ON THE ALGEBRAIC AND ARITHMETIC STRUCTURE OF THE MONOID OF PRODUCT-ONE SEQUENCES

JUN SEOK OH

ABSTRACT. Let G be a finite group. A finite unordered sequence $S = g_1 \cdot \ldots \cdot g_\ell$ of terms from G, where repetition is allowed, is a product-one sequence if its terms can be ordered such that their product equals 1_G, the identity element of the group. As usual, we consider sequences as elements of the free abelian monoid $\mathcal{F}(G)$ with basis G, and we study the submonoid $\mathcal{B}(G) \subset \mathcal{F}(G)$ of all product-one sequences. This is a finitely generated C-monoid, which is a Krull monoid if and only if G is abelian. In case of abelian groups, $\mathcal{B}(G)$ is a well-studied object. In the present paper we focus on non-abelian groups, and we study the class semigroup and the arithmetic of $\mathcal{B}(G)$.

1. Introduction. Let G be a finite group. By a sequence over G, we mean a finite unordered sequence of terms from G, where the repetition of elements is allowed (the terminology stems from Arithmetic Combinatorics). A sequence S is a product-one sequence if its terms can be ordered such that their product equals the identity element of the group. Clearly, juxtaposition of sequences is a commutative operation on the set of sequences. As usual we consider sequences as elements of the free abelian monoid $\mathcal{F}(G)$ with basis G, and clearly the subset $\mathcal{B}(G) \subset \mathcal{F}(G)$ of all product-one sequences is a submonoid. The small Davenport constant $\mathsf{d}(G)$ is the maximal integer ℓ for which there is a sequence of length ℓ which has no product-one subsequence. The large Davenport constant $\mathsf{D}(G)$ is the maximal length of a minimal product-one sequence (by a minimal product-one sequence we mean an irreducible element in the monoid $\mathcal{B}(G)$).

Suppose that G is abelian, and let us use additive notation in this case. Then product-one sequences are zero-sum sequences and their study is the main objective of Zero-Sum Theory ([**12, 25**]). The monoid $\mathcal{B}(G)$ is a Krull monoid with class group G (apart from the exceptional case where $|G| = 2$), and because it has intimate relationship with general Krull monoids having class group G, the study of $\mathcal{B}(G)$ is a central topic in factorization theory ([**18, 15**]).

Although the abelian setting has been the dominant one, many of the combinatorial problems on sequences over abelian groups have also been studied in the non-abelian setting. For example, an upper bound on the small Davenport constant was given already in the 1970s [**29**], and in recent years Gao's Theorem $\mathsf{E}(G) = |G| + \mathsf{d}(G)$ ([**25,** Chapter 16]) has been generalized to a variety of non-abelian groups ([**3, 14, 13, 26, 27**]). Fresh impetus came from invariant theory. If G is abelian, then $\mathsf{d}(G) + 1 = \boldsymbol{\beta}(G) = \mathsf{D}(G)$, where $\boldsymbol{\beta}(G)$ is the Noether number. If G is non-abelian and has a cyclic subgroup of index two, then the Davenport constants and the Noether number have been explicitely determined ([**8, 17**]), and it turned out that $\mathsf{d}(G)+1 \le \boldsymbol{\beta}(G) \le \mathsf{D}(G)$. For a survey on the interplay with invariant theory we refer to [**9**] and for recent progress to [**24, 6, 7, 10**].

Let F be a factorial monoid. A submonoid $H \subset F$ is a C-monoid if $H^\times = H \cap F^\times$ and the reduced class semigroup is finite. A commutative ring is called a C-ring if its monoid of regular elements is a C-monoid. To give an example of a C-ring, consider a Mori domain R. If its conductor $\mathfrak{f} = (R\colon \widehat{R})$ is non-zero and the residue class ring $\widehat{R}/\mathfrak{f}$ is finite, then R is a C-ring. For more on C-rings we refer to

2010 AMS *Mathematics subject classification.* 13A50, 20D60, 20M13.

Keywords and phrases. product-one sequences, Davenport constant, C-monoids, sets of lengths.

This work was supported by the Austrian Science Fund FWF, W1230 Doctoral Program Discrete Mathematics.

Received by the editors December 15, 2017.

[**30, 21**]. The finiteness of the reduced class semigroup is used to derive arithmetical finiteness result for C-monoids ([**18**]). However, the structure of the (reduced) class semigroup has never been studied before.

The monoid $\mathcal{B}(G)$ of product-one sequences is a finitely generated C-monoid, which is Krull if and only if G is abelian (in the Krull case, the class semigroup coincides with the class group which is isomorphic to G, apart from the exceptional case where $|G| = 2$). After putting together the needed background in Section 2, we study the structure of the class semigroup of $\mathcal{B}(G)$ in Section 3. Among others we show that the unit group of the class semigroup is isomorphic to the center of G, and we reveal a subgroup of the class semigroup which is isomorphic to G/G', which is the class group of the complete integral closure of $\mathcal{B}(G)$ (see Theorems 3.8 and 3.10 ; G' denotes the commutator subgroup of G). In Section 4 we provide a complete description of the class semigroup for non-abelian groups of small order. In Section 5 we study the arithmetic of $\mathcal{B}(G)$ and our focus is on sets of lengths. Among others we show that unions of sets of lengths are finite intervals (Theorem 5.5).

Throughout this paper, let G be a multiplicatively written finite group with identity element $1_G \in G$.

2. Preliminaries. We denote by $\mathbb{N}$ the set of positive integers. For integers $a, b \in \mathbb{Z}$, $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$ means the discrete interval. For every $n \in \mathbb{N}$, C_n denotes a cyclic group of order n. For an element $g \in G$, $\mathrm{ord}(g) \in \mathbb{N}$ is its order, and for a subset $G_0 \subset G$, $\langle G_0 \rangle \subset G$ denotes the subgroup generated by G_0. We will use the following standard notation of group theory :

- $\mathsf{Z}(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\} \lhd G$ is the *center* of G,
- $[x, y] = xyx^{-1}y^{-1} \in G$ is the *commutator* of the elements $x, y \in G$, and
- $G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle \lhd G$ is the *commutator subgroup* of G.

Semigroups. All our semigroups are commutative and have an identity element. Let S be a semigroup. We denote by $S^\times$ its group of invertible elements and by $\mathsf{E}(S)$ the set of all idempotents of S, endowed with the *Rees order* $\le$, defined by $e \le f$ if $ef = e$. Clearly, $ef \le e$ and $ef \le f$ for all $e, f \in \mathsf{E}(S)$. If $E \subset \mathsf{E}(S)$ is a finite subsemigroup, then E has a smallest element.

By a *monoid*, we mean a semigroup which satisfies the cancellation laws. Let H be a monoid. Then $\mathsf{q}(H)$ denotes the quotient group of H and $\mathcal{A}(H)$ the set of irreducibles (atoms) of H. The monoid H is called *atomic* if every non-unit of H can be written as a finite product of atoms. We say that H is reduced if $H^\times = \{1\}$, and we denote by $H_{\mathrm{red}} = H/H^\times = \{aH^\times \mid a \in H\}$ the associated reduced monoid of H. A monoid F is called *free abelian with basis* $P \subset F$ if every $a \in F$ has a unique representation of the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)} \quad \text{with} \quad \mathsf{v}_p(a) = 0 \quad \text{for almost all} \quad p \in P\,.$$

If F is free abelian with basis P, then P is the set of primes of F, we set $F = \mathcal{F}(P)$, and denote by

- $|a| = \sum_{p \in P} \mathsf{v}_p(a)$ the *length* of a, and by
- $\mathrm{supp}(a) = \{p \in P \mid \mathsf{v}_p(a) > 0\}$ the *support* of a.

A monoid F is factorial if and only if F_{red} is free abelian if and only if F is atomic and every atom is a prime. We denote by

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

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

and observe that $H \subset H' \subset \widetilde{H} \subset \widehat{H} \subset \mathsf{q}(H)$. Then the monoid H is called

- *seminormal* if $H = H'$ (equivalently, if $x \in \mathsf{q}(H)$ and $x^2, x^3 \in H$, then $x \in H$),
- *root closed* if $H = \widetilde{H}$,
- *completely integrally closed* if $H = \widehat{H}$.

If D is a monoid and $H \subset D$ a submonoid, then H is a *divisor-closed submonoid* if $a \in H, b \in D$, and $b \mid a$ implies that $b \in H$. A monoid homomorphism $\varphi\colon H \to D$ is said to be

- *cofinal* if for every $\alpha \in D$ there is an $a \in H$ such that $\alpha \mid \varphi(a)$.
- a *divisor homomorphism* if $a, b \in H$ and $\varphi(a) \mid \varphi(b)$ implies that $a \mid b$.
- a *divisor theory* if D is free abelian, φ is a divisor homomorphism, and for all $\alpha \in D$ there are $a_1, \ldots, a_m \in H$ such that $\alpha = \gcd\big(\varphi(a_1), \ldots, \varphi(a_m)\big)$.
- a *transfer homomorphism* if it satisfies the following two properties:

(T 1) $D = \varphi(H)D^\times$ and $\varphi^{-1}(D^\times) = H^\times$.

(T 2) If $u \in H$, $b, c \in D$ and $\varphi(u) = bc$, then there exist $v, w \in H$ such that $u = vw$, $\varphi(v)D^\times = bD^\times$, and $\varphi(w)D^\times = cD^\times$.

Transfer Krull monoids. A monoid H is said to be a *Krull monoid* if it satisfies one of the following equivalent conditions (see **[18,** Theorem 2.4.8]):

(a) H is completely integrally closed and satisfies the ACC on divisorial ideals.

(b) There is a divisor homomorphism $\varphi\colon H \to F$, where F is free abelian monoid.

(c) H has a divisor theory.

A commutative domain R is a Krull domain if and only if its multiplicative monoid of non-zero elements is Krull. Further examples of Krull monoids can be found in **[18, 16]**. Let H be a Krull monoid. Then a divisor theory $\varphi\colon H \to F$ is unique up to isomorphism and

$$\mathcal{C}(H) = \mathsf{q}(F)/\mathsf{q}\big(\varphi(H)\big)$$

is called the *class group* of H.

A monoid H is said to be a *transfer Krull monoid* if it allows a transfer homomorphism to a Krull monoid (since in our setting all monoids are commutative, **[2,** Lemma 2.3.3] shows that the present definition coincides with the definition in **[16]**). The significance of transfer homomorphisms $\varphi\colon H \to B$ stems from the fact that they allow to pull back arithmetical properties from the (simpler monoid) B to the monoid H (of original interest). In particular, if H is a transfer Krull monoid, then sets of lengths in H coincide with sets of lengths in a Krull monoid (see Equation (5.1)).

Since the identity map is a transfer homomorphism, every Krull monoid is a transfer Krull monoid. For a list of transfer Krull monoids which are not Krull we refer to **[16]**. To give one such example, consider a ring of integers $\mathcal{O}$ in an algebraic number field K, a central simple algebra A over K, and a classical maximal $\mathcal{O}$-order R of A. If every stably free left R-ideal is free, then the (non-commutative) semigroup of cancellative elements of R is a transfer Krull monoid over a finite abelian group (**[33]**).

Class semigroups and C-monoids. (a detailed presentation can be found in **[18,** Chapter 2]). Let F be a monoid and $H \subset F$ a submonoid. Two elements $y, y' \in F$ are called H-equivalent, denote $y \sim_H y'$,

if $y^{-1}H \cap F = y'^{-1}H \cap F$. H-equivalence is a congruence relation on F. For $y \in F$, let $[y]_H^F$ denote the congruence class of y, and let

$$\mathcal{C}(H,F) = \big\{[y]_H^F \mid y \in F\big\} \quad \text{and} \quad \mathcal{C}^*(H,F) = \big\{[y]_H^F \mid y \in (F \setminus F^\times) \cup \{1\}\big\}\,.$$

Then $\mathcal{C}(H,F)$ is a commutative semigroup with unit element $[1]_H^F$ (called the *class semigroup* of H in F) and $\mathcal{C}^*(H,F) \subset \mathcal{C}(H,F)$ is a subsemigroup (called the *reduced class semigroup* of H in F).

As usual, class groups and class semigroups will both be written additively. The following lemma describes the relationship between class groups and class semigroups. Its proof is elementary and can be found in [**18,** Propositions 2.8.7 and 2.8.8]

Lemma 2.1. *Let F be a monoid and $H \subset F$ be a submonoid.*

1. *If $H \subset F$ is cofinal, then the map $\theta\colon \mathcal{C}(H,F) \to \mathsf{q}(F)/\mathsf{q}(H)$, $[y]_H^F \mapsto y\mathsf{q}(H)$ for all $y \in F$, is an epimorphism. Moreover, θ is an isomorphism if and only if $H \hookrightarrow F$ is a divisor homomorphism.*
2. *If $\mathcal{C}(H,F)$ is a group, then $H \subset F$ is cofinal, and if $\mathcal{C}(H,F)$ is a torsion group, then $H \hookrightarrow F$ is a divisor homomorphism.*

A monoid H is called a C-*monoid* if H is a submonoid of a factorial monoid F such that $H \cap F^\times = H^\times$ and $\mathcal{C}^*(H,F)$ is finite. A commutative ring R is a C-ring if its monoid of regular elements is a C-monoid. A Krull monoid is a C-monoid if and only if it has finite class group. We refer to [**18, 30, 21, 28**] for more on C-monoids. To give an explicit example, consider a Mori ring R. If the conductor $\mathfrak{f} = (R\colon \widehat{R})$ is non-zero and $\widehat{R}/\mathfrak{f}$ is finite, then R is a C-ring. We will need the following lemma (for a proof see [**18,** Theorem 2.9.11]).

