On the monoid of product-one sequences over finite groups

Jun Seok Oh

Jeju National University

Conference on Rings and Polynomials

July 19, 2025

Factorizations and Set of lengths

Let H be a monoid, that is, a commutative, cancellative semigroup with identity.

- H is atomic if every non-unit element is a finite product of atoms (or irreducible elements).

Q. Are the arithmetical properties of two atomic monoids H_1 and H_2 characteristic for H_1 and H_2?

$\rightsquigarrow$ The sets of lengths are the best investigated properties.

Factorizations and Set of lengths

- If $a = u_1 \cdot \ldots \cdot u_k$ for atoms $u_1, \ldots, u_k$ in an atomic monoid H, k is called the length of factorization of a, and we denote by

$$\mathsf{L}(a) = \{k \in \mathbb{N} \mid a \text{ has a factorization of length } k\}\,.$$

- $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ denotes the system of sets of lengths of H.

Which monoids are we interested in?

ex) Let K be an algebraic number field with class group G. There exists a factorization preserving map β from $\mathcal{O}_K$ to the monoid $\mathcal{B}(G)$. More precisely, $\beta(a) = [P_1] \bullet \ldots \bullet [P_k]$, where $a\mathcal{O}_K = P_1 \cdots P_k$ is the factorization into prime ideals.

$\rightsquigarrow$ The associated inverse problem, which asks whether the system $\mathcal{L}(\mathcal{B}(G))$ is characteristic for the group G, is central to our main question.

Why $\mathcal{B}(G)$?

- If H is a Krull monoid with finite class group G such that each class contains a prime divisor, then $\mathcal{L}(H) = \mathcal{L}(\mathcal{B}(G))$.
- There exists a non-Krull monoid H such that $\mathcal{L}(H) = \mathcal{L}(\mathcal{B}(G))$ for some abelian group G.

$\rightsquigarrow$ While earlier work often focussed on the case of abelian groups, sequences over non-abelian groups have received wide attention due to their applications in various branches of algebra, such as the invariant theory and the factorization theory.

- For a finite (not necessarily abelian) group G, the monoid $\mathcal{B}(G)$ is a (combinatorial) C-monoid, which represents the first class of C-monoids for which we have some first insight into their structure.
- The combinatorial aspects of the monoid $\mathcal{B}(G)$ for a finite (not necessarily abelian) group G have a rich history, and they are quite closely related to the Noether number in invariant theory.

Product-one sequences

Let G be a finite group.

- An element of the free abelian monoid $\mathcal{F}(G)$ with a basis G is said to be a sequence over G, i.e., every sequence S over G has the form

$$S = (g_1, g_2, \ldots, g_\ell) = g_1 \cdot g_2 \cdot \ldots \cdot g_\ell = \prod^{\bullet}_{g \in G} g^{[\mathsf{v}_g(S)]}\,,$$

  where $\mathsf{v}_g(S)$ denotes the multiplicity of g in S.

- $|S| = \ell$ is called the length of S.
- T is a subsequence of S if $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in G$.
- S is called a product-one sequence if the terms can be ordered such that their product (in G) is equal to the identity element of G.
- S is called a product-one free sequence if it has no product-one subsequence.

The monoid of product-one sequences

ex) Let $G = \{\pm E, \pm I, \pm J, \pm K\}$ be the quaternion group of order 8.

- The sequence
$$I^{[4]} \cdot J^{[2]} = I \cdot I \cdot I \cdot I \cdot J \cdot J$$
is a (minimal) product-one sequence of length 6 ($\because E = IIIJIJ$).
- The sequence
$$I^{[3]} \cdot J = I \cdot I \cdot I \cdot J$$
is a product-one free sequence of length 4.

- The set $\mathcal{B}(G)$ of all product-one sequences is a submonoid of $\mathcal{F}(G)$, and it is called the monoid of product-one sequences over G.
- An atom (or irreducible element) in $\mathcal{B}(G)$ is called a minimal product-one sequence.

The Characterization Problem

Recall that

$$\mathcal{L}\big(\mathcal{B}(G)\big) = \{\mathsf{L}(B) \mid B \in \mathcal{B}(G)\} = \mathcal{L}(G) \text{ (for short)}\,,$$

where $\mathsf{L}(B)$ is the set of all factorization length k, with $k \in \mathbb{N}$ and $B = U_1 \cdot \ldots \cdot U_k$ for some atoms $U_1, \ldots, U_k$.

- Characterization Problem
  Given two finite (abelian) groups G_1 and G_2 such that $\mathcal{L}(G_1) = \mathcal{L}(G_2)$, does it follow that $G_1 \cong G_2$?

