

ON THE DAVENPORT CONSTANT AND GROUP ALGEBRAS

BY

DANIEL SMERTNIG (Graz)

Abstract. For a finite abelian group G and a splitting field K of G , let $\mathbf{d}(G, K)$ denote the largest integer $l \in \mathbb{N}$ for which there is a sequence $S = g_1 \cdot \dots \cdot g_l$ over G such that $(X^{g_1} - a_1) \cdot \dots \cdot (X^{g_l} - a_l) \neq 0 \in K[G]$ for all $a_1, \dots, a_l \in K^\times$. If $\mathbf{D}(G)$ denotes the Davenport constant of G , then there is the straightforward inequality $\mathbf{D}(G) - 1 \leq \mathbf{d}(G, K)$. Equality holds for a variety of groups, and a conjecture of W. Gao et al. states that equality holds for all groups. We offer further groups for which equality holds, but we also give the first examples of groups G for which $\mathbf{D}(G) - 1 < \mathbf{d}(G, K)$. Thus we disprove the conjecture.

1. Introduction and main result. Let G be an additive finite abelian group. For a (multiplicatively written) sequence $S = g_1 \cdot \dots \cdot g_l$ over G , $|S| = l$ is called the *length* of S , and S is said to be *zero-sum free* if $\sum_{i \in I} g_i \neq 0$ for every nonempty subset $I \subset [1, l]$. Let $\mathbf{d}(G)$ denote the maximal length of a zero-sum free sequence over G . Then $\mathbf{d}(G) + 1$ is the *Davenport constant* of G , a classical constant from combinatorial number theory (for surveys and historical comments, the reader is referred to [3], [8, Chapter 5], [7]). In general, the precise value of $\mathbf{d}(G)$ (in terms of the group invariants of G) and the structure of the extremal sequences is unknown; see [12, 1, 13, 10, 11, 4, 14, 15, 9] for recent progress.

The group algebras $R[G]$ (over suitable commutative rings R) have turned out to be powerful tools for a great variety of questions from combinatorics and number theory, including ones involving the Davenport constant. We recall the definition of an invariant (involving group algebras) which has been used for the investigation of the Davenport constant since the 1960s.

For a commutative ring R , let $\mathbf{d}(G, R) \in \mathbb{N} \cup \{\infty\}$ denote the supremum of all $l \in \mathbb{N}$ having the following property: there is some sequence $S = g_1 \cdot \dots \cdot g_l$ of length l over G such that

$$(X^{g_1} - a_1) \cdot \dots \cdot (X^{g_l} - a_l) \neq 0 \in R[G] \quad \text{for all } a_1, \dots, a_l \in R \setminus \{0\}.$$

If S is zero-sum free, R is an integral domain, $a_1, \dots, a_l \in R \setminus \{0\}$ and

$$f = (X^{g_1} - a_1) \cdot \dots \cdot (X^{g_l} - a_l) = \sum_{g \in G} c_g X^g,$$

2010 *Mathematics Subject Classification*: 11P70, 11B50, 11B30, 20K01.

Key words and phrases: Davenport constant, zero-sum sequence, group algebras.

then $c_0 \neq 0$. Hence $f \neq 0$, and it follows that

$$d(G) \leq d(G, R).$$

Theorem A below was proved by P. van Emde Boas, D. Kruyswijk and J. E. Olson in the 1960s (in fact, they did not explicitly define the invariants $d(G, K)$ but got these results implicitly). Historical remarks and proofs in the present terminology may be found in [7, Section 2.2] and [8, Theorem 5.5.9]; see also [5].

THEOREM A. *Let G be a finite abelian group with $\exp(G) = n \geq 2$.*

(i) *Let K be a splitting field of G with $\text{char}(K) \nmid \exp(G)$. Then*

$$d(G, K) \leq (n - 1) + n \log \frac{|G|}{n}.$$

(ii) *If G is a p -group, then $d(G) = d(G, \mathbb{Z}/p\mathbb{Z})$.*

Note that for a cyclic group G of order n , the above upper bound implies that $d(G) = d(G, K) = n - 1$, since $d(\mathbb{C}_n) \geq n - 1$ can be easily seen. Only recently did W. Gao and Y. Li show that $d(\mathbb{C}_2 \oplus \mathbb{C}_{2n}) = d(\mathbb{C}_2 \oplus \mathbb{C}_{2n}, K)$ ([6, Theorem 3.3]). We extend their result, but we also show that Conjecture 3.4 in [6], stating that $d(G) = d(G, K)$ for all groups G , does not hold. Here is the main result of the present paper.

THEOREM 1.1. *Let $G = \mathbb{C}_p \oplus \mathbb{C}_{pn}$ with $p \in \mathbb{P}$, $n \in \mathbb{N}$ and let K be a splitting field of G .*

(i) *If $p \leq 3$, then $d(G) = d(G, K)$.*

(ii) *If $p \geq 5$ and $n \geq 2$, then $d(G) < d(G, K)$.*

2. Preliminaries. Let \mathbb{N} denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers, and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$. For $n \in \mathbb{N}$ and $p \in \mathbb{P}$, let \mathbb{C}_n denote a cyclic group with n elements, $v_p(n) \in \mathbb{N}_0$ the p -adic valuation of n with $v_p(p) = 1$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the finite field with p elements.

Let G be an additive finite abelian group. Suppose that $G \cong \mathbb{C}_{n_1} \oplus \cdots \oplus \mathbb{C}_{n_r}$ with $1 < n_1 \mid \cdots \mid n_r$. Then $r = r(G)$ is the *rank* of G , $n_r = \exp(G)$ is the *exponent* of G , and we define $d^*(G) = \sum_{i=1}^r (n_i - 1)$. If $|G| = 1$, then $\exp(G) = 1$, $r(G) = 0$, and we set $d^*(G) = 0$. If $A, B \subset G$ are nonempty subsets, then $A + B = \{a + b \mid a \in A, b \in B\}$ is their sumset. We will make use of the following theorem of Cauchy–Davenport (for a proof see [8, Cor. 5.2.8.1]).

LEMMA 2.1. *Let G be a cyclic group of order $p \in \mathbb{P}$ and let $A, B \subset G$ be nonempty subsets. Then $|A + B| \geq \min\{|A| + |B| - 1, p\}$.*

Sequences over groups. Let $\mathcal{F}(G)$ be the (multiplicatively written) free abelian monoid with basis G . The elements of $\mathcal{F}(G)$ are called *sequences*

over G . We write sequences $S \in \mathcal{F}(G)$ in the form

$$S = \prod_{g \in G} g^{v_g(S)} \quad \text{with } v_g(S) \in \mathbb{N}_0 \text{ for all } g \in G.$$

We call $v_g(S)$ the *multiplicity* of g in S , and we say that S *contains* g if $v_g(S) > 0$. A sequence S_1 is called a *subsequence* of S if $S_1 \mid S$ in $\mathcal{F}(G)$ (equivalently, $v_g(S_1) \leq v_g(S)$ for all $g \in G$). If a sequence $S \in \mathcal{F}(G)$ is written in the form $S = g_1 \cdot \dots \cdot g_l$, we tacitly assume that $l \in \mathbb{N}_0$ and $g_1, \dots, g_l \in G$. For a sequence

$$S = g_1 \cdot \dots \cdot g_l = \prod_{g \in G} g^{v_g(S)} \in \mathcal{F}(G),$$

we call

$$|S| = l = \sum_{g \in G} v_g(S) \in \mathbb{N}_0$$

the *length* of S , and

$$\sigma(S) = \sum_{i=1}^l g_i = \sum_{g \in G} v_g(S)g \in G$$

the *sum* of S . The sequence S is called a *zero-sum sequence* if $\sigma(S) = 0$, and it is called *zero-sum free* if $\sum_{i \in I} g_i \neq 0$ for all $\emptyset \neq I \subset [1, l]$ (equivalently, if there is no nontrivial zero-sum subsequence). We denote by

- $D(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \geq l$ has a nontrivial zero-sum subsequence;
- $d(G)$ the maximal length of a zero-sum free sequence over G .

