International Journal of Number Theory
Vol. 7, No. 6 (2011) 1463–1502

DOI: 10.1142/S1793042111004721

A QUANTITATIVE ASPECT OF NON-UNIQUE FACTORIZATIONS: THE NARKIEWICZ CONSTANTS

WEIDONG GAO*,‡, ALFRED GEROLDINGER†,§
and QINGHONG WANG*,¶

*Center for Combinatorics, LPMC-TJKLC
Nankai University, Tianjin 300071, P. R. China

†Institut für Mathematik und Wissenschaftliches Rechnen
Karl–Franzens–Universität Graz
Heinrichstrasse 36, 8010 Graz, Austria
‡wdgao_1963@yahoo.com.cn
§alfred.geroldinger@uni-graz.at
¶wqh1208@yahoo.com.cn

Received 21 July 2010
Accepted 8 December 2010

Let K be an algebraic number field with non-trivial class group G and let $\mathcal{O}_K$ be its ring of integers. For $k \in \mathbb{N}$ and some real $x \geq 1$, let $F_k(x)$ denote the number of non-zero principal ideals $a\mathcal{O}_K$ with norm bounded by x such that a has at most k distinct factorizations into irreducible elements. It is well known that $F_k(x)$ behaves, for $x \to \infty$, asymptotically like $x(\log x)^{-1+1/|G|}(\log\log x)^{\mathsf{N}_k(G)}$. We study $\mathsf{N}_k(G)$ with new methods from Combinatorial Number Theory.

Keywords: Non-unique factorizations; Narkiewicz constants; zero-sum sequence; Erdős–Ginzburg–Ziv constant.

Mathematical Subject Classification 2010: 11R27, 11B30, 11P70, 20K01

1. Introduction

Le K be an algebraic number field, $\mathcal{O}_K$ be its ring of integers and G be its ideal class group. For a non-zero element $a \in \mathcal{O}_K$, let $\mathsf{Z}(a)$ denote the set of all (essentially distinct) factorizations of a into irreducible elements. Then $\mathcal{O}_K$ is factorial (in other words, $|\mathsf{Z}(a)| = 1$ for all non-zero $a \in \mathcal{O}_K$) if and only if $|G| = 1$. Suppose that $|G| \geq 2$ and let $k \in \mathbb{N}$. Inspired by a paper of Fogels [4] and a question of Turán, Narkiewicz initiated in the 1960s the systematic study of the asymptotic behavior of counting functions associated with non-unique factorizations (for an overview and historical references, see [14, 31]). Among others, the function

$$F_k(x) = |\{a\mathcal{O}_K \mid a \in \mathcal{O}_K\backslash\{0\},\ (\mathcal{O}_K : a\mathcal{O}_K) \leq x \text{ and } |\mathsf{Z}(a)| \leq k\}|$$

was considered. It counts the number of principal ideals $a\mathcal{O}_K$ where $0 \neq a \in \mathcal{O}_K$ has at most k distinct factorizations and whose norm is bounded by x. After a first paper in 1964, Narkiewicz proved in 1972 (see [28, 29]) that $F_k(x)$ behaves, for $x \to \infty$, asymptotically like

$$x(\log x)^{-1+1/|G|}(\log\log x)^{\mathsf{N}_k} \quad \text{for some } \mathsf{N}_k > 0.$$

This result was refined and extended in several ways: the asymptotics were sharpened in [21], while the function field case was handled in [19], Chebotarev formations in [16] and non-principal orders in global fields in [15]. For more and recent development, see [12, 14, Sec. 9.3; 22–25, 34]. In [30, 32], Narkiewicz and Śliwa showed that the exponents N_k depend only on the class group G, and they gave a combinatorial description of this constant $\mathsf{N}_k(G)$ (see Definition 2.1). This description was used by Gao for the first detailed investigation of $\mathsf{N}_k(G)$ in [5]. We continue these investigations of $\mathsf{N}_k(G)$ with new methods from Combinatorial Number Theory. Before going into details, we briefly outline how these investigations are embedded into the more general study of the arithmetic of $\mathcal{O}_K$.

Suppose that $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \cdots \mid n_r$. Since $|G| \geq 2$, $\mathcal{O}_K$ is not factorial. The non-uniqueness of factorizations in $\mathcal{O}_K$ is described by a variety of arithmetical invariants — such as sets of lengths or the catenary degree — and they depend only on the class group G (the same is true not only for rings of integers but more generally for Krull monoids with finite class group where every class contains a prime divisor). Thus the goal is to determine their precise values in terms of the group invariants $n_1, \ldots, n_r$, or to describe them in terms of classical combinatorial invariants, such as the Davenport constant or the Erdős–Ginzburg–Ziv constant. Roughly speaking, a good understanding of these combinatorial invariants is restricted to groups of rank at most two, and thus no more can be expected for the more sophisticated arithmetical invariants.

Back to the Narkiewicz constants. A straightforward example shows that $\mathsf{N}_1(G) \geq n_1 + \cdots + n_r$ (see inequality (2.2)), and in 1982, Narkiewicz and Śliwa stated the conjecture that the equality holds. Since, on the other hand, the Davenport constant $\mathsf{D}(G)$ is a lower bound for $\mathsf{N}_1(G)$ (see inequality (2.1)), the Narkiewicz–Śliwa Conjecture, if true, would provide an upper bound for the Davenport constant which is substantially stronger than all bounds known so far. Thus it is not surprising that up to now this conjecture has been validated only for a few classes of groups including cyclic groups, elementary 2-groups and elementary 3-groups (see [14, Theorem 6.2.8]). A main part of this paper deals with the study of $\mathsf{N}_1(G)$ for groups of rank two. A key strategy in Combinatorial Number Theory for such investigations divides the problem into the following two steps.

Step A. Determine the precise value for the invariant under investigation for groups of the form $C_p \oplus C_p$, where p is a prime.

Step B. Show that the problem is "multiplicative", in the sense that the precise value for the invariant can be lifted from groups of the above form to arbitrary groups of rank two.

This procedure is applied successfully in a variety of investigations — as, for example, in the study of the Davenport constant and of the Erdős–Ginzburg–Ziv constant in groups of rank two — and both steps usually require essentially different methods. In the present paper, we perform Step B for the Narkiewicz constant $\mathsf{N}_1(G)$ (indeed, we do more; see the discussions before Theorem 3.15 and after Theorem 4.1). For that purpose, we introduce a new combinatorial invariant, $\eta^*(G)$, which is of a similar type as the Erdős–Ginzburg–Ziv constant (see Sec. 3). In the final section, we study the Narkiewicz constants $\mathsf{N}_k(G)$ for higher values of k in the context of cyclic groups and of elementary 2-groups (see Theorems 5.1 and 5.3). Our investigations are based on the recent characterization of the structure of minimal zero-sum sequences of maximal length over groups of rank two (see [7, 35, 38]) and on a recent result on the structure of long zero-sum free sequences over cyclic groups (see Lemmas 3.7 and 5.2).

2. Preliminaries

We denote by $\mathbb{N}$ the set of positive integers, by $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers, and we set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$. By a *monoid*, we always mean a commutative semigroup with identity which satisfies the cancelation law (that is, if a, b, c are elements of the monoid with $ab = ac$, then $b = c$ follows).

Let H be a monoid and $a, b \in H$. We denote by $\mathcal{A}(H)$ the set of atoms (irreducible elements) of H and by $H^\times$ the set of invertible elements of H. The monoid H is said to be *reduced* if $H^\times = \{1\}$. Let $H_{\mathrm{red}} = H/H^\times = \{aH^\times \mid a \in H\}$ be the associated reduced monoid.

A monoid F is called *free* (*with basis* $P \subset F$) if every $a \in F$ has a unique representation of the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)} \quad \text{with } \mathsf{v}_p(a) \in \mathbb{N}_0 \quad \text{and} \quad \mathsf{v}_p(a) = 0 \quad \text{for almost all } p \in P.$$

We set $F = \mathcal{F}(P)$ and call

$$|a| = \sum_{p \in P} \mathsf{v}_p(a) \quad (\text{the } \textit{length} \text{ of } a) \quad \text{and} \quad \mathrm{supp}(a) = \{p \in P \mid \mathsf{v}_p(a) > 0\} \quad (\text{the } \textit{support} \text{ of } a).$$

The monoid $\mathsf{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\mathrm{red}}))$ is the *factorization monoid* of H and $\pi\colon \mathsf{Z}(H) \to H_{\mathrm{red}}$ denotes the natural homomorphism given by mapping a factorization to the element it factorizes. Then the set $\mathsf{Z}(a) = \pi^{-1}(aH^\times) \subset \mathsf{Z}(H)$ is called the *set of factorizations* of a, and we say that a has *unique factorization* if $|\mathsf{Z}(a)| = 1$. The set $\mathsf{L}(a) = \{|z| \mid z \in \mathsf{Z}(a)\} \subset \mathbb{N}_0$ is called the *set of lengths* of a.

All abelian groups will be written additively. For $n \in \mathbb{N}$, let C_n denote a cyclic group with n elements. Let G be an abelian group and $G_0 \subset G$ be a subset. Then $\langle G_0 \rangle \subset G$ is the subgroup generated by G_0, $G_0^\bullet = G_0 \setminus \{0\}$, and

$-G_0 = \{-g \mid g \in G_0\}$. A family $(e_i)_{i \in I}$ of non-zero elements of G is said to be *independent* if

$$\sum_{i \in I} m_i e_i = 0 \quad \text{implies } m_i e_i = 0 \text{ for all } \ i \in I, \text{ where } \ m_i \in \mathbb{Z}.$$

If $I = [1, r]$ and $(e_1, \ldots, e_r)$ is independent, then we simply say that $e_1, \ldots, e_r$ are independent elements of G. The tuple $(e_i)_{i \in I}$ is called a *basis* if $(e_i)_{i \in I}$ is independent and $\langle \{e_i \mid i \in I\} \rangle = G$. If $1 < |G| < \infty$, then we have

$$G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}, \quad \text{and we set } \mathsf{d}^*(G) = \sum_{i=1}^{r} (n_i - 1),$$

where $r = \mathsf{r}(G) \in \mathbb{N}$ is the *rank* of G, $n_1, \ldots, n_r \in \mathbb{N}$ are integers with $1 < n_1 \mid \cdots \mid n_r$ and $n_r = \exp(G)$ is the exponent of G. If $|G| = 1$, then $\mathsf{r}(G) = 0$, $\exp(G) = 1$, and $\mathsf{d}^*(G) = 0$.