Lemma 2.2. *Let $F = F^\times \times \mathcal{F}(P)$ be factorial and $H \subset F$ be a C-monoid. Suppose that $\mathsf{v}_p(H) \subset \mathbb{N}_0$ is a numerical monoid for all $p \in P$ (this is a minimality condition on F which can always be assumed without restriction).*

1. *$\widehat{H}$ is a Krull monoid with non-empty conductor $(H\colon \widehat{H})$ and finite class group $\mathcal{C}(\widehat{H})$.*
2. *The map $\partial\colon \widehat{H} \to \mathcal{F}(P)$, defined by*

$$\partial(a) = \prod_{p \in P} p^{\mathsf{v}_p(a)}\,,$$

is a divisor theory, and there is an epimorphism $\mathcal{C}^*(H,F) \to \mathcal{C}(\widehat{H})$.

3. Algebraic Properties of the monoid of product-one sequences. We introduce sequences over a finite group G. Our notation and terminology follows the articles [**17, 24, 9**]. Let $G_0 \subset G$ be a subset. The elements of the free abelian monoid $\mathcal{F}(G_0)$ will be called *sequences* over G_0. This terminology goes back to Arithmetic Combinatorics. Indeed, a sequence over G_0 can be viewed as a finite unordered sequence of terms from G_0, where the repetition of elements is allowed. In order to avoid confusion between the multiplication in G and multiplication in $\mathcal{F}(G_0)$, we denote multiplication in $\mathcal{F}(G_0)$ by the boldsymbol $\boldsymbol{\cdot}$ and we use brackets for all exponentiation in $\mathcal{F}(G_0)$. In particular, a sequence $S \in \mathcal{F}(G_0)$ has the form

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell = \bullet_{i \in [1,\ell]} g_i = \bullet_{g \in G_0} g^{[\mathsf{v}_g(S)]} \in \mathcal{F}(G_0)\,, \tag{3.1}$$

where $g_1, \ldots, g_\ell \in G_0$ are the terms of S. Moreover, if $S_1, S_2 \in \mathcal{F}(G_0)$ and $g_1, g_2 \in G_0$, then $S_1 \boldsymbol{\cdot} S_2 \in \mathcal{F}(G_0)$ has length $|S_1|+|S_2|$, $S_1 \boldsymbol{\cdot} g_1 \in \mathcal{F}(G_0)$ has length $|S_1|+1$, $g_1g_2 \in G$ is an element of G, but $g_1 \boldsymbol{\cdot} g_2 \in \mathcal{F}(G_0)$ is a sequence of length 2. If $g \in G_0$, $T \in \mathcal{F}(G_0)$, and $k \in \mathbb{N}_0$, then

$$g^{[k]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{k} \in \mathcal{F}(G_0) \quad \text{and} \quad T^{[k]} = \underbrace{T \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T}_{k} \in \mathcal{F}(G_0)\,.$$

Let $S \in \mathcal{F}(G_0)$ be a sequence as in (3.1). Then we denote by

$$\pi(S) = \{g_{\tau(1)} \ldots g_{\tau(\ell)} \in G \mid \tau \text{ a permutation of } [1, \ell]\} \subset G \quad \text{and} \quad \Pi(S) = \bigcup_{\substack{T \mid S \\ |T| \ge 1}} \pi(T) \subset G\,,$$

the *set of products* and *subsequence products* of S, and it can easily be seen that $\pi(S)$ is contained in a G'-coset. Note that $|S| = 0$ if and only if $S = 1_{\mathcal{F}(G_0)}$, and in that case we use the convention that $\pi(S) = \{1_G\}$. The sequence S is called

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

Definition 3.1. Let $G_0 \subset G$ be a subset.

1. The submonoid
$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid 1_G \in \pi(S)\} \subset \mathcal{F}(G_0)$$
is called the *monoid of product-one sequences*, and $\mathcal{A}(G_0) = \mathcal{A}\big(\mathcal{B}(G_0)\big)$ denotes its set of atoms.
2. We call
$$\mathsf{D}(G_0) = \sup\{|S| \mid S \in \mathcal{A}(G_0)\} \in \mathbb{N} \cup \{\infty\}$$
the *large Davenport constant* of G_0 and
$$\mathsf{d}(G_0) = \sup\{|S| \mid S \in \mathcal{F}(G_0) \text{ is product-one free}\} \in \mathbb{N}_0 \cup \{\infty\}$$
the *small Davenport constant* of G_0.

Note that obviously the set $\mathcal{B}(G_0)$ is a multiplicatively closed subset of the commutative cancellative semigroup $\mathcal{F}(G_0)$ whence $\mathcal{B}(G_0)$ is indeed a monoid. Our object of interest is the monoid $\mathcal{B}(G)$ but for technical reasons we also need the submonoids $\mathcal{B}(G_0)$ for subsets $G_0 \subset G$. The next lemma gathers some elementary properties. Its simple proof can be found in [**9,** Lemma 3.1].

Lemma 3.2. *Let $G_0 \subset G$ be a subset.*

1. *$\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is a reduced finitely generated submonoid, $\mathcal{A}(G_0)$ is finite, and $\mathsf{D}(G_0) \le |G|$.*
2. *Let $S \in \mathcal{F}(G)$ be product-one free.*
   (a) *If $g_0 \in \pi(S)$, then $g_0^{-1} \boldsymbol{\cdot} S \in \mathcal{A}(G)$. In particular, $\mathsf{d}(G) + 1 \le \mathsf{D}(G)$.*
   (b) *If $|S| = \mathsf{d}(G)$, then $\Pi(S) = G \setminus \{1_G\}$ and hence $\mathsf{d}(G) = \max\big\{|S|\colon S \in \mathcal{F}(G)$ with $\Pi(S) = G \setminus \{1_G\}\big\}$.*
3. *If G is cyclic, then $\mathsf{d}(G) + 1 = \mathsf{D}(G) = |G|$.*

The Davenport constant of finite abelian groups is a frequently studied invariant in Zero-sum Theory (for an overview see [**18**] and for recent progress [**31, 5**]). For the Davenport constant of non-abelian groups we refer to [**17, 24, 10**].

Lemma 3.3. *Let $G_0 \subset G$ be a subset. A submonoid $H \subset \mathcal{B}(G_0)$ is divisor-closed if and only if $H = \mathcal{B}(G_1)$ for a subset $G_1 \subset G_0$.*

Proof. If $G_1 \subset G_0$, then clearly $\mathcal{B}(G_1) \subset \mathcal{B}(G_0)$ is a divisor-closed submonoid. Conversely, let $H \subset \mathcal{B}(G_0)$ be a divisor-closed submonoid. We set

$$G_1 = \bigcup_{B \in H} \operatorname{supp}(B)$$

and obtain that $H \subset \mathcal{B}(G_1)$. We have to show that equality holds. Let $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{B}(G_1)$. Then for every $i \in [1, \ell]$ there is some $B_i \in H$ such that $g_i \in \operatorname{supp}(B_i)$. Then $B_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} B_\ell \in H$ and S divides $B_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} B_\ell$, which implies that $S \in H$. □

Proposition 3.4. *The following statements are equivalent*:

(a) *G is abelian.*

(b) *$\mathcal{B}(G)$ is a Krull monoid.*

(c) *$\mathcal{B}(G)$ is a transfer Krull monoid.*

Proof. The implications (a) ⇒ (b) and (b) ⇒ (c) are well-known and immediate. Indeed, if G is abelian, then the embedding $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor homomorphism whence $\mathcal{B}(G)$ is Krull. By definition, every Krull monoid is a transfer Krull monoid.

(c) ⇒ (a) Assume to the contrary that G is non-abelian, but $\mathcal{B}(G)$ is a transfer Krull monoid. Thus there is a transfer homomorphism $\theta_1 \colon \mathcal{B}(G) \to H$, where H is a Krull monoid. Since there is a transfer homomorphism $\theta_2 \colon H \to \mathcal{B}(G_0)$, where $G_0 \subset \mathcal{C}(H)$ is a subset of the class group, and since the composition of transfer homomorphisms is a transfer homomorphism, we obtain a transfer homomorphism $\theta \colon \mathcal{B}(G) \to \mathcal{B}(G_0)$, where G_0 is a subset of an abelian group.

Since G is non-abelian, there exist $g, h \in G$ such that $gh \neq hg$. Consider the sequence

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

From **[18,** Proposition 3.2.3**]**, we have that $\theta(U) \in \mathcal{A}(G_0)$, say $\theta(U) = a_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} a_\ell$, where $a_i \in G_0$ for all $i \in [1, \ell]$. Let $m = \operatorname{ord}(hgh^{-1}g^{-1}) \in \mathbb{N}$. Then

$$U^{[m]} = (g \boldsymbol{\cdot} g^{-1})^{[m]} \boldsymbol{\cdot} (h \boldsymbol{\cdot} (gh^{-1}g^{-1}))^{[m]}\,,$$

and hence it follows that

$$\begin{aligned}(a_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} a_\ell)^{[m]} &= \theta(U^{[m]}) \\ &= \big(\theta(g \boldsymbol{\cdot} g^{-1})\big)^{[m]} \boldsymbol{\cdot} \theta\big((h \boldsymbol{\cdot} (gh^{-1}g^{-1}))^{[m]}\big)\,.\end{aligned}$$

Since $\mathcal{B}(G_0) \hookrightarrow \mathcal{F}(G_0)$ is a divisor homomorphism (and hence $\mathcal{B}(G_0)$ is root closed), the fact that $\big(\theta(g \boldsymbol{\cdot} g^{-1})\big)^{[m]}$ divides $(a_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} a_\ell)^{[m]}$ in $\mathcal{B}(G_0)$ implies that $\theta(g \boldsymbol{\cdot} g^{-1})$ divides $a_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} a_\ell$ in $\mathcal{B}(G_0)$. Since $\theta(g \boldsymbol{\cdot} g^{-1})$ and $a_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} a_\ell \in \mathcal{A}(G_0)$, it follows that $\theta(g \boldsymbol{\cdot} g^{-1}) = a_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} a_\ell = \theta(U)$. Thus $\theta\big((h \boldsymbol{\cdot} (gh^{-1}g^{-1}))^{[m]}\big) = 1_{\mathcal{F}(G_0)}$, a contradiction. □

Clearly, if $|G| \le 2$, then $\mathcal{B}(G)$ is factorial whence it is both a Krull monoid (with trivial class group) and a C-monoid (with trivial class semigroup). In order to avoid trivial case distinctions, we exclude this case whenever convenient. By Proposition 3.4, $\mathcal{B}(G)$ is not Krull when G is non-abelian. The next proposition reveals that $\mathcal{B}(G)$ is a C-monoid in all cases and determines the class group of its complete integral closure.

Proposition 3.5. *Suppose that $|G| \ge 3$.*

1. *If $G_0 \subset G$ is a subset, then $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is cofinal and $\mathcal{B}(G_0)$ is a* C*-monoid.*
2. *The embedding $\widehat{\mathcal{B}(G)} \hookrightarrow \mathcal{F}(G)$ is a divisor theory and the map*

$$\begin{aligned} \Phi \colon \mathcal{C}\big(\widehat{\mathcal{B}(G)}\big) = \mathsf{q}\big(\mathcal{F}(G)\big)/\mathsf{q}\big(\mathcal{B}(G)\big) \quad &\longrightarrow \quad G/G' \\ S\mathsf{q}\big(\mathcal{B}(G)\big) \quad &\longmapsto \quad gG' \,, \end{aligned}$$

   where $S \in \mathcal{F}(G)$ and $g \in \pi(S)$, is an isomorphism. Clearly, $\mathsf{v}_g\big(\mathcal{B}(G)\big) = \mathbb{N}_0$ for all $g \in G$.
3. *There is an epimorphism $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big) \to G/G'$.*

Proof. 1. and 2. Let $G_0 \subset G$. If $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{F}(G_0)$ and $g \in \pi(S)$, then $S' = g^{-1} \boldsymbol{\cdot} S \in \mathcal{B}(G_0)$, $S \mid S'$, and hence $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is cofinal. Let $k \in \mathbb{N}_0$. If $g \in G$ with $\mathrm{ord}(g) > 2$, then $U = g \cdot g^{-1} \in \mathcal{B}(G)$, $\mathsf{v}_g(U^{[k]}) = k$. If $g = 1_G$, then $\mathsf{v}_g(g^{[k]}) = k$. If $\mathrm{ord}(g) = 2$, then there is an $h \in G \setminus \{1_G, g\}$ and $U = g \cdot h \cdot (gh)^{-1} \in \mathcal{B}(G)$ and $\mathsf{v}_g(U^{[k]}) = k$. Thus in all cases we have $\mathsf{v}_g(\mathcal{B}(G)) = \mathbb{N}_0$.

It is easy to check that Φ is an isomorphism (details can be found in **[9,** Theorem 3.2]). Since $\mathcal{C}\big(\widehat{\mathcal{B}(G)}\big)$ is finite, $\mathcal{C}\big(\widehat{\mathcal{B}(G_0)}\big)$ is finite and since $\mathcal{B}(G_0)$ is finitely generated, it is a C-monoid by **[19,** Proposition 4.8].

3. This follows from 2. and from Lemma 2.2.2. □

We start with the study of the class semigroup and recall that, by definition, for two sequences $S, S' \in \mathcal{F}(G)$ the following statements are equivalent:

- $S \sim_{\mathcal{B}(G)} S'$.
- For all $T \in \mathcal{F}(G)$, we have $S \boldsymbol{\cdot} T \in \mathcal{B}(G)$ if and only if $S' \boldsymbol{\cdot} T \in \mathcal{B}(G)$.
- For all $T \in \mathcal{F}(G)$, we have $1_G \in \pi(S \boldsymbol{\cdot} T)$ if and only if $1_G \in \pi(S' \boldsymbol{\cdot} T)$.