Then $D(G)$ is called the *Davenport constant* of G , and we trivially have

$$d^*(G) \leq d(G) = D(G) - 1.$$

We will use without further mention the fact that equality holds for p -groups and for groups of rank $r(G) \leq 2$ ([8, Theorems 5.5.9 and 5.8.3]) (equality holds for further groups, but not in general [7, Corollary 4.2.13]).

Group algebras and characters. Let R be a commutative ring (throughout, we assume that R has a unit element $1 \neq 0$) and G a finite abelian group. The *group algebra* $R[G]$ of G over R is a free R -module with basis $\{X^g \mid g \in G\}$ (built with a symbol X), where multiplication is defined by

$$\left(\sum_{g \in G} a_g X^g\right) \left(\sum_{g \in G} b_g X^g\right) = \sum_{g \in G} \left(\sum_{h \in G} a_h b_{g-h}\right) X^g.$$

We view R as a subset of $R[G]$ by means of $a = aX^0$ for all $a \in R$. An element of R is a zero-divisor [a unit] of $R[G]$ if and only if it is a zero-divisor [a unit] of R .

Let K be a field, G a finite abelian group with $\exp(G) = n \in \mathbb{N}$, and $\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\}$ the group of n th roots of unity in K . An n th root of unity ζ is called *primitive* if $\zeta^m \neq 1$ for all $m \in [1, n - 1]$, and we denote by $\mu_n^*(K) \subset \mu_n(K)$ the subset of all primitive n th roots of unity. We denote by $\text{Hom}(G, K^\times) = \text{Hom}(G, \mu_n(K))$ the *character group of G with values in K* (whose operation is given by pointwise multiplication, with the constant 1 function as identity), and we briefly set $\widehat{G} = \text{Hom}(G, K^\times)$ if there is no danger of confusion. Every character $\chi \in \widehat{G}$ has a unique extension to a K -algebra homomorphism $\chi: K[G] \rightarrow K$ (again denoted by χ) acting by means of

$$\chi\left(\sum_{g \in G} a_g X^g\right) = \sum_{g \in G} a_g \chi(g).$$

We call K a *splitting field* of G if $|\mu_n(K)| = n$. Let K be a splitting field of G and $\widehat{G} = \text{Hom}(G, K^\times)$. We gather the properties needed later (for details see [8, Section 5.5] and [2, §17]). We have $\text{char}(K) \nmid \exp(G)$, $|G| = |G| 1_K \in K^\times$, $G \cong \text{Hom}(G, K^\times)$, and the map

$$\text{Hom}(G, K^\times) \times G \rightarrow K^\times, \quad (\chi, g) \mapsto \chi(g),$$

is a nondegenerate pairing (that is, if $\chi(g) = 1$ for all $\chi \in \widehat{G}$, then $g = 0$, and if $\chi(g) = 1$ for all $g \in G$, then clearly $\chi = 1$, the constant 1 function).

Furthermore, the orthogonality relations hold ([8, Proposition 5.5.2]), and for every $f \in K[G]$ we have (see [8, Proposition 5.5.2])

$$f = 0 \in K[G] \quad \text{if and only if} \quad \chi(f) = 0 \text{ for every } \chi \in \text{Hom}(G, K^\times).$$

Moreover, if $\chi(f) \neq 0$ for all $\chi \in \text{Hom}(G, K^\times)$, then $f \in K[G]^\times$; explicitly, a simple calculation using the orthogonality relations shows that

$$f^{-1} = \frac{1}{|G|} \sum_{g \in G} \left(\sum_{\chi \in \text{Hom}(G, K^\times)} \frac{\chi(-g)}{\chi(f)} \right) X^g.$$

For a subgroup $H \subset G$, we set

$$H^\perp = \{\chi \in \widehat{G} \mid \chi(h) = 1 \text{ for all } h \in H\}.$$

We clearly have a natural isomorphism $H^\perp \cong \widehat{G/H}$.

3. Proof of the Theorem. We fix our notation, which will remain valid throughout this section. Let $G = C_m \oplus C_{mn}$ with $m \in \mathbb{N}_{\geq 2}$, $n \in \mathbb{N}$ and let $e_1, e_2 \in G$ be such that $G = \langle e_1 \rangle \oplus \langle e_2 \rangle$, $\text{ord}(e_1) = m$ and $\text{ord}(e_2) = mn$. Furthermore, let K be a splitting field of G , $\zeta \in \mu_{mn}^*(K)$, and let $\psi, \varphi \in \widehat{G}$ be defined by $\psi(e_1) = \zeta^n$, $\psi(e_2) = 1$ and $\varphi(e_1) = 1$, $\varphi(e_2) = \zeta$. Then $\text{ord}(\psi) = m$, $\text{ord}(\varphi) = mn$ and $\widehat{G} = \langle \psi \rangle \oplus \langle \varphi \rangle$.

Note that, in the case $m = p \in \mathbb{P}$,

$$\theta: \mathbb{F}_p \times \langle \psi, \varphi^n \rangle \rightarrow \langle \psi, \varphi^n \rangle, \quad (k + p\mathbb{Z}, \chi) \mapsto \chi^k,$$

is an \mathbb{F}_p -vector space structure on $(\langle \psi, \varphi^n \rangle, \cdot)$. Whenever $\langle \psi, \varphi^n \rangle$ is considered as an \mathbb{F}_p -vector space it is with respect to θ .

Lemmas 3.1 and 3.2 below will allow us to restrict ourselves, in the proof of Theorem 1.1(i), to sequences consisting of certain special elements. Lemma 3.2 is a generalization of a statement used by W. Gao and Y. Li [6] in their proof of the case $m = 2$.

LEMMA 3.1. *Let R be a commutative ring, $g_1 \dots g_l \in \mathcal{F}(G)$ a sequence over G , and let $a_1, \dots, a_l \in R \setminus \{0\}$ be such that $(X^{g_1} - a_1) \dots (X^{g_l} - a_l) = 0 \in R[G]$. Then, for any $k_1, \dots, k_l \in \mathbb{N}$, also $(X^{k_1 g_1} - a_1^{k_1}) \dots (X^{k_l g_l} - a_l^{k_l}) = 0 \in R[G]$.*

Proof. For all $i \in [1, l]$,

$$X^{k_i g_i} - a_i^{k_i} = (X^{g_i} - a_i) \sum_{j=0}^{k_i-1} X^{j g_i} (a_i)^{k_i-1-j},$$

from which the lemma immediately follows. ■

LEMMA 3.2. *Let R be a commutative ring and*

$$G_0 = \{e_1\} \cup \left\{ ke_1 + \prod_{p \in \mathbb{P}, p|m} p^{u_p} e_2 \mid k \in [0, m-1], u_p \in \mathbb{N}_0 \right\}.$$

Let $M \in \mathbb{N}$ be such that, for every sequence $S = g_1 \dots g_{M+1} \in \mathcal{F}(G_0)$, there exist $a_1, \dots, a_{M+1} \in R \setminus \{0\}$ such that

$$f = (X^{g_1} - a_1) \dots (X^{g_{M+1}} - a_{M+1}) = 0 \in R[G].$$

Then $d(G, R) \leq M$.

Proof. By Lemma 3.1 and the definition of $d(G, R)$, it is sufficient to show that every element $g \in G$ is a multiple of an element in G_0 .

