PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 9, September 2017, Pages 3695–3708
http://dx.doi.org/10.1090/proc/13534
Article electronically published on April 12, 2017

DEGREE BOUND FOR SEPARATING INVARIANTS OF ABELIAN GROUPS

M. DOMOKOS

(Communicated by Jerzy Weyman)

Abstract. It is proved that the universal degree bound for separating polynomial invariants of a finite abelian group (in non-modular characteristic) is typically strictly smaller than the universal degree bound for generators of polynomial invariants. More precisely, these degree bounds can be equal only if the group is cyclic or is the direct sum of r even order cyclic groups where the number of two-element direct summands is not less than the integer part of the half of r. A characterization of separating sets of monomials is given in terms of zero-sum sequences over abelian groups.

1. Introduction

Let G be a finite group and $\mathbb{F}$ an algebraically closed field. A *G-module* is a finite dimensional $\mathbb{F}$-vector space V endowed with an action of G on V via linear transformations. In other words, the G-module consists of the pair (V, ρ) where ρ is a group homomorphism $G \to GL(V)$. The coordinate ring $\mathcal{O}(V)$ of V contains the subalgebra

$$\mathcal{O}(V)^G := \{f \in \mathcal{O}(V) \colon f(gv) = f(v) \quad \forall v \in V, \forall g \in G\}$$

of G-invariants. For $f \in \mathcal{O}(V)$ and $g \in G$ write $g \cdot f \in \mathcal{O}(V)$ for the function $v \mapsto f(g^{-1}v)$. This way we get an action of G on $\mathcal{O}(V)$ via $\mathbb{F}$-algebra automorphisms, and $\mathcal{O}(V)^G = \{f \in \mathcal{O}(V) \colon g \cdot f = f \quad \forall g \in G\}$. Choosing a basis $x_1, \dots, x_k$ in the dual space V^* of V, the coordinate ring $\mathcal{O}(V)$ is identified with the polynomial algebra $\mathbb{F}[x_1, \dots, x_k]$, on which G acts via linear substitutions of the variables.

Following Definition 2.3.8 in [5], we call a subset $S \subset \mathcal{O}(V)^G$ a *separating set of invariants* if the following holds: if for $v, w \in V$ there exists an $h \in \mathcal{O}(V)^G$ with $h(v) \neq h(w)$, then there is an $f \in S$ with $f(v) \neq f(w)$. Clearly if v and w belong to the same G-orbit in V, then $h(v) = h(w)$ holds for all $h \in \mathcal{O}(V)^G$. It is well known that the finiteness of G implies the converse as well: if v and w have different G-orbits, then there exists an $h \in \mathcal{O}(V)^G$ with $h(v) \neq h(w)$ (see the proof of Theorem 3.9.13 in [5]). So $S \subset O(V)^G$ is a separating set if and only if for any $v, w \in V$ with $Gv \neq Gw$ there is an $f \in S$ such that $f(v) \neq f(w)$. For a survey on separating sets of invariants see [20].

Received by the editors March 22, 2016 and, in revised form, October 5, 2016.
2010 *Mathematics Subject Classification.* Primary 13A50; Secondary 11B75, 20K01.
Key words and phrases. Separating invariants, zero-sum sequences, Noether number, Davenport constant.
This research was partially supported by National Research, Development and Innovation Office, NKFIH K 119934.

©2017 American Mathematical Society

Since the G-action preserves the standard grading on $\mathbb{F}[x_1,\dots,x_k]$, the algebra $\mathcal{O}(V)^G$ is generated by homogeneous elements. Write $\beta(G,V)$ (respectively $\beta_{\mathrm{sep}}(G,V)$) for the minimal positive integer k such that $\mathcal{O}(V)^G$ contains a generating set (respectively separating set) consisting of homogeneous elements of degree at most k. Moreover, set

$$\beta(G) := \sup_V\{\beta(G,V)\} \quad \text{and} \quad \beta_{\mathrm{sep}}(G) := \sup_V\{\beta_{\mathrm{sep}}(G,V)\}$$

where the supremum above is taken over all G-modules V. The number $\beta_{\mathrm{sep}}(G)$ was introduced and studied in [20], [21], inspired by the number $\beta(G)$ first appearing in [29]. Obviously $\beta_{\mathrm{sep}}(G,V) \le \beta(G,V)$ and hence $\beta_{\mathrm{sep}}(G) \le \beta(G)$. When the characteristic of $\mathbb{F}$ does not divide the group order $|G|$, we have $\beta(G) \le |G|$ (this is the famous Noether bound proved in [24] for the case $\mathrm{char}(\mathbb{F}) = 0$ and in [10], [11] for positive non-modular characteristic). One nice feature of $\beta_{\mathrm{sep}}(G)$ is that the inequality $\beta_{\mathrm{sep}}(G) \le |G|$ holds also in the modular case $\mathrm{char}(\mathbb{F}) \mid |G|$ as well, see Corollary 3.9.14 in [5]. In comparison we mention that when $\mathrm{char}(\mathbb{F})$ divides $|G|$ we have $\beta(G) = \infty$ by [28]. However, as far as we know, not much is said in the literature about the following question:

Question 1.1. Is $\beta_{\mathrm{sep}}(G)$ typically strictly smaller than $\beta(G)$ in the non-modular case $\mathrm{char}(\mathbb{F}) \nmid |G|$?

A difficulty in answering Question 1.1 is that the exact value of the Noether number is known only for a very limited class of groups; see for example [2], [3], [4] (see also [18] for asymptotic upper bounds). It is shown in [1] that for the non-abelian semidirect product $C_p \rtimes C_3$ (where p is a prime) and $\mathrm{char}(\mathbb{F}) = 0$ we have $\beta(C_p \rtimes C_3) = p+2$ whereas $\beta_{\mathrm{sep}}(C_p \rtimes C_3) = p+1$.

In the present paper we shall deal with abelian groups. Our main result Theorem 3.10 implies that for abelian groups the answer to Question 1.1 is yes. More precisely, Corollary 3.11 asserts that when G is abelian, $\beta_{\mathrm{sep}}(G) = \beta(G)$ implies that G is cyclic or G is the direct sum of r cyclic groups of even order, where at least $\lfloor \frac{r}{2} \rfloor$ of the cyclic direct summands have order 2.

An interesting special feature of the case of abelian groups is that the investigation of separating invariants can be tied up with the theory of zero-sum sequences over abelian groups. Given a finite abelian group G (written additively) and an ordered sequence $a_1,\dots,a_k$ of elements of G (repetition is allowed) set

$$\mathcal{G}(a_1,\dots,a_k) := \{(m_1,\dots,m_k) \in \mathbb{Z}^k \colon \sum m_i a_i = 0 \in G\}.$$

This is a subgroup of the free abelian group $\mathbb{Z}^k$. It contains the submonoid

$$\mathcal{B}(a_1,\dots,a_k) := \mathbb{N}_0^k \cap \mathcal{G}(a_1,\dots,a_k).$$

Denote by e_i the ith standard basis vector in $\mathbb{Z}^k$. Clearly $\mathrm{ord}_G(a_i)e_i \in \mathcal{B}(a_1,\dots,a_k)$, where $\mathrm{ord}_G(a_i)$ is the order of a_i in G. Since for any $m \in \mathcal{G}(a_1,\dots,a_k)$ there exist non-negative integers $t_1,\dots,t_k \in \mathbb{N}_0$ with $m + \sum t_i \mathrm{ord}_G(a_i)e_i \in \mathcal{B}(a_1,\dots,a_k)$, it follows that $\mathcal{G}(a_1,\dots,a_k)$ is the quotient group of the monoid $\mathcal{B}(a_1,\dots,a_k)$. In particular, the abelian group $\mathcal{G}(a_1,\dots,a_k)$ is generated by its submonoid $\mathcal{B}(a_1,\dots,a_k)$. In the special case when $a_1,\dots,a_k$ are distinct and $\{a_1,\dots,a_k\} = G$, we recover the monoid $\mathcal{B}(G)$ of zero-sum sequences over G, a well-studied object in arithmetic combinatorics. In particular, the *Davenport constant* $\mathsf{D}(G)$ is defined as the maximal length of an atom in the monoid $\mathcal{B}(G)$, where for $s \in \mathcal{B}(G) \subset \mathbb{N}_0^{|G|}$ the *length*

of s is $|s| = \sum_{g\in G} s_g$. More generally, the study of the monoid $\mathcal{B}(G_0)$ of zero-sum sequences over an arbitrary subset G_0 of G has an extensive literature; see Proposition 2.5.6 in [15] for the first abstract algebraic properties of the monoid $\mathcal{B}(G_0)$, or [27] for recent combinatorial work on $\mathsf{D}(G_0)$ (for some very special subset G_0).