If $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{B}(G)$ such that $1_G = g_1 \ldots g_\ell$, then $1_G = g_i \ldots g_\ell g_1 \ldots g_{i-1}$ for every $i \in [1, \ell]$. We will use this simple fact without further mention. Moreover, $\sim$ means $\sim_{\mathcal{B}(G)}$ and we write $[S] = [S]^{\mathcal{F}(G)}_{\mathcal{B}(G)}$.

Lemma 3.6. *Let $S \in \mathcal{F}(G)$.*

1. *If $S' \in \mathcal{F}(G)$ such that $S \sim S'$, then $\pi(S) = \pi(S')$.*
2. *Let $S' \in \mathcal{F}(G)$. In the following cases, $S \sim S'$ if and only if $\pi(S) = \pi(S')$:*
   (a) *S and S' are sequences over the center of G.*
   (b) *There is $g \in \pi(S)$ such that $\pi(S) = gG'$.*
3. *If $g, h \in G$ with $g \neq h$, then $g \nsim h$. In particular, $|G| \le |\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)|$.*
4. *If $g \in \mathsf{Z}(G)$ and $h \in G$, then $g \cdot h \sim gh$.*
5. *$|\pi(S)| = 1$ if and only if $\langle \mathrm{supp}(S) \rangle$ is abelian.*

Proof. 1. Suppose that $S' \in \mathcal{F}(G)$ with $S \sim S'$. Then for every $g \in G$ we obtain that

$$g \in \pi(S) \quad \Leftrightarrow \quad g^{-1} \cdot S \in \mathcal{B}(G) \quad \Leftrightarrow \quad g^{-1} \cdot S' \in \mathcal{B}(G) \quad \Leftrightarrow \quad g \in \pi(S') \,,$$

which implies that $\pi(S) = \pi(S')$.

2. From 1., it remains to verify the reverse implication. Suppose that $\pi(S) = \pi(S')$.

(a) Since $S, S' \in \mathcal{F}\big(\mathsf{Z}(G)\big)$, we have $|\pi(S)| = |\pi(S')| = 1$, say $\pi(S) = \pi(S') = \{g\}$. Then for every $T \in \mathcal{F}(G)$ we have

$$\pi(S \cdot T) = g\pi(T) \quad \text{and} \quad \pi(S' \cdot T) = g\pi(T)\,,$$

which implies that $S \sim S'$.

(b) Suppose that there is a $g \in \pi(S)$ such that $\pi(S) = gG'$. Let $T \in \mathcal{F}(G)$ such that $T \cdot S \in \mathcal{B}(G)$. Then we have

$$\pi(T)\pi(S) \subset \pi(T \cdot S) \subset G'\,.$$

Since $\pi(S) = gG'$, there are $t \in \pi(T)$ and $e \in G'$ such that $tg = e$. Hence we obtain that

$$1_G = ee^{-1} = tge^{-1} \in \pi(T)\pi(S) = \pi(T)\pi(S') \subset \pi(T \cdot S')\,.$$

It follows that $T \cdot S' \in \mathcal{B}(G)$. By symmetry, we infer that $S \sim S'$.

3. Let $g, h \in G$. Then $g, h \in \mathcal{F}(G)$ and if $g \sim h$, then 1. implies that $\{g\} = \pi(g) = \pi(h) = \{h\}$. Therefore, $g \neq h$ implies that $g \nsim h$, and hence we obtain that $|G| \le |\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)|$.

4. This follows from the fact that $g \in \mathsf{Z}(G)$.

5. Obvious. □

Lemma 3.7. *Let $S \in \mathcal{F}(G)$.*

1. *If $[S]$ is an idempotent of $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$, then $\pi(S) \subset G'$ is a subgroup.*
2. *$[1_{\mathcal{F}(G)}] = \mathcal{B}\big(\mathsf{Z}(G)\big)$. In particular, if $g \in \mathsf{Z}(G)$, then $g^{[\mathrm{ord}(g)]} \sim 1_{\mathcal{F}(G)}$.*
3. *$[S]$ is the smallest idempotent in $\mathsf{E}\Big(\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)\Big)$ (with respect to the Rees order) if and only if $\pi(S) = G'$.*

Proof. 1. Suppose that $[S]$ is an idempotent of $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$. Then $[S] = \big[S^{[2]}\big]$ whence $S \sim S^{[2]}$, and Lemma 3.6.1 implies that

$$\pi(S)\pi(S) \subset \pi\big(S^{[2]}\big) = \pi(S)\,.$$

Thus $\pi(S) \subset G'$ is a subgroup.

2. Suppose that $S \in \mathcal{B}\big(\mathsf{Z}(G)\big)$. Then $\pi(S) = \{1_G\}$, and for all $T \in \mathcal{F}(G)$ we have

$$\pi(S \cdot T) = \pi(T) = \pi(1_{\mathcal{F}(G)} \cdot T)\,,$$

whence $S \sim 1_{\mathcal{F}(G)}$.

Conversely, suppose that $S \sim 1_{\mathcal{F}(G)}$. Then $S \in \mathcal{B}(G)$, and we set $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$ such that $g_1 \ldots g_\ell = 1_G$. Assume to the contrary that there is an $i \in [1, \ell]$ such that $g_i \notin \mathsf{Z}(G)$, say $i = 1$. Then there is an element $h \in G$ such that $hg_1 \neq g_1 h$. Then $T = (hg_1) \cdot (h^{-1}g_1^{-1}) \in \mathcal{F}(G) \setminus \mathcal{B}(G)$, but

$$1_G = g_1(hg_1)(g_2 \ldots g_\ell)(h^{-1}g_1^{-1}) \in \pi(T \cdot S)\,.$$

Since $S \sim 1_{\mathcal{F}(G)}$, we infer that $1_G \in \pi(T \cdot 1_{\mathcal{F}(G)}) = \pi(T)$, a contradiction.

In particular, if $g \in \mathsf{Z}(G)$, then $g^{[\mathrm{ord}(g)]} \in \mathcal{B}\big(\mathsf{Z}(G)\big)$ and hence $g^{[\mathrm{ord}(g)]} \sim 1_{\mathcal{F}(G)}$.

3. First, we suppose that $\pi(S) = G'$. Then $[S]$ is an idempotent by Lemma 3.6.2, and it remains to verify that $[S]$ is the smallest idempotent of $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$. Let $S' \in \mathcal{F}(G)$ such that $[S']$ is an

idempotent. We have to show that $S \sim S \cdot S'$. Since $\pi(S') \subset G'$ is a subgroup by 1., $S, S' \in \mathcal{B}(G)$, and since $\pi(S \cdot S')$ is a G'-coset, it follows that

$$G' \subset \pi(S)\pi(S') \subset \pi(S \cdot S') \subset G' \quad \text{whence} \quad G' = \pi(S \cdot S')\,.$$

Again Lemma 3.6.2 implies that $S \sim S \cdot S'$.

To show the converse, suppose that $[S]$ is the smallest idempotent. We construct an element $S' \in \mathcal{F}(G)$ such that $\pi(S') = G'$. Then the proof above shows that $[S']$ is the smallest idempotent whence $S \sim S'$ and $\pi(S) = \pi(S') = G'$. We set $G' = \{g_1, \ldots, g_n\}$, and for each $i \in [1, n]$ we set

$$g_i = \prod_{\nu=1}^{k_i} a_{i,\nu} b_{i,\nu} a_{i,\nu}^{-1} b_{i,\nu}^{-1}\,, \quad \text{where } k_i \in \mathbb{N} \text{ and all } \quad a_{i,\nu}, b_{i,\nu} \in G\,,$$

and define

$$S_i = \bullet_{\nu \in [1,k_i]} (a_{i,\nu} \cdot b_{i,\nu} \cdot a_{i,\nu}^{-1} \cdot b_{i,\nu}^{-1}) \in \mathcal{B}(G)\,.$$

Then obviously $\pi(S_1 \cdot \ldots \cdot S_n) = G'$. □

Theorem 3.8.

1. *Suppose that $G/G' = \{g_0G', \ldots, g_kG'\}$, and for each $i \in [0, k]$ let $S_i \in \mathcal{F}(G)$ such that $\pi(S_i) = g_iG'$. Then the map*
$$\begin{array}{rcl} G/G' & \to & \big\{[S_i] \mid i \in [0,k]\big\} = \mathcal{C} \subset \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big) \\ g_iG' & \mapsto & [S_i] \end{array}$$
is a group isomorphism. Thus $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ contains a subgroup isomorphic to the class group of $\widehat{\mathcal{B}(G)}$. Moreover, for any $i \in [0, k]$ and for any $S \in \mathcal{F}(G)$, we have $[S \cdot S_i] \in \mathcal{C}$.
2. *The map*
$$\begin{array}{rcl} \mathsf{Z}(G) & \to & \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)^\times \\ g & \mapsto & [g] \end{array}$$
is a group isomorphism.

Proof. 1. We first verify the existence of such sequences $S_0, \ldots, S_k$. Since $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ is finite, the set $\mathsf{E}\Big(\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)\Big)$ has the smallest element, say $[S]$. For each $i \in [0, k]$, we set $S_i = g_i \cdot S$. Since $\pi(S) = G'$ by Lemma 3.7.3, it follows that for each $i \in [0, k]$

$$g_iG' \subset \pi(g_i \cdot S) \subset g_iG'\,, \quad \text{whence } \pi(S_i) = \pi(g_i \cdot S) = g_iG'\,.$$

We now use Lemma 3.6.2. If $i, j \in [0, k]$, then $g_ig_j \in \pi(S_i)\pi(S_j) \subset \pi(S_i \cdot S_j)$, and hence $\pi(S_i \cdot S_j) = g_ig_jG' = g_\ell G' = \pi(S_\ell)$ for some $\ell \in [0, k]$. Thus it follows that $\mathcal{C}$ is a subgroup of the class semigroup and the given map is an isomorphism. By Proposition 3.5.2, G/G' is isomorphic to the class group of $\widehat{\mathcal{B}(G)}$.

Moreover, let $S \in \mathcal{F}(G)$, $g \in \pi(S)$, and $i \in [0, k]$. Then

$$gg_iG' = g\pi(S_i) \subset \pi(S)\pi(S_i) \subset \pi(S \cdot S_i)\,,$$

whence $\pi(S \cdot S_i) = gg_iG' = g_jG' = \pi(S_j)$ for some $j \in [0, k]$. Again by Lemma 3.6.2, we have $S \cdot S_i \sim S_j$, and thus $[S \cdot S_i] \in \mathcal{C}$.

2. Let $S \in \mathcal{F}(G)$ such that $[S] \in \mathcal{C}\big(\mathcal{F}(G), \mathcal{B}(G)\big)$ is invertible. Then there is an $S' \in \mathcal{F}(G)$ such that

$$0_{\mathcal{C}(\mathcal{F}(G),\mathcal{B}(G))} = [1_{\mathcal{F}(G)}] = [S] + [S'] = [S \cdot S']\,,$$

whence $S \cdot S' \sim 1_{\mathcal{F}(G)}$. Then Lemma 3.7.2 implies that $S \cdot S' \in \mathcal{B}\big(\mathsf{Z}(G)\big)$ whence $S, S' \in \mathcal{F}\big(\mathsf{Z}(G)\big)$. If $g \in \pi(S)$, then Lemma 3.6.2 implies that $S \sim g$. This proves that the given map is well-defined and surjective. Lemma 3.6 (items 3 and 4) shows that the map is a monomorphism. □

Our next goal is a detailed investigation of the case where $|G'| = 2$. We derive a couple of special properties which do not hold in general (Theorem 3.10 and Remark 3.11).

Lemma 3.9. *Suppose that $|G'| = 2$, and let $g \in G$ with $\mathrm{ord}(g) = n$.*

1. *We have $g \sim g^{[n+1]}$, and hence $\big[g^{[n]}\big] \in \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ is idempotent.*
2. *If $k \in [1, n]$ is odd and $g^k \notin \mathsf{Z}(G)$, then $g^{[k]} \sim g^k$.*
3. *If $g, h \in G \setminus \mathsf{Z}(G)$ with $gh = hg$, then $g \cdot h \nsim gh$ provided that one of the following conditions holds:*
   (a) *$gh \in \mathsf{Z}(G)$.*
   (b) *There is $g_0 \in G$ such that $g_0 g \ne g g_0$ and $g_0 h \ne h g_0$.*

Proof. 1. Let $T \in \mathcal{F}(G)$. Since $g^n = 1_G$, $1_G \in \pi(g \cdot T)$ implies that $1_G \in \pi\big(g^{[n+1]} \cdot T\big)$. Conversely, suppose that $1_G \in \pi\big(g^{[n+1]} \cdot T\big)$. If every element in $\mathrm{supp}(T)$ commutes with g, then

$$\pi\big(g^{[n+1]} \cdot T\big) = \pi(g \cdot T) \quad \text{and hence} \quad 1_G \in \pi(g \cdot T)\,.$$

Now suppose that there is at least one $h \in \mathrm{supp}(T)$ such that $hg \ne gh$. Then $\pi(g \cdot T)$ has at least two elements. Since $|G'| = 2$ and

$$\pi(g \cdot T) \subset \pi\big(g^{[n+1]} \cdot T\big) \subset G'\,,$$

we obtain that $\pi(g \cdot T) = G'$ and hence $1_G \in \pi(g \cdot T)$. Thus $[g] = \big[g^{[n+1]}\big]$ and thus

$$\big[g^{[n]}\big] + \big[g^{[n]}\big] = \big[g^{[2n]}\big] = \big[g^{[n+1]} \cdot g^{[n-1]}\big] = \big[g^{[n]}\big]\,.$$

2. Let $k \in [1, n]$ be odd, $g^k \notin \mathsf{Z}(G)$, and $T \in \mathcal{F}(G)$. If $1_G \in \pi\big(g^k \cdot T\big)$, then $1_G \in \pi\big(g^{[k]} \cdot T\big)$. Conversely, suppose that $1_G \in \pi\big(T \cdot g^{[k]}\big)$. If $hg = gh$ for all $h \in \mathrm{supp}(T)$, then obviously $1_G \in \pi\big(g^k \cdot T\big)$.