The multiplicative monoid of non-zero elements in a ring of integers (more generally, in an arbitrary Dedekind or Krull domain) is a Krull monoid. The arithmetic of Krull monoids is studied by using two classes of auxiliary monoids: the monoid of zero-sum sequences and the monoid of zero-sum types (see [14, Secs. 3.4 and 3.5] or [13]). We need both concepts for our investigations.

Monoid of zero-sum sequences. The elements of the free monoid $\mathcal{F}(G_0)$ are called *sequences* over G_0. Let

$$S = \prod_{g \in G_0} g^{\mathsf{v}_g(S)}, \quad \text{where } \ \mathsf{v}_g(S) \in \mathbb{N}_0 \text{ for all } g \in G_0 \text{ and}$$

$$\mathsf{v}_g(S) = 0 \quad \text{for almost all } g \in G_0,$$

be a sequence over G_0. We call $\mathsf{v}_g(S)$ the *multiplicity* of g in S, and we say that S *contains* g if $\mathsf{v}_g(S) > 0$. A sequence S_1 is called a *subsequence* of S if $S_1 \mid S$ in $\mathcal{F}(G)$ (equivalently, $\mathsf{v}_g(S_1) \le \mathsf{v}_g(S)$ for all $g \in G$). If a sequence $S \in \mathcal{F}(G_0)$ is written in the form $S = g_1 \cdot \ldots \cdot g_l$, we tacitly assume that $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G$. For a sequence

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0),$$

we call $\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G_0} \mathsf{v}_g(S) g \in G$ the *sum* of S, and $\Sigma(S) = \{\sum_{i \in I} g_i \mid \emptyset \ne I \subset [1, l]\}$ the *set of subsums* of S. For $g \in G$, we set $g + S = (g + g_1) \cdot \ldots \cdot (g + g_l) \in \mathcal{F}(G)$. The sequence S is called

- a *zero-sum sequence* if $\sigma(S) = 0$,
- *short* (in G) if $1 \le |S| \le \exp(G)$,
- *zero-sum free* if there is no non-empty zero-sum subsequence,
- a *minimal zero-sum sequence* if S is a non-empty zero-sum sequence and every subsequence S' of S with $1 \le |S'| < |S|$ is zero-sum free.

By definition, the empty sequence $1 \in \mathcal{F}(G)$ is both zero-sum free and a zero-sum sequence of length $|1| = 0$. We denote by $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\}$ the *monoid of zero-sum sequences* over G_0, by $\mathcal{A}(G_0)$ the set of all minimal zero-sum sequences over G_0 (this is the set of atoms of the monoid $\mathcal{B}(G_0)$), and by

$$\mathsf{D}(G_0) = \sup\{|U| \mid U \in \mathcal{A}(G_0)\} \in \mathbb{N} \cup \{\infty\}$$

the *Davenport constant* of G_0.

Monoid of zero-sum types. The elements of the free monoid $\mathcal{F}(G_0 \times \mathbb{N})$ are called *types* over G_0. Clearly, they are sequences over $G_0 \times \mathbb{N}$, but we think of them as labeled sequences over G_0 where each element from G_0 carries a label from the positive integers. Let $\boldsymbol{\alpha} \colon \mathcal{F}(G_0 \times \mathbb{N}) \to \mathcal{F}(G_0)$ denote the unique homomorphism (called the *unlabeling homomorphism*) satisfying

$$\boldsymbol{\alpha}((g,n)) = g \quad \text{for all } (g,n) \in G_0 \times \mathbb{N},$$

and let $\overline{\sigma} = \sigma \circ \boldsymbol{\alpha} \colon \mathcal{F}(G_0 \times \mathbb{N}) \to G$. For a type $T \in \mathcal{F}(G_0 \times \mathbb{N})$, note that $\boldsymbol{\alpha}(T) \in \mathcal{F}(G_0)$ is the associated (unlabeled) sequence. A type T_1 is called a *subtype* of T if $T_1 \mid T$ in $\mathcal{F}(G_0 \times \mathbb{N})$. We say that T is a *zero-sum type* (*short*, *zero-sum free* or a *minimal zero-sum type*) if the associated sequence has the relevant property, and we set $\Sigma(T) = \Sigma(\boldsymbol{\alpha}(T))$. We denote by

$$\mathcal{T}(G_0) = \{T \in \mathcal{F}(G_0 \times \mathbb{N}) \mid \overline{\sigma}(T) = 0\} = \boldsymbol{\alpha}^{-1}\big(\mathcal{B}(G_0)\big) \subset \mathcal{F}(G_0 \times \mathbb{N})$$

the *monoid of zero-sum types* over G_0 (briefly, the *type monoid* over G_0). Type monoids were introduced by Halter-Koch in [18] and applied successfully in the analytic theory of so-called type-dependent factorization properties (see [14, Sec. 9.1], and [16, 17] for some early papers).

Let G_1 be an abelian group. Every map $\varphi: G_0 \to G_1$ extends to a unique homomorphism $\varphi \colon \mathcal{F}(G_0) \to \mathcal{F}(G_1)$ extending φ, and there is a unique homomorphism $\varphi \colon \mathcal{F}(G_0 \times \mathbb{N}) \to \mathcal{F}(G_1 \times \mathbb{N})$ satisfying $\varphi((g,n)) = (\varphi(g), n)$ for all $(g,n) \in G_0 \times \mathbb{N}$. Suppose that $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G_0)$. Then, obviously, $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$, and if φ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \mathrm{Ker}(\varphi)$. We denote by $\overline{\varphi} = \varphi \circ \boldsymbol{\alpha} : \mathcal{F}(G_0 \times \mathbb{N}) \to \mathcal{F}(G_1)$ the unique homomorphism satisfying $\varphi((g,n)) = \varphi(g)$ for all $(g,n) \in G_0 \times \mathbb{N}$. For the sum function $\sigma \colon \mathcal{F}(G_0) \to G$, we have $\overline{\sigma} \circ \varphi = \sigma \circ \overline{\varphi} = \varphi \circ \overline{\sigma} : \mathcal{F}(G_0 \times \mathbb{N}) \to G_1$.

The greatest common divisor of sequences $S, S' \in \mathcal{F}(G_0)$ will always be taken in the monoid $\mathcal{F}(G_0)$, and the sequences will be called coprime if $\gcd(S, S') = 1$. The greatest common divisor of types $T, T' \in \mathcal{F}(G_0 \times \mathbb{N})$ will always be taken in the monoid $\mathcal{F}(G_0 \times \mathbb{N})$, and the types will be called coprime if $\gcd(T, T') = 1$.

Let $\tau \colon \mathcal{F}(G_0) \to \mathcal{F}(G_0 \times \mathbb{N})$ be defined by

$$\tau(S) = \prod_{g \in G_0} \prod_{k=1}^{\mathsf{v}_g(S)} (g,k) \in \mathcal{F}(G_0 \times \mathbb{N}).$$

Thus τ is a *labeling function*, and for $S \in \mathcal{F}(G_0)$, we call $\tau(S)$ the *type associated with* S. The map $\boldsymbol{\beta} = \boldsymbol{\alpha} \,|\, \mathcal{T}(G_0) : \mathcal{T}(G_0) \to \mathcal{B}(G_0)$ is a transfer homomorphism (see [14, Proposition 3.5.5]), and hence we have in particular that $\mathsf{L}(B) = \mathsf{L}(\tau(B))$ for all $B \in \mathcal{B}(G^\bullet)$.

Narkiewicz constants. We start with the definition of the Narkiewicz constants (see [14, Definition 6.2.1]). Theorem 9.3.2 in [14] provides an asymptotic formula for the $F_k(x)$ function — the Narkiewicz constants occur as exponents of the $\log\log x$ term — in the frame of obstructed quasi-formations (this setting includes non-principal orders in holomorphy rings in global fields).

Definition 2.1. A type $T \in \mathcal{F}(G \times \mathbb{N})$ is called *squarefree* if $\mathsf{v}_{g,n}(T) \le 1$ for all $(g,n) \in G \times \mathbb{N}$. For every $k \in \mathbb{N}$, the *Narkiewicz constant* $\mathsf{N}_k(G)$ of G is defined by

$$\mathsf{N}_k(G) = \sup\{|T| \,|\, T \in \mathcal{T}(G^\bullet) \text{ squarefree}, |\mathsf{Z}(T)| \le k\} \in \mathbb{N}_0 \cup \{\infty\}.$$

The labeling function τ — defined as above — maps a sequence onto a squarefree type, and the labeling is done in such a way to meet the requirements of the analytic theory (see [14, Sec. 9.1]). For the combinatorial work on $\mathsf{N}_k(G)$, any other such function — mapping a sequence onto a squarefree type — would do. For instance, one could simply fix some indexing of the sequence $T = g_1 \cdot \ldots \cdot g_l$ and then label each g_i with its index i, thus using the type $(g_1, 1) \cdot \ldots \cdot (g_l, l)$. In other words, study of the Narkiewicz Constants can be done by simply replacing the usual un-indexed sequences with their natural indexed (i.e. ordered) counterparts. More formally, if T and T' are two squarefree zero-sum types with $\boldsymbol{\alpha}(T) = \boldsymbol{\alpha}(T')$, then there is a bijection from $\mathsf{Z}(T)$ to $\mathsf{Z}(T')$, and hence $|\mathsf{Z}(T)| = |\mathsf{Z}(T')|$. In particular, we have

- $|\mathsf{Z}(T)| = |\mathsf{Z}(\tau(\boldsymbol{\alpha}(T)))|$.
- if $T = (g_1, a_1) \cdot \ldots \cdot (g_l, a_l)$, where $g_1, \ldots, g_l \in G^\bullet$ and $a_1, \ldots, a_l \in \mathbb{N}$, and $\widetilde{T} = (g_1, \widetilde{a_1}) \cdot \ldots \cdot (g_l, \widetilde{a_l})$, where $\widetilde{a_1}, \ldots, \widetilde{a_l} \in \mathbb{N}$ are pairwise distinct, then $|\mathsf{Z}(T)| = |\mathsf{Z}(T')|$.

Thus we have

$$\mathsf{N}_k(G) = \sup\{|T| \,|\, T \in \mathcal{T}(G^\bullet) \text{ has pairwise distinct labels and } |\mathsf{Z}(T)| \le k\} \\ \in \mathbb{N}_0 \cup \{\infty\}.$$

If $U \in \mathcal{A}(G^\bullet)$, then $\tau(U)$ has unique factorization, and hence we get

$$\mathsf{D}(G) \le \mathsf{N}_1(G). \tag{2.1}$$

Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \,|\, \cdots \,|\, n_r$ and let $(e_1, \ldots, e_r)$ be a basis of G with $\operatorname{ord}(e_i) = n_i$ for all $i \in [1, r]$. If

$$B = \prod_{i=1}^{r} e_i^{n_i}, \quad \text{then } \tau(B) = \prod_{i=1}^{r} \prod_{k=1}^{n_i} (e_i, k)$$

has unique factorization, and hence

$$\sum_{i=1}^{r} n_i \le \mathsf{N}_1(G) \le \mathsf{N}_2(G) \le \cdots \tag{2.2}$$

In [32], Narkiewicz and Śliwa conjectured that $\mathsf{N}_1(G)$ equals the above lower bound for all finite abelian groups. We will use the above chain of inequalities without further mention and continue with a simple lemma needed in the sequel.