Let $g = ke_1 + le_2$ with $k \in [0, m-1]$ and $l \in [0, mn-1]$. If $l = 0$, then g is obviously a multiple of e_1 . Consider the case $l \neq 0$. Then $l = \prod_{p \in \mathbb{P}, p|m} p^{v_p(l)} \cdot q$ with $q \in [1, mn-1]$ and $\gcd(q, m) = 1$. Therefore there exists an $a \in [1, m-1]$ with $qa \equiv 1 \pmod m$. From $\text{ord}(e_1) = m$, it follows that $g = q(ake_1 + \prod_{p \in \mathbb{P}, p|m} p^{v_p(l)} e_2)$. Choosing $k' \in [0, m-1]$ such that $k' \equiv ak \pmod m$, we obtain $g = q(k'e_1 + \prod_{p \in \mathbb{P}, p|m} p^{v_p(l)} e_2)$, which is a multiple of an element in G_0 . ■

LEMMA 3.3. *Let $g \in G$ and $\chi, \chi' \in \widehat{G}$. Then $\chi'(g) = \chi(g)$ if and only if $\chi' \in \chi(g)^\perp$. Also*

- (i) $\langle ke_1 + e_2 \rangle^\perp = \langle \psi \varphi^{-nk} \rangle$ for $k \in [0, m-1]$;
- (ii) $\langle \varphi^n \rangle \subset \langle ke_1 + mle_2 \rangle^\perp$ for $k \in [0, m-1]$ and $l \in [0, n-1]$.

Proof. Clearly $\chi'(g) = \chi(g)$ if and only if $\chi^{-1}\chi'(g) = 1$, i.e., $\chi' \in \chi\langle g \rangle^\perp$.

(i) From $\psi^{-1}(ke_1 + e_2) = \zeta^{-nk} = \varphi^{-nk}(ke_1 + e_2)$, it follows that $\langle \psi\varphi^{-nk} \rangle \subset \langle ke_1 + e_2 \rangle^\perp$. Then $\text{ord}(ke_1 + e_2) = mn$ and $\langle ke_1 + e_2 \rangle^\perp \cong (G/\langle ke_1 + e_2 \rangle)^\wedge$ imply $|\langle ke_1 + e_2 \rangle^\perp| = m$, from which $\langle ke_1 + e_2 \rangle^\perp = \langle \psi\varphi^{-nk} \rangle$ follows.

(ii) Observe that $\varphi^n(ke_1 + mle_2) = \zeta^{nml} = (\zeta^{nm})^l = 1$ implies $\langle \varphi^n \rangle \subset \langle ke_1 + mle_2 \rangle^\perp$. ■

LEMMA 3.4. *Let $H \subset \widehat{G}$ and $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$. Then the following statements are equivalent:*

- (a) *There exist $a_1, \dots, a_l \in K^\times$ such that $\chi(\prod_{i=1}^l (X^{g_i} - a_i)) = 0$ for all $\chi \in H$.*
- (b) *There exist $s \in [0, l]$ and $\chi_1, \dots, \chi_s \in H$ such that $H \subset \bigcup_{i=1}^s \chi_i \langle g_i \rangle^\perp$.*
- (c) *$H = \emptyset$ or there exist $\chi_1, \dots, \chi_l \in H$ such that $H \subset \bigcup_{i=1}^l \chi_i \langle g_i \rangle^\perp$.*

Proof. For $H = \emptyset$ all statements are trivially true. Let $H \neq \emptyset$.

(a) \Rightarrow (b). The extension of $\chi \in \widehat{G}$ to $K[G]$ is a K -algebra homomorphism, and thus

$$\chi\left(\prod_{i=1}^l (X^{g_i} - a_i)\right) = 0$$

if and only if there is an $i \in [1, l]$ with $\chi(X^{g_i} - a_i) = 0$, i.e., $\chi(g_i) = a_i$. Let

$$s = |\{i \in [1, l] \mid \text{there exists a } \chi \in H \text{ such that } \chi(g_i) = a_i\}| \in [0, l].$$

Without restriction let g_1, \dots, g_s and a_1, \dots, a_s be such that there exist $\chi_i \in H$ with $\chi_i(g_i) = a_i$ for $i \in [1, s]$. Let $\chi \in H$. Then, by assumption, $\chi(g_i) = a_i$ for some $i \in [1, s]$. Therefore $\chi_i^{-1}\chi(g_i) = 1$, i.e. $\chi \in \chi_i \langle g_i \rangle^\perp$.

(b) \Rightarrow (a). Let $a_i = \chi_i(g_i)$ for $i \in [1, s]$ and let $a_{s+1} = \dots = a_l = 1$. Let $\chi \in H$. Then, by assumption, there exists an $i \in [1, s]$ such that $\chi \in \chi_i \langle g_i \rangle^\perp$, i.e., $\chi(g_i) = \chi_i(g_i) = a_i$. Hence $\chi(X^{g_i} - a_i) = 0$.

(b) \Leftrightarrow (c). Obvious. ■

Note that, in particular, $d(G, K)$ is the supremum of all $l \in \mathbb{N}_0$ such that there exists a sequence $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$ with

$$\bigcup_{i=1}^l \chi_i \langle g_i \rangle^\perp \subsetneq \widehat{G}$$

for any choice of $\chi_1, \dots, \chi_l \in \widehat{G}$. Or, equivalently, $d(G, K)+1$ is the minimum of all $l \in \mathbb{N}_0$ such that, for any sequence $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$, there exist $\chi_1, \dots, \chi_l \in \widehat{G}$ such that \widehat{G} can be covered as above:

$$\widehat{G} = \bigcup_{i=1}^l \chi_i \langle g_i \rangle^\perp.$$

Consider $m = p \in \mathbb{P}$. Our strategy to find an upper bound on $d(G, K)$ will be to subdivide \widehat{G} into cosets modulo $\langle \psi, \varphi^n \rangle$ and cover each of these cosets individually. Lemma 3.2 allows us to restrict ourselves to certain special elements $g \in G$, and from Lemma 3.3, we see that for these g , the $\langle g \rangle^\perp$ contain (or are) 1-dimensional subspaces, i.e., lines of the 2-dimensional \mathbb{F}_p -vector space $\langle \psi, \varphi^n \rangle$. Then, for $\chi \in \langle \psi, \varphi^n \rangle$, $\chi \langle g \rangle^\perp$ is an affine line in $\langle \psi, \varphi^n \rangle$ containing the “point” χ , and our task essentially boils down to covering n copies of $\langle \psi, \varphi^n \rangle$ by such lines (where the slopes are fixed by S).

Before doing so, we study some simple configurations in Lemmas 3.5 and 3.6. The main part of the proof for the cases $m \in \{2, 3\}$ then follows in Lemma 3.7. It is based on the proof by Gao and Li of the case $m = 2$, but is stated in terms of group characters instead of working with the group algebra directly.