From now on we assume that G is a finite abelian group and the characteristic of the base field $\mathbb{F}$ does not divide $|G|$. Then V decomposes as a direct sum

$$V = V_1 \oplus \cdots \oplus V_k$$

of 1-dimensional G-modules. Accordingly the variables in $\mathcal{O}(V) = \mathbb{F}[x_1, \dots, x_k]$ will be chosen to be G-eigenvectors, so there exist characters $\chi_i \in \widehat{G} = \hom(G, \mathbb{F}^\times)$ such that $g \cdot x_i = \chi_i(g)x_i$ for $i = 1, \dots, k$. For $m \in \mathbb{N}_0^k$ write $x^m = x_1^{m_1} \cdots x_k^{m_k}$. Each monomial spans a G-invariant subspace in $\mathcal{O}(V)$, and $g \cdot x^m = (\prod_{i=1}^k \chi_i(g)^{m_i})x^m$. It follows that $\mathcal{O}(V)^G$ is spanned by G-invariant monomials, namely

$$\mathcal{O}(V)^G = \bigoplus_{m\in\mathcal{B}(\chi_1,\dots,\chi_k)} \mathbb{F}x^m. \tag{1}$$

Note that here we use the notation introduced in the above paragraph for the finite abelian group $\widehat{G}$ which is isomorphic to G. A consequence of (1) is the equality

$$\beta(G) = \mathsf{D}(G) \tag{2}$$

which was used in [29], and later in [9] or in [4]. In view of the above connection between the Noether number $\beta(G)$ and the Davenport constant $\mathsf{D}(G)$ it is natural to ask for the meaning of $\beta_{\mathrm{sep}}(G)$ in terms of zero-sum sequences. This is the second motivation of the present paper. In Theorem 2.1 and Corollary 2.6 we provide a characterization of separating sets of monomials and $\beta_{\mathrm{sep}}(G)$ purely in terms of zero-sum sequences over G. Corollary 2.6 is used in Section 3 to derive our main result Theorem 3.10.

We finish the introduction by mentioning some prior works related to separating invariants for diagonalizable linear actions of finite abelian groups. Namely, a separating set of monomials in $\mathcal{O}(V)^G$ is constructed in Proposition 5 of [23]. An algorithm to produce invariant monomials that generate the field of rational invariants is described in [19]. The focus of the present paper is on degree bounds for separating invariants, and therefore it is sufficient to deal with invariant monomials. Note that a different current research direction is the study of the minimal cardinality of a separating system; see for example [8].

2. Characterization of separating sets of monomials

Let G be a finite abelian group, and let $V = V_1 \oplus \cdots \oplus V_k$ be a k-dimensional G-module as in Section 1, so $\mathcal{O}(V) = \mathbb{F}[x_1, \dots, x_k]$ with $g \cdot x_i = \chi_i(g)x_i$ for $i = 1, \dots, k$. For $m \in \mathbb{N}_0^k$ set $\mathrm{supp}(m) := \{i \in \{1, \dots, k\} \colon m_i \neq 0\} \subset \{1, \dots, k\}$. Similarly, when x^m is a monomial, we shall use the notation $\mathrm{supp}(x^m)$ for $\mathrm{supp}(m)$. Given a subset $J \subset \{1, \dots, k\}$ and a set $M \subset \mathbb{N}_0^k$ we write $M_J := \{m \in M \colon \mathrm{supp}(m) \subset J\}$.

The *Helly dimension* $\kappa(G)$ of G was defined in [6] as the minimal positive integer k such that any set of cosets in G with empty intersection contains a subset of at most k cosets with empty intersection. It was shown in [7] that $\kappa(G)$ is one larger than the minimal number of generators of the finite abelian group G (the *rank* of G).

Theorem 2.1. *For a subset $M \subset \mathcal{B}(\chi_1, \dots, \chi_k)$ the following are equivalent:*

(i) *$\{x^m : m \in M\}$ is a separating subset in $\mathcal{O}(V)^G$.*

(ii) *For all subsets $\{j_1 < \cdots < j_s\} = J \subset \{1, \dots, k\}$, the abelian group $\mathcal{G}(\chi_{j_1}, \dots, \chi_{j_s})$ is generated by M_J.*

(iii) *For all subsets $\{j_1 < \cdots < j_s\} = J \subset \{1, \dots, k\}$ with $|J| \leq \kappa(G)$, the abelian group $\mathcal{G}(\chi_{j_1}, \dots, \chi_{j_s})$ is generated by M_J.*

The proof will be split into a couple of statements. Consider the G-module direct summand $V_J := \bigoplus_{j \in J} V_j$ of V, where $J \subset \{1, \dots, k\}$. Its coordinate ring $\mathcal{O}(V_J)$ is an algebra retract of $\mathcal{O}(V)$: it is the subalgebra generated by the variables $\{x_j : j \in J\}$. For $v \in V$ we write v_J for the component of V in the direct summand V_J of V. The statement and proof of Lemma 2.2 below remain valid when the finite group G is not assumed to be abelian and the direct summands V_j are not assumed to be 1-dimensional.

Lemma 2.2. *Assume that $k \geq \kappa(G)$ and for all $J \subset \{1, \dots, k\}$ with $|J| = \kappa(G)$ we are given a separating subset S_J in $\mathcal{O}(V_J)^G$. Then their union $S := \bigcup_J S_J$ is a separating subset in $\mathcal{O}(V)^G$.*

Proof. Suppose that for $v, w \in V$ we have $f(v) = f(w)$ for all $f \in S$. Then in particular, for a fixed $J \subset \{1, \dots, k\}$ with $|J| = \kappa(G)$ we have $f(v_J) = f(w_J)$ for all $f \in S_J$. Since S_J is a separating subset in $\mathcal{O}(V_J)^G$, we conclude that $Gv_J = Gw_J$. This holds for all $J \subset \{1, \dots, k\}$ with $|J| = \kappa(G)$, hence by Lemma 4.1 in [7] we get that $Gv = Gw$. □

Proposition 2.3. *Let M be a subset of $\mathcal{B}(\chi_1, \dots, \chi_k)$ such that for all $J = \{j_1 < \cdots < j_s\} \subset \{1, \dots, k\}$ the abelian group $\mathcal{G}(\chi_{j_1}, \cdots, \chi_{j_s})$ is generated by M_J. Then $\{x^m : m \in M\}$ is a separating set in $\mathcal{O}(V)^G$.*

Proof. Take $v, w \in V$ such that $x^m(v) = x^m(w)$ for all $m \in M$. The assumption says in particular that $M_{\{j\}}$ generates $\mathcal{G}(\chi_j)$ for $j = 1, \dots, d$. Since $\mathcal{G}(\chi_j)$ is the subgroup of $\mathbb{Z}$ generated by $\mathrm{ord}_{\widehat{G}}(\chi_j)$, it follows that some positive power of x_j belongs to $\{x^m : m \in M\}$. Thus $x_j(v) = 0$ if and only if $x_j(w) = 0$, so $\mathrm{supp}(v) = \mathrm{supp}(w)$; set $J := \mathrm{supp}(v)$. Take an arbitrary G-invariant monomial x^n. If $\mathrm{supp}(n) \nsubseteq J$, then $x^n(v) = 0 = x^n(w)$. Otherwise $\mathrm{supp}(n) \subset J = \{j_1 < \cdots < j_s\}$. Since M_J generates $\mathcal{G}(\chi_{j_1}, \dots, \chi_{j_s})$, there exist $u_1, \dots, u_q, t_1, \dots, t_l \in M_J$ such that $n = u_1 + \cdots + u_q - t_1 - \cdots - t_l \in \mathbb{Z}^s$, implying $x^n x^{t_1} \dots x^{t_l} = x^{u_1} \dots x^{u_q}$. By our assumption on v, w we have $x^{u_i}(v) = x^{u_i}(w)$ for $i = 1, \dots, q$ and $x^{t_i}(v) = x^{t_i}(w) \neq 0$ for $i = 1, \dots, l$. It follows that

$$x^n(v) = \frac{x^{u_1}(v) \dots x^{u_q}(v)}{x^{t_1}(v) \dots x^{t_l}(v)} = \frac{x^{u_1}(w) \dots x^{u_q}(w)}{x^{t_1}(w) \dots x^{t_l}(w)} = x^n(w).$$

Thus we proved that $x^n(v) = x^n(w)$ holds for an arbitrary G-invariant monomial x^n, implying in turn that $h(v) = h(w)$ for any $h \in \mathcal{O}(V)^G$. □