⇝ [Gao+Geroldinger+Schmid+Zhong] Yes, if abelian groups of rank at most 2, or isomorphic to C_n^r, and others.

⇝ [Geroldinger+Grynkiewicz+O.+Zhong] Yes, if $\mathsf{D}(G) \le 6$, or isomorphic to a dihedral group of order $2n$ with n odd.

The Isomorphism Problem

- Isomorphism Problem
  Given two (finite) groups G_1 and G_2 such that $\mathcal{B}(G_1) \cong \mathcal{B}(G_2)$, does it follow that $G_1 \cong G_2$?

$\rightsquigarrow$ An affirmative answer to the Isomorphism Problem is a necessary condition for an affirmative answer to the Characterization Problem.

- The answer to the Isomorphism Problem was known so far only for abelian groups, and its proof heavily depends on the ideal-theoretic properties of monoids.

Theorem (Geroldinger+O., 2025)

Let G_1 and G_2 be (not necessarily finite) groups and suppose that G_1 is a torsion group. Then, $\mathcal{B}(G_1) \cong \mathcal{B}(G_2)$ if and only if $G_1 \cong G_2$.

The Davenport constant

- $\mathsf{d}(G)$ is the maximal length of a product-one free sequence in $\mathcal{F}(G)$.
- $\mathsf{D}(G)$ is the maximal length of an atom in $\mathcal{B}(G)$.

⇝ The Davenport constants of G.

ex) If $G \cong C_n$, a cyclic group of order n, then

$$\mathsf{d}(G) = n - 1 \quad \text{and} \quad \mathsf{D}(G) = n\,.$$

ex) If G is the quaternion group of order 8, then

$$\mathsf{d}(G) = 4 \quad \text{and} \quad \mathsf{D}(G) = 6\,.$$

- $\mathsf{d}(G) + 1 \overset{(1)}{\le} \mathsf{D}(G) \overset{(2)}{\le} |G|$:
  - ⇝ [Grynkiewicz, JPAA, 2013] (2) satisfies equality iff $G \cong C_n$ or $G \cong D_{2m}$ with m odd.
  - ⇝ (1) satisfies equality if G is abelian.

The Davenport constant

- If $G \cong \prod_{i=1}^{r} C_{n_i}$ with $n_1 \mid \cdots \mid n_r$, then $\sum_{i=1}^{r}(n_i - 1) + 1 \leq \mathsf{D}(G)$:
  - ⇝ [Olson, JNT, 1969] Equality holds if G is a p-group or $r \leq 2$.
  - ⇝ [Geroldinger+Schneider, JCTA, 1992] If $r \geq 4$, then there are infinitely many groups G of rank r with strict inequality.

- [Geroldinger+Grynkiewicz, JPAA, 2013] If G is a non-cyclic group having a cyclic index 2 subgroup, then $\mathsf{d}(G) = \frac{|G|}{2}$ and $\mathsf{D}(G) = \mathsf{d}(G) + |G'|$.

- [Qu+Li+Teeuwen, IJM, 2025] If G is a non-cyclic group with p the smallest prime divisor of $|G|$, then $\mathsf{d}(G) = \frac{|G|}{p} + p - 2$ iff G has a cyclic index p subgroup.

⇝ For a fixed positive integer r, structural results characterizing which finite groups G satisfy $\mathsf{D}(G) = r$ are rare.

Union of sets of lengths

- For any $k \in \mathbb{N}$, we denote by

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

the union of sets of lengths containing k.

⇝ [O., JCA, 2020] $\mathcal{U}_k(G)$ is a finite interval, and if we denote by $\rho_k(G) = \max \mathcal{U}_k(G)$, then

$$\rho_k(G) \le \frac{k\mathsf{D}(G)}{2} \quad \text{and} \quad \rho_{2k}(G) = k\mathsf{D}(G)\,.$$

NOTE

$$\begin{aligned}\mathcal{L}(G_1) = \mathcal{L}(G_2) \quad &\Longrightarrow \quad \mathcal{U}_k(G_1) = \mathcal{U}_k(G_2) \\ &\Longrightarrow \quad \mathsf{D}(G_1) = \rho_2(G_1) = \rho_2(G_2) = \mathsf{D}(G_2)\end{aligned}$$

Strategy

- [András + Cziszter + Domokos + Szöllősi, RPRF(conference proceeding), 2025] *The directed Cayley diameter and the Davenport constant*.

$\rightsquigarrow$ They computed $\mathsf{d}(G)$ and $\mathsf{D}(G)$ for all non-abelian groups G of order at most 42 using computer program.