LEMMA 3.5. *Let $s \in [0, m]$ and let $S = g_1 \cdots g_{s+(m-s)m} \in \mathcal{F}(G)$ be such that either $g_1 = \cdots = g_s = ke_1 + e_2$ with $k \in [0, m - 1]$ or $g_1, \dots, g_s \in \{ke_1 + mle_2 \mid k \in [0, m - 1], l \in \mathbb{N}_0\}$. Then there exist $\chi_1, \dots, \chi_{s+(m-s)m}$ such that $\langle \psi, \varphi^n \rangle \subset \bigcup_{i=1}^{s+(m-s)m} \chi_i \langle g_i \rangle^\perp$.*

Proof. Let $L = \langle \psi \varphi^{-nk} \rangle$ in the case $g_1 = \cdots = g_s = ke_1 + e_2$, and let $L = \langle \varphi^n \rangle$ otherwise. Since L is a subgroup of $\langle \psi, \varphi^n \rangle$ and has cardinality $|L| = m$, there exist $\tau_1, \dots, \tau_m \in \langle \psi, \varphi^n \rangle$ such that $\langle \psi, \varphi^n \rangle = \bigoplus_{i=1}^m \tau_i L$. By Lemma 3.3, $L \subset \langle g_i \rangle^\perp$ for $i \in [1, s]$. Then

$$\langle \psi, \varphi^n \rangle \subset \bigcup_{i=1}^s \tau_i \langle g_i \rangle^\perp \cup \bigoplus_{i=s+1}^m \tau_i L.$$

For $j \in [s + 1, s + (m - s)m]$, let $\chi'_j \in \langle g_j \rangle^\perp$, and let $L = \{\lambda_1, \dots, \lambda_m\}$. Then, for $i \in [s + 1, m]$,

$$\tau_i L = \{\tau_i \lambda_j \mid j \in [1, m]\} \subset \bigcup_{j=1}^m \tau_i \lambda_j \chi'_{s+(i-(s+1))m+j} \langle g_{s+(i-(s+1))m+j} \rangle^\perp. \blacksquare$$

LEMMA 3.6. *Let $m = p \in \mathbb{P}$, $g \in \{ke_1 + ple_2 \mid k \in [0, p - 1], l \in \mathbb{N}_0\}$ and $S = \prod_{i=0}^{p-1} (ie_1 + e_2)g$. Then $\langle \psi, \varphi^n \rangle \subset \bigcup_{i=0}^{p-1} \langle ie_1 + e_2 \rangle^\perp \cup \langle g \rangle^\perp$.*

Proof. By Lemma 3.3,

$$\bigcup_{i=0}^{p-1} \langle \psi \varphi^{-ni} \rangle \cup \langle \varphi^n \rangle \subset \bigcup_{i=0}^{p-1} \langle ie_1 + e_2 \rangle^\perp \cup \langle g \rangle^\perp.$$

Let $\psi^k \varphi^{nl} \in \langle \psi, \varphi^n \rangle$ with $k, l \in [0, p - 1]$. In the case $k = 0$, clearly $\varphi^{nl} \in \langle \varphi^n \rangle$. Otherwise, there exists an $i \in [0, p - 1]$ such that $-ik \equiv l \pmod p$. Hence $\psi^k \varphi^{nl} = (\psi \varphi^{-ni})^k \in \langle \psi \varphi^{-ni} \rangle$. \blacksquare

LEMMA 3.7. *Let $m = p \in \mathbb{P}$, $G_1 = \{e_1\} \cup \{ke_1 + p^u e_2 \mid k \in [0, p - 1], u \in \mathbb{N}\}$, and*

$$G_0 = \{e_1\} \cup \{ke_1 + p^u e_2 \mid k \in [0, p - 1], u \in \mathbb{N}_0\} \\ = \{ke_1 + e_2 \mid k \in [0, p - 1]\} \uplus G_1.$$

If, for all sequences $T = h_1 \cdot \dots \cdot h_{rp-1} \in \mathcal{F}(G_0)$ with $r \in [2, \min\{p - 1, n + 1\}]$ and $v_g(T) < p$ for all $g \in G_0$ as well as $\sum_{g \in G_1} v_g(T) < p$, there exist $\chi_1, \dots, \chi_{rp-1} \in \widehat{G}$ such that $\bigcup_{i=0}^{r-2} \varphi^i \langle \psi, \varphi^n \rangle \subset \bigcup_{i=1}^{r-1} \chi_i \langle h_i \rangle^\perp$, then $d(G, K) = d^(G)$.*

Proof. Since $d^*(G) \leq d(G) \leq d(G, K)$ always holds, it is sufficient to show that $d(G, K) \leq d^*(G) = (pn - 1) + (p - 1) = (n + 1)p - 2$. By Lemma 3.2, it is sufficient to show that, for any sequence $S = g_1 \cdot \dots \cdot g_{(n+1)p-1} \in \mathcal{F}(G_0)$, there exist $a_1, \dots, a_{(n+1)p-1} \in K^\times$ such that

$$f = \prod_{i=1}^{(n+1)p-1} (X^{g_i} - a_i) = 0 \in K[G].$$

To see this, we will use Lemma 3.4 to show that there exist $\chi_1, \dots, \chi_{(n+1)p-1}$ such that

$$\widehat{G} = \biguplus_{i=0}^{n-1} \varphi^i \langle \psi, \varphi^n \rangle \subset \bigcup_{i=1}^{(n+1)p-1} \chi_i \langle g_i \rangle^\perp.$$

We group the elements of S into as many p -tuples of the forms (e_2, \dots, e_2) , $(e_1 + e_2, \dots, e_1 + e_2)$, \dots , $((p - 1)e_1 + e_2, \dots, (p - 1)e_1 + e_2)$ and $(g'_1, \dots, g'_p) \in G_1^p$ as possible to obtain $l \in [0, n]$ such tuples. Without restriction, let these p -tuples be $(g_1, \dots, g_p), \dots, (g_{(l-1)p+1}, \dots, g_{lp})$.

For each $i \in [1, l]$, the tuple $(g_{(i-1)p+1}, \dots, g_{ip})$ fulfills the conditions of Lemma 3.5 with $s = p$. Therefore, there exist $\chi_{(i-1)p+1}, \dots, \chi_{ip}$ such that

$$\varphi^{n-i} \langle \psi, \varphi^n \rangle \subset \bigcup_{j=(i-1)p+1}^{ip} \chi_j \langle g_j \rangle^\perp.$$

It remains to show that $\chi_{lp+1}, \dots, \chi_{(n+1)p-1}$ can be chosen such that

$$\bigcup_{i=0}^{n-l-1} \varphi^i \langle \psi, \varphi^n \rangle \subset \bigcup_{j=lp+1}^{(n+1)p-1} \chi_j \langle g_j \rangle^\perp.$$

In the case $l \geq n$, this is trivially so, and hence we assume $l \leq n - 1$. We denote by $T = g_{lp+1} \cdot \dots \cdot g_{(n+1)p-1}$ the subsequence of S consisting of the remaining elements. We have $|T| = |S| - lp = (n + 1 - l)p - 1$. In the process of creating p -tuples, we partitioned the elements of G_0 into $p + 1$ different types. If there were at least p elements of one type, we could create another tuple, in contradiction to the maximal choice of l . Thus we must have $v_g(T) < p$

for all $g \in G_0$, $\sum_{g \in G_1} \nu_g(T) < p$, and $|T| \leq (p+1)(p-1) = p^2 - 1$, which implies $n+1-l \leq p$.

Altogether, we have $n+1-l \in [2, p]$. In the case $n+1-l \leq p-1$, we set $r = n+1-l \in [2, \min\{p-1, n+1\}]$. Then, by assumption, $\chi_{lp+1}, \dots, \chi_{(n+1)p-1}$ can be chosen such that

$$\bigcup_{i=0}^{r-2} \varphi^i \langle \psi, \varphi^n \rangle \subset \bigcup_{j=lp+1}^{(n+1)p-1} \chi_j \langle g_j \rangle^\perp.$$

Since $r-2 = n-l-1$, this already means $\widehat{G} \subset \bigcup_{i=1}^{(n+1)p-1} \chi_i \langle g_i \rangle^\perp$.