Lemma 2.2. *Let G be an abelian group with $|G| > 1$ and let $T \in \mathcal{T}(G^\bullet)$ be a squarefree zero-sum type. Then the following statements are equivalent.*

(a) $|\mathsf{Z}(T)| = 1$.
(b) *If $U, V \in \mathcal{T}(G)\setminus\{1\}$ with $T = UV$, then $\Sigma(U) \cap \Sigma(V) = \{0\}$.*
(c) *If $U, V \in \mathcal{T}(G)$ with $U \,|\, T$ and $V \,|\, T$, then $\gcd(U, V)$ has sum zero.*
(d) *If $U, V \in \mathcal{A}(\mathcal{T}(G))$ are distinct with $U \,|\, T$ and $V \,|\, T$, then $\gcd(U, V) = 1$.*

Proof. (a) ⇒ (b) Let $T = U_1 \cdot \ldots \cdot U_r$ with $r \in \mathbb{N}$, $U_1, \ldots, U_r \in \mathcal{A}(\mathcal{T}(G))$, and let $U, V \in \mathcal{T}(G)\setminus\{1\}$ with $T = UV$. Since T has unique factorization, there exists a nonempty subset $I \subset [1, r]$, say $I = [1, q]$ with $q \in [1, r-1]$, such that $U = U_1 \cdot \ldots \cdot U_q$ and $V = U_{q+1} \cdot \ldots \cdot U_r$. Assume to the contrary that there are $U', U'', V', V'' \in \mathcal{F}(G \times \mathbb{N})$ such that $U = U'U''$, $V = V'V''$ and $\overline{\sigma}(U') = \overline{\sigma}(V') \neq 0$. Then $U'V'', U''V' \in \mathcal{T}(G)$. Since T is squarefree, factorizations of $U'V''$ and $U''V'$ give rise to a factorization of $T = (U'V'')(U''V')$ which is different from the factorization $(U_1 \cdot \ldots \cdot U_q)(U_{q+1} \cdot \ldots \cdot U_r)$, a contradiction.

(b) ⇒ (c) Let $U, V \in \mathcal{T}(G)$ with $U \,|\, T$ and $V \,|\, T$. We write T in the form $T = U'WV'X$ where $W = \gcd(U, V)$, $U', V', X \in \mathcal{F}(G \times \mathbb{N})$, $U = U'W$ and $V = V'W$. Then $-\overline{\sigma}(W) = \overline{\sigma}(U') = \overline{\sigma}(V') \in \Sigma(U'W) \cap \Sigma(V'X) = \{0\}$.

(c) ⇒ (d) Let $U, V \in \mathcal{A}(\mathcal{T}(G))$ be distinct with $U \,|\, T$ and $V \,|\, T$. Since $\gcd(U, V)$ has sum zero and divides the atom U, it follows that $\gcd(U, V) = 1$.

(d) ⇒ (a) Let $T = U_1 \cdot \ldots \cdot U_r = V_1 \cdot \ldots \cdot V_s$ where $U_1, \ldots, U_r, V_1, \ldots, V_s \in \mathcal{A}(\mathcal{T}(G))$. For every $i \in [1, r]$ there is a $j \in [1, s]$ such that $\gcd(U_i, V_j) \neq 1$, and hence (d) implies that $U_i = V_j$. Thus $r = s$ and, after renumbering if necessary, $U_i = V_i$ for all $i \in [1, r]$. □

3. On a Variant of the Erdős–Ginzburg–Ziv Constant

We introduce a variant of the Erdős–Ginzburg–Ziv constant which will play a crucial role for the investigation of $\mathsf{N}_1(G)$. We will outline the program of this section after Definition 3.3.

Definition 3.1. Let G be a finite abelian group and $g \in G$. Let $\eta^*(G)$ (respectively, $\eta^*_g(G)$) denote the smallest integer $\ell \in \mathbb{N}_0$ such that every squarefree type $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|T| \ge \ell$ (respectively, with sum $\overline{\sigma}(T) = g$) has two distinct short minimal zero-sum subtypes which are not coprime.

Let T be a squarefree type. When in the following we consider two subtypes with special properties, then we always mean two distinct subtypes. The next lemma shows that $\eta^*(G)$ (and questions related to it) can also be formulated in the setting of sequences. In what follows, we will use both languages (the language of sequences and those of types), and always choose the one which is most convenient for the particular situation. Although the proof of Lemma 3.2 is completely straightforward, we give it in detail. It should help the reader to get acquainted with the definitions.

Lemma 3.2. *Let G be an abelian group and $g \in G$.*

(1) *For a squarefree type $T \in \mathcal{T}(G^\bullet)$ the following conditions are equivalent.*
   - (a) *T has two short minimal zero-sum subtypes T_1 and T_2 which are not coprime, i.e.* $\gcd(T_1, T_2) \neq 1$.
   - (b) *$\boldsymbol{\alpha}(T)$ has short minimal zero-sum subsequences S_1 and S_2 with the following properties*:
     - *S_1 and S_2 are not coprime, i.e.* $\gcd(S_1, S_2) \neq 1$;
     - *$S_1 = S_2$ implies that there exists some $g \in G$ such that $0 < \mathsf{v}_g(S_1) < \mathsf{v}_g(\boldsymbol{\alpha}(T))$.*

(2) *$\eta^*(G)$ (respectively, $\eta_g^*(G)$) is the smallest integer $\ell \in \mathbb{N}_0$ such that every sequence $S \in \mathcal{F}(G^\bullet)$ of length $|S| \geq \ell$ (respectively, with sum $\sigma(S) = g$) satisfies the properties given in condition* (1)(b).

(3) $\eta^*(G) = \sup\{\eta_h^*(G) \mid h \in G\}$.

(4) *Let $T \in \mathcal{T}(G^\bullet)$ be a squarefree type that does not have two short minimal zero-sum subtypes which are not coprime, and let $s \in \mathbb{N}_0$ and $T_1, \ldots, T_s$ be all short minimal zero-sum subtypes of T. Then T can be written in the form $T = T_0 \cdot \ldots \cdot T_s$ with $T_0 \in \mathcal{T}(G^\bullet), T_0, \ldots, T_s$ are pairwise coprime (in $\mathcal{F}(G^\bullet \times \mathbb{N})$) and $\boldsymbol{\alpha}(T_0), \ldots, \boldsymbol{\alpha}(T_s)$ are pairwise coprime (in $\mathcal{F}(G^\bullet)$).*

Proof. (1) (a) $\Rightarrow$ (b) Let $T = (g_1, a_1) \cdot \ldots \cdot (g_l, a_l)$ where $l \in \mathbb{N}$, $g_1, \ldots, g_l \in G^\bullet$, $a_1, \ldots, a_l \in \mathbb{N}$ and $(g_1, a_1), \ldots, (g_l, a_l)$ pairwise distinct. Let $I_1, I_2 \subset [1, l]$ such that $T_1 = \prod_{\lambda \in I_1} (g_\lambda, a_\lambda)$ and $T_2 = \prod_{\lambda \in I_2} (g_\lambda, a_\lambda)$ have the required properties. Since $(g_1, a_1), \ldots, (g_l, a_l)$ are pairwise distinct, it follows that $1 \neq \gcd(T_1, T_2) = \prod_{\lambda \in I_1 \cap I_2} (g_\lambda, a_\lambda)$. Since T_1 and T_2 are distinct, we get $I_1 \cap I_2 \subsetneq I_1$ and $I_1 \cap I_2 \subsetneq I_2$. For $\nu \in [1, 2]$, we set $S_\nu = \prod_{\lambda \in I_\nu} g_\lambda = \boldsymbol{\alpha}(T_\nu)$, and $S = \boldsymbol{\alpha}(T)$. Clearly, S_1 and S_2 are short minimal zero-sum subsequences of S and $1 \neq \prod_{\lambda \in I_1 \cap I_2} g_\lambda$ divides $\gcd(S_1, S_2)$. Suppose that $S_1 = S_2$. Then there exist $\lambda_1 \in I_1 \setminus I_2$, $\lambda_2 \in I_2 \setminus I_1$ and $g \in G$ such that $g = g_{\lambda_1} = g_{\lambda_2}$, and it follows that $0 < \mathsf{v}_g(S_1) < \mathsf{v}_{g_{\lambda_1}}(S_1) + \mathsf{v}_{(g_{\lambda_2}, a_{\lambda_2})}(T_2) \leq \mathsf{v}_g(S)$.

(b) $\Rightarrow$ (a) The proof is similar.

(2) Since every sequence S is the image of a squarefree type under $\boldsymbol{\alpha}$, the assertion follows from condition (1).

(3) The proof is obvious.

(4) First one has to show that $T_1, \ldots, T_s$ are pairwise coprime, and then define $T_0 = T(T_1 \cdot \ldots \cdot T_s)^{-1}$. We outline only the details that $\boldsymbol{\alpha}(T_0), \ldots, \boldsymbol{\alpha}(T_s)$ are pairwise coprime (the coprimeness of $T_1, \ldots, T_s$ is even simpler). Assume to the contrary that there are $i, j \in [0, s]$ with $j < i$ and $g \in G$ such that $g \,|\, \boldsymbol{\alpha}(T_i)$ and $g \,|\, \boldsymbol{\alpha}(T_j)$. Then there exist $k, l \in \mathbb{N}$ with $k \neq l$, $(g, k) \,|\, T_i$ and $(g, l) \,|\, T_j$. This implies that $T_i' = (g, l)(g, k)^{-1} T_i$ is a short minimal zero-sum subtype of T with $T_i' \neq T_i$ and $|T_i| \geq 2$ implies that $\gcd(T_i', T_i) \neq 1$, a contradiction. □

The requirement in Lemma 3.2(1) that the short zero-sum sequences T_1 and T_2 (respectively, the short zero-sum subtypes) are minimal is essential, as the following example shows. Let (e_1, e_2, e_3) be independent with $\operatorname{ord}(e_1) = \operatorname{ord}(e_2) = \operatorname{ord}(e_3) = m \leq \exp(G)/2$. Then $S = e_1^m e_2^m e_3^m$ does not satisfy condition (1)(b), but S satisfies a modified condition (1)(b) where the requirement of minimality is canceled (with $T_1 = e_1^m e_2^m$ and $T_2 = e_1^m e_3^m$). We recall the definition of the Erdős–Ginzburg–Ziv constant and of two of its variants.