Suppose there is an element $h \in \mathrm{supp}(T)$ such that $hg \ne gh$. Then $\pi\big(T \cdot g^{[k]}\big) = G'$. We set $T = h_1 \cdot \ldots \cdot h_\ell$ with $h_1 = h$ and consider the elements

$$g_0 = h_1 g^k h_2 \ldots h_\ell \quad \text{and} \quad g_0^{(1)} = g h_1 g^{k-1} h_2 \ldots h_\ell \ \text{ in } G'.$$

Then $G' = \big\{g_0, g_0^{(1)}\big\}$. If $g_0 = 1$, then we are done. Suppose that $g_0^{(1)} = 1_G$. Then

$$g_0^{(2)} = g g h_1 g^{k-2} h_2 \ldots h_\ell \ne g_0^{(1)}\,,$$

whence $g_0^{(2)} = g_0$ and $hg^2 = g^2 h$. Thus we obtain

$$1_G = g_0^{(1)} = g_0^{(3)} = \ldots = g_0^{(k)} = g^k h_1 \ldots h_\ell \in \pi\big(T \cdot g^k\big)\,.$$

3. Let $g, h \in G \setminus \mathsf{Z}(G)$ with $gh = hg$.

(a) Suppose that $gh \in \mathsf{Z}(G)$ and assume to the contrary that $g \cdot h \sim gh$. By Lemma 3.7.2, we infer that

$$(g \cdot h)^{[\mathrm{ord}(gh)]} \sim gh^{[\mathrm{ord}(gh)]} \sim 1_{\mathcal{F}(G)}\,.$$

a contradiction to $[1_{\mathcal{F}(G)}] = \mathcal{B}\big(\mathsf{Z}(G)\big)$.

(b) Let $g_0 \in G$ such that $g_0 g \neq g g_0$ and $g_0 h \neq h g_0$. If

$$T = (g^{-1} g_0) \cdot (h^{-1} g_0^{-1}) \in \mathcal{F}(G)\,,$$

then $1_G \notin \pi\big(T \cdot (gh)\big)$ but $1_G = g(g^{-1}g_0)h(h^{-1}g_0^{-1}) \in \pi(T \cdot g \cdot h)$. This shows that $g \cdot h \nsim gh$. □

It is well-known that a finitely generated monoid is Krull if and only if it is root-closed. Thus if G is non-abelian, then $\mathcal{B}(G)$ is not root-closed by Proposition 3.4. The next result shows that it is seminormal if $|G'| = 2$. We say that an element c of a semigroup is a *regular* if c lies in a subgroup of the semigroup, and the semigroup is *Clifford* if every element is regular.

Theorem 3.10. *Suppose that* $|G'| = 2$.

1. $\mathcal{B}(G)$ *is seminormal.*
2. $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ *is a Clifford semigroup. In particular, if* $S \in \mathcal{F}(G)$ *with* $\pi(S) = \{g\}$, *then* $[S]$ *generates a cyclic subgroup of order* $\mathrm{ord}(g)$.
3. $\big|\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)\big| \le |\mathsf{Z}(G)| + \prod_{g \in G \setminus \mathsf{Z}(G)} \mathrm{ord}(g)$.

Proof. 1. Let $S \in \mathsf{q}\big(\mathcal{B}(G)\big)$ such that $S^{[2]}, S^{[3]} \in \mathcal{B}(G)$. Since $S \in \mathsf{q}\big(\mathcal{F}(G)\big)$ with $S^{[2]}, S^{[3]} \in \mathcal{F}(G)$, we have that $S \in \mathcal{F}(G)$. Let $g \in \pi(S)$. Since $S^{[2]}, S^{[3]} \in \mathcal{B}(G)$, it follows that

$$g^2 \in \pi\big(S^{[2]}\big) \subset G' \quad \text{and} \quad g^3 \in \pi\big(S^{[3]}\big) \subset G'\,.$$

Since G' is a subgroup of G, we obtain $g \in G'$. If $g = 1_G$, then we are done. Suppose that $g \neq 1_G$. Then $G' = \{1_G, g\}$. If each two elements in $\mathrm{supp}(S)$ would commute, then

$$\pi(S) = \{g\}, \quad \pi\big(S^{[2]}\big) = \{g^2\}, \text{ and } \quad \pi\big(S^{[3]}\big) = \{g^3\}\,,$$

which implies $g^2 = 1_G = g^3$ and $g = 1_G$, a contradiction. Thus $\mathrm{supp}(S)$ contains two elements which do not commute, say $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$, $g_1 g_2 \neq g_2 g_1$, and $g = g_1 \ldots g_\ell$. Then $1_G = g_2 g_1 g_3 \ldots g_\ell \in \pi(S)$.

2. Let $S \in \mathcal{F}(G)$. If $\pi(S)$ has two elements, then $[S]$ lies in the group given in Theorem 3.8.1. Suppose that $\pi(S)$ has only one element, say $\pi(S) = \{g\}$ and $\mathrm{ord}(g) = n$. We assert that $S \sim S^{[n+1]}$. Suppose this holds true. Then $\Big\{[S], \ldots, \big[S^{[n]}\big]\Big\}$ is a cyclic subgroup of the class semigroup, and hence the assertion follows. Let $m \in [1, n]$ and $\big[S^{[m]}\big]$ the identity element of the subgroup. Then it is an idempotent of the class semigroup, and Lemma 3.7.1 shows that $\pi\big(S^{[m]}\big) = \{g^m\} \subset G'$ is a subgroup. This implies $m = n$.

Thus it remains to show that $S \sim S^{[n+1]}$. To do so, let $T \in \mathcal{F}(G)$ be given. Since $S^{[n]} \in \mathcal{B}(G)$,

$$1_G \in \pi(T \boldsymbol{\cdot} S) \quad \text{implies that} \quad 1_G \in \pi\big(T \boldsymbol{\cdot} S^{[n+1]}\big)\,.$$

Conversely, suppose that $1_G \in \pi\big(T \boldsymbol{\cdot} S^{[n+1]}\big)$. If every element of $\mathrm{supp}(T)$ commutes with every element of $\mathrm{supp}(S)$, then $\pi\big(T \boldsymbol{\cdot} S^{[n+1]}\big) = \pi(T \boldsymbol{\cdot} S)$ and thus $1_G \in \pi(T \boldsymbol{\cdot} S)$. If there are $t \in \mathrm{supp}(T)$ and $s \in \mathrm{supp}(S)$ such that $ts \neq st$, then $|\pi(T \boldsymbol{\cdot} S)| \ge 2$ and hence $1_G \in \pi(T \boldsymbol{\cdot} S)$.

3. We set $G = \{g_1, \ldots, g_n\}$ and $\mathsf{Z}(G) = \{g_1, \ldots, g_k\}$ for some $k \in [1, n]$. Let $S \in \mathcal{F}(G)$. Then we can write S of the form

$$S = g_1^{[k_1 \,\mathrm{ord}(g_1) + r_1]} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_n^{[k_n \,\mathrm{ord}(g_n) + r_n]}\,,$$

where $k_1, \ldots, k_n \in \mathbb{N}_0$ and $r_i \in [1, \mathrm{ord}(g_i)]$ for each $i \in [1, n]$. By Lemma 3.9.1, we have

$$S \sim g_1^{[r_1]} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_n^{[r_n]}\,.$$

By Lemma 3.6.4., $g_1^{[r_1]} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_k^{[r_k]} \sim g_0$, where $g_0 = g_1^{r_1} \ldots g_k^{r_k} \in \mathsf{Z}(G)$. Thus

$$S \sim g_0 \boldsymbol{\cdot} g_{k+1}^{[r_{k+1}]} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_n^{[r_n]} \,,$$

and hence the assertion follows. □

Remark 3.11.

1. Suppose that $|G'| = 2$. Let $g, h \in G$ be distinct with $\mathrm{ord}(g) = n$ and $\mathrm{ord}(h) = m$. By Theorem 3.10.2, $[g] \in \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ generates a cyclic subgroup of order n and $[h]$ generates a cyclic subgroup of order m.

Suppose that $\langle [g] \rangle \cap \langle [h] \rangle \neq \emptyset$. Then there are $i \in [1, n]$ and $j \in [1, m]$ such that $g^{[i]} \sim h^{[j]}$. Let $m_j = \mathrm{ord}(h^j) = \frac{m}{\gcd(j,m)}$. Since $\big[h^{[m]}\big]$ is an idempotent, we have

$$g^{[im_j]} \sim h^{[m]} \,.$$

By Lemma 3.6.1, $im_j = kn$ for some $k \in \mathbb{N}$. Since $\big[g^{[n]}\big]$ is also idempotent, we have

$$g^{[n]} \sim h^{[m]} \,.$$

Again by Lemma 3.6.1, we obtain $gh = hg$ because $\mathcal{B}(G)$-equivalence is a congruence relation on $\mathcal{F}(G)$.

It follows that if $gh \neq hg$, then $\langle [g] \rangle \cap \langle [h] \rangle = \emptyset$, and for each $i \in [1, n]$ and $j \in [1, m]$,

$$\big[g^{[i]}\big] + \big[h^{[j]}\big] = \big[g^{[i]} \boldsymbol{\cdot} h^{[j]}\big] \in \mathcal{C} \,,$$

where $\mathcal{C}$ is the group given in Theorem 3.8.1.

2. Suppose that $\mathcal{B}(G)$ is seminormal and let $G_0 \subset G$ be a subset. Let $S \in \mathsf{q}\big(\mathcal{B}(G_0)\big)$ such that $S^{[2]}, S^{[3]} \in \mathcal{B}(G_0)$. Since $\mathcal{B}(G)$ is seminormal, it follows that $S \in \mathcal{B}(G)$ and hence $S \in \mathcal{B}(G) \cap \mathsf{q}\big(\mathcal{B}(G_0)\big) = \mathcal{B}(G_0)$. Thus $\mathcal{B}(G_0)$ is seminormal.

3. Let $D_{2n} = \langle a, b \rangle = \{1_G, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}$ be the dihedral group with $n \equiv 3 \mod 4$, where $\mathrm{ord}(a) = n, \mathrm{ord}(b) = 2$, and $a^k b a^\ell b = a^{k-\ell}$ for all $k, \ell \in \mathbb{Z}$. Then

$$S = a^{[\frac{n-1}{2}]} \boldsymbol{\cdot} b^{[2]} \in \mathsf{q}\big(\mathcal{B}(D_{2n})\big) \setminus \mathcal{B}(D_{2n}), \quad \text{but } S^{[2]}, S^{[3]} \in \mathcal{B}(D_{2n}).$$

Thus if G contains D_{2n} as a subgroup, then 2. shows that $\mathcal{B}(G)$ is not seminormal.

4. Examples of Class Semigroups for Non-abelian Groups of small order. In this section, we discuss the three smallest non-abelian groups and provide a complete description of the class semigroup. Among others we will see that the monoid of product-one sequences over the dihedral group with 6 elements is not seminormal and the associated class semigroup is not Clifford.

Example 4.1. Let $G = Q_8 = \{E, I, J, K, -E, -I, -J, -K\}$ be the quaternion group with the relations

$$IJ = -JI = K, \quad JK = -KJ = I, \quad KI = -IK = J, \qquad \text{and} \qquad IJK = -E \,.$$

Then $\mathsf{Z}(G) = G' = \{E, -E\}$ and $G/G' \simeq C_2 \oplus C_2$. Furthermore, $\mathsf{d}(G) = 4$ and $\mathsf{D}(G) = 6$ by [**17,** Theorem 1.1].

Let $S \in \mathcal{F}(G)$. If $|\pi(S)| = 2$, then, by Theorem 3.8.1, S is $\mathcal{B}(G)$-equivalent to an element in the group $\mathcal{C}$ which is isomorphic to G/G'. We only consider the case $|\pi(S)| = 1$. By Lemma 3.6.5, $\langle \mathrm{supp}(S) \rangle$ is an abelian subgroup of G. Suppose that $S \in \mathcal{F}\big(\langle I \rangle\big)$. Then S has of the form

$$S = E^{[n_1]} \cdot I^{[n_2]} \cdot (-E)^{[n_3]} \cdot (-I)^{[n_4]} \,,$$

where $n_1, \ldots, n_4 \in \mathbb{N}_0$. By Lemma 3.6.4 and Lemma 3.9 (items 1 and 2), we have

$$S \sim I^{[n]} \ \text{ for some } \ n \in [1, 4] \,.$$

By symmetry, we obtain the same results in the case $S \in \mathcal{F}\big(\langle J \rangle\big)$ and $S \in \mathcal{F}\big(\langle K \rangle\big)$. Moreover, If $S \in \mathcal{F}\big(\langle -E \rangle\big)$, then, by Theorem 3.8.2, S is $\mathcal{B}(G)$-equivalent to an element in the group of units of the class semigroup $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$, which is isomorphic to $\mathsf{Z}(G)$. It follows that

$$|\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)| = 18 \,.$$

Figure 1 presents the subgroup lattice of the class semigroup over Q_8. Note that the subgroup lattice of G is not preserved in the class semigroup $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$. Furthermore, observe that the bottom elements in the lattice are all idempotent elements of the class semigroup.