In the case $n+1-l = p$, we have $|T| = p^2 - 1 = (p+1)(p-1)$. This can only happen if each of the $p+1$ different types of elements occurs exactly $p-1$ times. Therefore

$$T = \prod_{j=0}^{p-1} (je_1 + e_2)^{p-1} \cdot \prod_{i=0}^{p-2} h_j = \prod_{i=0}^{p-2} \left(\prod_{j=0}^{p-1} (je_1 + e_2) \cdot h_i \right)$$

with $h_0, \dots, h_{p-2} \in G_1$. Without restriction, for $i \in [0, p-2]$, let $g_{lp+i(p+1)+1} \cdots g_{lp+i(p+1)+(p+1)} = \prod_{j=0}^{p-1} (je_1 + e_2) \cdot h_i$. For every $i \in [0, p-2]$, we set $\chi_{lp+i(p+1)+1} \cdots \chi_{lp+i(p+1)+(p+1)} = \varphi^i$. Then, from Lemma 3.6 it follows that $\varphi^i \langle \psi, \varphi^n \rangle \subset \bigcup_{j=i(p+1)+1}^{i(p+1)+(p+1)} \chi_{lp+j} \langle g_{lp+j} \rangle^\perp$. Since $n-l-1 = p-2$, this again implies $\widehat{G} \subset \bigcup_{i=1}^{(n+1)p-1} \chi_i \langle g_i \rangle^\perp$. ■

Proof of Theorem 1.1(i). For $p = 2$, i.e. $G = \mathbb{C}_2 \oplus \mathbb{C}_{2n}$, the conclusion follows trivially from Lemma 3.7, since there are no admissible sequences.

Consider $p = 3$, i.e., $G = \mathbb{C}_3 \oplus \mathbb{C}_{3n}$. Let $G_1 = \{e_1\} \cup \{ke_1 + 3^u e_2 \mid k \in [0, 2], u \in \mathbb{N}\}$ and $G_0 = \{e_2, e_1 + e_2, 2e_1 + e_2\} \uplus G_1$. Then, by Lemma 3.7, it is sufficient to show that, for $T = h_1 \cdots h_5 \in \mathcal{F}(G_0)$, we can choose $\chi_1, \dots, \chi_5 \in \widehat{G}$ such that $\langle \psi, \varphi^n \rangle \subset \chi_1 \langle h_1 \rangle^\perp \cup \dots \cup \chi_5 \langle h_5 \rangle^\perp$. We divide the elements into four types: e_2 , $e_1 + e_2$, $2e_1 + e_2$ and elements from G_1 . Since $|T| = 5$, one of these types must occur at least twice. Without restriction, let h_1 and h_2 be of the same type. Thus we have either $h_1 = h_2 = ke_1 + e_2$ for some $k \in [0, 2]$, or $h_1, h_2 \in G_1$. Then T fulfills the conditions of Lemma 3.5 with $s = 2$, and it follows that χ_1, \dots, χ_5 can be chosen such that $\langle \psi, \varphi^n \rangle \subset \bigcup_{i=1}^5 \chi_i \langle h_i \rangle^\perp$. ■

Lemma 3.8 below recapitulates a few simple facts, which are well known in the context of affine lines, and will be used extensively in the construction of a counterexample in the case $p \geq 5$ and $n \geq 2$.

LEMMA 3.8. *Let $m = p \in \mathbb{P}$, $g_1 = k_1 e_1 + e_2$, $g_2 = k_2 e_1 + e_2$ with $k_1, k_2 \in [0, p-1]$, $\chi \in \widehat{G}$ and $\chi_1, \chi_2 \in \chi \langle \psi, \varphi^n \rangle$.*

- (i) $\chi^{-1} \chi_i \langle g_i \rangle^\perp = \varphi^{ns_i} \langle g_i \rangle^\perp$ with $s_i \in [0, p-1]$ for $i \in \{1, 2\}$.

- (ii) $\chi^{-1}\chi_i\langle g_i \rangle^\perp = \{\psi^u\varphi^{nv} \mid u, v \in [0, p-1] \text{ with } k_iu + v \equiv s_i \pmod p\}$
for $i \in \{1, 2\}$.
- (iii) (a) $|\chi_1\langle g_1 \rangle^\perp \cap \chi_2\langle g_2 \rangle^\perp| = 1$ if and only if $g_1 \neq g_2$.
 (b) $|\chi_1\langle g_1 \rangle^\perp \cap \chi_2\langle g_2 \rangle^\perp| = 0$ if and only if $g_1 = g_2$ and $s_1 \neq s_2$.
 (c) $|\chi_1\langle g_1 \rangle^\perp \cap \chi_2\langle g_2 \rangle^\perp| = p$ if and only if $g_1 = g_2$ and $s_1 = s_2$.

Proof. (i) Let $i \in \{1, 2\}$ and $\chi^{-1}\chi_i = \psi^{u_i}\varphi^{nv_i}$ with $u_i, v_i \in [0, p-1]$. By Lemma 3.3(i), we have $\langle g_i \rangle^\perp = \langle \psi\varphi^{-nk_i} \rangle$. Therefore $\varphi^{-n(k_iu_i+v_i)}\chi^{-1}\chi_i = \psi^{u_i}\varphi^{-nk_iu_i} \in \langle g_i \rangle^\perp$, and hence $\chi^{-1}\chi_i\langle g_i \rangle^\perp = \varphi^{ns_i}\langle g_i \rangle^\perp$ with $s_i \in [0, p-1]$ chosen such that $s_i \equiv k_iu_i + v_i \pmod p$.

(ii) In view of Lemma 3.3(i) we have, for $u, v \in [0, p-1]$, $\psi^u\varphi^{nv} \in \chi^{-1}\chi_i\langle g_i \rangle^\perp = \varphi^{ns_i}\langle \psi\varphi^{-nk_i} \rangle$ if and only if $\psi^u\varphi^{nv} = \psi^w\varphi^{n(s_i-k_iw)}$ for some $w \in [0, p-1]$. This is the case if and only if $u \equiv w \pmod p$ and $v \equiv s_i - k_iw \pmod p$, i.e., if and only if $u \equiv w \pmod p$ and $k_iu + v \equiv s_i \pmod p$ (recall by Lemma 3.3(i) that $\langle g_i \rangle^\perp \subset \langle \psi, \varphi^n \rangle$).

(iii) By (ii), we have $\chi^{-1}\chi_1\langle g_1 \rangle^\perp \cap \chi^{-1}\chi_2\langle g_2 \rangle^\perp = \{\psi^u\varphi^{nv} \mid u, v \in [0, p-1] \text{ with } k_1u + v \equiv s_1 \pmod p \text{ and } k_2u + v \equiv s_2 \pmod p\}$. Since

$$|\chi^{-1}\chi_1\langle g_1 \rangle^\perp \cap \chi^{-1}\chi_2\langle g_2 \rangle^\perp| = |\chi_1\langle g_1 \rangle^\perp \cap \chi_2\langle g_2 \rangle^\perp|,$$

it is sufficient to consider the number of solutions of the linear system

$$k_1u + v \equiv s_1 \pmod p \quad \text{and} \quad k_2u + v \equiv s_2 \pmod p$$

for $u, v \in [0, p-1]$ over \mathbb{F}_p . In the case $g_1 \neq g_2$, i.e., $k_1 \neq k_2$, it possesses a unique solution. In the case $g_1 = g_2$, it has no solution for $s_1 \neq s_2$. For $s_1 = s_2$, the two equations coincide, and we obtain p solutions. ■

In the construction of the counterexamples, we use the same characterization of $d(G, K)$, derived from Lemma 3.4, as in the proof of Theorem 1.1(i)—except that now we show that it is not possible to cover \widehat{G} with such subsets. To do so, we first consider a special type of sequence in Lemma 3.9, which will turn out to be the only one which cannot be discarded with simpler combinatorial arguments, to be given in the proof of Theorem 1.1(ii) that follows the lemma.