Definition 3.3. Let G be a finite abelian group and $g \in G$. We denote by

- $\mathsf{s}(G)$ the smallest integer $\ell \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \geq \ell$ has a zero-sum subsequence T of length $|T| = \exp(G)$. The invariant $\mathsf{s}(G)$ is called the *Erdős–Ginzburg–Ziv constant* of G.
- $\eta(G)$ the smallest integer $\ell \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \geq \ell$ has a short zero-sum subsequence (equivalently, S has a short minimal zero-sum subsequence).
- $\mathsf{g}(G)$ the smallest integer $\ell \in \mathbb{N}$ such that every squarefree sequence $S \in \mathcal{F}(G)$ of length $|S| \geq \ell$ has a zero-sum subsequence T of length $|T| = \exp(G)$.

Together with the Davenport constant $\mathsf{D}(G)$, the invariants $\mathsf{s}(G)$ and $\eta(G)$ are classical invariants in Combinatorial Number Theory (see [13, Secs. 4 and 5] for a survey, or [3] for recent progress). By definition, we have

$$\mathsf{D}(G) \leq \eta(G) \leq \eta^*(G),$$

and Proposition 3.10 will show that $\eta^*(G) < \infty$. A straightforward argument will show that in the case of a cyclic group we have $\eta_0^*(G) = \eta^*(G) = |G| + 1$. The main aim of this section is to study $\eta^*(G)$ for groups of the form $G = C_n \oplus C_n$ with $n \geq 2$. A simple example shows that $\eta^*(C_n \oplus C_n) \geq 3n + 1$ (see Proposition 3.10(2)), and our conjecture is that

$$\eta^*(C_n \oplus C_n) = 3n + 1 \quad \text{for all } n \geq 2.$$

We will show that it suffices to verify the above conjecture for primes, and that moreover, for every $m \in \mathbb{N}$ there is a multiple $n \in m\mathbb{N}$ satisfying the above conjecture (Theorem 3.15 and Corollary 3.16). The direct problem, to find the precise value of $\eta^*(C_n \oplus C_n)$, is intimately connected with the associated inverse problem which asks for the structure of squarefree types $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|T| = \eta^*(G) - 1$

that do not have two short zero-sum subtypes which are not coprime. We formulate a conjecture and a simple consequence, whose proof will be given right after Corollary 3.11.

Conjecture 3.4. *Let $G = C_n \oplus C_n$ with $n \ge 2$ and let $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a squarefree type of length $|T| = 3n$. If T does not have two short minimal zero-sum subtypes which are not coprime, then there exist a basis (e_1, e_2) of G and $a_1, a_2 \in [1, n-1]$ with $\gcd(a_1, a_2, n) = 1$ such that $\boldsymbol{\alpha}(T) = e_1^n e_2^n (a_1 e_1 + a_2 e_2)^n$.*

Note that $\operatorname{ord}(a_1 e_1 + a_2 e_2) = n$ if and only if $\gcd(a_1, a_2, n) = 1$.

Lemma 3.5. *Let $G = C_n \oplus C_n$ with $n \ge 2$, and suppose that G satisfies Conjecture 3.4. Then*

$$\eta_0^*(G) = \eta^*(G) = 3n + 1 \quad \textit{and} \quad \eta_g^*(G) \le 3n \quad \textit{for all } g \in G^\bullet.$$

In the present paper we will not work on the inverse problem, but focus on the direct problem which is precisely what is needed for the subsequent investigation of the Narkiewicz constant in Sec. 4. We have formulated Conjecture 3.4 because it reveals the structural reason why $\eta^*(C_n \oplus C_n) = 3n + 1$ should hold true for all $n \ge 2$. In general, the inverse problems are much harder than the direct problems: even for groups of rank two, the inverse problem with respect to the Davenport constant has been solved only recently with considerable effort (see [7, 35, 38]), and the inverse problem with respect to the classical Erdős–Ginzburg–Ziv constant $\mathsf{s}(G)$ is still open (see [13, Sec. 5.2]).

We gather the results on $\mathsf{s}(G)$, $\eta(G)$ and $\mathsf{g}(G)$ which are needed in what follows. The precise values of $\mathsf{D}(G)$, $\mathsf{s}(G)$ and $\eta(G)$ (in terms of the group invariants) are well-known, among others, for groups of rank at most two. We will use them without further mention.

Lemma 3.6. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \mid n_2$. Then*

$$\mathsf{s}(G) = 2n_1 + 2n_2 - 3, \quad \eta(G) = 2n_1 + n_2 - 2 \quad \textit{and} \quad \mathsf{D}(G) = n_1 + n_2 - 1.$$

Proof. For the proof, see [14, Theorem 5.8.3]. □

We need the solution for the inverse problem with respect to the $\eta(G)$-invariant, which is based on the recent characterization of all minimal zero-sum sequences of maximal length over groups of the form $C_n \oplus C_n$ with $n \ge 2$.

Lemma 3.7. *Let $G = C_n \oplus C_n$ with $n \ge 2$, and let $S \in \mathcal{F}(G)$ be a sequence of length $|S| = \eta(G) - 1$. Then the following statements are equivalent.*

(a) *S has no short zero-sum subsequence.*
(b) *There exists a basis (e_1, e_2) of G and some $x \in [1, n-1]$ with $\gcd(x, n) = 1$ such that*

$$S = (e_1 e_2 (x e_1 + e_2))^{n-1}.$$

Proof. The group G has Property **B** by [35], and hence it has Property **C** by [13, Theorem 5.2.5]. Therefore the assertion follows from [13, Proposition 5.2.6], which is based on [37]. ◻

The invariant $\mathsf{g}(G)$ was introduced by Harborth in 1973 for groups of the form $G = C_n^r$ (see [20]). If $G = C_3^r$, then $\mathsf{g}(G) - 1$ is the maximal size of a cap in $AG(r, 3)$ (see [2, Lemma 5.2] and also [9, Sec. 5.2]). In [11] it is conjectured that $\mathsf{g}(C_n \oplus C_n)$ is equal to $2n-1$ for every odd $n \ge 3$ and equal to $2n+1$ for every even $n \ge 3$, and it is observed that these values are lower bounds. We will need the following result.

Lemma 3.8. *Let $G = C_p \oplus C_p$ with $p \in \mathbb{P}$. If $p \le 7$ or $p \ge 47$, then $\mathsf{g}(G) = 2p - 1$.*

Proof. For the proof see [8, Theorem 5.1; 26, 27]. ◻

Lemma 3.9. *Let G be a finite abelian group with $|G| > 1$, and let $T = U_1 \cdot \ldots \cdot U_r \in \mathcal{T}(G^\bullet)$ be a squarefree type with $r \in \mathbb{N}$ and $U_1, \ldots, U_r \in \mathcal{A}(\mathcal{T}(G^\bullet))$.*

(1) *If $|\mathsf{Z}(T)| = 1$, then $\prod_{i=1}^r |U_i| \le |G|$.*
(2) *Let $S_1, \ldots, S_t \in \mathcal{F}(G \times \mathbb{N})$ such that $S_1 \cdot \ldots \cdot S_t$ is a zero-sum subtype of T and $\overline{\sigma}(S_1), \ldots, \overline{\sigma}(S_t)$ are all non-zero. If $|\mathsf{Z}(T)| = 1$ and $b_1, \ldots, b_t \in \mathbb{N}$ are pairwise distinct, then the squarefree type $(\overline{\sigma}(S_1), b_1) \cdot \ldots \cdot (\overline{\sigma}(S_t), b_t)$ has unique factorization.*
(3) *If T does not have two short minimal zero-sum subtypes which are not coprime and $|T| \le 2\exp(G) + 1$, then $|\mathsf{Z}(T)| = 1$.*

Proof. (1) A special case was proved in [14, Proposition 6.2.6], and we follow the lines of that proof. For every $i \in [1, r]$, we set $U_i = (g_{i,1}, a_{i,1}) \cdot \ldots \cdot (g_{i,m_i}, a_{i,m_i})$, where $m_i = |U_i| \ge 2$, and for all $j \in [1, m_i]$, $g_{i,j} \in G$ and $a_{i,j} \in \mathbb{N}$. In order to show that $m_1 \cdot \ldots \cdot m_r \le |G|$, we shall prove that the $m_1 \cdot \ldots \cdot m_r$ elements

$$\sum_{i=1}^{r} \sum_{\lambda=1}^{l_i} g_{i,\lambda} \quad \text{where } l_i \in [1, m_i] \text{ for all } i \in [1, r]$$

are distinct. Assume the contrary. Then we may suppose that there exists some $r' \in [1, r]$ and $l_i, l_i' \in [1, m_i]$ such that $l_i' < l_i$ for all $i \in [1, r']$, $l_i' \ge l_i$ for all $i \in [r'+1, r]$, and

$$\sum_{i=1}^{r} \sum_{\lambda=1}^{l_i} g_{i,\lambda} = \sum_{i=1}^{r} \sum_{\lambda=1}^{l_i'} g_{i,\lambda}.$$

Then we have

$$g = \sum_{i=1}^{r'} \sum_{\lambda=l_i'+1}^{l_i} g_{i,\lambda} = \sum_{i=r'+1}^{r} \sum_{\lambda=l_i+1}^{l_i'} g_{i,\lambda}.$$

Since $g \in \Sigma(U_1 \cdot \ldots \cdot U_{r'}) \cap \Sigma(U_{r'+1} \cdot \ldots \cdot U_t)$, Lemma 2.2(b) implies that $g = 0$. Then

$$V = \prod_{i=1}^{r'} \left(\prod_{\lambda=l_i'+1}^{l_i} (g_{i,\lambda}, a_{i,\lambda}) \right) \in \mathcal{T}(G) \setminus \{1\}.$$

If $V_1 \in \mathcal{A}(\mathcal{T}(G))$ with $(g_{1,l_1}, a_{1,l_1}) \,|\, V_1 \,|\, V$, then $V_1 \neq U_1$ (because $(g_{1,1}, a_{1,1}) \nmid V$) and $(g_{1,l_1}, a_{1,l_1}) \,|\, \gcd(U_1, V_1)$, a contradiction to Lemma 2.2(d).