Proposition 2.4. *Let M be a subset of $\mathcal{B}(\chi_1, \dots, \chi_k)$ such that $\{x^m : m \in M\}$ is a separating set in $\mathcal{O}(V)^G$. Then the abelian group $\mathcal{G}(\chi_1, \dots, \chi_k)$ is generated by M.*

Proof. For $i = 1, \dots, k$ let ξ_i be a non-zero vector in the summand V_i of V such that $x_1, \dots, x_k$ is the basis of V^* dual to the basis $\xi_1, \dots, \xi_k$ of V. Since $\xi_i \in V$ can be separated from 0 by x^m for some $m \in M$, a positive power $x_i^{n_i}$ belongs to

$\{x^m : m \in M\}$ for each $i = 1, \dots, k$. Obviously it is sufficient to prove the statement when G acts faithfully on V, so $G \subset GL(V)$ and hence $\widehat{G} = \langle \chi_1, \dots, \chi_k \rangle$. On the other hand $\langle \chi_1, \dots, \chi_k \rangle \cong \mathbb{Z}^k / \mathcal{G}(\chi_1, \dots, \chi_k)$, since $\mathcal{G}(\chi_1, \dots, \chi_k)$ was defined as the kernel of the natural surjection $\mathbb{Z}^k \to \widehat{G}$ with $e_i \mapsto \chi_i$. Denote by H the abelian group $\mathbb{Z}^k / \mathbb{Z}M$. This group is finite, as $n_i e_i \in M$, hence it is isomorphic to its character group $\widehat{H}$. Therefore we may choose generators $\psi_1, \dots, \psi_k \in \widehat{H}$ such that the natural surjection $\mathbb{Z}^k \to \widehat{H}$, $e_i \mapsto \psi_i$ $(i = 1, \dots, k)$ has kernel $M\mathbb{Z}$. For $h \in H$ let $\rho(h) \in GL(V)$ be the linear transformation given by $\rho(h)\xi_i = \psi_i(h^{-1})\xi_i$. Then $\rho : H \to GL(V)$ is an injective group homomorphism. Note that for any $q \in \mathbb{N}_0^k$ we have $x^q(\rho(h)(\xi_1 + \cdots + \xi_k)) = \prod_{i=1}^k \psi_i(h^{-1})^{q_i}$. By the choice of ψ_i, for any $m \in M$ and any $h \in H$ we have $\prod_{i=1}^k \psi_i(h^{-1})^{m_i} = 1$. Therefore we have

$$x^m(\rho(h)(\xi_1 + \cdots + \xi_k)) = 1$$

for all $m \in M$ and $h \in H$. On the other hand $x^m(\xi_1 + \cdots + \xi_k) = 1$ as well. Since $\{x^m : m \in M\}$ is a separating set in $\mathcal{O}(V)^G$, we conclude that the H-orbit of $\xi_1 + \cdots + \xi_k$ is contained in the G-orbit of $\xi_1 + \cdots + \xi_k$. Thus for each $h \in H$ there exists a $g \in G$ such that $\rho(h)(\xi_1 + \cdots + \xi_k) = g(\xi_1 + \cdots + \xi_k)$, implying in turn that $\rho(h)\xi_i = g\xi_i$ for each basis vector $\xi_i \in V$, and hence $\rho(h) = g$. So we have $H \cong \rho(H) \subset G \subset GL(V)$. Therefore $\psi_i = \chi_i \circ \rho$ for $i = 1, \dots, k$, and it follows that the natural surjection $\mathbb{Z}^k \to \widehat{H}$, $e_i \mapsto \psi_i$ factors through the natural surjection $\mathbb{Z}^k \to \widehat{G}$, $e_i \mapsto \chi_i$, so $\mathbb{Z}M \supset \mathcal{G}(\chi_1, \dots, \chi_k)$. Now as M was a subset of $\mathcal{B}(\chi_1, \dots, \chi_k) \subset \mathcal{G}(\chi_1, \dots, \chi_k)$, the reverse inclusion $\mathbb{Z}M \subset \mathcal{G}(\chi_1, \dots, \chi_k)$ also holds, forcing the equality $\mathbb{Z}M = \mathcal{G}(\chi_1, \dots, \chi_k)$. □

Lemma 2.5. *If $\{x^m : m \in M\}$ is a separating set in $\mathcal{O}(V)^G$, then for all subsets $J \subset \{1, \dots, k\}$ the monomials $\{x^m : m \in M_J\}$ constitute a separating set in $\mathcal{O}(V_J)^G$.*

Proof. We claim that if S is a separating set in $\mathcal{O}(V)^G$, then its restriction $\{f|_{V_J} : f \in S\}$ to V_J is a separating set in $\mathcal{O}(V_J)^G$. Indeed, suppose $h(v) \neq h(w)$ for some $v, w \in V_J$ and $h \in \mathcal{O}(V_J)^G$. Since the algebra $\mathcal{O}(V_J)^G$ is contained in $\mathcal{O}(V)^G$, it follows that there exists an $f \in S$ with $f(v) \neq f(w)$, so $f|_{V_J}$ separates v and w. This proves the claim. Now observe that if m does not belong to M_J, then the monomial x^m vanishes identically on V_J. Consequently the restriction to V_J of $\{x^m : m \in M\}$ is contained in $\{x^m : m \in M_J\} \cup \{0\}$, and our statement follows. □

Proof of Theorem 2.1. (i)⇒(ii): Suppose that $\{x^m : m \in M\}$ is a separating set in $\mathcal{O}(V)^G$, and take a subset $J = \{j_1 < \cdots < j_s\} \subset \{1, \dots, k\}$. By Lemma 2.5 $\{x^m : m \in M_J\}$ is a separating set in $\mathcal{O}(V_J)^G$. Applying Proposition 2.4 for V_J and M_J we conclude that the abelian group $\mathcal{G}(\chi_{j_1}, \dots, \chi_{j_s})$ is generated by M_J.

(ii)⇒ (iii): Trivial.

(iii)⇒(i): Suppose that (iii) holds. Then for any subset $J = \{j_1 < \cdots < j_s\} \subset \{1, \dots, k\}$ with $s = |J| \leq \kappa(G)$, the set M_J generates the abelian group $\mathcal{G}(\chi_{j_1}, \dots, \chi_{j_s})$, hence by Proposition 2.3 $\{x^m : m \in M_J\}$ is a separating set in $\mathcal{O}(V_J)^G$. If $k \leq \kappa(G)$, then we may take $J = \{1, \dots, k\}$ and we are done. Otherwise the union of the $\{x^m : m \in M_J\}$ as J ranges over the subsets of $\{1, \dots, k\}$ of size $\kappa(G)$ is a separating set in $\mathcal{O}(V)^G$ by Lemma 2.2. □

Corollary 2.6. *The number $\beta_{\mathrm{sep}}(G)$ is the minimal positive integer d such that for any positive integer $s \leq \kappa(G)$ and any finite sequence $a_1, \dots, a_s$ of distinct elements of G the abelian group $\mathcal{G}(a_1, \dots, a_s)$ is generated by $\{m \in \mathcal{B}(a_1, \dots, a_s) \colon |m| \leq d\}$.*

Proof. For a finite abelian group H denote by $\delta(H)$ (respectively $\delta_0(H)$) the minimal positive integer d such that for any $s \leq \kappa(H)$ and any sequence $a_1, \dots, a_s$ of not necessarily distinct (respectively distinct) elements of H the group $\mathcal{G}(a_1, \dots, a_s)$ is generated by the $m \in \mathcal{B}(a_1, \dots, a_s)$ with $|m| \leq d$. Obviously $\delta_0(H) \leq \mathsf{D}(H) \leq |H|$. We claim that $\delta(H) = \delta_0(H)$. Indeed, the inequality $\delta_0(H) \leq \delta(H)$ holds by definition of δ and δ_0. To see the reverse inequality take an arbitrary sequence $a_1, \dots, a_s \in H$, $s \leq \kappa(H)$. By induction on s we show that $\mathcal{G}(a_1, \dots, a_s)$ is generated by $\{m \in \mathcal{B}(a_1, \dots, a_s) \colon |m| \leq \delta_0(H)\}$. If $a_1, \dots, a_s$ are distinct, then we are done by definition of δ_0. Otherwise suppose $a_1 = a_2$. Clearly $\delta_0(H) \geq \mathrm{ord}_H(a_1) = q$, and $n := (1, q-1, 0, \dots, 0) \in \mathcal{B}(a_1, \dots, a_s)$ satisfies $|n| \leq \delta_0(H)$. Moreover, given any $m \in \mathcal{G}(a_1, \dots, a_s)$, replace m by $\tilde{m} := m - m_1 n$. Then $\tilde{m}$ belongs to $\mathcal{G}(a_2, \dots, a_s)$ (viewed as the subset of $\mathcal{G}(a_1, \dots, a_s)$ consisting of the elements whose first coordinate is zero). By the induction hypothesis $\tilde{m}$ belongs to the group generated by $\{w \in \mathcal{B}(a_2, \dots, a_s) \colon |w| \leq \delta_0(H)\}$, implying in turn that m belongs to the group generated by $\{w \in \mathcal{B}(a_1, \dots, a_s) \colon |w| \leq \delta_0(H)\}$. This shows $\delta(H) = \delta_0(H)$.