LEMMA 3.9. *Let $m = p \in \mathbb{P}$, $p \geq 5$ and $k_1, k_2, k_3 \in [0, p-1]$ be distinct. Let $l \in [2, p-1]$,*

$$T = (k_1e_1 + e_2)^l(k_2e_1 + e_2)^l(k_3e_1 + e_2)^l \in \mathcal{F}(G),$$

and $\chi \in \widehat{G}$. For $i \in [1, 3]$ and $j \in [1, l]$, let $\chi_{i,j} \in \widehat{G}$. Then

$$\left| \left(\bigcup_{i=1}^3 \bigcup_{j=1}^l \chi_{i,j}\langle k_i e_1 + e_2 \rangle^\perp \right) \cap \chi\langle \psi, \varphi^n \rangle \right| < l(3p - 2l).$$

Proof. We set $g_i = k_i e_1 + e_2$ for $i \in [1, 3]$. Let $i \in [1, 3]$ and $j \in [1, l]$. We can assume $\chi_{i,j} \in \chi\langle \psi, \varphi^n \rangle$ as otherwise $\chi_{i,j}\langle g_i \rangle^\perp \cap \chi\langle \psi, \varphi^n \rangle = \emptyset$ (because

$\langle g_i \rangle^\perp = \langle \psi \varphi^{-nk_i} \rangle \subset \langle \psi, \varphi^n \rangle$. Using Lemma 3.8(i), we can furthermore assume $\chi^{-1} \chi_{i,j} = \varphi^{ns_{i,j}}$ with $s_{i,j} \in [0, p-1]$. We can then also assume $s_{i,j} \neq s_{i,j'}$ for $j' \in [1, l] \setminus \{j\}$, since otherwise $\chi_{i,j} \langle g_i \rangle^\perp = \chi_{i,j'} \langle g_i \rangle^\perp$.

For $i \in [1, 3]$, let $E_i = \bigcup_{j=1}^l \chi_{i,j} \langle g_i \rangle^\perp$. Then

$$\left(\bigcup_{i=1}^3 \bigcup_{j=1}^l \chi_{i,j} \langle g_i \rangle^\perp \right) \cap \chi \langle \psi, \varphi^n \rangle = E_1 \cup E_2 \cup E_3$$

and

$$|E_1 \cup E_2 \cup E_3| = \sum_{i=1}^3 |E_i| - \sum_{1 \leq i < i' \leq 3} |E_i \cap E_{i'}| + |E_1 \cap E_2 \cap E_3|.$$

For $i, i' \in [1, 3]$ distinct, we will show that $|E_i| = lp$, $|E_i \cap E_{i'}| = l^2$ and $|E_1 \cap E_2 \cap E_3| < l^2$. Then $|E_1 \cup E_2 \cup E_3| < 3lp - 3l^2 + l^2 = l(3p - 2l)$.

Let $i \in [1, 3]$. By Lemma 3.8(iii)(b), $\chi_{i,j} \langle g_i \rangle^\perp \cap \chi_{i,j'} \langle g_i \rangle^\perp = \emptyset$ for $j, j' \in [1, l]$ with $j \neq j'$, and $|\langle g_i \rangle^\perp| = |\langle \psi \varphi^{-nk_i} \rangle| = p$ (by Lemma 3.3(i)). Therefore $|E_i| = lp$.

Let $i, i' \in [1, 3]$ be distinct. For $j, j' \in [1, l]$ distinct, we have $\chi_{i,j} \langle g_i \rangle^\perp \cap \chi_{i,j'} \langle g_i \rangle^\perp = \emptyset$ and $\chi_{i',j} \langle g_{i'} \rangle^\perp \cap \chi_{i',j'} \langle g_{i'} \rangle^\perp = \emptyset$ (by Lemma 3.8(iii)(b)). This implies that in the formula

$$\begin{aligned} E_i \cap E_{i'} &= \left(\bigcup_{j=1}^l \chi_{i,j} \langle g_i \rangle^\perp \right) \cap \left(\bigcup_{j'=1}^l \chi_{i',j'} \langle g_{i'} \rangle^\perp \right) \\ &= \bigsqcup_{j=1}^l \bigsqcup_{j'=1}^l (\chi_{i,j} \langle g_i \rangle^\perp \cap \chi_{i',j'} \langle g_{i'} \rangle^\perp), \end{aligned}$$

the union is disjoint. By Lemma 3.8(iii)(a), $|\chi_{i,j} \langle g_i \rangle^\perp \cap \chi_{i',j'} \langle g_{i'} \rangle^\perp| = 1$ for $j, j' \in [1, l]$, and therefore $|E_i \cap E_{i'}| = l^2$.

Assume $|E_1 \cap E_2 \cap E_3| \geq l^2$. Then, since $|E_1 \cap E_2| = l^2$, it follows that $|E_1 \cap E_2 \cap E_3| = l^2$. For $a \in \mathbb{Z}$, let $\bar{a} = a + p\mathbb{Z} \in \mathbb{F}_p$. Let $u, v \in [0, p-1]$. By Lemma 3.8(ii), we have $\chi \psi^u \varphi^{nv} \in E_1 \cap E_2 \cap E_3$ if and only if there are $b_i \in \{s_{i,1}, \dots, s_{i,l}\}$, for $i \in [1, 3]$, such that

$$\bar{k}_1 \bar{u} + \bar{v} = \bar{b}_1, \quad \bar{k}_2 \bar{u} + \bar{v} = \bar{b}_2, \quad \bar{k}_3 \bar{u} + \bar{v} = \bar{b}_3.$$

Since \bar{k}_1, \bar{k}_2 and \bar{k}_3 are pairwise distinct, $(\bar{k}_1, \bar{1})$, $(\bar{k}_2, \bar{1})$ and $(\bar{k}_3, \bar{1})$ are pairwise \mathbb{F}_p -linearly independent. For $i \in [1, 3]$, define $\Phi_i : \chi \langle \psi, \varphi^n \rangle \rightarrow \mathbb{F}_p$ by $\Phi_i(\chi \psi^u \varphi^{nv}) = \bar{k}_i \bar{u} + \bar{v}$. Then the linear independence of $(\bar{k}_1, \bar{1})$ and $(\bar{k}_2, \bar{1})$ implies that $\Phi = (\Phi_1, \Phi_2) : \chi \langle \psi, \varphi^n \rangle \rightarrow \mathbb{F}_p^2$ is bijective. We have $\Phi(E_1 \cap E_2 \cap E_3) \subset \{\bar{s}_{1,1}, \dots, \bar{s}_{1,l}\} \times \{\bar{s}_{2,1}, \dots, \bar{s}_{2,l}\}$, and as $l^2 = |E_1 \cap E_2 \cap E_3| \leq |\{\bar{s}_{1,1}, \dots, \bar{s}_{1,l}\} \times \{\bar{s}_{2,1}, \dots, \bar{s}_{2,l}\}| = l^2$, equality holds. In particular, $\Phi_1(E_1 \cap E_2 \cap E_3) = \{\bar{s}_{1,1}, \dots, \bar{s}_{1,l}\}$ and $\Phi_2(E_1 \cap E_2 \cap E_3) = \{\bar{s}_{2,1}, \dots, \bar{s}_{2,l}\}$.