(2) Assume to the contrary that $(\overline{\sigma}(S_1), b_1) \cdot \ldots \cdot (\overline{\sigma}(S_t), b_t)$ does not have unique factorization. By Lemma 2.2(c), there exist $I, J \subset [1, t]$ such that $\prod_{i \in I} (\overline{\sigma}(S_i), b_i)$ and $\prod_{i \in J} (\overline{\sigma}(S_i), b_i)$ are zero-sum types, but $\gcd(\prod_{i \in I} (\overline{\sigma}(S_i), b_i), \prod_{i \in J} (\overline{\sigma}(S_i), b_i)) = \prod_{i \in I \cap J} (\overline{\sigma}(S_i), b_i)$ does not have sum zero. It follows that $\prod_{i \in I} S_i$ and $\prod_{i \in J} S_i$ are zero-sum types such that $\gcd(\prod_{i \in I} S_i, \prod_{i \in J} S_i) = \prod_{i \in I \cap J} S_i$ does not have sum zero. Now Lemma 2.2(c) implies that $|Z(T)| > 1$, a contradiction.

(3) Assume to the contrary that $|\mathsf{Z}(T)| \geq 2$. For $\nu \in [1, 2]$, let

$$z_\nu = U_{\nu,1} \cdot \ldots \cdot U_{\nu,r_\nu} \in \mathsf{Z}(T) \quad \text{where } U_{\nu,1}, \ldots, U_{\nu,r_\nu} \in \mathcal{A}(\mathcal{T}(G^\bullet)).$$

After renumbering if necessary, there is a $u \in [0, r_1]$ such that $U_{1,\nu} = U_{2,\nu}$ for all $\nu \in [1, u]$ and $U_{1,\nu} \neq U_{2,\nu'}$ for all $\nu \in [u+1, r_1]$ and all $\nu' \in [u+1, r_2]$, and that $|U_{2,u+1}| \leq \cdots \leq |U_{2,r_2}|$. Note that $r_1 - u \geq 2$, $r_2 - u \geq 2$ and thus $|U_{2,u+1}| \leq \lfloor |T|/2 \rfloor \leq \exp(G)$. There are at least two indices $j \in [u+1, r_1]$ such that $\gcd(U_{2,u+1}, U_{1,j}) \neq 1$. We pick a $j \in [u+1, r_1]$ with this property for which $|U_{1,j}|$ is minimal, and thus it follows that $|U_{1,j}| \leq \lfloor |T|/2 \rfloor \leq \exp(G)$. Therefore, $U_{1,j}$ and $U_{2,u+1}$ are two short minimal zero-sum subtypes of T which are not coprime, a contradiction. □

Now we are well-prepared for our investigations on $\eta^*(G)$.

Proposition 3.10. *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ where $r, n_1, \ldots, n_r \in \mathbb{N}$ with $1 < n_1 \,|\, \cdots \,|\, n_r$.*

(1) $\eta_0^*(G) \leq \eta^*(G) \leq 2\,\eta(G) - 1 \leq 2|G| - 1$.
(2) *If $r \geq 2$, then* $\eta^*(G) \geq \eta_0^*(G) \geq \sum_{i=1}^r n_i + n_r + 1$.
(3) *Let $g, h \in G$ with $\operatorname{ord}(g) = \operatorname{ord}(h) = n_r$. Then $\eta_g^*(G) = \eta_h^*(G)$.*

Proof. (1) By definition, we have $\eta_0^*(G) \leq \eta^*(G)$, and [13, Theorem 4.2.7] shows that $\eta(G) \leq |G|$. Assume to the contrary that $\eta^*(G) \geq 2\eta(G)$. Then there exists a squarefree type $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|S| \geq 2\eta(G) - 1$ that does not have two short minimal zero-sum subtypes which are not coprime. Let $t \in \mathbb{N}_0$ and $S_1, \ldots, S_t$ be all short minimal zero-sum subtypes of S. Then $S_1, \ldots, S_t$ are pairwise coprime, and thus S can be written in the form

$$S = S_0 S_1 \cdot \ldots \cdot S_t \quad \text{with } S_0 \in \mathcal{F}(G^\bullet \times \mathbb{N}).$$

For every $\nu \in [1,t]$ we choose an element $g_\nu \in \mathrm{supp}(S_\nu)$. Then the type $S_0(g_1^{-1}S_1) \cdot \ldots \cdot (g_t^{-1}S_t)$ does not have a short minimal zero-sum subtype which implies that

$$t \le |(g_1^{-1}S_1) \cdot \ldots \cdot (g_t^{-1}S_t)| \le |S_0(g_1^{-1}S_1) \cdot \ldots \cdot (g_t^{-1}S_t)| \le \eta(G) - 1,$$

and hence

$$|S| = |S_0S_1 \cdot \ldots \cdot S_t| = t + |S_0(g_1^{-1}S_1) \cdot \ldots \cdot (g_t^{-1}S_t)| \le 2\eta(G) - 2.$$

a contradiction.

(2) Let $r \ge 2$, $(e_1, \ldots, e_r)$ be a basis of G with $\mathrm{ord}(e_i) = n_i$ for every $i \in [1,r]$, and set $e_0 = e_1 + \cdots + e_r$. The sequence

$$S = e_1^{n_1} \cdot \ldots \cdot e_r^{n_r} e_0^{n_r}$$

has sum zero and precisely $r+1$ short minimal zero-sum subsequences, namely $e_1^{n_1}, \ldots, e_r^{n_r}, e_0^{n_r}$. Using Lemma 3.2(2) we infer that $\eta_0^*(G) > |S| = \sum_{i=1}^r n_i + n_r$.

(3) If $\varphi \colon G \to G'$ is a group isomorphism and $g \in G$, then we obviously have $\eta_g^*(G) = \eta_{\varphi(g)}^*(G')$. Since $\mathrm{ord}(g) = \mathrm{ord}(h) = \exp(G)$, there exists a group automorphism $\varphi \colon G \to G$ with $\varphi(g) = h$, and thus the assertion follows. □

Corollary 3.11. *Let G be a finite abelian group with $|G| > 1$.*

(1) *If G is cyclic, then $\eta_0^*(G) = \eta^*(G) = |G| + 1$.*
(2) *If G is an elementary 2-group, then $\eta_0^*(G) = \eta^*(G) = 2|G| - 1$.*

Proof. (1) Let G be cyclic of order $n \ge 2$ and $g \in G$ with $\mathrm{ord}(g) = n$. Then the sequence $S = g^n$ has precisely one short minimal zero-sum subsequence, and hence $\eta_0^*(G) > |S| = n$. In order to show that $\eta^*(G) \le n + 1$, we choose a squarefree type $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|T| = n+1$. Let $t \in \mathbb{N}_0$ and $A_1, \ldots, A_t$ be all short minimal zero-sum subtypes of T. Assume to the contrary that they are pairwise coprime. By Lemma 3.2(4), $S = \boldsymbol{\alpha}(T)$ can be written in the form $S = S_0S_1 \cdot \ldots \cdot S_t$, where $S_i = \boldsymbol{\alpha}(T_i)$ for all $i \in [1,t]$ and $S_0 \in \mathcal{F}(G^\bullet)$ is zero-sum free. For every $i \in [1,t]$ we choose an element $a_i \in \mathrm{supp}(S_i)$. Then $S(a_1 \cdot \ldots \cdot a_t)^{-1}$ is zero-sum free, and thus [14, Proposition 5.3.5] implies that

$$\begin{aligned}|\Sigma(S(a_1 \cdots a_t)^{-1})| &\ge |S(a_1 \cdot \ldots \cdot a_t)^{-1}| + |\mathrm{supp}(S(a_1 \cdot \ldots \cdot a_t)^{-1})| - 1\\ &\ge n + 1 - t + t - 1 = n,\end{aligned}$$

a contradiction.

(2) Let G be an elementary 2-group, set $G^\bullet = \{g_1, \ldots, g_l\}$ and consider the sequence $S = g_1^2 \cdot \ldots \cdot g_l^2$. Then every short minimal zero-sum subsequence of S has the form g^2 for some $g \in G^\bullet$. Hence, by Lemma 3.2(2), we obtain that $\eta_0^*(G) > |S| = 2|G| - 2$. So the assertion follows from Proposition 3.10(1). □

Now we can give the simple proof of Lemma 3.5.

Proof of Lemma 3.5. Assume to the contrary that $\eta^*(G) > 3n+1$. Then there exists a squarefree type T of length $|T| = 3n+1$ that does not have two short minimal zero-sum subtypes which are not coprime. Clearly, the same is true for $g_1^{-1}T$ and $g_2^{-1}T$, where $g_1, g_2 \in \operatorname{supp}(T)$, and hence the structural statement of Conjecture 3.4 shows that there is an element $g \in G$ with $\mathsf{v}_g(\boldsymbol{\alpha}(T)) \geq n+1$. This implies that condition (1)(b) of Lemma 3.2 is satisfied, a contradiction. Thus it follows that $\eta^*(G) \leq 3n+1$, and using Proposition 3.10(2) we infer that

$$3n+1 \leq \eta_0^*(G) \leq \eta^*(G) \leq 3n+1.$$

Let $g \in G^\bullet$ and assume to the contrary that $\eta_g^*(G) \geq 3n+1$. Then there exists a type $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|T| = 3n$ and with $\sigma(T) = g$ that does not have two short minimal zero-sum subtypes which are not coprime, a contradiction to the statement of Conjecture 3.4. □

Next we show that for the first small primes we have $\eta_0^*(C_p \oplus C_p) = \eta^*(C_p \oplus C_p) = 3p+1$ (note that this is based on the deep and recent results formulated in Lemmas 3.7 and 3.8). Whereas it would be possible to increase the list of primes, the handling of the general case definitely requires a different method.