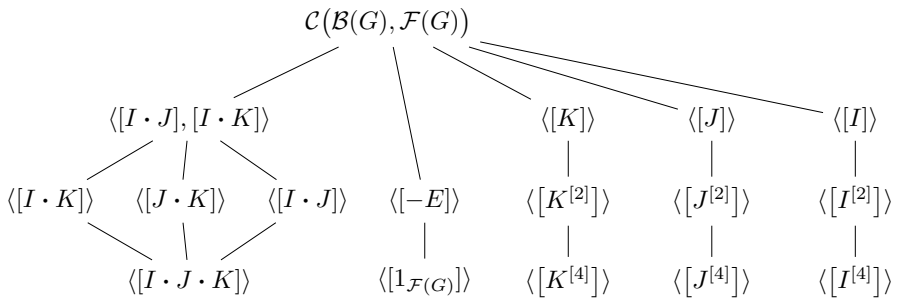

FIGURE 1. Subgroup Lattice of the Class Semigroup over Q_8

Example 4.2. Let $G = D_8 = \langle a, b \,|\, a^4 = b^2 = 1_G \ \text{ and } \ ba = a^3 b \rangle = \{1_G, a, a^2, a^3, b, ab, a^2 b, a^3 b\}$ be the dihedral group of order 8. Then $\mathsf{Z}(G) = G' = \langle a^2 \rangle = \{1_G, a^2\}$ and $G/G' \simeq C_2 \oplus C_2$. Furthermore, $\mathsf{d}(G) = 4$ and $\mathsf{D}(G) = 6$ by [**17,** Theorem 1.1].

All arguments run along the same lines as the ones given in the previous example. However, in this case, there are two elements $g, h \in G \setminus \mathsf{Z}(G)$ such that $gh = hg$. Consider the sequence $b \cdot a^2 b \in \mathcal{F}(G)$ having $\pi(b \cdot a^2 b) = \{a^2\}$, and suppose that $b \cdot a^2 b \sim S$ for some $S \in \mathcal{F}(G)$. By Lemma 3.6 (items 1 and 5), we have $\pi(S) = \{a^2\}$ and hence $\langle \mathrm{supp}(S) \rangle \subset G$ is abelian subgroup containing a^2. It follows that $\langle \mathrm{supp}(S) \rangle$ is one of $\langle a \rangle$, $\langle a^2 \rangle$, $\langle a^2, b \rangle$, and $\langle a^2, ab \rangle$.

CASE 1. $S \in \mathcal{F}\big(\langle a^2 \rangle\big)$.

Then $S = a^2$ is only possible choice, but it never happen by Lemma 3.9.3.

CASE 2. $S \in \mathcal{F}\big(\langle a \rangle\big)$.

Then $S = a^{[2]}$ is only possible choice by Lemma 3.6.4 and Lemma 3.9 (items 1 and 2). Since $\mathcal{B}(G)$-equivalence is a congruence relation on $\mathcal{F}(G)$,

$$b \cdot a^2 b \sim a^{[2]} \ \text{ implies that } \ b \cdot a^2 b \cdot a \sim a^{[3]} \,.$$

But $\{a^3\} = \pi(a^{[3]}) = \pi(b \cdot a^2 b \cdot a) = \{a, a^3\}$, a contradiction.

In the case that $S \in \mathcal{F}\big(\langle a^2, ab\rangle\big)$, we can obtain a contradiction by the same argument of CASE 2. It follows that $S = b \cdot a^2 b$, and by Lemma 3.6.4,

$$S^{[2]} \sim b^{[2]} \text{ is an idempotent element of the class semigroup } \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$$

with the relation $b^{[2]} \sim (a^2 b)^{[2]} \sim S^{[2]}$.

For the sequence $T = ab \cdot a^3 b \in \mathcal{F}(G)$, we can obtain the same result by above argument. Thus $\big[T^{[2]}\big]$ is an idempotent element of the class semigroup $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ with the relation $(ab)^{[2]} \sim (a^3 b)^{[2]} \sim T^{[2]}$. It follows that

$$|\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)| = 18\,.$$

Figure 2 presents the subgroup lattice of the class semigroup over D_8. Note that, as in the previous example, the subgroup lattice of G is not preserved in the class semigroup $\mathcal{C}(\big(\mathcal{B}(G), \mathcal{F}(G)\big)$. Furthermore, observe that the bottom elements in the lattice are all idempotent elements of the class semigroup.

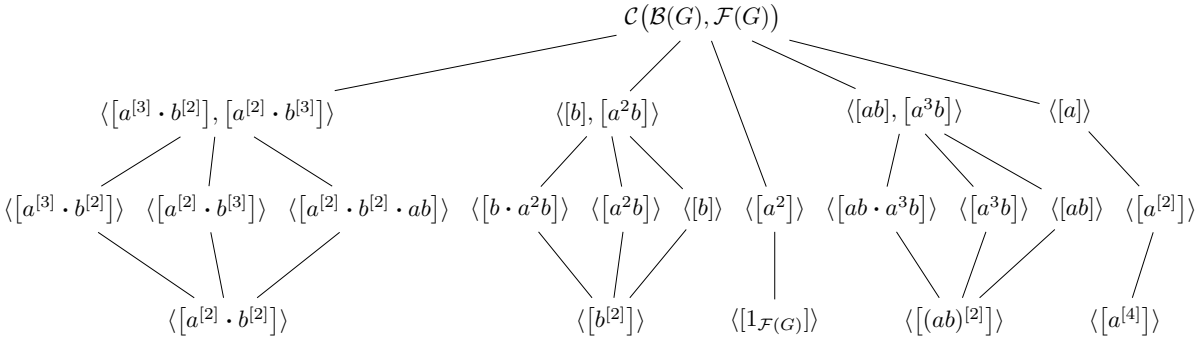

FIGURE 2. Subgroup Lattice of the Class Semigroup over D_8

Remark 4.3. In general, the group of units $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)^\times$ of the class semigroup is not a direct factor. For example, let G be the group described in Example 4.1. Assume to the contrary that $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ has a decomposition of the form

$$\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big) = \mathcal{C}_0 \times \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)^\times\,,$$

where $\mathcal{C}_0$ is a subsemigroup having 9 elements. Figure 1. shows that there are three elements $x \in \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ such that $x \neq x^3$. It follows that there exist three elements satisfying such property in the decomposition. Since $|\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)^\times| = 2$, $\mathcal{C}_0$ has at least two such elements, whence $|\mathcal{C}_0| > 9$. Indeed, if $[I]$ and $[J]$ are in $\mathcal{C}_0$, then $[I \cdot J] = [I] + [J] \in \mathcal{C}_0$ and thus we obtain that $\mathcal{C}_0$ has at least 10 elements. The similar argument works for the group described in Example 4.2.

Example 4.4. Let $G = D_6 = \langle a, b \,|\, a^3 = b^2 = 1_G \text{ and } ba = a^2 b\rangle = \{1_G, a, a^2, b, ab, a^2 b\}$ be the dihedral group of order 6. Then $\mathsf{Z}(G) = \{1_G\}$, $G' = \langle a\rangle = \{1_G, a, a^2\}$, and $G/G' \simeq C_2$. Furthermore, $\mathsf{d}(G) = 3$ and $\mathsf{D}(G) = 6$ by [**17,** Theorem 1.1].

Let $S \in \mathcal{F}(G)$. If $|\pi(S)| = 3$, then, by Theorem 3.8.1, we obtain

$$S \sim a^{[2]} \cdot b^{[2]} \quad \text{or} \quad S \sim a \cdot a^2 \cdot b\,,$$

where $\pi(a^{[2]} \cdot b^{[2]}) = \{1_G, a, a^2\}$ and $\pi(a \cdot a^2 \cdot b) = \{b, ab, a^2b\}$.

If $|\pi(S)| = 2$, then S is $\mathcal{B}(G)$-equivalent with one of the following sequences:

$$\begin{aligned} &a \cdot b^{[n]}, \quad a \cdot (ab)^{[n]}, \quad a \cdot (a^2b)^{[n]}, \quad a^2 \cdot b^{[n]}, \quad a^2 \cdot (ab)^{[n]}, \quad a^2 \cdot (a^2b)^{[n]}\,, \\ &b^{[n]} \cdot ab, \quad b \cdot (ab)^{[n]}, \quad b^{[n]} \cdot a^2b, \quad b \cdot (a^2b)^{[n]}, \quad (ab)^{[n]} \cdot a^2b, \quad ab \cdot (a^2b)^{[n]}\,, \end{aligned} \tag{4.1}$$

where $n \in \mathbb{N}$.

We now start with the following claims.

CLAIM.A:
$$\begin{aligned} &b^{[2]} \sim b^{[4]}, \quad (ab)^{[2]} \sim (ab)^{[4]}, \quad (a^2b)^{[2]} \sim (a^2b)^{[4]}, \quad a^{[2]} \sim a^{[5]}, \quad (a^2)^{[2]} \sim (a^2)^{[5]}\,, \\ &(a^2)^{[2]} \sim a^{[4]}, \quad (a^2)^{[3]} \sim a^{[3]}, \quad (a^2)^{[4]} \sim a^{[2]}, \quad a \cdot a^2 \sim a^{[3]}\,, \\ &a \cdot b \sim a^2 \cdot b \sim a \cdot b^{[3]} \sim b^{[2]} \cdot ab \sim b^{[2]} \cdot a^2b\,, \\ &a \cdot ab \sim a^2 \cdot ab \sim a \cdot (ab)^{[3]} \sim ab^{[2]} \cdot a^2b \sim ab^{[2]} \cdot b\,, \\ &a \cdot a^2b \sim a^2 \cdot a^2b \sim a \cdot (a^2b)^{[3]} \sim (a^2b)^{[2]} \cdot ab \sim (a^2b)^{[2]} \cdot b\,. \end{aligned}$$

CLAIM.B:
$$\begin{aligned} &b \nsim b^{[3]}, \quad ab \nsim (ab)^{[3]}, \quad a^2b \nsim (a^2b)^{[3]}, \quad a \nsim a^{[4]}, \quad a^{[2]} \nsim a^2\,, \\ &b \cdot ab \nsim b \cdot a^2b, \quad ab \cdot a^2b, \quad a \cdot b^{[2]}, \quad a \cdot (ab)^{[2]}, \quad a \cdot (a^2b)^{[2]}\,, \\ &b \cdot a^2b \nsim ab \cdot a^2b, \quad a \cdot b^{[2]}, \quad a \cdot (ab)^{[2]}, \quad a \cdot (a^2b)^{[2]}\,, \\ &ab \cdot a^2b \nsim a \cdot b^{[2]}, \quad a \cdot (ab)^{[2]}, \quad a \cdot (a^2b)^{[2]}\,. \end{aligned}$$

Suppose that the Claims hold true. Then we obtain that

$$|\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)| = 26 \quad \text{and} \quad \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big) = G_1 \cup G_2 \cup G_3 \cup G_4\,,$$

where

- $G_1 = \Big\{[b], \big[b^{[2]}\big], \big[b^{[3]}\big], [ab], \big[(ab)^{[2]}\big], \big[(ab)^{[3]}\big], [a^2b], \big[(a^2b)^{[2]}\big], \big[(a^2b)^{[3]}\big], [a], \big[a^{[2]}\big], \big[a^{[3]}\big], \big[a^{[4]}\big], \big[a^2\big]\Big\}$,
- $G_2 = \Big\{[a \cdot b], [a \cdot ab], \big[a \cdot a^2b\big], \big[a \cdot b^{[2]}\big], \big[a \cdot (ab)^{[2]}\big], \big[a \cdot (a^2b)^{[2]}\big], [b \cdot ab], \big[b \cdot a^2b\big], \big[ab \cdot a^2b\big]\Big\}$,
- $G_3 = \Big\{\big[a^{[2]} \cdot b^{[2]}\big], \big[a \cdot a^2 \cdot b\big]\Big\}$ (that is isomprphic to G/G'), and
- $G_4 = \Big\{[1_{\mathcal{F}(G)}]\Big\}$ $\big($that is isomorphic to $\mathsf{Z}(G)\big)$.

Figure 3 presents the subgroup lattice of the class semigroup over D_6. Note that, as in the previous example, the subgroup lattice of G is not preserved in the class semigroup $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$. Furthermore, observe that the elements in the set

$$\Big\{[b], [ab], \big[a^2b\big], [a], \big[a^2\big]\Big\} \cup G_2$$

are not regular, whence $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$ is not Clifford semigroup, and the bottom elements in the lattice are all idempotent elements of the class semigroup.

Proof of the Claim. We only show the first assertions, and others can be proved by the same way. Let $T \in \mathcal{F}(G)$. Since $b^2 = 1_G$, it suffices to show that if $b^{[4]} \cdot T \in \mathcal{B}(G)$, then $b^{[2]} \cdot T \in \mathcal{B}(G)$. Suppose that $b^{[4]} \cdot T \in \mathcal{B}(G)$.

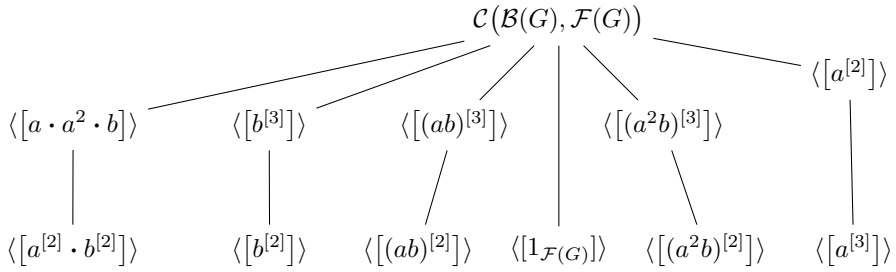

FIGURE 3. Subgroup Lattice of Class Semigroup over D_6

CASE 1. $|\pi(T)| = 3$.