Because $(\bar{k}_1, \bar{1})$, $(\bar{k}_2, \bar{1})$ and $(\bar{k}_3, \bar{1})$ are pairwise \mathbb{F}_p -linearly independent, there exist $x, y \in \mathbb{F}_p^\times$ such that $(\bar{k}_3, \bar{1}) = x(\bar{k}_1, \bar{1}) + y(\bar{k}_2, \bar{1})$. Hence $\Phi_3 =$

$x\Phi_1 + y\Phi_2$. Now $|x\Phi_1(E_1 \cap E_2 \cap E_3)| = |y\Phi_2(E_1 \cap E_2 \cap E_3)| = l$. Also, since $x, y \neq 0$, we find (just as for Φ) that $(x\Phi_1, y\Phi_2) : \chi\langle\psi, \varphi^n\rangle \rightarrow \mathbb{F}_p^2$ is a bijective map. Thus, in view of $|x\Phi_1(E_1 \cap E_2 \cap E_3)| = |y\Phi_2(E_1 \cap E_2 \cap E_3)| = l$ and $|E_1 \cap E_2 \cap E_3| = l^2$, we see $(x\Phi_1, y\Phi_2)(E_1 \cap E_2 \cap E_3) = x\Phi_1(E_1 \cap E_2 \cap E_3) \times y\Phi_2(E_1 \cap E_2 \cap E_3)$. Therefore

$$\Phi_3(E_1 \cap E_2 \cap E_3) = x\Phi_1(E_1 \cap E_2 \cap E_3) + y\Phi_2(E_1 \cap E_2 \cap E_3),$$

where the inclusion “ \subset ” is obvious and “ \supset ” follows since for any $\alpha, \beta \in E_1 \cap E_2 \cap E_3$ we can find $\theta \in E_1 \cap E_2 \cap E_3$ such that $(x\Phi_1(\alpha), y\Phi_2(\beta)) = (x\Phi_1(\theta), y\Phi_2(\theta))$, and so in particular $x\Phi_1(\alpha) + y\Phi_2(\beta) = x\Phi_1(\theta) + y\Phi_2(\theta) = \Phi_3(\theta)$. From the Cauchy–Davenport Theorem (Lemma 2.1), it then follows that $|\Phi_3(E_1 \cap E_2 \cap E_3)| \geq \min\{2l - 1, p\} > l$, a contradiction, since $\Phi_3(E_1 \cap E_2 \cap E_3) \subset \{\overline{s_{3,1}}, \dots, \overline{s_{3,l}}\}$. ■

Proof of Theorem 1.1(ii). Consider $m = p \in \mathbb{P}_{\geq 5}$ and $n \geq 2$. Let $k_1, \dots, k_4 \in [0, p - 1]$ be pairwise distinct and set $g_i = k_i e_1 + e_2 \in G$ for $i \in [1, 4]$. Furthermore, set $m_1 = (n - 2)p + (p - 1)$, $m_2 = m_3 = p - 1$ and $m_4 = 2$. We consider the sequence

$$S = \prod_{i=1}^4 g_i^{m_i} \in \mathcal{F}(G)$$

and, for any choice of $\chi_{i,j} \in \widehat{G}$ for $i \in [1, 4]$ and $j \in [1, m_i]$, we will show that

$$\bigcup_{i=1}^4 \bigcup_{j=1}^{m_i} \chi_{i,j} \langle g_i \rangle^\perp \subsetneq \widehat{G}.$$

Then, by Lemma 3.4 and the definition of $d(G, K)$,

$$d(G, K) \geq |S| = p + pn - 1 > p + pn - 2 = d^*(G).$$

Let $\chi_{i,j} \in \widehat{G}$ for $i \in [1, 4]$ and $j \in [1, m_i]$ be arbitrary. Assume, to the contrary, $\bigcup_{i=1}^4 \bigcup_{j=1}^{m_i} \chi_{i,j} \langle g_i \rangle^\perp = \widehat{G}$. For $i \in [1, 4]$ and $j, j' \in [1, m_i]$ distinct, we can assume $\chi_{i,j} \langle g_i \rangle^\perp \neq \chi_{i,j'} \langle g_i \rangle^\perp$.

For any permutation $\sigma \in \mathfrak{S}_n$ (which will be fixed later),

$$\widehat{G} = \bigoplus_{\nu=1}^n \varphi^{\sigma(\nu)} \langle \psi, \varphi^n \rangle.$$

For given $i \in [1, 4]$ and $j \in [1, m_i]$, Lemma 3.3 yields $\chi_{i,j} \langle g_i \rangle^\perp \subset \varphi^{\sigma(\nu)} \langle \psi, \varphi^n \rangle$ for a unique $\nu \in [1, n]$. For $i \in [1, 4]$ and $\nu \in [1, n]$, we can therefore define

$$B_i^{(\nu)} = \{\chi_{i,j} \mid j \in [1, m_i] \text{ with } \chi_{i,j} \langle g_i \rangle^\perp \subset \varphi^{\sigma(\nu)} \langle \psi, \varphi^n \rangle\}.$$

We also define $n^{(\nu)} = \max\{|B_i^{(\nu)}| \mid i \in [1, 4]\}$ as well as $l^{(\nu)} = \sum_{i=1}^4 |B_i^{(\nu)}|$, for $\nu \in [1, n]$.

Let $\nu \in [1, n]$. By assumption,

$$\varphi^{\sigma(\nu)} \langle \psi, \varphi^n \rangle = \bigcup_{i=1}^4 \bigcup_{\chi \in B_i^{(\nu)}} \chi \langle g_i \rangle^\perp.$$

Thus, since $|\langle \psi, \varphi^n \rangle| = p^2$ and $|\langle g_i \rangle^\perp| = p$ for all $i \in [1, 4]$, we have $l^{(\nu)} \geq p$. On the other hand, $n^{(\nu)} \leq p$ because otherwise there would exist $i \in [1, 4]$ and $j, j' \in [1, m_i]$ distinct such that $\chi_{i,j} \langle g_i \rangle^\perp \cap \chi_{i,j'} \langle g_i \rangle^\perp \neq \emptyset$; but this would already imply $\chi_{i,j} \langle g_i \rangle^\perp = \chi_{i,j'} \langle g_i \rangle^\perp$, contrary to assumption.

Fix $\sigma \in \mathfrak{S}_n$ so that there is a $k \in \mathbb{N}_0$ such that $n^{(1)}, \dots, n^{(k)} < p$ and $n^{(k+1)} = \dots = n^{(n)} = p$. Since $m_i < p$ for $i \geq 2$, we see (for $\nu \in [1, n]$) that $n^{(\nu)} = p$ is only possible if $|B_1^{(\nu)}| = p$. As $m_1 = (n - 2)p + (p - 1)$, this is possible for at most $n - 2$ different $\nu \in [1, n]$. Thus $k \geq 2$.

We can also estimate $|\bigcup_{i=1}^4 \bigcup_{\chi \in B_i^{(\nu)}} \chi \langle g_i \rangle^\perp|$ in a different way: Assume for the purpose of showing (1) below that $n^{(\nu)} = |B_1^{(\nu)}| \geq |B_2^{(\nu)}| \geq |B_3^{(\nu)}| \geq |B_4^{(\nu)}|$ (the other cases are handled identically). Each of the characters $\chi \in B_1^{(\nu)}$ contributes $\chi \langle g_1 \rangle^\perp$, and therefore exactly p characters, to the union. Each of the characters $\chi \in B_2^{(\nu)}$ contributes at most $p - |B_1^{(\nu)}|$ characters, since $|\chi_1 \langle g_1 \rangle^\perp \cap \chi \langle g_2 \rangle^\perp| = 1$ for all $\chi_1 \in B_1^{(\nu)}$. Similarly, each of the characters $\chi \in B_3^{(\nu)}$ contributes at most $p - \max\{|B_1^{(\nu)}|, |B_2^{(\nu)}|\}$ = $p - |B_1^{(\nu)}|$ characters, since $|\chi_1 \langle g_1 \rangle^\perp \cap \chi \langle g_3 \rangle^\perp| = 1$ for all $\chi_1 \in B_1^{(\nu)}$ and $|\chi_2 \langle g_2 \rangle^\perp \cap \chi \langle g_3 \rangle^\perp| = 1$ for all $\chi_2 \in B_2^{(\nu)}$. Continuing this thought for $B_4^{(\nu)}$, we obtain

$$\begin{aligned} p^2 &= \left| \bigcup_{i=1}^4 \bigcup_{\chi \in B_i^{(\nu)}} \chi \langle g_i \rangle^\perp \right| \leq p|B_1^{(\nu)}| + (p - |B_1^{(\nu)}|) \sum_{i=2}^4 |B_i^{(\nu)}| \\ &= pn^{(\nu)} + (p - n^{(\nu)})(l^{(\nu)} - n^{(\nu)}). \end{aligned}$$

Therefore

$$(1) \quad (n^{(\nu)} - (l^{(\nu)} - p))(n^{(\nu)} - p) = pn^{(\nu)} + (p - n^{(\nu)})(l^{(\nu)} - n^{(\nu)}) - p^2 \geq 0.$$

Thus either $n^{(\nu)} \geq p$ (and therefore already $n^{(\nu)} = p$), or $n^{(\nu)} \leq l^{(\nu)} - p$.