Now take a G-module V with the notation of the beginning of Section 2. For any subset $\{i_1 < \dots < i_s\} \subset \{1, \dots, k\}$ with $s \leq \kappa(\widehat{G})$ the abelian group $\mathcal{G}(\chi_{i_1}, \dots, \chi_{i_s})$ is generated by the elements $m \in \mathcal{B}(\chi_{i_1}, \dots, \chi_{i_s})$ with $|m| \leq \delta(\widehat{G})$. It follows by Theorem 2.1 that $\{x^m \colon m \in \mathcal{B}(\chi_1, \dots, \chi_k), \quad |m| \leq \delta(\widehat{G})\}$ is a separating set in $\mathcal{O}(V)^G$. Thus $\beta_{\mathrm{sep}}(G, V) \leq \delta(\widehat{G})$. Since V was an arbitrary G-module, we deduce the inequality $\beta_{\mathrm{sep}}(G) \leq \delta(\widehat{G})$. Note finally that the isomorphism $G \cong \widehat{G}$ implies $\delta(G) = \delta(\widehat{G})$. Combining with the first paragraph we obtain $\beta_{\mathrm{sep}}(G) \leq \delta_0(G)$.

To show the reverse inequality $\beta_{\mathrm{sep}}(G) \geq \delta_0(G)$, take a sequence $\chi_1, \dots, \chi_k$ of distinct characters of G such that $k \leq \kappa(\widehat{G})$ and the abelian group $\mathcal{G}(\chi_1, \dots, \chi_k)$ is not generated by $\{m \in \mathcal{B}(\chi_1, \dots, \chi_k) \colon |m| < \delta_0(\widehat{G})\}$. Such a sequence $\chi_1, \dots, \chi_k$ exists by definition of $\delta_0(\widehat{G})$. Hence by Theorem 2.1 $\{x^m \colon m \in \mathcal{B}(\chi_1, \dots, \chi_k), \quad |m| < \delta_0(G)\}$ is not a separating set in $\mathbb{F}[x_1, \dots, x_k]^G = \mathcal{O}(V)^G$, where the G-module V is determined by $g \cdot x_i = \chi_i(g) x_i$ for $i = 1, \dots, k$. Taking into account (1) we conclude $\beta_{\mathrm{sep}}(G, V) \geq \delta_0(G)$, implying in turn $\beta_{\mathrm{sep}}(G) \geq \delta_0(G)$. □

3. Degree bounds

We fix the following notation for the whole Section 3. Decompose our (additively written) abelian group G as a direct sum of cyclic groups

$$G = C_{n_1} \oplus \dots \oplus C_{n_r}$$

where $n_r \mid n_{r-1} \mid \dots \mid n_1$ and $n_r > 1$, so in particular n_1 is the *exponent* of G and r is the *rank* (the minimal number of generators) of G, hence the Helly dimension of G is $\kappa(G) = r + 1$. Set

$$\mathsf{d}^*(G) = \sum_{i=1}^{r} (n_i - 1).$$

It is well known (see for example Section 3 in [14]) that

$$\mathsf{d}^*(G) + 1 \leq \mathsf{D}(G) \tag{3}$$

where $\mathsf{D}(G)$ is the Davenport constant of G (cf. Section 1). Classical results in arithmetic combinatorics assert that we have equality in (3) if G is a p-group (see [25]) or if G has rank two (see [26]). On the other hand there are some infinite sequences of finite abelian groups for which the inequality in (3) is known to be strict; see Theorem 3.4 in [14]. Beyond that it is not well understood when equality holds in (3). We refer to the surveys [14] and [13] for further information on zero-sum sequences in finite abelian groups.

We shall need the following technical and elementary lemma.

Lemma 3.1. *Let $(n_1, \dots, n_r), (m_1, \dots, m_r) \in \mathbb{N}^r$ be distinct r-tuples of positive integers such that the following divisibility conditions hold for them:*

$$m_r \mid n_r \mid m_{r-1} \mid n_{r-1} \mid \cdots \mid m_2 \mid n_2 \mid m_1 \mid n_1.$$

Then the following inequality holds:

$$\sum_{i=1}^{r}(n_i - 1) \geq \sum_{i=1}^{r}(m_i - 1) + \prod_{i=1}^{r}\frac{n_i}{m_i} - 1. \tag{4}$$

Moreover, equality holds in (4) if and only if there exists a $j \in \{0, 1, \dots, r-1\}$ such that $m_k = n_k$ for $k = 1, \dots, j$ and $m_k = n_{k+1}$ for $k = j+1, \dots, r$ (with the convention $n_{r+1} = 1$).

Proof. When $r = 1$, (4) becomes $n_1 - 1 \geq (m_1 - 1) + \frac{n_1}{m_1} - 1$, which is equivalent to the obvious $(m_1 - 1)(\frac{n_1}{m_1} - 1) \geq 0$. Assume from now on that $r > 1$. If $n_1 = m_1$, then we may omit them and deal with the sequences $(n_2, \dots, n_r)$ and $(m_2, \dots, m_r)$, since the inequality (4) for these shorter sequences is obviously equivalent to the corresponding inequality for the original sequences. So from now on we assume that $n_1 > m_1$, that is, m_1 is a proper divisor of n_1.

The conditions imply that $\prod_{i=1}^{r}\frac{n_i}{m_i}$ divides n_1, and $\prod_{i=1}^{r}\frac{n_i}{m_i} = n_1$ if and only if $m_r = 1$, $n_r = m_{r-1}$, $\dots$, $n_2 = m_1$. Assume first that these equalities hold. Then we have

$$\sum_{i=1}^{r}(n_i - 1) = \prod_{i=1}^{r}\frac{n_i}{m_i} - 1 + \sum_{i=2}^{r}(n_i - 1) = \prod_{i=1}^{r}\frac{n_i}{m_i} - 1 + \sum_{i=1}^{r-1}(m_i - 1)$$

and taking into account that $m_r = 1$, we see that (4) holds with equality in this case. Suppose finally that $\prod_{i=1}^{r}\frac{n_i}{m_i}$ is a proper divisor of n_1. Let p be a minimal prime divisor of n_1. Then $\prod_{i=1}^{r}\frac{n_i}{m_i} \leq \frac{n_1}{p}$ and $m_1 \leq \frac{n_1}{p}$. Consequently we have

$$n_1 - 1 = \frac{n_1}{p} \cdot p - 1 \geq \frac{n_1}{p} + \frac{n_1}{p} - 1 \geq \prod_{i=1}^{r}\frac{n_i}{m_i} + m_1 - 1 > \prod_{i=1}^{r}\frac{n_i}{m_i} - 1 + (m_1 - 1).$$

Since for $i = 2, \dots, r$ we have $n_i - 1 \geq m_i - 1$, we conclude (4). □

Lemma 4.1 in [17] (see also Exercise 1.6 in [16]) asserts that $\mathsf{d}^*(G) \geq \mathsf{d}^*(H) + \mathsf{d}^*(G/H)$ for any subgroup H of G. In Lemma 3.2 we provide a different proof of the special case when G/H is cyclic, and state also the condition for equality.