Proposition 3.12. *Let $G = C_p \oplus C_p$ with $p \in \mathbb{P}$. If $p \leq 7$, then $\eta_0^*(G) = \eta^*(G) = 3p+1$.*

Proof. By Proposition 3.10(2) we have $3p+1 \leq \eta_0^*(G)$, and thus it remains to show that $\eta^*(G) \leq 3p+1$. Assume to the contrary that $\eta^*(G) > 3p+1$. Then there exists a squarefree type $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|S| = l = 3p+1$ that does not have two short minimal zero-sum subtypes which are not coprime. Let $t \in \mathbb{N}_0$ and $S_1, \ldots, S_t$ be all short minimal zero-sum subtypes of S. Then $S_1, \ldots, S_t$ are pairwise coprime, and thus S can be written in the form

$$S = S_0 S_1 \cdot \ldots \cdot S_t \quad \text{with } S_0 \in \mathcal{F}(G^\bullet \times \mathbb{N}).$$

For every $\nu \in [1,t]$ we choose an element $g_\nu \in \operatorname{supp}(S_\nu)$, and we set $l_\nu = |S_\nu|$. After renumbering if necessary we may suppose that $l_1 \leq \cdots \leq l_t$, and we define

$$\mathfrak{L} = \prod_{\nu=1}^{t} l_\nu \in \mathcal{F}(\mathbb{N}) = F.$$

Assume to the contrary that $t \leq 3$. Then $S(g_1 \cdot \ldots \cdot g_t)^{-1}$ has length at least $3p-2$, and hence by Lemma 3.6 it has a short minimal zero-sum subtype S'. By construction, S' is different from $S_1, \ldots, S_t$, a contradiction. Assume to the contrary that $t = 4$. Then $S(g_1g_2g_3g_4)^{-1}$ has length $3p-3$. Since $S_1, \ldots, S_t$ are all short minimal zero-sum subtypes of S, each two elements of $\boldsymbol{\alpha}(S_i)$ and $\boldsymbol{\alpha}(S_j)$, $i \neq j \in [1,4]$, are distinct. Thus $\boldsymbol{\alpha}(S_1S_2S_3S_4(g_1g_2g_3g_4)^{-1})$ contains at least four distinct elements and hence the same is true for $\boldsymbol{\alpha}(S(g_1g_2g_3g_4)^{-1})$. Now Lemma 3.7

implies that $S(g_1g_2g_3g_4)^{-1}$ has a short minimal zero-sum subtype, a contradiction. Therefore it follows that $t \ge 5$.

Now we discuss the individual primes.

Case 1: $p = 2$. We obtain that $7 = 3p + 1 = |S| \ge \sum_{i=1}^{t} |S_i| \ge 2t \ge 10$, a contradiction.

Case 2: $p = 3$. We obtain that $10 = 3p + 1 = |S| \ge \sum_{i=1}^{t} |S_i| \ge 10$, which implies that $|S_1| = \cdots = |S_t| = 2$ and $|\operatorname{supp}(\boldsymbol{\alpha}(S))| \ge |\operatorname{supp}(\boldsymbol{\alpha}(S_1 \cdot \ldots \cdot S_t))| \ge 10 > |G^\bullet|$, a contradiction.

Case 3: $p = 5$. We will apply repeatedly Lemma 3.9 (items (1) and (3), with $T = \prod_{\nu \in I} S_\nu$, $U_\nu = S_\nu$ and $I \subset [1,t]$).

Assume to the contrary that $5 \,|\, {}_F\mathfrak{L}$. Then $l_5 = 5$ and $l_1 + l_2 + l_3 + l_4 \le |S| - 5 = 11$, and thus $l_1 = 2$. If $3 \,|\, {}_F\mathfrak{L}$, then $2 + 3 + 5 \le 2\exp(G) + 1$ and $2 \cdot 3 \cdot 5 > |G|$, a contradiction to Lemma 3.9. Thus $3 \nmid_F \mathfrak{L}$, and the same argument shows that $4 \nmid_F \mathfrak{L}$. Since $l_2 + l_3 + l_4 \le |S| - l_1 - l_5 = 9$, it follows that $l_2 = l_3 = 2$. However, $l_1 + l_2 + l_3 + l_5 = 11 \le 2\exp(G) + 1$ and $l_1 l_2 l_3 l_5 > |G|$, a contradiction to Lemma 3.9.

Assume to the contrary that $2 \nmid_F \mathfrak{L}$. Since $3 + 3 + 3 \le 2\exp(G) + 1$ and $3 \cdot 3 \cdot 3 > |G|$, Lemma 3.9 implies that $3^3 \nmid_F \mathfrak{L}$ and hence $4^2 \,|\, {}_F\mathfrak{L}$. Again Lemma 3.9 implies that $3 \cdot 4^2 \nmid_F \mathfrak{L}$. Therefore we get that $l_1 = \cdots = l_5 = 4$ and $l_1 + \cdots + l_5 = 20 > |S|$, a contradiction.

Assume to the contrary that $3 \nmid_F \mathfrak{L}$. Then $l_1, \ldots, l_5 \in \{2, 4\}$. Lemma 3.9 implies that $2 \cdot 4^2 \nmid_F \mathfrak{L}$. Thus we obtain that either $\mathfrak{L} = 2^5$ or $\mathfrak{L} = 4 \cdot 2^4$. In each case Lemma 3.9 yields a contradiction.

Summing up we know that $2 \cdot 3 \,|\, {}_F\mathfrak{L}$ and that $5 \nmid_F \mathfrak{L}$. Using Lemma 3.9 again we infer that $3^3 \nmid \mathfrak{L}$ and that $2 \cdot 4^2 \nmid \mathfrak{L}$. Thus $\mathsf{v}_3(\mathfrak{L}) \le 2$, $\mathsf{v}_4(\mathfrak{L}) \le 1$ and hence $\mathsf{v}_2(\mathfrak{L}) \ge 2$. Again by Lemma 3.9 we infer that $2^2 \cdot 3^2 \nmid_F \mathfrak{L}$ and that $2^2 \cdot 3 \cdot 4 \nmid_F \mathfrak{L}$ which implies that $\mathsf{v}_3(\mathfrak{L}) = 1$ and that $\mathsf{v}_4(\mathfrak{L}) = 0$. Therefore we obtain that $2^4 \cdot 3 \,|\, {}_F\mathfrak{L}$, which again is a contradiction to Lemma 3.9.

Case 4: $p = 7$. Again we apply Lemma 3.9. If $t \ge 6$, then the proof is similar to that of Case 3. Suppose that $t = 5$. If $\mathfrak{L} \ne 2^5$ and $\mathfrak{L} \ne 2^4 \cdot 3$, then we obtain a contradiction by Lemma 3.9. Thus we distinguish these two cases.

Case 4.1: $l_1 = \cdots = l_5 = 2$. Since S does not have two short minimal zero-sum subtypes which are not coprime we infer that

$$|\operatorname{supp}(\boldsymbol{\alpha}(S_1 \cdot \ldots \cdot S_5))| = |\boldsymbol{\alpha}(S_1 \cdot \ldots \cdot S_5)| = 10 \quad \text{and}$$

$$\operatorname{supp}(\boldsymbol{\alpha}(S_1 \cdot \ldots \cdot S_5)) \cap \operatorname{supp}(\boldsymbol{\alpha}(S_0)) = \emptyset.$$

Assume to the contrary that $|\operatorname{supp}(\boldsymbol{\alpha}(S_0))| \ge 3$. Let S_0' be a subtype of S_0 such that $\boldsymbol{\alpha}(S_0')$ consists of three distinct elements. By Lemma 3.8, $S_0' S_1 \cdot \ldots \cdot S_5$ has a zero-sum subtype T of length $|T| = 7$. Therefore T has a short minimal zero-sum subtype T' of length $|T'| \ne 2$, and hence T' is distinct from $S_1, \ldots, S_5$, a contradiction. Thus $|\operatorname{supp}(\boldsymbol{\alpha}(S_0))| \le 2$, and since S_0 has no short zero-sum subtype, it follows that

$$\boldsymbol{\alpha}(S_0) = b^6 c^6 \quad \text{with } b, c \in G^\bullet.$$

We assert that S_5S_0 has a minimal zero-sum subtype S' of length $|S'| = 8$. Suppose this holds true. Then $l_1+l_2+l_3+|S'| = 14 \le 2\exp(G)+1$ and $l_1l_2l_3|S'| = 64 > |G|$, a contradiction to Lemma 3.9.

To verify this assertion, we set $\boldsymbol{\alpha}(S_5) = (-a)a$ with $a \in G^\bullet$. Since $\mathsf{D}(G) = 13$, the sequence ab^6c^6 has a minimal zero-sum subsequence $a^\epsilon b^u c^v$ with $\epsilon \in \{0,1\}$ and $u, v \in [0,6]$. Since $S_1, \ldots, S_5$ are all short minimal zero-sum subtypes of S, it follows that

$$\epsilon + u + v = |a^\epsilon b^u c^v| \ge 8 \quad \text{and hence } u, v \in [1,6].$$

Assume to the contrary that $\epsilon = 0$. Then $b^{7-u}c^{7-v}$ is a zero-sum subsequence of b^6c^6. Since $|b^6c^6| + |b^{7-u}c^{7-v}| = 14$, it follows that b^uc^u or $b^{7-u}c^{7-v}$ has a short minimal zero-sum subsequence, and by construction, the associated type differs from $S_1, \ldots, S_5$, a contradiction. Thus we infer that $\epsilon = 1$. Then $(-a)b^{7-u}c^{7-v}$ is a zero-sum subsequence of $(-a)b^6c^6$. Since $|ab^uc^v| + |(-a)b^{7-u}c^{7-v}| = 16$ and $S_1, \ldots, S_5$ are all short minimal zero-sum subtypes of S, it follows that both, ab^uc^v and $(-a)b^{7-u}c^{7-v}$, are minimal zero-sum subsequences of $\boldsymbol{\alpha}(S_0S_5)$ having length 8.

Case 4.2: $l_1 = \cdots = l_4 = 2$ and $l_5 = 3$. Then $|S_5| = 3$. We set $\boldsymbol{\alpha}(S_5) = a_1a_2a_3$ with $a_1, a_2 \in G$ distinct, and let S_5' be a subtype of S_5 such that $\boldsymbol{\alpha}(S_5') = a_1a_2$. Since S does not have two short minimal zero-sum subtypes which are not coprime we infer that

$$|\operatorname{supp}(\boldsymbol{\alpha}(S_1 \cdot \ldots \cdot S_4S_5'))| = |\boldsymbol{\alpha}(S_1 \cdot \ldots \cdot S_4S_5')| = 10 \quad \text{and}$$
$$\operatorname{supp}(\boldsymbol{\alpha}(S_1 \cdot \ldots \cdot S_4S_5')) \cap \operatorname{supp}(\boldsymbol{\alpha}(S_0)) = \emptyset.$$

As above we obtain that $|\operatorname{supp}(\boldsymbol{\alpha}(S_0))| = 2$, and we set

$$\boldsymbol{\alpha}(S_0) = b^6c^5 \quad \text{with } b, c \in G^\bullet.$$

We assert that S_5S_0 has a minimal zero-sum subtype S' of length $|S'| \in [8,9]$. Suppose this holds true. Then $l_1+l_2+l_3+|S'| \le 15 = 2\exp(G)+1$ and $l_1l_2l_3|S'| \ge 64 > |G|$, a contradiction to Lemma 3.9.