Then we have

$$T \sim a^{[2]} \cdot b^{[2]} \quad \text{or} \quad T \sim a \cdot a^2 \cdot b\,.$$

Since $b^{[4]} \cdot T \in \mathcal{B}(G)$, it follows that we have the only case $T \sim a^{[2]} \cdot b^{[2]}$. Then, since $b^{[2]} \cdot a \cdot b \cdot a \cdot b \in \mathcal{B}(G)$,

$$b^{[2]} \cdot T \sim b^{[2]} \cdot a^{[2]} \cdot b^{[2]} \text{ implies that } b^{[2]} \cdot T \in \big[b^{[2]} \cdot a^{[2]} \cdot b^{[2]}\big] \subset \mathcal{B}(G)\,.$$

CASE 2. $|\pi(T)| = 2$.

Then T is $\mathcal{B}(G)$-equivalent with one of the sequence described in (4.1). Since $b^{[4]} \cdot T \in \mathcal{B}(G)$, the possible choice of T under $\mathcal{B}(G)$-equivalence is one the following sequences:

$$a \cdot (ab)^{[\text{even}]}, \quad a \cdot (a^2b)^{[\text{even}]}, \quad a^2 \cdot (ab)^{[\text{even}]}, \quad a^2 \cdot (a^2b)^{[\text{even}]}\,,$$
$$b \cdot (ab)^{[\text{odd}_{\ge 3}]}, \quad b \cdot (a^2b)^{[\text{odd}_{\ge 3}]}, \quad (ab)^{[\text{odd}]} \cdot a^2b, \quad ab \cdot (a^2b)^{[\text{odd}]}\,.$$

Then we obtain the following simple calculation, and it can cover all other cases:

$$ab \cdot b \cdot ab \cdot b \cdot a, \quad a^2b \cdot b \cdot a^2b \cdot a \cdot b, \quad ab \cdot b \cdot ab \cdot a^2 \cdot b, \quad a^2b \cdot b \cdot a^2b \cdot b \cdot a^2,$$
$$ab \cdot b \cdot ab \cdot b \cdot ab \cdot b, \quad a^2b \cdot b \cdot a^2b \cdot b \cdot a^2b \cdot b, \quad ab \cdot b \cdot a^2b \cdot b,$$

which are all product-one sequences, and thus it follows that $b^{[2]} \cdot T \in \mathcal{B}(G)$.

CASE 3. $|\pi(T)| = 1$.

Then $\langle \text{supp}(T) \rangle$ is abelian subgroup by Lemma 3.6.5. If $\langle \text{supp}(T) \rangle = \langle 1_G \rangle$, then we are done because $T \in \mathcal{B}(G)$.

If $\langle \text{supp}(T) \rangle = \langle b \rangle$, then $T = b^{[n]}$ for some $n \in \mathbb{N}$ by Lemma 3.6.4. Since $b^{[4]} \cdot T \in \mathcal{B}(G)$, it follows that n should be even number, and hence we are done.

By symmetry, we can obtain the same result whenever $\langle \text{supp}(T) \rangle = \langle ab \rangle$ or $\langle a^2b \rangle$.

Suppose now that $\langle \text{supp}(T) \rangle = \langle a \rangle$. Then $T = a^{[n_1]} \cdot (a^2)^{[n_2]}$ for some $n_1, n_2 \in \mathbb{N}_0$.

i) $n_1 = 0$.
   In this case, $b^{[4]} \cdot (a^2)^{[n_2]} \in \mathcal{B}(G)$ implies that $n_2 \ge 2$. It follows that $b^{[2]} \cdot (a^2)^{[n_2]} \in \mathcal{B}(G)$.
ii) $n_2 = 0$.
   In this case, $b^{[4]} \cdot a^{[n_1]} \in \mathcal{B}(G)$ implies that $n_1 \ge 2$. It follows that $b^{[2]} \cdot a^{[n_1]} \in \mathcal{B}(G)$.
iii) $n_1 \ge 1$ and $n_2 \ge 1$.
   To avoid the trivial case, we may assume that $n_1 \ne n_2$.

If $|n_1 - n_2| = 1$, then, since any choice of n_1, n_2 can be reduced to the case

$$n_1 = 1, n_2 = 2 \quad \text{or} \quad n_1 = 2, n_2 = 1\,,$$

it suffices to verify only such two cases, and we have the followings:

$$\begin{aligned} a \cdot b \cdot a^2 \cdot a^2 \cdot b^{[3]} \in \mathcal{B}(G) \quad &\text{implies that} \quad a \cdot b \cdot a^2 \cdot a^2 \cdot b \in \mathcal{B}(G), \\ a \cdot a \cdot b \cdot a^2 \cdot b^{[3]} \in \mathcal{B}(G) \quad &\text{implies that} \quad a \cdot a \cdot b \cdot a^2 \cdot b \in \mathcal{B}(G). \end{aligned}$$

If $|n_1 - n_2| \ge 2$, then it can be reduced to the case $n_1 = 0$ or $n_2 = 0$.

Therefore, in any cases, we can obtain $b^{[2]} \cdot T \in \mathcal{B}(G)$, and it follows that $b^{[2]} \sim b^{[4]}$. Moreover, $b \nsim b^{[3]}$ because $b^{[3]} \cdot (ab)^{[3]} \in \mathcal{B}(G)$, but $b \cdot (ab)^{[3]} \notin \mathcal{B}(G)$. Hence

$$[b], \quad \big[b^{[2]}\big], \quad \big[b^{[3]}\big]$$

are distinct $\mathcal{B}(G)$-equivalence classes in the class semigroup $\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$. □

5. Arithmetic Properties of the monoid of product-one sequences. The goal of this section is to study the arithmetic of the monoid $\mathcal{B}(G)$ of product-one sequences. To do so we briefly recall some arithmetical concepts (details can be found in [**18**]).

Let H be an atomic monoid and $a, b \in H$. If $a = u_1 \cdot \ldots \cdot u_k$, where $k \in \mathbb{N}$ and $u_1, \ldots, u_k \in \mathcal{A}(H)$, then k is called the length of the factorization and $\mathsf{L}_H(a) = \mathsf{L}(a) = \{k \in \mathbb{N} \mid a \text{ has a factorization of length } k\} \subset \mathbb{N}$ is the *set of lengths* of a. As usual we set $\mathsf{L}(a) = \{0\}$ if $a \in H^\times$, and then

$$\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$$

denotes the *system of sets of lengths* of H. Let $k \in \mathbb{N}$ and suppose that $H \neq H^\times$. Then

$$\mathcal{U}_k(H) = \bigcup_{k \in L, L \in \mathcal{L}(H)} L \ \subset \ \mathbb{N}$$

denotes the union of sets of lengths containing k, and we set

$$\rho_k(H) = \sup \mathcal{U}_k(H)\,.$$

If $L = \{m_1, \ldots, m_k\} \subset \mathbb{Z}$ is a finite subset of the integers, where $k \in \mathbb{N}$ and $m_1 < \ldots < m_k$, then $\Delta(L) = \{m_i - m_{i-1} \mid i \in [2, k]\} \subset \mathbb{N}$ is the set of distances of L. If all sets of lengths are finite, then

$$\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L)$$

is the *set of distances* of H. It is easy to check that $\min \Delta(H) = \gcd \Delta(H)$. If $\theta\colon H \to B$ is a transfer homomorphism between atomic monoids having finite sets of lengths, then ([**18,** Proposition 3.2.3])

$$\mathcal{L}(H) = \mathcal{L}(B) \ \text{ whence } \Delta(H) = \Delta(B) \text{ and } \mathcal{U}_k(H) = \mathcal{U}_k(B) \ \text{ for all } k \in \mathbb{N}. \tag{5.1}$$

It is well-known that if H is finitely generated, then then all unions $\mathcal{U}_k(H)$ of sets of lengths (in particular, all sets of lengths) and the set of distances $\Delta(H)$ are finite ([**18,** Theorem 3.1.4]).

We will study the system of sets of lengths and all further mentioned invariants for the monoid $\mathcal{B}(G)$. As usual, we set

$$\mathcal{L}(G) = \mathcal{L}\big(\mathcal{B}(G)\big), \ \Delta(G) = \Delta\big(\mathcal{B}(G)\big), \ \mathcal{U}_k(G) = \mathcal{U}_k\big(\mathcal{B}(G)\big)$$

and $\rho_k(G) = \rho_k\big(\mathcal{B}(G)\big)$ for all $k \in \mathbb{N}$. Since $\mathcal{B}(G)$ is finitely generated by Lemma 3.2, all these invariants are finite. The significance of the monoid $\mathcal{B}(G)$ for abelian groups stems from its relevance for general Krull monoids. Indeed, if H is a commutative Krull monoid with class group G such that every class contains a prime divisor, then there is a transfer homomorphism $\theta\colon H \to \mathcal{B}(G)$ and hence $\mathcal{L}(H) = \mathcal{L}(G)$. This transfer process from monoids of zero-sum sequences to more general monoids carries over to transfer Krull monoids ([**16**]).

We study the structure of $\mathcal{U}_k(G)$ and of $\Delta(G)$ for general finite groups G and we will derive canonical bounds for their size. Most results are known in the abelian case partly with different bounds (for a recent survey on the abelian case we refer to [**32**]). However, if G is non-abelian, then $\mathcal{B}(G)$ is not a transfer Krull monoid by Proposition 3.4. Thus the present results cannot be derived from the abelian setting. If $|G| \le 2$, then $\mathcal{B}(G)$ is factorial, $\mathcal{L}(G) = \{\{k\} \mid k \in \mathbb{N}_0\}$, $\Delta(G) = \emptyset$, and $\mathcal{U}_k(G) = \{k\}$ for all $k \in \mathbb{N}$. To avoid annoying case distinctions we exclude this trivial case.

Throughout this section, let G be a finite group with $|G| \ge 3$.

Although the forthcoming proofs parallel the proofs given in the commutative setting there is a main difference. It stems from the fact that, in the non-abelian case, the embedding $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is not a divisor homomorphism. Thus there exist $U, V \in \mathcal{B}(G)$ such that U divides V in $\mathcal{F}(G)$, but not in $\mathcal{B}(G)$. Moreover, U and V can be atoms (e.g., if G is the quaternion group, as discussed in Examples 4.1, then $U = I^{[4]} \in \mathcal{A}(G)$ and $V = I^{[4]} \cdot J^{[2]} \in \mathcal{A}(G)$ have this property).

Lemma 5.1. *Let $k, \ell \in \mathbb{N}$ with $k < \ell$ and $U_1, \ldots, U_k, V_1, \ldots, V_\ell \in \mathcal{A}(G)$ such that $U_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} U_k = V_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} V_\ell$. There exist $\mu \in [1,k]$, $\lambda, \lambda' \in [1,\ell]$ with $\lambda \ne \lambda'$, and $g_1, g_2 \in G$ such that $U_\mu = g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_m$ with $m \ge 2$, $1_G = g_1 \ldots g_m$, $g_1 \,|\, V_\lambda$, and $g_2 \,|\, V_{\lambda'}$ in $\mathcal{F}(G)$.*

Proof. Assume to the contrary that the assertion does not hold. Since 1_G is a prime element of $\mathcal{B}(G)$, we may suppose without restriction that all U_i and V_j have length at least two. We set $U_1 = g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_m$ where $m \ge 2$ and $1_G = g_1 \ldots g_m$. Then $g_1 \cdot g_2$ divides V_λ for some $\lambda \in [1,\ell]$, say $\lambda = 1$. Then we consider $g_2 \cdot g_3$. Since the assertion does not hold, it follows that $g_1 \cdot g_2 \cdot g_3$ divides V_1. Proceeding recursively we obtain that $U_1 \,|\, V_1$, say $V_1 = U_1 \cdot V_1'$ with $V_1' \in \mathcal{F}(G)$. Thus we obtain the equation

$$U_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} U_k = V_1' \cdot V_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} V_\ell \,.$$

Proceeding in this way we end up with an equation of the form

$$1_{\mathcal{F}(G)} = S_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} S_\eta \cdot V_{\eta+1} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} V_\ell \,,$$

where $\eta \le k$ and $S_1, \ldots, S_\eta \in \mathcal{F}(G)$, a contradiction to $k < \ell$. □

We consider the following property:

P. If $U = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{A}(G)$ and $g_1 = h_1 h_2$ with $h_1, h_2 \in G$, then $U' = h_1 \cdot h_2 \cdot g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$ is either an atom or a product of two atoms at most.

Remark 5.2. Of course, every abelian group satisfies Property **P** and the same is true for some non-abelian groups such as the quaternion group. However, for every $n \ge 9$, the dihedral group D_{2n} does not have Property **P** as the following example shows.

Example 5.3. 1. Let $G = Q_8$ be the quaternion group as discussed in Example 4.1. Then $\mathsf D(G) = 6$, and clearly any atom having length at most 4 satisfies Property **P**. Any atom U having the length 6 has the form

$$U = g_1^{[4]} \cdot g_2^{[2]}, \quad \text{where } g_1, g_2 \in \{I, J, K, -I, -J, -K\} \text{ with } g_2 \neq \pm g_1,$$

and any atom V having length 5 is one of the following three types:

- $V = g_1^{[3]} \cdot g_2 \cdot g_3$, where $g_1, g_2, g_3 \in \{I, J, K, -I, -J, -K\}$ with $g_2 \neq g_3$ and $g_2, g_3 \neq \pm g_1$.
- $V = g_1^{[2]} \cdot g_2^{[2]} \cdot (-E)$, where $g_1, g_2 \in \{I, J, K, -I, -J, -K\}$ with $g_2 \neq \pm g_1$.
- $V = g_1 \cdot (-g_1) \cdot g_2 \cdot (-g_2) \cdot (-E)$, where $g_1, g_2 \in \{I, J, K\}$ with $g_1 \neq g_2$.