Lemma 3.2. *Let H be a proper subgroup of G such that the factor group G/H is cyclic. Then $\mathsf{d}^*(G) \geq \mathsf{d}^*(H) + [G : H] - 1$, with equality if and only if $\operatorname{rank}(H) = \operatorname{rank}(G) - 1$, and $H \cong \bigoplus_{i \in \{1,\dots,r\} \setminus \{j\}} C_{n_i}$ for some $j \in \{1, \dots, r\}$.*

Proof. Take a finite abelian p-group A. It is isomorphic to $C_{p^{\lambda_1}} \oplus \cdots \oplus C_{p^{\lambda_k}}$ where $\lambda_1 \geq \cdots \geq \lambda_k > 0$. We call the partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ the *type* of A. Any subgroup B of A has type $\mu = (\mu_1, \ldots, \mu_k)$, $\mu_1 \geq \cdots \geq \mu_k \geq 0$, where $\mu_i \leq \lambda_i$ for $i = 1, \ldots, k$. Moreover, A has a subgroup B of type μ such that the factor group A/B is cyclic (necessarily of order p^d, where $d := \sum(\lambda_i - \mu_i)$) if and only if the Littlewood-Richardson coefficient $c^{\lambda}_{\mu,(d)}$ is non-zero (see for example II.4.3 in [22]), and by Pieri's rules (see for example I.5.16 in [22]) this happens if and only if the additional inequalities $\mu_1 \geq \lambda_2$, $\mu_2 \geq \lambda_3$,, $\ldots$, $\mu_{r-1} \geq \lambda_r$ hold as well.

Note that both G and H are the direct sums of their unique Sylow subgroups. Therefore it follows from the above paragraph that the subgroup H is isomorphic to $H \cong C_{m_1} \oplus \cdots \oplus C_{m_r}$ where $1 \leq m_r \mid m_{r-1} \mid \cdots \mid m_1$, and $m_i \mid n_i$ for $i = 1, \ldots, r$. Moreover, since G/H is cyclic, for any prime p the factor of the Sylow p-subgroup of G modulo the Sylow p-subgroup of H is cyclic, so again by the above paragraph the conditions $n_{i+1} \mid m_i$ for $i = 1, \ldots, r-1$ hold as well. This means that the assumptions of Lemma 3.1 hold for the r-tuples $(n_1, \ldots, n_r)$, $(m_1, \ldots, m_r)$. Thus by Lemma 3.1 the inequality (4) holds, which is the same as the desired inequality in our statement. □

Given the finite abelian groups G, H, K, there exists a subgroup G_1 of G such that $G_1 \cong H$ and $G/G_1 \cong K$ if and only if there exists a subgroup G_2 of G with $G_2 \cong K$ and $G/G_2 \cong H$. Therefore Lemma 3.2 has its dual form as well:

Lemma 3.3. *Let K be a non-trivial cyclic subgroup of G. Then $\mathsf{d}^*(G) \geq \mathsf{d}^*(G/K) + |K| - 1$, with equality if and only if $\operatorname{rank}(G/K) = \operatorname{rank}(G) - 1$, and for some $j \in \{1, \ldots, r\}$ we have $G/K \cong \bigoplus_{i \in \{1,\ldots,r\} \setminus \{j\}} C_{n_i}$.*

Corollary 3.4. *Let $a_1, \ldots, a_k$ be a sequence of elements generating G, and for $i = 1, \ldots, k$ denote by d_i the order of a_i modulo the subgroup $\langle a_1, \ldots, a_{i-1} \rangle$ (so $d_1 \ldots d_k = |G|$). Then $\mathsf{d}^*(G) \geq \sum_{i=1}^{k}(d_i - 1)$, with equality if and only if the multiset $\{n_1, \ldots, n_r\}$ coincides with the multiset $\{d_{i_1}, \ldots, d_{i_r}\}$ obtained by omitting all occurrences of 1 in the sequence $d_1, \ldots, d_k$.*

Proof. Apply induction for k. The case $k = 1$ is obvious, since then G is cyclic of order d_1, so $r = 1$, $n_1 = d_1$, and $\mathsf{d}^*(G) = d_1 - 1 = n_1 - 1$. Assume next that $k > 1$, and set $H := \langle a_1, \ldots, a_{k-1} \rangle$. If $H = G$, then $d_k = 1$, $\mathsf{d}^*(G) = \mathsf{d}^*(H)$, and the statement follows by the induction hypothesis applied to H. If H is a proper subgroup of G, then $d_k > 1$. By Lemma 3.2 we have $\mathsf{d}^*(G) \geq \mathsf{d}^*(H) + d_k - 1$, with equality only if $H \cong \bigoplus_{i \in \{1,\ldots,r\} \setminus \{j\}} C_{n_i}$ for some $j \in \{1, \ldots, r\}$, implying also $n_j = d_k$. Now we may conclude by applying the induction hypothesis for H and the sequence $a_1, \ldots, a_{k-1}$. □

We shall use the following terminology. Given an ordered sequence $a_1, \ldots, a_k \in G$ of elements generating G, any $b \in G$ can be uniquely written as

$$b = \sum_{i=1}^{k} l_i a_i, \qquad 0 \leq l_i \leq d_i - 1 \text{ for } i = 1, \ldots, k \tag{5}$$

where d_i denotes the smallest positive integer d such that da_i belongs to the subgroup $\langle a_1, \ldots, a_{i-1} \rangle$. Indeed, consider the chain

$$\{0\} \subset \langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \cdots \subset \langle a_1, \ldots, a_k \rangle = G$$

of subgroups. It has cyclic factors of order $d_1, \dots, d_k$. The factor $G/\langle a_1, \dots, a_{k-1}\rangle$ is generated by the coset of a_k, hence $b + \langle a_1, \dots, a_{k-1}\rangle = l(a_k + \langle a_1, \dots, a_{k-1}\rangle)$ for a unique $0 \le l \le d_k - 1$. Now continue in the same way with the element $b - la_k$ in the group $\langle a_1, \dots, a_{k-1}\rangle$. We shall refer to (5) as the *normal form* of b with respect to $a_1, \dots, a_k$, and we call $\sum_{i=1}^{k}(d_i - 1 - l_i)$ the *deficit of* b.

Lemma 3.5. *Let $a_1, \dots, a_k$ be an arbitrary sequence of elements in G, and denote by d_k the order of a_k modulo the subgroup $\langle a_1, \dots, a_{k-1}\rangle$. Then there exists an $m = (m_1, \dots, m_k) \in \mathcal{B}(a_1, \dots, a_k)$ such that $m_k = d_k$ and $|m| = m_1 + \cdots + m_k \le \mathsf{d}^*(G) + 1$.*

Proof. The group $\langle a_1, \dots, a_{k-1}\rangle$ contains $d_k a_k$. Set $m := (l_1, \dots, l_{k-1}, d_k)$ where $-d_k a_k = \sum_{i=1}^{k-1} l_i a_i$ is the normal form of $-d_k a_k$ with respect to $a_1, \dots, a_{k-1}$. Then m belongs to $\mathcal{B}(a_1, \dots, a_k)$, and $|m| \le \sum_{i=1}^{k-1}(d_i - 1) + d_k \le \mathsf{d}^*(G) + 1$, where the last inequality holds by Corollary 3.4. □

Lemma 3.6. *Suppose that $a_1, \dots, a_k$ are distinct non-zero elements in G, and denote by d_i the order of a_i modulo $\langle a_1, \dots, a_{i-1}\rangle$ for $i = 1, \dots, k$. If there is no $m \in \mathcal{B}(a_1, \dots, a_k)$ such that $|m| \le \mathsf{d}^*(G)$ and $m_k = d_k$, then either $k = 1$ and $G = \langle a_1\rangle$, or $G = \langle a_1, \dots, a_{k-1}\rangle$, the multiset $\{d_1, \dots, d_{k-1}\}$ coincides with the multiset $\{n_1, \dots, n_r\}$ (so in particular $k - 1 = r$ is the rank of G), and the deficit of $-a_k$ with respect to $a_1, \dots, a_{k-1}$ is zero.*

Proof. Suppose that $k > 1$ and for the m constructed in the proof of Lemma 3.5 we have $|m| > \mathsf{d}^*(G)$, so

$$-d_k a_k = \sum_{i=1}^{k-1}(d_i - 1)a_i \tag{6}$$

and $\mathsf{d}^*(G) = \sum_{j=1}^{k}(d_j - 1)$. We claim that $d_1, \dots, d_{k-1} > 1$. Indeed, assume on the contrary that for some $i \in \{1, \dots, k-1\}$ we have $d_i = 1$. Then $a_i \in \langle a_1, \dots, a_{i-1}\rangle$, so we may write

$$a_i = l_1 a_1 + \cdots + l_{i-1} a_{i-1} \tag{7}$$

in its normal form with respect to $a_1, \dots, a_{i-1}$. Equations (6) and (7) imply

$$-d_k a_k = \sum_{j=1}^{i-1}(d_j - 1 - l_j) + a_i + \sum_{q=i+1}^{k-1}(d_q - 1)a_q.$$

Setting $m' := (d_1 - 1 - l_1, \dots, d_{i-1} - 1 - l_{i-1}, 1, d_{i+1} - 1, \dots, d_{k-1} - 1, d_k)$ we get that $m' \in \mathcal{B}(a_1, \dots, a_k)$. Moreover, as $a_1, \dots, a_i$ are distinct, we have that $l_1 + \cdots + l_{i-1} \ge 2$, hence $|m'| = \sum_{i=1}^{k}(d_i - 1) + 2 - (l_1 + \cdots + l_{i-1}) \le \sum_{j=1}^{k}(d_j - 1) = \mathsf{d}^*(G)$. So we found an $m' \in \mathcal{B}(a_1, \dots, a_k)$ with $m'_k = d_k$ and $|m'| \le \mathsf{d}^*(G)$. This contradicts the assumption of the lemma, hence $d_1, \dots, d_{k-1}$ are all greater than 1.