Now we verify this assertion. Since $\mathsf{D}(G) = 13$, the sequence $a_1a_2b^6c^5$ has a minimal zero-sum subsequence

$$a_1^{\epsilon_1}a_2^{\epsilon_2}b^uc^v \quad \text{with } \epsilon_1, \epsilon_2 \in [0,1],\ u \in [0,6] \quad \text{and} \quad v \in [0,5].$$

If $\epsilon_1+\epsilon_2+u+v \le 9$, then the assertion follows. Suppose that $\epsilon_1+\epsilon_2+u+v \ge 10$. Then $u \ge 3$ and $v \ge 2$. We distinguish four subcases.

Case 4.2.1: $\epsilon_1 = \epsilon_2 = 0$. As in Case 4.1 it follows that b^uc^v or $b^{7-u}c^{7-v}$ has a short minimal zero-sum subsequence, and, by construction, the associated type differs from $S_1, \ldots, S_5$, a contradiction.

Case 4.2.2: $\epsilon_1 = 0$ and $\epsilon_2 = 1$. Then $a_1a_3b^{7-u}c^{7-v}$ is a zero-sum subsequence of $a_1a_3b^6c^5$. Since $|a_2b^uc^v| + |a_1a_3b^{7-u}c^{7-v}| = 17$ and since $S_1, \ldots, S_5$ are all short minimal zero-sum subtypes of S, it follows that the shorter sequence of $a_2 b^u c^v$ and $a_1 a_3 b^{7-u} c^{7-v}$ is a minimal zero-sum sequence of length 8.

Case 4.2.3: $\epsilon_1 = 1$ and $\epsilon_2 = 0$. Similar to Case 4.2.2.

Case 4.2.4: $\epsilon_1 = \epsilon_2 = 1$. Similar to Case 4.2.2. □

The following two lemmas constitute the essential tools in the proof of our main result, which is Theorem 3.15.

Lemma 3.13. *Let $G = C_n \oplus C_n$ with $n \ge 2$ and let $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be squarefree. Suppose that one of the following two conditions holds*:

(a) $|S| \ge 4n-1$ *and there are two distinct elements $g_1, g_2 \in G$ such that* $\mathsf{v}_{g_1}(\boldsymbol{\alpha}(S)) + \mathsf{v}_{g_2}(\boldsymbol{\alpha}(S)) \ge 2n$.

(b) $|S| \ge 4n$ *and there are three distinct elements $g_1, g_2, g_3 \in G$ such that* $\mathsf{v}_{g_1}(\boldsymbol{\alpha}(S)) + \mathsf{v}_{g_2}(\boldsymbol{\alpha}(S)) + \mathsf{v}_{g_3}(\boldsymbol{\alpha}(S)) \ge 2n$.

Then S has two short minimal zero-sum subtypes which are not coprime.

Proof. For every subsequence T of $\boldsymbol{\alpha}(S)$, let $\boldsymbol{\alpha}^{-1}(T)$ denote the corresponding subtype of S. By Proposition 3.12 we may suppose that $n \ge 4$. Let $\psi \in \{2, 3\}$ such that $\sum_{\nu=1}^{\psi} \mathsf{v}_{g_\nu}(\boldsymbol{\alpha}(S)) \ge 2n$. We may suppose that $|S| = 4n - \delta$ with $\delta \in \{0, 1\}$, where $\delta = 1$ implies that $\psi = 2$. Let $S_1, \ldots, S_t$ be all short minimal zero-sum subtypes of $S \prod_{\nu=1}^{\psi} g_\nu^{-\mathsf{v}_{g_\nu}(S)}$. Assume to the contrary that S does not have two short minimal zero-sum subtypes which are not coprime. Let $W = \boldsymbol{\alpha}^{-1}(\prod_{\nu=1}^{\psi} g_\nu^{\mathsf{v}_{g_\nu}(\boldsymbol{\alpha}(S))})$. Then $\mathrm{supp}(\boldsymbol{\alpha}(S_i)) \cap \mathrm{supp}(\boldsymbol{\alpha}(S_j)) = \emptyset$ for all $i \ne j \in [1, t]$,

$$S_1 \cdot \ldots \cdot S_t \,|\, SW^{-1} \quad \text{and hence } |S_1 \cdot \ldots \cdot S_t| \le 2n - \delta.$$

For every $\nu \in [1, t]$ we choose an element $h_\nu \in \mathrm{supp}(S_\nu)$. Then $S(g_1 \cdot \ldots \cdot g_\psi h_1 \cdot \ldots \cdot h_t)^{-1}$ has no short zero-sum subtype, and hence $|S| - \psi - t < \eta(G) = 3n-2$. Since $|S_\nu| \ge 2$ for all $\nu \in [1, t]$, the inequality $|S_1 \cdot \ldots \cdot S_t| \le 2n - \delta$ implies that $t \le n - \delta$. Thus we obtain that $3n - 2 > |S| - \psi - t \ge 4n - \delta - \psi - (n - \delta) = 3n - \psi$, which implies that $\psi = 3$, $\delta = 0$, $|S| = 4n$, $|S| - \psi - t = 3n - 3$ and $t = n$. Since $\mathrm{supp}(\boldsymbol{\alpha}(S_1)), \ldots, \mathrm{supp}(\boldsymbol{\alpha}(S_n))$ are pairwise disjoint, $\boldsymbol{\alpha}(S(g_1 g_3 g_3 h_1 \cdot \ldots \cdot h_n)^{-1})$ has at least $n \ge 4$ distinct elements, a contradiction to Lemma 3.7. □

Lemma 3.14. *Let $G = C_{mn} \oplus C_{mn}$ with $m, n \ge 2$, $\varphi \colon G \to G$ be the multiplication by m, and $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be squarefree. Let $u \in \mathbb{N}_0$ and $S_1, \ldots, S_u \in \mathcal{F}(G^\bullet \times \mathbb{N})$ with the following properties.*

(i) $S_1 \cdot \ldots \cdot S_u \,|\, S$.

(ii) *For every $\nu \in [1, u]$, $\overline{\varphi}(S_\nu)$ is a short zero-sum sequence over $\varphi(G)$.*

(iii) *The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.*

Let T_1 and T_2 be subtypes of $S(S_1 \cdot \ldots \cdot S_u)^{-1}$ such that $\varphi(T_1)$ and $\varphi(T_2)$ are short minimal zero-sum types which are not coprime. Then one of the following three conditions holds.

(a) *The sequence $\overline{\sigma}(T_1)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.*
(b) *The sequence $\overline{\sigma}(T_2)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.*
(c) *S has two short minimal zero-sum subtypes which are not coprime.*

Proof. Suppose that for $\lambda \in [1,2]$, the sequence $\overline{\sigma}(T_\lambda)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u)$ has a short zero-sum subsequence. Then there exist, for $\lambda \in [1,2]$, subsets $I_\lambda \subset [1,u]$ with $|I_\lambda| + 1 \in [1,m]$ such that

$$T_\lambda V_\lambda, \quad \text{where } V_\lambda = \prod_{\nu \in I_\lambda} S_\nu,$$

are zero-sum types, and since

$$\left| T_\lambda \prod_{\nu \in I_\lambda} S_\nu \right| \le n + |I_\lambda| n \le mn,$$

they are short. We assert that $\gcd(T_1V_1, T_2V_2) \notin \mathcal{T}(G)$. In order to verify this, note that by construction, we have $\gcd(T_i, V_j) = 1$ for all $i, j \in [1,2]$, and therefore

$$\gcd(T_1V_1, T_2V_2) = \gcd(T_1, T_2)\gcd(V_1, V_2).$$

Now we obtain that

$$\gcd(V_1, V_2) = \prod_{\nu \in I_1 \cap I_2} S_\nu, \quad \overline{\sigma} \circ \varphi(\gcd(V_1, V_2)) = \sum_{\nu \in I_1 \cap I_2} \overline{\sigma} \circ \varphi(S_\nu)$$
$$= \sum_{\nu \in I_1 \cap I_2} \sigma \circ \overline{\varphi}(S_\nu) = 0$$

and hence

$$\varphi \circ \overline{\sigma}(\gcd(T_1V_1, T_2V_2)) = \overline{\sigma} \circ \varphi(\gcd(T_1V_1, T_2V_2)) = \overline{\sigma} \circ \varphi(\gcd(T_1, T_2))$$
$$= \overline{\sigma}(\gcd(\varphi(T_1), \varphi(T_2)) \ne 0.$$

Therefore, $\gcd(T_1V_1, T_2V_2) \notin \mathcal{T}(G)$, and hence there exist minimal zero-sum subtypes $W_1 \mid T_1V_1$ and $W_2 \mid T_2V_2$ such that $\gcd(W_1, W_2) \ne 1$. Since $|W_\lambda V_\lambda| \le |T_\lambda V_\lambda| \le mn$ for $\lambda \in [1,2]$, it follows that W_1 and W_2 are short. □

Now we formulate the main result of this section. It shows that, if $\eta^*(C_p \oplus C_p) = 3p + 1$ holds for all primes, then $\eta^*(C_n \oplus C_n) = 3n + 1$ holds for all positive integers $n \ge 2$. Moreover, Corollary 3.16 shows that every integer $m \in \mathbb{N}$ has a multiple $n \in m\mathbb{N}$ satisfying $\eta^*(C_n \oplus C_n) = 3n + 1$. We will make substantial use of Lemma 3.7.

Theorem 3.15. *Let $G = C_{mn} \oplus C_{mn}$ with $m, n \geq 2$.*

(1) *Suppose that $\eta^*(C_m \oplus C_m) = 3m + 1$.*
   (a) *If $\eta^*(C_n \oplus C_n) = 3n + 1$, then $\eta^*(G) = 3mn + 1$.*
   (b) *If $\gcd(6, m) = 1$ and $n = p \in \mathbb{P}$ with $m \geq \frac{33p^3}{4}$, then $\eta^*(G) = 3mp + 1$.*

(2) *If $\eta_0^*(C_m \oplus C_m) = 3m + 1$ and $\eta_0^*(C_n \oplus C_n) = 3n + 1$, then $\eta_0^*(G) = 3mn + 1$.*

Proof. The proof of (2) runs along the same lines as the proof of (1)(a). Thus we show only (1).

(1) By Proposition 3.10(2), it suffices to prove that $\eta^*(G) \leq 3mn + 1$. Let $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a squarefree type of length $|S| = l = 3mn + 1$, which has pairwise distinct labels. We have to show that S has two short minimal zero-sum subtypes which are not coprime. Let $\varphi : G \to G$ denote the multiplication by m. Then $\mathrm{Ker}(\varphi) \cong C_m^2$ and $\varphi(G) = mG \cong C_n^2$.