It is easy to check that G satisfies Property **P**.

2. Let $G = D_{2n} = \langle a, b \,|\, a^n = b^2 = 1_G \text{ and } ba = a^{-1}b \rangle$ be the dihedral group, where $n \ge 9$. Consider the following sequences:

$$U = b^{[2]} \cdot (ba)^{[3]} \cdot a^2 \cdot ba^5 \quad \text{and} \quad U' = b^{[2]} \cdot (ba)^{[3]} \cdot ba^2 \cdot ba^4 \cdot ba^5 .$$

Then U' is a product of $b^{[2]}$, $(ba)^{[2]}$, and $ba^2 \cdot ba \cdot ba^4 \cdot ba^5$, which are atoms. Now we need to verify that U is an atom. Assume to the contrary that U is not atom, say $U = W_1 \cdot W_2$ with $W_1, W_2 \in \mathcal B(G)$, and let W_1 be an atom with $a^2 \,|\, W_1$. Write $W_1 = g_1 \cdot g_2 \cdot \ldots \cdot g_\ell$ with $g_1 = a^2$ and $g_1 g_2 \ldots g_\ell = 1_G$. Then $\ell = 3$ or $\ell = 5$. If $\ell = 3$, then $g_2 g_3 = a^{-2}$ and $g_2, g_3 \in \{b, ba, ba^5\}$. Since $n \ge 9$, this is impossible. If $\ell = 5$, then $W_2 = b^{[2]}$ or $W_2 = (ba)^{[2]}$ which implies that $W_1 = (ba)^{[3]} \cdot a^2 \cdot ba^5$ or $W_1 = b^{[2]} \cdot ba \cdot a^2 \cdot ba^5$. It is easy to check that W_1 is not an atom. Thus G does not have Property **P**.

Lemma 5.4. *Suppose that G satisfies Property **P**. Then for every $S \in \mathcal B(G)$ with $\max \Delta\big(\mathsf L(S)\big) \ge 2$, there exists $T \in \mathcal B(G)$ such that $|T| < |S|$ and $\max \Delta\big(\mathsf L(T)\big) \ge \max \Delta\big(\mathsf L(S)\big) - 1$.*

Proof. Let $S \in \mathcal B(G)$ and $d = \max \Delta\big(\mathsf L(S)\big) \ge 2$. Then there are $k, \ell \in \mathbb N$ and $U_1, \ldots, U_k, V_1, \ldots, V_\ell \in \mathcal A(G)$ such that

$$S = U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_\ell$$

with $\ell - k = d$ and $U_1 \cdot \ldots \cdot U_k$ has no factorization of length in $[k+1, \ell-1]$. Since $1_G \in \mathcal B(G)$ is a prime element, we may assume that 1_G does not divide S, and thus all U_i and V_j have length at least two.

By Lemma 5.1, we may assume that there are $g_1, g_2 \in G$ such that

$$g_1 \cdot g_2 \,|\, U_1, \quad g_1 \,|\, V_1 \quad \text{and} \quad g_2 \,|\, V_2 \ \text{ in } \mathcal F(G).$$

Let $U_1 = g_1 \cdot g_2 \cdot U_1'$, $V_1 = g_1 \cdot V_1'$ and $V_2 = g_2 \cdot V_2'$ with $U_1', V_1', V_2' \in \mathcal F(G)$. Then we set $g_0 = g_1 g_2 \in G$, and consider

$$U_1'' = g_0 \cdot U_1' \ \text{ and } \ V_1'' = g_0 \cdot V_1' \cdot V_2'.$$

Clearly, $U_1'' \in \mathcal A(G)$. Since V_1 gives rise to a product-one equation with g_1 being the finial element and V_2 gives rise to a product-one equation with g_2 being the first element, it follows that $V_1'' \in \mathcal B(G)$. We obtain that

$$U_1'' \cdot U_2 \cdot \ldots \cdot U_k = V_1'' \cdot V_3 \cdot \ldots \cdot V_\ell .$$

We set $T = U_1'' \cdot U_2 \cdot \ldots \cdot U_k$ and observe that $|T| < |S|$. If $T = W_1 \cdot \ldots \cdot W_t$ with $W_1, \ldots, W_t \in \mathcal A(G)$ and $g_0 \,|\, W_1$ in $\mathcal F(G)$, then $W_1 = g_0 \cdot W_1'$ and $W_1'' = g_1 \cdot g_2 \cdot W_1'$ is either atom or product of precisely two atoms. Thus $S = U_1 \cdot \ldots \cdot U_k$ has a factorization of length t or $t+1$. It follows that T has no factorization

of length in $[k+1, \ell-2]$, and thus we obtain

$$\max \Delta\big(\mathsf{L}(T)\big) \ge \ell - 1 - k = d - 1 = \max \Delta\big(\mathsf{L}(S)\big) - 1\,.$$

□

The next result shows that the set of distances and all unions of sets of lengths of $\mathcal{B}(G)$ are finite intervals. This is far from being true in general. Indeed, for every finite set $\Delta \subset \mathbb{N}$ with $\min \Delta = \gcd \Delta$ there is a finitely generated Krull monoid H such that $\Delta(H) = \Delta$ ([**22**]).

Theorem 5.5.

1. *$\mathcal{U}_k(G)$ is a finite interval for all $k \in \mathbb{N}$.*
2. *If G satisfies Property* **P**, *then $\Delta(G)$ is a finite interval with $\min \Delta(G) = 1$.*

Proof. 1. Let $k \in \mathbb{N}$. We set $\lambda_k(G) = \min \mathcal{U}_k(G)$. Then $\mathcal{U}_k(G) \subset [\lambda_k(G), \rho_k(G)]$, and we have to show equality. Note that it is sufficient to prove that $[k, \rho_k(G)] \subset \mathcal{U}_k(G)$. Indeed, suppose that this is done, and let $\ell \in [\lambda_k(G), k]$. Then $\ell \le k \le \rho_\ell(G)$, hence $k \in \mathcal{U}_\ell(G)$ and consequently $\ell \in \mathcal{U}_k(G)$. It follows that $[\lambda_k(G), \rho_k(G)] = \mathcal{U}_k(G)$.

To prove the assertion, let $\ell \in [k, \rho_k(G)]$ be minimal such that $[\ell, \rho_k(G)] \subset \mathcal{U}_k(G)$. Assume to the contrary that $\ell > k$. We set $\Omega = \{A \in \mathcal{B}(G) \mid \{k, j\} \subset \mathsf{L}(A) \text{ for some } j \ge \ell\}$ and choose $B \in \Omega$ such that $|B|$ is minimal. Then

$$B = U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_j, \quad \text{where } U_1, \ldots, U_k, V_1, \ldots, V_j \in \mathcal{A}(G)\,,$$

and by Lemma 5.1, we may assume that

$$U_k = g_1 \cdot g_2 \cdot U \ \text{ with } \ g_1 \mid V_{j-1} \ \text{ and } \ g_2 \mid V_j\,,$$

where $U = g_3 \cdot \ldots \cdot g_t$ and $g_1 \ldots g_t = 1_G$. We set $g_0 = g_1 g_2 \in G$ and obtain that $U_k' = g_0 \cdot U \in \mathcal{A}(G)$. Write

$$V_{j-1} = h_1 \cdot \ldots \cdot h_n \cdot g_1 \ \text{ and } \ V_j = g_2 \cdot s_1 \cdot \ldots \cdot s_m$$

with $h_1 \ldots h_n g_1 = 1_G$ and $g_2 s_1 \ldots s_m = 1_G$. Let $V_{j-1}' = g_0 \cdot V \in \mathcal{B}(G)$, where $V = h_1 \cdot \ldots \cdot h_n \cdot s_1 \cdot \ldots \cdot s_m \in \mathcal{F}(G)$, and consider

$$B' = U_1 \cdot \ldots \cdot U_{k-1} \cdot U_k'\,.$$

Then $|B'| < |B|$, and

$$B' = U_1 \cdot \ldots \cdot U_{k-1} \cdot U_k' = V_1 \cdot \ldots \cdot V_{j-2} \cdot W_1 \cdot \ldots \cdot W_t\,,$$

where $V_{j-1}' = W_1 \cdot \ldots \cdot W_t$ with $W_1, \ldots, W_t \in \mathcal{A}(G)$. By the minimality of $|B|$, we have $(j-2)+t < \ell \le j$. Hence $t = 1$ and $j = \ell$. Thus $\ell - 1 \in \mathcal{U}_k(G)$, a contradiction to the minimality of ℓ. Therefore $\ell = k$ and hence $[k, \rho_k(G)] \subset \mathcal{U}_k(G)$.

2. Since $\Delta(G)$ is finite as mentioned before, we can take $S_0 \in \mathcal{B}(G)$ with minimal length such that $\max \Delta\big(\mathsf{L}(S_0)\big) = \max \Delta(G)$. By Lemma 5.4, we can find $S_1 \in \mathcal{B}(G)$ with minimal length such that $|S_1| < |S_0|$ and $\max \Delta\big(\mathsf{L}(S_1)\big) \ge \max \Delta(G) - 1$. By the minimality of S_0,

$$|S_1| < |S_0| \qquad \text{implies} \qquad \max \Delta\big(\mathsf{L}(S_1)\big) < \max \Delta(G)\,.$$

It follows that $\max \Delta(G) - 1 = \max \Delta\big(\mathsf{L}(S_1)\big) \in \Delta(G)$. Again Lemma 5.4 implies that we can find $S_2 \in \mathcal{B}(G)$ with minimal length such that $|S_2| < |S_1|$ and $\max \Delta\big(\mathsf{L}(S_2)\big) \ge \max \Delta(G) - 2$. By the minimality of S_1,

$$|S_2| < |S_1| \qquad \text{implies} \qquad \max \Delta\big(\mathsf{L}(S_2)\big) < \max \Delta(G) - 1\,.$$

It follows that $\max \Delta(G) - 2 = \max \Delta\big(\mathsf L(S_2)\big) \in \Delta(G)$. Continuing this process, we can obtain $S_n \in \mathcal B(G)$ such that

$$1 = \max \Delta(G) - n = \max \Delta\big(\mathsf L(S_n)\big) \in \Delta(G)\,.$$

Thus $\Delta(G) = [1, \max \Delta(G)]$ is an interval. □

Next we study the maxima of the sets $\mathcal U_k(G)$. Recall that we have defined $\rho_k(G) = \max \mathcal U_k(G)$ for all $k \in \mathbb N$. Even in case of abelian groups, precise values of $\rho_{2k+1}(G)$ are unknown in general ([**11**]).

Proposition 5.6. *Let $k \in \mathbb N$.*

1. $\rho_k(G) \le \frac{k\mathsf D(G)}{2}$ *for all* $k \in \mathbb N$.
2. $\rho_{2k}(G) = k\mathsf D(G)$ *for all* $k \in \mathbb N$.

In particular, $1 + k\mathsf D(G) \le \rho_{2k+1}(G) \le k\mathsf D(G) + \frac{\mathsf D(G)}{2}$ *for all* $k \in \mathbb N$.

Proof. 1. Let $k \in \mathbb N$. Let $A \in \mathcal B(G)$ with $k \in \mathsf L(A)$. We have to show that $\max \mathsf L(A) \le \frac{k\mathsf D(G)}{2}$. There are $U_1, \ldots, U_k \in \mathcal A(G)$ such that

$$A = U_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} U_k\,.$$

Since $1_G \in \mathcal B(G)$ is a prime element, we may assume that 1_G does not divide A, and hence any atom dividing A has length at least 2. If $A = V_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} V_\ell$ for $V_1, \ldots, V_\ell \in \mathcal A(G)$, then we obtain

$$2\ell \le \sum_{i=1}^{\ell} |V_i| = |A| = \sum_{j=1}^{k} |U_j| \le k\mathsf D(G)\,.$$

It follows that $\ell \le \frac{k\mathsf D(G)}{2}$, and thus $\max \mathsf L(A) \le \frac{k\mathsf D(G)}{2}$.

2. Let $k \in \mathbb N$. Then, by 1., we have $\rho_{2k}(G) \le k\mathsf D(G)$. Now let $U = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal A(G)$ with $\ell = |U| = \mathsf D(G)$, where $g_1, \ldots, g_\ell \in G$. Consider the sequence

$$V = g_1^{-1} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell^{-1} \in \mathcal A(G)\,.$$

Then $k\mathsf D(G) \in \mathsf L\big((U \boldsymbol{\cdot} V)^{[k]}\big)$. Since $2k \in \mathsf L\big((U \boldsymbol{\cdot} V)^{[k]}\big)$, we obtain $\rho_{2k}(G) \ge k\mathsf D(G)$, and hence $\rho_{2k}(G) = k\mathsf D(G)$.

It remains to prove the "In particular" statement. For all $i, j \in \mathbb N$, we have $\mathcal U_i(G) + \mathcal U_j(G) \subset \mathcal U_{i+j}(G)$ whence $\rho_i(G) + \rho_j(G) \le \rho_{i+j}(G)$. Thus the "In particular" statement follows from 1. and 2. □

Our next goal is to study the maximum of the set of distances $\Delta(G)$. If G is abelian, then precise values for $\max \Delta(G)$ are known only for very special classes of groups including cyclic groups ([**23**]). For general groups G, we study $\max \Delta(G)$ via a further invariant (introduced in Definition 5.7). The main result is Proposition 5.12.