For $\nu \in [1, k]$, we obtain $n^{(\nu)} \leq l^{(\nu)} - p$. Since $|B_4^{(\nu)}| \leq m_4 = 2$, we also have $l^{(\nu)} = \sum_{i=1}^4 |B_i^{(\nu)}| \leq 3n^{(\nu)} + 2$. Then

$$3l^{(\nu)} \geq 3n^{(\nu)} + 3p = 3n^{(\nu)} + 2 + 3p - 2 \geq l^{(\nu)} + 3p - 2,$$

and hence $l^{(\nu)} \geq \frac{3}{2}p - 1$ for all $\nu \in [1, k]$. Because of $\sum_{i=1}^n l^{(\nu)} = |S| = pn + (p - 1)$ and $l^{(\nu)} \geq n^{(\nu)} = p$ for all $\nu \in [k + 1, n]$, we have $l^{(1)} + \dots + l^{(k)} \leq pk + (p - 1)$. For the remainder of the argument, we assume $\nu \in [1, k]$.

Then, by the above, $\sum_{i=1, i \neq \nu}^k l^{(\nu)} \geq (k-1)(\frac{3}{2}p-1)$, and hence

$$(2) \quad (k-1)(\frac{3}{2}p-1) + l^{(\nu)} \leq pk + (p-1),$$

which implies

$$\begin{aligned} l^{(\nu)} &\leq pk + (p-1) - (k-1)(\frac{3}{2}p-1) = pk + p - 1 - \frac{3}{2}kp + k + \frac{3}{2}p - 1 \\ &= \frac{3}{2}p + (p-2) - \frac{1}{2}k(p-2). \end{aligned}$$

Hence, as $k \geq 2$, it follows that $l^{(\nu)} \leq \lfloor \frac{3}{2}p \rfloor$ ⁽¹⁾. Together with $l^{(\nu)} \geq \lceil \frac{3}{2}p - 1 \rceil$, this implies $l^{(\nu)} = \frac{3}{2}p - \frac{1}{2}$.

Since $|B_4^{(1)}| + \dots + |B_4^{(k)}| \leq m_4 = 2$ and $k \geq 2$, there exists a $\nu \in [1, k]$ with $|B_4^{(\nu)}| \leq 1$. Then

$$|B_1^{(\nu)}|, \dots, |B_3^{(\nu)}| \leq n^{(\nu)} \leq l^{(\nu)} - p = \frac{1}{2}(p-1),$$

$|B_4^{(\nu)}| \leq 1$ and $\sum_{i=1}^4 |B_i^{(\nu)}| = l^{(\nu)} = \frac{3}{2}(p-1) + 1$. Therefore we must have

$$|B_1^{(\nu)}| = |B_2^{(\nu)}| = |B_3^{(\nu)}| = n^{(\nu)} = \frac{1}{2}(p-1)$$

and $|B_4^{(\nu)}| = 1$.

With the help of Lemma 3.9, we now show that this leads to a contradiction. Consider $T = g_1^{\frac{1}{2}(p-1)} g_2^{\frac{1}{2}(p-1)} g_3^{\frac{1}{2}(p-1)} \in \mathcal{F}(G)$. Then, by Lemma 3.9 (with $l = \frac{1}{2}(p-1)$ and $\chi = \varphi^{\sigma^{(\nu)}}$),

$$\left| \bigcup_{i=1}^3 \bigcup_{\chi' \in B_i^{(\nu)}} \chi' \langle g_i \rangle^\perp \right| < \frac{1}{2}(p-1)(2p+1).$$

Thus, with $B_4^{(\nu)} = \{\tau\}$,

$$\begin{aligned} p^2 &= \left| \left(\bigcup_{i=1}^3 \bigcup_{\chi' \in B_i^{(\nu)}} \chi' \langle g_i \rangle^\perp \right) \cup \tau \langle g_4 \rangle^\perp \right| \leq \left| \bigcup_{i=1}^3 \bigcup_{\chi' \in B_i^{(\nu)}} \chi' \langle g_i \rangle^\perp \right| + (p - n^{(\nu)}) \\ &< \frac{1}{2}(p-1)(2p+1) + \frac{1}{2}(p+1) = p^2, \end{aligned}$$

a contradiction. ■

Acknowledgements. I am indebted to Alfred Geroldinger for his constant feedback and help during the writing of this paper. I would also like to thank David Gryniewicz and Günter Lettl for their comments on preliminary versions. In particular, G. Lettl suggested the use of the Cauchy–Davenport Theorem in Lemma 3.9, which significantly shortened the proof.

⁽¹⁾ Alternatively (2), together with $l^{(\nu)} \geq \frac{3}{2}p - 1$, $p \geq 5$ and $k \leq 2$, already implies $k = 2$, which yields the same estimate for $l^{(\nu)}$.

This work was supported by the Austrian Science Fund FWF, Doctoral Program C75-N13 Discrete Mathematics.

REFERENCES

- [1] G. Bhowmik and J.-C. Schlage-Puchta, *Davenport's constant for groups of the form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$* , in: Additive Combinatorics, A. Granville et al. (eds.), CRM Proc. Lecture Notes 43, Amer. Math. Soc., 2007, 307–326.
- [2] C. W. Curtis and I. Reiner, *Methods of Representation Theory, Volume I*, Wiley, 1981.
- [3] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. 24 (2006), 337–369.
- [4] W. Gao, A. Geroldinger and D. J. Grynkiewicz, *Inverse zero-sum problems III*, Acta Arith. 141 (2010), 103–152.
- [5] W. Gao, A. Geroldinger and F. Halter-Koch, *Group algebras of finite abelian groups and their applications to combinatorial problems*, Rocky Mountain J. Math. 39 (2009), 805–823.
- [6] W. Gao and Y. Li, *Remarks on group rings and the Davenport constant*, Ars Combin., to appear.
- [7] A. Geroldinger, *Additive group theory and non-unique factorizations*, in: Combinatorial Number Theory and Additive Group Theory, A. Geroldinger and I. Ruzsa (eds.), Adv. Courses in Math. CRM Barcelona, Birkhäuser, 2009, 1–86.
- [8] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, 2006.
- [9] A. Geroldinger, M. Liebmann and A. Philipp, *On the Davenport constant and on the structure of extremal zero-sum free sequences*, Period. Math. Hungar., to appear.
- [10] B. Girard, *Inverse zero-sum problems in finite Abelian p -groups*, Colloq. Math. 120 (2010), 7–21.
- [11] —, *A new upper bound for the cross number of finite abelian groups*, Israel J. Math. 172 (2009), 253–278.
- [12] G. Lettl and W. A. Schmid, *Minimal zero-sum sequences in $C_n \oplus C_n$* , Eur. J. Combin. 28 (2007), 742–753.
- [13] P. Rath, K. Srilakshmi and R. Thangadurai, *On Davenport's constant*, Int. J. Number Theory 4 (2008), 107–115.
- [14] W. A. Schmid, *Inverse zero-sum problems II*, Acta Arith. 143 (2010), 333–343.
- [15] Z. W. Sun, *Zero-sum problems for abelian p -groups and covers of the integers by residue classes*, Israel J. Math. 170 (2009), 235–252.

Daniel Smertnig
Institut für Mathematik und Wissenschaftliches Rechnen
Karl-Franzens-Universität Graz
Heinrichstraße 36
8010 Graz, Austria
E-mail: 06smertn@edu.uni-graz.at