Suppose that $H := \langle a_1, \dots, a_{k-1}\rangle \subsetneq G$. If $d_k = 1$, then $\langle a_1, \dots, a_k\rangle = H \subsetneq G$, and by Lemma 3.5 there exists an $m \in \mathcal{B}(a_1, \dots, a_k)$ with $m_k = d_k$ and $|m| \le \mathsf{d}^*(H) + 1 \le \mathsf{d}^*(G)$. If $d_i > 1$ for all $i = 1, \dots, k$, by Corollary 3.4 the equality $\mathsf{d}^*(G) = \sum_{j=1}^{k}(d_j - 1)$ implies that the multiset $\{d_1, \dots, d_k\}$ coincides with $\{n_1, \dots, n_r\}$. In particular, $k = r$ is the rank of G. However, since d_1 is the order of a_1, equation (6) implies that a_1 is contained in $\langle a_2, \dots, a_k\rangle$. Thus G can be

generated by $k-1=r-1$ elements. This is a contradiction, so this case does not occur.

Therefore $\langle a_1,\dots,a_{k-1}\rangle = G$, and consequently $d_k=1$. Equation (6) becomes $-a_k = \sum_{i=1}^{k-1}(d_i-1)a_i$, so the deficit of $-a_k$ is zero. Moreover, the equality $\mathsf{d}^*(G) = \sum_{j=1}^{k}(d_j-1) = \sum_{j=1}^{k-1}(d_j-1)$ implies by Corollary 3.4 that the multisets $\{d_1,\dots,d_{k-1}\}$ and $\{n_1,\dots,n_r\}$ coincide, finishing the proof. □

Lemma 3.7. *Let $a_1,\dots,a_k$ be a sequence of elements of a non-cyclic group G, and denote by g_i the order of a_i modulo the subgroup $\langle a_1,\dots,a_{i-1},a_{i+1},\dots,a_k\rangle$. Assume that the following hold:*

(a) *There does not exist an $m=(m_1,\dots,m_k)\in\mathcal{B}(a_1,\dots,a_k)$ with $|m|\le \mathsf{d}^*(G)$ such that $m_i=g_i$ for some $i\in\{1,\dots,k\}$.*
(b) *There does not exist a pair $m',m''\in\mathcal{B}(a_1,\dots,a_k)$ with $|m'|\le\mathsf{d}^*(G)$, $|m''|\le\mathsf{d}^*(G)$, such that $m'_i=2$ and $m''_i=3$ for some $i\in\{1,\dots,k\}$.*

Then $2=n_{s+1}=\dots=n_r$ where $r=2s$ or $r=2s-1$.

Proof. No element in $\{a_1,\dots,a_k\}$ is zero, since $a_i=0$ implies $g_i=1$, and $e_i\in\mathcal{B}(a_1,\dots,a_k)$ where e_i is the ith standard basis vector in $\mathbb{Z}^k$, hence (a) implies $\mathsf{d}^*(G)<1$, a contradiction. The elements $a_1,\dots,a_k$ are distinct. Indeed, assume to the contrary that say $a_1=a_2$. Then denoting by d the order of a_1, we have that $g_1=1$ and $m=(1,d-1,0,\dots,0)\in\mathcal{B}(a_1,\dots,a_k)$, hence by (a) we have $\mathsf{d}^*(G)<d$, a contradiction (recall that G is not cyclic).

Thus $a_1,\dots,a_k$ are distinct non-zero elements of G, and Lemma 3.6 applies for them with an arbitrary ordering of the elements in the sequence. In particular, by condition (a) and Lemma 3.6 the rank of G is $k-1$, and any $k-1$ of the elements $a_1,\dots,a_k$ generate G. Furthermore, after an arbitrary renumbering of the elements in the set $\{a_1,\dots,a_k\}$, the deficit of $-a_k$ with respect to $a_1,\dots,a_{k-1}$ is 0, and the multiset $\{d_1,\dots,d_{k-1}\}$ coincides with $\{n_1,\dots,n_r\}$, where d_i stands for the order of a_i modulo $\langle a_1,\dots,a_{i-1}\rangle$.

We claim that for any $i\in\{1,\dots,k\}$ with $2a_i\neq 0$ there exists a $j\neq i$ such that $2a_i=2a_j$. Indeed, suppose for example that $2a_k\neq 0$. Recall that the deficit of $-a_k$ with respect to $a_1,\dots,a_{k-1}$ is zero, so

$$-a_k=\sum_{i=1}^{k-1}(d_i-1)a_i. \tag{8}$$

Since $-a_k\neq -2a_k$, the deficit of $-2a_k$ is different from the deficit of $-a_k$, so the deficit of $-2a_k$ is non-zero. Also a_k is different from each of $a_1,\dots,a_{k-1}$, implying that the deficit of $-2a_k$ is not 1. Consequently, the deficit of $-2a_k$ is at least 2, hence $m':=(l_1,\dots,l_{k-1},2)$ where $-2a_k=l_1a_1+\dots+l_{k-1}a_{k-1}$ is the normal form of $-2a_k$ satisfies $m'\in\mathcal{B}(a_1,\dots,a_k)$, $m'_k=2$ and $|m'|=2+l_1+\dots+l_{k-1}\le\mathsf{d}^*(G)$. It follows by assumption (b) that the deficit of $-3a_k$ is at most 2. It cannot be 0, the deficit of $-a_k$, since $-a_k\neq -3a_k$ by the assumption $2a_k\neq 0$. The deficit of $-3a_k$ cannot be 1, otherwise $2a_k$ coincides with one of $a_1,\dots,a_{k-1}$, say $2a_k=a_2$, and therefore $G=\langle a_2,a_3,\dots,a_k\rangle=\langle a_3,\dots,a_k\rangle$ is generated by $k-2=r-1$ elements, a contradiction. Thus the deficit of $-3a_k$ is 2. There are two possible cases: $-3a_k=(d_1-2)a_1+(d_2-2)a_2+\sum_{i=3}^{k-1}(d_i-1)a_i$ or $-3a_k=(d_1-3)a_1+(d_2-1)a_2+\sum_{i=3}^{k-1}(d_i-1)a_i$ (with a suitable ordering of $a_1,\dots,a_{k-1}$). Comparing this with (8) in the first case we deduce $2a_k=a_1+a_2$, hence $-a_1=-2a_k+a_2$.

The latter equality shows that the deficit of $-a_1$ with respect to $a_k, a_2, a_3, \dots, a_{k-1}$ cannot be zero, a contradiction. Thus this case does not occur. The only remaining possibility is that $-3a_k = (d_1 - 3)a_1 + \sum_{i=2}^{k-1}(d_i - 1)a_i$ (with a suitable ordering of $a_1, \dots, a_{k-1}$). Comparing this with (8) we conclude $2a_k = 2a_1$. So the claim is proved.

