 203 – 230.

[33] J.S. Oh and Q. Zhong, *On Erdős-Ginzburg-Ziv inverse theorems for dihedral and dicyclic groups*, Israel J. Math., to appear, https://arxiv.org/abs/1904.13171.

[34] ———, *On minimal product-one sequences of maximal length over dihedral and dicyclic groups*, Communications of the Korean Math. Soc., to appear, http://ckms.kms.or.kr/journal/view.html?doi=10.4134/CKMS.c190013.

[35] 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.
[36] C. O'Neill and R. Pelayo, *Realisable sets of catenary degrees of numerical monoids*, Bull. Australian Math. Soc. **97** (2018), 240 – 245.
[37] A. Plagne and W.A. Schmid, *On congruence half-factorial Krull monoids with cyclic class group*, Journal of Combinatorial Algebra, to appear.
[38] B.J. Schmid, *Finite groups and invariant theory*, Topics in Invariant Theory, Lecture Notes in Mathematics, vol. 1478, Springer, 1991, pp. 35 – 66.
[39] W.A. Schmid, *The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups*, Electron. J. Comb. **18(1)** (2011), Research Paper 33.
[40] ———, *Some recent results and open problems on sets of lengths of Krull monoids with finite class group*, in Multiplicative Ideal Theory and Factorization Theory, Springer, 2016, pp. 323 – 352.
[41] S. Tringali, *Structural properties of subadditive families with applications to factorization theory*, Israel J. Math., to appear, https://arxiv.org/abs/1706.03525.
[42] Q. Zhong, *Sets of minimal distances and characterizations of class groups of Krull monoids*, Ramanujan J. **45** (2018), 719 – 737.
[43] ———, *On elasticities of locally finitely generated monoids*, J. Algebra **534** (2019), 145–167.

University of Graz, NAWI Graz, Institute for Mathematics and Scientific Computing, Heinrichstrasse 36, 8010 Graz, Austria
Email address: alfred.geroldinger@uni-graz.at, junseok.oh@uni-graz.at, qinghai.zhong@uni-graz.at
URL: https://imsc.uni-graz.at/geroldinger, https://imsc.uni-graz.at/zhong/

University of Memphis, Department of Mathematical Sciences, Memphis, TN 38152, USA
Email address: diambri@hotmail.com