Definition 5.7. Let H be an atomic monoid.

1. For $b \in H$, let $\omega(H, b)$ denote the smallest $N \in \mathbb N_0 \cup \{\infty\}$ with the following property:
   For all $n \in \mathbb N$ and $a_1, \ldots, a_n \in H$, if $b \mid a_1 \ldots a_n$, then there exists a subset $\Omega \subset [1, n]$ such that $|\Omega| \le N$ and $b \mid \prod_{\nu \in \Omega} a_\nu$.
2. We set
$$\omega(H) = \sup\{\omega(H, u) \mid u \in \mathcal A(H)\} \in \mathbb N_0 \cup \{\infty\}\,.$$

If H is an atomic monoid with $\Delta(H) \neq \emptyset$, then $2 + \max \Delta(H) \le \omega(H)$ (see **[18,** Theorem 1.6.3] and **[20,** Proposition 3.6]). As usual we set $\omega(G) = \omega\big(\mathcal{B}(G)\big)$ and observe that $2 + \max \Delta(G) \le \omega(G)$. If G is a cyclic group or an elementary 2-group, then $2 + \max \Delta(G) = \omega(G) = \mathsf{D}(G)$.

Lemma 5.8. *We have $\mathsf{D}(G) \le \omega(G)$, and equality holds if G is abelian.*

Proof. Let $U = g_1 \cdot \ldots \cdot g_\ell \in \mathcal{A}(G)$ with $\ell = |U| = \mathsf{D}(G)$. Put $V_i = g_i \cdot g_i^{-1} \in \mathcal{A}(G)$ for all $i \in [1, \ell]$. Then we obtain

$$U \,|\, V_1 \cdot \ldots \cdot V_\ell \ \text{ in } \mathcal{B}(G)\,.$$

Assume to the contrary that U divides a proper subproduct in $\mathcal{B}(G)$, say $U \,|\, V_1 \cdot \ldots \cdot V_k$ for some $k \in [1, \ell-1]$. Then $2k \ge \ell$. If $2k = \ell$, then $U = V_1 \cdot \ldots \cdot V_k$ is not atom in $\mathcal{B}(G)$. If $2k > \ell$, then $\ell - k < k$, and, for each $j = [1, \ell - k]$, we may assume that $g_{k+j} = g_j^{-1}$. Hence we have

$$U = (g_1 \cdot g_{k+1}) \cdot \ldots \cdot (g_{\ell-k} \cdot g_\ell) \cdot (g_{\ell-k+1} \cdot \ldots \cdot g_k)\,,$$

and each terms is in $\mathcal{B}(G)$. It follows that U is not atom in $\mathcal{B}(G)$, a contradiction. Thus U cannot divide a proper subproduct, and hence $\mathsf{D}(G) \le \omega(G)$.

Suppose that G is abelian. It remains to show that $\omega(G) \le \mathsf{D}(G)$. Let $U \in \mathcal{A}(G)$. If $U \,|\, V_1 \cdot \ldots \cdot V_k$ for $V_1, \ldots, V_k \in \mathcal{B}(G)$, then there is a subproduct of at most $|U|$ factors such that U divides this subproduct in $\mathcal{F}(G)$. Since $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor homomorphism, this divisibility holds in $\mathcal{B}(G)$. Hence $\omega(G, U) \le |U| \le \mathsf{D}(G)$, and it follows that $\omega(G) \le \mathsf{D}(G)$. □

Next we define Davenport constants of additive commutative semigroups (as studied in **[35, 1, 34]**) and will apply these concepts to the class semigroup of $\mathcal{B}(G)$. Recall that all our semigroups have an identity element (a zero element in the additive case) and we use the convention that an empty sum equals the zero element.

Definition 5.9. Let $\mathcal{C}$ be an additive commutative semigroup.

1. We denote by $\mathsf{d}(\mathcal{C})$ the smallest $d \in \mathbb{N}_0 \cup \{\infty\}$ with the following property:
   For all $n \in \mathbb{N}$ and $c_1, \ldots, c_n \in \mathcal{C}$, there exists $\Omega \subset [1, n]$ such that $|\Omega| \le d$ and $\sum_{\nu=1}^n c_\nu = \sum_{\nu \in \Omega} c_\nu$.
2. We denote by $\mathsf{D}(\mathcal{C})$ the smallest $\ell \in \mathbb{N} \cup \{\infty\}$ with the following property:
   For all $n \in \mathbb{N}$ with $n \ge \ell$ and $c_1, \ldots, c_n \in \mathcal{C}$, there exists $\Omega \subsetneq [1, n]$ such that $\sum_{\nu=1}^n c_\nu = \sum_{\nu \in \Omega} c_\nu$.

If G is a finite abelian group, then of course the definitions for $\mathsf{D}(G)$ and $\mathsf{d}(G)$ given in Definition 3.1 and in Definition 5.9 coincide.

Lemma 5.10. *If $\mathcal{C}$ is a finite commutative semigroup, then $\mathsf{D}(\mathcal{C}) = \mathsf{d}(\mathcal{C}) + 1 \le |\mathcal{C}|$.*

Proof. The equality $\mathsf{D}(\mathcal{C}) = \mathsf{d}(\mathcal{C}) + 1$ is verified in **[1,** Proposition 1.2]. Since we could not find a reference that $|\mathcal{C}|$ is an upper bound, we provide the short argument. To show that $\mathsf{D}(\mathcal{C}) \le |\mathcal{C}|$, it suffices to verify that $|\mathcal{C}|$ has the property given in Definition 5.9. So let $n \in \mathbb{N}$ with $n \ge |\mathcal{C}|$ and $c_1, \ldots, c_n \in \mathcal{C}$. If all sums

$$0 = \sum_{\nu \in \emptyset} c_\nu, c_1, c_1 + c_2, \ldots, c_1 + \ldots + c_{n-1}$$

are pairwise distinct, then one of the sums coincides with $c_1 + \ldots + c_n$ as required. Suppose there are $k, \ell \in [0, n-1]$ with $k < \ell$ and $c_1 + \ldots + c_k = c_1 + \ldots + c_\ell$. Then $c_1 + \ldots + c_n = c_1 + \ldots + c_k + c_{\ell+1} + \ldots + c_n$ as required. □

Lemma 5.11. *Let F be a monoid, $H \subset F$ a submonoid with $H^\times = H \cap F^\times$ and $\mathcal{C} = \mathcal{C}^*(H, F)$.*

If $n \in \mathbbm{N}$ and $f, a_1, \ldots, a_n \in F$ with $fa_1 \ldots a_n \in H$, then there exists a subset $\Omega \subset [1, n]$ such that

$$|\Omega| \le \mathsf d(\mathcal{C}) \quad \text{and} \quad f \prod_{\nu \in \Omega} a_\nu \in H \,.$$

Proof. By the definition of $\mathsf d(\mathcal{C})$, there exists a subset $\Omega \subset [1, n]$ such that $|\Omega| \le \mathsf d(\mathcal{C})$ and

$$\sum_{\nu=1}^{n} [a_\nu]_H^F = \sum_{\nu \in \Omega} [a_\nu]_H^F \,.$$

Since $fa_1 \ldots a_n \in H$, we have

$$f \prod_{\nu \in \Omega} a_\nu \in \Big[f \prod_{\nu \in \Omega} a_\nu \Big]_H^F = [f]_H^F + \sum_{\nu \in \Omega} [a_\nu]_H^F = [f]_H^F + \sum_{\nu=1}^{n} [a_\nu]_H^F = \Big[f \prod_{\nu=1}^{n} a_\nu \Big]_H^F \subset H \,.$$

□

Proposition 5.12.

1. $\mathsf D(G) \le \omega(G) \le \mathsf D(G) + \mathsf d\Big(\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)\Big)$.
2. $\mathsf D(G/G') \le \mathsf D\Big(\mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)\Big)$, *and equality holds if G is abelian.*

Proof. We set $\mathcal{C} = \mathcal{C}\big(\mathcal{B}(G), \mathcal{F}(G)\big)$.

1. The first inequality follows from Lemma 5.8. For the second inequality, let $U \in \mathcal{A}(G)$, and $A_1, \ldots, A_n \in \mathcal{B}(G)$ such that

$$U \mid A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n \quad \text{in } \mathcal{B}(G) \,.$$

After renumbering if necessary, we may assume that $U \mid A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_{|U|}$ in $\mathcal{F}(G)$, say $A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_{|U|} = U \boldsymbol{\cdot} W$ with $W \in \mathcal{F}(G)$. Then $W \boldsymbol{\cdot} A_{|U|+1} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_n \in \mathcal{B}(G)$. By Lemma 5.11, there is a subset $\Omega \subset \big[|U|+1, n\big]$, say $\Omega = \big[|U|+1, m\big]$, such that $|\Omega| \le \mathsf d(\mathcal{C})$ and $W \boldsymbol{\cdot} A_{|U|+1} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_m \in \mathcal{B}(G)$. Thus we obtain

$$A_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_m = U \boldsymbol{\cdot} (W \boldsymbol{\cdot} A_{|U|+1} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} A_m)$$

and $m \le |U| + \mathsf d(\mathcal{C}) \le \mathsf D(G) + \mathsf d(\mathcal{C})$.

2. By Theorem 3.8.1, G/G' is an isomorphic to a subsemigroup of $\mathcal{C}$. Clearly, this implies that $\mathsf D(G/G') \le \mathsf D(\mathcal{C})$. Suppose that G is abelian. Then $|G'| = 1$ and G/G' is isomorphic to G. Furthermore, $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory, the class semigroup $\mathcal{C}$ is isomorphic to the class group of $\mathcal{B}(G)$ by Lemma 2.1, and the class group of $\mathcal{B}(G)$ is isomorphic to G. Thus equality holds. □

Acknowledgments. I would like to thank Alfred Geroldinger for his constant feedback and helping me make this paper. I would also like to thank Andreas Reinhart, Qinghai Zhong for their comments and to thank the anonymous referee for the careful reading and for all his/her comments.

REFERENCES

1. S.D. Adhikari, W. Gao, and Guoqing Wang, *Erdős-Ginzburg-Ziv theorem for finite commutative semigroups*, Semigroup Forum **88** (2014), 555 – 568.

2. N.R. Baeth and D. Smertnig, *Factorization theory: From commutative to noncommutative settings*, J. Algebra **441** (2015), 475 – 551.

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 Mathematics(2017), https://doi.org/10.1016/j.disc.2017.09.024.

5. F. Chen and S. Savchev, *Long minimal zero-sum sequences in the groups* $C_2^{r-1} \oplus C_{2k}$, Integers **14** (2014), Paper A23.

6. K. Cziszter and M. Domokos, *On the generalized Davenport constant and the Noether number*, Central European J. Math. **11** (2013), 1605 – 1615.

7. ———, *Groups with large Noether bound*, Ann. Inst. Fourier (Grenoble) **64** (2014), 909 – 944.

8. ———, *The Noether number for the groups with a cyclic subgroup of index two*, J. Algebra **399** (2014), 546 – 560.

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

10. K. Cziszter, M. Domokos, and I. Szöllősi, *The Noether number and the Davenport constants of the groups of order less than* 32, arXiv:1702.02997.

11. Y. Fan and Q. Zhong, *Products of k atoms in Krull monoids*, Monatsh. Math. **181** (2016), 779 – 795.

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

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

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

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

16. ———, *Sets of lengths*, Amer. Math. Monthly **123** (2016), 960 – 988.

17. 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.

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

19. A. Geroldinger and W. Hassler, *Arithmetic of Mori domains and monoids*, J. Algebra **319** (2008), 3419 – 3463.

20. 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.

21. A. Geroldinger, S. Ramacher, and A. Reinhart, *On v-Marot Mori rings and* C*-rings*, J. Korean Math. Soc. **52** (2015), 1 – 21.

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

23. A. Geroldinger and Q. Zhong, *The catenary degree of Krull monoids II*, J. Australian Math. Soc. **98** (2015), 324 – 354.

24. D.J. Grynkiewicz, *The large Davenport constant II: General upper bounds*, J. Pure Appl. Algebra **217** (2013), 2221 – 2246.

25. ———, *Structural Additive Theory*, Developments in Mathematics, vol. 30, Springer, 2013.

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

27. Dongchun Han and Hanbin Zhang, *Erdős-Ginzburg-Ziv Theorem and Noether number for* $C_m \ltimes_\varphi C_{mn}$, arXiv:1707.03639.

28. F. Kainrath, *Arithmetic of Mori domains and monoids: The Global Case*, Multiplicative Ideal Theory and Factorization Theory, Springer, 2016, pp. 183 – 218.

29. 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.

30. A. Reinhart, *On integral domains that are* C*-monoids*, Houston J. Math. **39** (2013), 1095 – 1116.

31. 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.

32. ———, *Some recent results and open problems on sets of lengths of Krull monoids with finite class group*, Multiplicative Ideal Theory and Factorization Theory (S.T. Chapman, M. Fontana, A. Geroldinger, and B. Olberding, eds.), Springer, 2016, pp. 323 – 352.

33. D. Smertnig, *Sets of lengths in maximal orders in central simple algebras*, J. Algebra **390** (2013), 1 – 43.

34. Guoquing Wang, *Davenport constants for semigroups II*, J. Number Theory **153** (2015), 124 – 134.

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

Institute for Mathematics and Scientific Computing, University of Graz, NAWI Graz, Heinrichstrasse 36, 8010 Graz, Austria

Email address: **junseok.oh@uni-graz.at**