It follows from the above claim that the set $\{2a_1, \dots, 2a_k\}$ contains at most $\frac{k}{2}$ distinct non-zero elements, hence the rank of the group $\langle 2a_1, \dots, 2a_k\rangle = \{2a \colon a \in G\}$ is at most $\frac{r+1}{2}$. On the other hand the rank of $\{2a \colon a \in G\}$ equals $|\{i \in \{1, \dots, r\} \colon n_i > 2\}|$. Consequently we have $|\{j \in \{1, \dots, r\} \colon n_j = 2\}| \geq \frac{r-1}{2}$. □

Proposition 3.8. *Suppose that $G = C_{n_1} \oplus \cdots \oplus C_{n_s} \oplus C_2 \oplus \cdots \oplus C_2$ where $r = 2s-1$ or $r = 2s$, so $2 = n_{s+1} = \cdots = n_r$, and $2 \mid n_s \mid n_{s-1} \mid \cdots \mid n_1$. Denote by $e_1, \dots, e_s, f_1, \dots, f_{r-s}$ the generators of the direct factors of G, thus the order of e_i is n_i for $i = 1, \dots, s$, and the order of f_j is 2 for $j = 1, \dots, r-s$. Set $a_1 = e_1$, $a_{2i} = e_i + f_i$ and $a_{2i+1} = f_i + e_{i+1}$ for $i = 1, \dots, s-1$, and $a_{2s} = e_s$ if $r = 2s-1$ whereas $a_{2s} = e_s + f_s$, $a_{2s+1} = f_s$ if $r = 2s$. Then the abelian group $\mathcal{G}(a_1, \dots, a_{r+1})$ is not generated by $\{m \in \mathcal{B}(a_1, \dots, a_{r+1}) \colon |m| \leq \mathsf{d}^*(G)\}$.*

Proof. The element a_1 is contained in the group $\langle a_2, \dots, a_{r+1}\rangle$, whence there exists an element $u \in \mathcal{B}(a_1, \dots, a_{r+1})$ with $u_1 = 1$. On the other hand we shall show that for any $m \in \mathcal{B}(a_1, \dots, a_{r+1})$ with $|m| \leq \mathsf{d}^*(G)$ we have that m_1 is even, and consequently u is not contained in the subgroup of $\mathcal{G}(a_1, \dots, a_{r+1})$ generated by $\{m \in \mathcal{B}(a_1, \dots, a_{r+1}) \colon |m| \leq \mathsf{d}^*(G)\}$. Indeed, take $m = (m_1, \dots, m_{r+1}) \in \mathcal{B}(a_1, \dots, a_{r+1})$ with m_1 odd and $|m|$ minimal possible. Consider the case when $r = 2s-1$, and so $\mathsf{d}^*(G) = n_1 + \cdots + n_s - 1$. The order of a_{2i-1} and a_{2i} is n_i, hence $0 \leq m_{2i}, m_{2i-1} \leq n_i - 1$ hold for $i = 1, \dots, s$. We have

$$0 = \sum_{i=1}^{2s} m_i a_i = \sum_{i=1}^{s} (m_{2i-1} + m_{2i}) e_i + \sum_{i=1}^{s-1} (m_{2i} + m_{2i+1}) f_i.$$

The coefficient $m_1 + m_2$ of e_1 above is divisible by n_1, we have $m_1 + m_2 > 0$ since m_1 is odd, and $m_1 + m_2 \leq 2n_1 - 2$. We deduce that $m_1 + m_2 = n_1$, implying in turn that m_2 is odd. From the coefficient of f_1 above we infer that m_3 is odd as well. From the coefficient of e_2 above we deduce that $m_3 + m_4 = n_2$, and consequently m_4 is odd. Continuing in the same way and looking at step-by-step the coefficient of $f_2, e_3, f_3, e_4, \dots, f_{s-1}, e_s$ we arrive at the conclusion that $m_{2i-1} + m_{2i} = n_i$ for all $i = 1, \dots, s$, whence $|m| = \sum_{i=1}^{s}(m_{2i-1} + m_{2i}) = \sum_{i=1}^{s} n_i > (\sum_{i=1}^{s} n_i) - 1 = \mathsf{d}^*(G)$. The case when $r = 2s$ is similar. □

Proposition 3.9. *Let $a_1, \dots, a_k$ be a sequence of elements of G.*

(i) *The abelian group $\mathcal{G}(a_1, \dots, a_k)$ is generated by $\{m \in \mathcal{B}(a_1, \dots, a_k) \colon |m| \leq \mathsf{d}^*(G) + 1\}$.*

(ii) *If $r > 1$ and $n_{s+1} \neq 2$ where $r = 2s$ or $r = 2s-1$, then $\mathcal{G}(a_1, \dots, a_k)$ is generated by $\{m \in \mathcal{B}(a_1, \dots, a_k) \colon |m| \leq \mathsf{d}^*(G)\}$.*

Proof. (i) Take an arbitrary $u \in \mathcal{G}(a_1, \dots, a_k)$. Since $u_k a_k = -\sum_{i=1}^{k-1} u_i a_i$ belongs to $\langle a_1, \dots, a_{k-1}\rangle$, there exists an integer l_1 such that $u_k = l_1 d_k$, where d_k is the order a_k modulo $\langle a_1, \dots, a_{k-1}\rangle$. By Lemma 3.5 there exists an $m^{(1)} \in \mathcal{B}(a_1, \dots, a_k)$ with $m_k^{(1)} = d_k$ and $|m^{(1)}| \leq \mathsf{d}^*(G) + 1$. Set $u' := u - l_1 m^{(1)}$. Then $u'_k = 0$, so

u' belongs to $\mathcal{G}(a_1,\dots,a_{k-1})$ identified with the subset $\{m \in \mathcal{G}(a_1,\dots,a_k)\colon m_k = 0\}$ in $\mathcal{G}(a_1,\dots,a_k)$. Repeat the same step for u' to obtain $l_2 \in \mathbb{Z}$ and $m^{(2)} \in \mathcal{B}(a_1,\dots,a_{k-1})$ such that $|m^{(2)}| \le \mathsf{d}^*(G)+1$ and $u' - l_2 m^{(2)} \in \mathcal{G}(a_1,\dots,a_{k-2})$. Continue in the same way and eventually we get that

$$u = \sum_{i=1}^{k} l_i m^{(i)} \text{ where } m^{(i)} \in \mathcal{B}(a_1,\dots,a_i), \quad |m^{(i)}| \le \mathsf{d}^*(G)+1 \text{ for } i \in \{1,\dots,k\}.$$

(ii) We slightly adjust the poof of (i). By our assumption on G, it follows from Lemma 3.7 that after a possible reordering of the elements $a_1,\dots,a_k$ and denoting by g_k the order of a_k modulo $\langle a_1,\dots,a_{k-1}\rangle$ at least one of the following two possibilities holds:

(a) there is an $m \in \mathcal{B}(a_1,\dots,a_k)$ with $|m| \le \mathsf{d}^*(G)$ and $m_k = g_k$;
(b) there are $m', m'' \in \mathcal{B}(a_1,\dots,a_k)$ with $|m'|, |m''| \le \mathsf{d}^*(G)$ and $m'_k = 2$, $m''_k = 3$.

Now take an arbitrary $u \in \mathcal{G}(a_1,\dots,a_k)$. We have $u_k = lg_k$ for some $l \in \mathbb{Z}$. Set $u' := u - lm$ if (a) holds and $u' := u - l(m'' - m')$ if (b) holds (note that in this case necessarily $g_k = 1$). Then u' belongs to $\mathcal{G}(a_1,\dots,a_{k-1})$. Continue in the same way with the sequence $a_1,\dots,a_{k-1}$ and $u' \in \mathcal{G}(a_1,\dots,a_{k-1})$. In k steps we get a presentation of u as an integral linear combination of elements from $\{m \in \mathcal{B}(a_1,\dots,a_k)\colon |m| \le \mathsf{d}^*(G)\}$. □

Theorem 3.10. *For any finite abelian group G we have the inequality*

$$\beta_{\mathrm{sep}}(G) \le \mathsf{d}^*(G)+1$$

with equality holding if and only if G is cyclic or $2 = n_{s+1} = \cdots = n_r$ where $r = 2s-1$ or $r = 2s$.

Proof. Proposition 3.9 (i) and Corollary 2.6 imply the inequality $\beta_{\mathrm{sep}}(G) \le \mathsf{d}^*(G)+1$. Furthermore, if G is not cyclic and $n_{s+1} \ne 2$ where $r = 2s$ or $r = 2s-1$, then by Proposition 3.9 (ii) and Corollary 2.6 we even get the stronger inequality $\beta_{\mathrm{sep}}(G) \le \mathsf{d}^*(G)$.

For a cyclic group G any faithful 1-dimensional G-module V gives $\beta_{\mathrm{sep}}(G,V) = |G| = \mathsf{d}^*(G)+1$. Suppose finally that $2 = n_{s+1} = \cdots = n_r$ where $r = 2s-1 > 1$ or $r = 2s$. By Proposition 3.8 and Corollary 2.6 we conclude $\beta_{\mathrm{sep}}(G) > \mathsf{d}^*(G)$. Summarizing, for these groups G we have the equality $\beta_{\mathrm{sep}}(G) = \mathsf{d}^*(G)+1$. □

Corollary 3.11. *We have the strict inequality*

$$\beta_{\mathrm{sep}}(G) < \beta(G)$$

for any non-cyclic finite abelian group G with $n_{s+1} \ne 2$, where $r = 2s-1$ or $r = 2s$.