- Since $\mathsf{D}(H) \le \mathsf{D}(G)$ for any subgroup H of G, the main approach is to find the certain subgroup having the Davenport constant at least 10, or to construct a minimal product-one sequence of sufficiently large length.

Exception: non-abelian 2-groups

- However, the difficulty of classification arises in the case of non-abelian 2-groups.
- There are many non-abelian 2-groups where we need to clarify the generators and relations (for example, there are 256 non-abelian groups of order 64, and 2313 of order 128, etc), and many of these non-abelian 2-groups have subgroups with relatively small values of their Davenport constant.

Theorem (O., 2025)

Let G be a finite non-abelian group with $|G| > 42$.

1. *If G has a proper subgroup of order 32, then $\mathsf{D}(G) \geq 8$.*
2. *If G has no proper subgroup of order 32, then $\mathsf{D}(G) \geq 10$.*

Classification

Theorem (O., 2025)

Let G be a finite group with $|G| \geq 2$.

1. *If* $\mathsf{D}(G) \leq 7$*, then* G *is isomorphic to one of the groups listed in* Table.1.
2. *If* $8 \leq \mathsf{D}(G) \leq 9$*, then* G *is either a non-abelian group having a proper subgroup of order* 32*, or isomorphic to one of the groups listed in* Table.2.

D(G)	G	GAP
2	C_2	$(2,1)$
3	C_3	$(3,1)$
	C_2^2	$(4,2)$
4	C_4	$(4,1)$
	C_2^3	$(8,5)$
5	C_5	$(5,1)$
	$C_2 \times C_4$	$(8,2)$
	C_3^2	$(9,2)$
	C_2^4	$(16,14)$
6	C_6	$(6,2)$
	$C_2^2 \times C_4$	$(16,10)$
	C_2^5	$(32,51)$
	D_6	$(6,1)$
	D_8	$(8,3)$
	Q_8	$(8,4)$
7	C_7	$(7,1)$
	$C_2 \times C_6$	$(12,5)$
	C_4^2	$(16,2)$
	C_3^3	$(27,5)$
	$C_2^3 \times C_4$	$(32,45)$
	C_2^6	$(64,267)$
	A_4	$(12,3)$
	$C_2^2 \rtimes C_4$	$(16,3)$
	$C_2 \times D_8$	$(16,11)$
	$C_2 \times Q_8$	$(16,12)$
	$(C_2 \times C_4) \rtimes C_2$	$(16,13)$

Table 1.

D(G)	G	GAP
8	C_8	$(8,1)$
	$C_3 \times C_6$	$(18,5)$
	$C_2^2 \times C_6$	$(24,15)$
	$C_2 \times C_4^2$	$(32,21)$
	$C_2^4 \times C_4$	$(64,260)$
	C_2^7	$(128,2328)$
	$C_4 \rtimes C_4$	$(16,4)$
	H_{27}	$(27,3)$
	$C_2 \times (C_2^2 \rtimes C_4)$	$(32,22)$
	$C_2^2 \times D_8$	$(32,46)$
	$C_2^2 \times Q_8$	$(32,47)$
	$C_2 \times \big((C_4 \times C_2) \rtimes C_2\big)$	$(32,48)$
	$C_2^3 \rtimes C_2^2$	$(32,49)$
	$(C_2 \times Q_8) \rtimes C_2$	$(32,50)$
9	C_9	$(9,1)$
	$C_2 \times C_8$	$(16,5)$
	C_5^2	$(25,2)$
	$C_2^3 \times C_6$	$(48,52)$
	$C_2^2 \times C_4^2$	$(64,192)$
	C_3^4	$(81,15)$
	$C_2^5 \times C_4$	$(128,2319)$
	C_2^8	$(256,56092)$
	Q_{12}	$(12,1)$
	D_{12}	$(12,4)$
	$(C_2 \times C_4) \rtimes C_4$	$(32,2)$
	$C_2 \times (C_4 \rtimes C_4)$	$(32,23)$
	$C_4^2 \rtimes C_2$	$(32,24)$
	$C_4 \times D_8$	$(32,25)$
	$C_4 \times Q_8$	$(32,26)$
	$C_2^4 \rtimes C_2$	$(32,27)$

Table 2.

Thank you for your attention!

A. Geroldinger and J.S. Oh, *On the isomorphism problem for monoids of product-one sequences*, Bull, London Math. Soc. **57** (2025), 1482–1495.

J.S. Oh, *A classification of finite groups with small Davenport constant*, Comm. Algebra, to appear.