Proof. Theorem 3.10 for a non-cyclic G satisfying $n_{s+1} \ne 2$ together with (3) and (2) yield the inequalities

$$\beta_{\mathrm{sep}}(G) \le \mathsf{d}^*(G) < \mathsf{d}^*(G)+1 \le \mathsf{D}(G) = \beta(G).$$

□

Remark 3.12. (i) Since for a finite abelian group G with $n_{s+1} = \cdots = n_r = 2$ we have $\beta_{\mathrm{sep}}(G) = \mathsf{d}^*(G)+1$ by Theorem 3.10, therefore for such a group we have $\beta_{\mathrm{sep}}(G) < \beta(G)$ if and only if we have the strict inequality $\mathsf{d}^*(G)+1 < \mathsf{D}(G)$.

A complete description of the groups G with $n_{s+1} = \cdots = n_r = 2$ and $\mathsf{D}(G) > \mathsf{d}^*(G)+1$ is not known. On the other hand there are infinitely many known examples of groups G where $n_{s+1} = \cdots = n_r = 2$ both with equality $\mathsf{d}^*(G) + 1 = \mathsf{D}(G)$ and with strict inequality $\mathsf{d}^*(G) + 1 < \mathsf{D}(G)$; see for example Corollary 2 in [12] or Corollary 4.2.3 in [13]. We note also that denoting for $j \in \{1, \dots, r\}$ the subgroup $G_j := \bigoplus_{i\in\{1,\dots,k\}\setminus\{j\}} C_{n_i}$ of G, we have $\mathsf{d}^*(G) = \mathsf{d}^*(G_j) + n_j - 1$, whereas $\mathsf{D}(G) \geq \mathsf{D}(G_j) + \mathsf{D}(G/G_j) - 1 = \mathsf{D}(G_j) + n_j - 1$ (see for example Proposition 5.1.11 (1) in [15]). Therefore if we have a strict inequality $\mathsf{d}^*(G_j) + 1 < \mathsf{D}(G_j)$, then we also have the strict inequality $\mathsf{d}^*(G) + 1 < \mathsf{D}(G)$.

(ii) Set $G_n := C_{p^n} \oplus C_p$ for $n = 1, 2, \dots$ where p is an odd prime. Then $\beta_{\mathrm{sep}}(G_n) \geq \beta_{\mathrm{sep}}(C_{p^n}) = p^n$ and $\beta(G_n) = \mathsf{D}(G_n) = p^n + p - 1$, hence

$$1 \geq \lim_{n\to\infty} \frac{\beta_{\mathrm{sep}}(G_n)}{\beta(G_n)} \geq \lim_{n\to\infty} \frac{p^n}{p^n + p - 1} = 1.$$

This shows that the inequality $\beta_{\mathrm{sep}}(G)/\beta(G) < 1$ in Corollary 3.11 cannot be strengthened to $\beta_{\mathrm{sep}}(G)/\beta(G) < c$ with a positive constant $c < 1$.

Acknowledgment

The author thanks Alfred Geroldinger for helpful comments on the manuscript.

References

[1] Kálmán Cziszter, *The Noether number of the non-abelian group of order* $3p$, Period. Math. Hungar. **68** (2014), no. 2, 150–159, DOI 10.1007/s10998-014-0025-4. MR3217554

[2] Kálmán Cziszter and Mátyás Domokos, *Groups with large Noether bound* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **64** (2014), no. 3, 909–944. MR3330158

[3] Kálmán Cziszter and Mátyás Domokos, *The Noether number for the groups with a cyclic subgroup of index two*, J. Algebra **399** (2014), 546–560, DOI 10.1016/j.jalgebra.2013.09.044. MR3144602

[4] 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, (Scott T. Chapman and M. Fontana and A. Geroldinger and B. Olberding, eds.), Springer-Verlag, 2016, pp. 43-95.

[5] Harm Derksen and Gregor Kemper, *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130. MR1918599

[6] M. Domokos, *Typical separating invariants*, Transform. Groups **12** (2007), no. 1, 49–63, DOI 10.1007/s00031-005-1131-4. MR2308028

[7] Mátyás Domokos and Endre Szabó, *Helly dimension of algebraic groups*, J. Lond. Math. Soc. (2) **84** (2011), no. 1, 19–34, DOI 10.1112/jlms/jdq101. MR2819688

[8] Emilie Dufresne and Jack Jeffries, *Separating invariants and local cohomology*, Adv. Math. **270** (2015), 565–581, DOI 10.1016/j.aim.2014.11.003. MR3286543

[9] Bryson W. Finklea, Terri Moore, Vadim Ponomarenko, and Zachary J. Turner, *Invariant polynomials and minimal zero sequences*, Involve **1** (2008), no. 2, 159–165, DOI 10.2140/involve.2008.1.159. MR2429656

[10] Peter Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. Math. **156** (2000), no. 1, 23–32, DOI 10.1006/aima.2000.1952. MR1800251

[11] John Fogarty, *On Noether's bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5–7 (electronic), DOI 10.1090/S1079-6762-01-00088-9. MR1826990

[12] Alfred Geroldinger and Rudolf Schneider, *On Davenport's constant*, J. Combin. Theory Ser. A **61** (1992), no. 1, 147–152, DOI 10.1016/0097-3165(92)90061-X. MR1178393

[13] Alfred Geroldinger, *Additive group theory and non-unique factorizations*, Combinatorial number theory and additive group theory, Adv. Courses Math. CRM Barcelona, Birkhäuser Verlag, Basel, 2009, pp. 1–86, DOI 10.1007/978-3-7643-8962-8. MR2522037

[14] Weidong Gao and Alfred Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), no. 4, 337–369, DOI 10.1016/j.exmath.2006.07.002. MR2313123

[15] Alfred Geroldinger and Franz Halter-Koch, *Non-unique factorizations*, Pure and Applied Mathematics (Boca Raton), vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory. MR2194494

[16] David J. Grynkiewicz, *Structural additive theory*, Developments in Mathematics, vol. 30, Springer, Cham, 2013. MR3097619

[17] David J. Grynkiewicz, Luz E. Marchan, and Oscar Ordaz, *Representation of finite abelian group elements by subsequence sums* (English, with English and French summaries), J. Théor. Nombres Bordeaux **21** (2009), no. 3, 559–587. MR2605534

[18] P. Hegedűs and L. Pyber, *Upper bounds for the Noether number of a finite group*, preprint (2015).

[19] Evelyne Hubert and George Labahn, *Computation of invariants of finite abelian groups*, Math. Comp. **85** (2016), no. 302, 3029–3050, DOI 10.1090/mcom/3076. MR3522980

[20] Gregor Kemper, *Separating invariants*, J. Symbolic Comput. **44** (2009), no. 9, 1212–1222, DOI 10.1016/j.jsc.2008.02.012. MR2532166

[21] Martin Kohls and Hanspeter Kraft, *Degree bounds for separating invariants*, Math. Res. Lett. **17** (2010), no. 6, 1171–1182, DOI 10.4310/MRL.2010.v17.n6.a15. MR2729640

[22] I. G. Macdonald, *Symmetric functions and Hall polynomials*, 2nd ed., Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1995. With contributions by A. Zelevinsky; Oxford Science Publications. MR1354144

[23] Mara D. Neusel and Müfit Sezer, *Separating invariants for modular p-groups and groups acting diagonally*, Math. Res. Lett. **16** (2009), no. 6, 1029–1036, DOI 10.4310/MRL.2009.v16.n6.a11. MR2576691

[24] Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen* (German), Math. Ann. **77** (1915), no. 1, 89–92, DOI 10.1007/BF01456821. MR1511848

[25] John E. Olson, *A combinatorial problem on finite Abelian groups. I*, J. Number Theory **1** (1969), 8–10. MR0237641

[26] John E. Olson, *A combinatorial problem on finite Abelian groups. II*, J. Number Theory **1** (1969), 195–199. MR0240200

[27] Alain Plagne and Salvatore Tringali, *The Davenport constant of a box*, Acta Arith. **171** (2015), no. 3, 197–219, DOI 10.4064/aa171-3-1. MR3416944

[28] David R. Richman, *Invariants of finite groups over fields of characteristic p*, Adv. Math. **124** (1996), no. 1, 25–48, DOI 10.1006/aima.1996.0076. MR1423197

[29] Barbara J. Schmid, *Finite groups and invariant theory*, Topics in invariant theory (Paris, 1989/1990), Lecture Notes in Math., vol. 1478, Springer, Berlin, 1991, pp. 35–66, DOI 10.1007/BFb0083501. MR1180987

MTA Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, 1053 Budapest, Hungary

E-mail address: domokos.matyas@renyi.mta.hu