We set $S = g_1 \cdot \ldots \cdot g_l$, where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G^\bullet \times \mathbb{N}$, such that for some $t \in [0, l]$ we have $\overline{\varphi}(g_i) = 0$ for all $i \in [1, t]$ and $\overline{\varphi}(g_i) \neq 0$ for all $i \in [t + 1, l]$. If $t \geq 3m + 1 = \eta^*(\mathrm{Ker}(\varphi))$, then $g_1 \cdot \ldots \cdot g_t \in \mathcal{F}(\mathrm{Ker}(\varphi) \times \mathbb{N})$ has two short minimal zero-sum subtypes which are not coprime. So we may suppose that $t \in [0, 3m]$.

Let $r \in \mathbb{N}_0$ and let $B_1, \ldots, B_r$ be all short minimal zero-sum subtypes of $g_1 \cdot \ldots \cdot g_t$. If two of them are not coprime, then we are done. Otherwise, $B_1 \cdot \ldots \cdot B_r \mid g_1 \cdot \ldots \cdot g_t$, and for every $\nu \in [1, r]$ we choose an element $\tau_\nu \in \mathrm{supp}(B_\nu)$. It follows that $g_1 \cdot \ldots \cdot g_t (\tau_1 \cdot \ldots \cdot \tau_r)^{-1}$ has no short zero-sum subtype. Since $|B_\nu| \geq 2$ for all $\nu \in [1, r]$, we infer that $r \leq t/2$. Let $u_0 = |g_1 \cdot \ldots \cdot g_t (\tau_1 \cdot \ldots \cdot \tau_r)^{-1}| = t - r$. After renumbering if necessary we may assume $g_1 \cdot \ldots \cdot g_{u_0} = g_1 \cdot \ldots \cdot g_t (\tau_1 \cdot \ldots \cdot \tau_r)^{-1}$. We set

$$S_\nu = g_\nu \quad \text{for every } \nu \in [1, u_0], \text{ and note that } u_0 \in [t/2, t]. \tag{3.1}$$

(1)(a) Let $u_1 \in \mathbb{N}_0$ be maximal such that there are types $S_{u_0+1}, \ldots, S_{u_0+u_1} \in \mathcal{F}(G^\bullet \times \mathbb{N})$ with the following properties.

- $S_1 \cdot \ldots \cdot S_{u_0+u_1} \mid S$.
- For every $\nu \in [1, u_0 + u_1]$, $\overline{\varphi}(S_\nu)$ is a short zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

Lemma 3.6 implies that $\eta(\mathrm{Ker}(\varphi)) = 3m - 2$ and hence $u_0 + u_1 \in [0, 3m - 3]$. Note that the number of nonzero terms in $\overline{\varphi}(S(S_1 \cdot \ldots \cdot S_{u_0+u_1})^{-1})$ is equal to

$$\begin{aligned}
&|S(g_1 \cdot \ldots \cdot g_t)^{-1}(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}| \\
&\quad \geq l - t - (3m - 3 - u_0)n \\
&\quad \geq 3mn + 1 - (3m - 3)n + u_0 n - t \geq 3n + 1.
\end{aligned}$$

Since $\eta^*(\varphi(G)) = 3n + 1$, there are subtypes T_1 and T_2 of $S(S_1 \cdot \ldots \cdot S_u)^{-1}$ such that $\varphi(T_1), \varphi(T_2) \in \mathcal{F}(\varphi(G)^\bullet \times \mathbb{N})$ are two short minimal zero-sum types which are not coprime. Since u_1 is maximal, Lemma 3.14 implies that S has two short minimal zero-sum subtypes which are not coprime.

(1)(b) The proof of (1)(b) uses the same ideas as the proof of (1)(a). But since it is of higher technical complexity we discuss its strategy before going into details. We will always use Lemma 3.14 which requires the construction of an integer $u \in \mathbb{N}_0$ and of types $S_1, \ldots, S_u$ satisfying the given conditions. In order to obtain the types T_1 and T_2 we proceed as follows. We have to find a subtype T of $S(S_1 \cdot \ldots \cdot S_u)^{-1}$ such that $\varphi(T) \in \mathcal{F}(\varphi(G)^\bullet \times \mathbb{N})$ has two short minimal zero-sum subtypes which are not coprime. This is guaranteed in each of the following cases.

- $|\varphi(T)| \geq \eta^*(\varphi(G))$. Note that $\varphi(G) \cong C_p \oplus C_p$, and that by Lemma 3.6 and Proposition 3.10(1), $\eta^* C_p \oplus C_p) \leq 6p - 5$.
- There is an element $a \in \varphi(G)^\bullet$ such that $\mathsf{v}_a(\overline{\varphi}(T)) > \mathrm{ord}(a) = p$.
- The group $\varphi(G)$ and the type $\varphi(T)$ satisfy the assumptions of Lemma 3.13.
- The sequence $\overline{\varphi}(T)$ has a short minimal zero-sum subsequence $\xi_1^{\ell_1}\xi_2^{\ell_2}\xi_3^{\ell_3}$, and $\xi_1^{\ell_1}\xi_2^{\ell_2}\xi_3^{\ell_3+1}$ is also a subsequence of $\overline{\varphi}(T)$.

We will proceed by constradiction, and hence during the constructions we can alwayss assume that a given subtype $\varphi(T) \in \mathcal{F}(\varphi(G)^\bullet \times \mathbb{N})$ does not have any of the above properties. In particular, Lemma 3.14 is used as follows: since condition (c) in Lemma 3.14 does not hold, we obtain (step by step) types satisfying conditions (i)–(iii) in Lemma 3.14.

Now let $\gcd(6, m) = 1$ and let $n = p$ be a prime with $m \geq 33p^3/4$. By (1)(a) and Proposition 3.12, we may suppose that $p \geq 11$, and we assume to the contrary that S does not have two short minimal zero-sum subtypes which are not coprime. We set

$$W = S(g_1 \cdot \ldots \cdot g_t)^{-1} \quad \text{and} \quad \overline{\varphi}(W) = e_1^{r_1} \cdot \ldots \cdot e_k^{r_k}, \tag{3.2}$$

where $e_1, \ldots, e_k \in \varphi(G)$ are distinct and $r_1, \ldots, r_k \in \mathbb{N}$. For every $i \in [1, k]$, let W_{e_i} denote the subtype of W with $\overline{\varphi}(W_{e_i}) = e_i^{r_i}$. After renumbering if necessary there is some $f \in [0, k]$ such that $r_i \geq (6p-6)(p-2)+1$ for $i \in [1, f]$ and $r_j \leq (6p-6)(p-2)$ for every $i \in [f+1, k]$. We continue with the following assertion.

Assertion A1. $f \geq 2$.

Proof of Assertion A1. By rearranging if necessary we may assume that $r_1 = \max\{r_i \,|\, i \in [1, k]\}$. We assert that $r_1 \leq 2mp + 2m - 4$. If this holds, then

$$\max\{r_i \,|\, i \in [2, k]\} \geq \frac{|S| - t - \mathsf{v}_{e_1}(\overline{\varphi}(W))}{|\varphi(G) \backslash \{0, e_1\}|} \geq \frac{3mp + 1 - 3m - (2mp + 2m - 4)}{p^2 - 2}$$
$$\geq (6p - 6)(p - 2) + 1,$$

and hence $f \geq 2$. Assume to the contrary that $r_1 \geq 2mp + 2m - 3$. Then $W_{e_1} = (g + h_1) \cdot \ldots \cdot (g + h_v)$ where $g \in G \times \mathbb{N}$ with $\overline{\varphi}(g) = e_1$, $h_1, \ldots, h_v \in \mathrm{Ker}(\varphi) \times \mathbb{N}$ and $v \geq 2mp + 2m - 3$. Let $U_1, \ldots, U_\ell$ be all short minimal zero-sum subtypes of W_{e_1}.

By our assumption on S, they are pairwise coprime and hence $U_1 \cdot \ldots \cdot U_\ell \,|\, W_{e_1}$. For every $\nu \in [1,\ell]$, we choose an element $x_\nu \in \mathrm{supp}(U_\nu)$, and clearly we have $|U_\nu| \ge 2$ which implies that $\ell \le \frac{|W_{e_1}|}{2}$. Then $W_{e_1}(x_1 \cdot \ldots \cdot x_\ell)^{-1}$ has no short zero-sum subtype, and $|W_{e_1}(x_1 \cdot \ldots \cdot x_\ell)^{-1}| \ge v/2 \ge mp + m - 3/2$. After renumbering if necessary, we may assume that $W_{e_1}(x_1 \cdot \ldots \cdot x_\ell)^{-1} = (g+h_1) \cdot \ldots \cdot (g+h_{v-\ell})$. Note that $v - \ell \ge mp + m - 3/2 \ge 4m - 3$. Since, by Lemma 3.6, $\mathsf{s}(\mathrm{Ker}(\varphi)) = 4m-3$, the type $h_1 \cdot \ldots \cdot h_v \in \mathcal{F}(\mathrm{Ker}(\varphi) \times \mathbb{N})$ may be written as

$$h_1 \cdot \ldots \cdot h_v = V_1 \cdot \ldots \cdot V_{2p-1} V',$$

where $V', V_1, \ldots, V_{2p-1} \in \mathcal{F}(\mathrm{Ker}(\varphi) \times \mathbb{N})$ and, for every $\nu \in [1, 2p-1]$, V_ν has sum zero and length $|V_\nu| = m$. Furthermore, we suppose that $V_1 \,|\, h_1 \cdot \ldots \cdot h_{v-\ell}$. We set $W_1 = \prod_{\nu=1}^{p}(g+V_\nu)$ and $W_2 = (g+V_1)\prod_{\nu=p+1}^{2p-1}(g+V_\nu)$. Note that

$$\overline{\sigma}(W_1) = mp\boldsymbol{\alpha}(g) + \sum_{\nu=1}^{p}\overline{\sigma}(V_\nu) = 0 = mp\boldsymbol{\alpha}(g) + \overline{\sigma}(V_1) + \sum_{\nu=p+1}^{2p-1}\overline{\sigma}(V_\nu) = \overline{\sigma}(W_2),$$

and that $g + V_1 = \gcd(W_1, W_2)$. Since $g + V_1 \,|\, W_{e_1}(x_1 \cdot \ldots \cdot x_\ell)^{-1}$, it follows that $g + V_1$ is zero-sum free. Therefore, there exist two short minimal zero-sum subtypes T_1 and T_2, $T_1 \,|\, W_1$ and $T_2 \,|\, W_2$, which are not coprime, a contradiction. □

We set

$$W' = \prod_{i=1}^{f} W_{e_i}, \quad W'' = \prod_{i=f+1}^{k} W_{e_i} \quad \text{and then} \quad W = W'W''. \tag{3.3}$$

Case 1. There exist distinct $i, j \in [1, f]$ such that the sequence $e_i^{p-1}e_j^{p-1}$ has a short zero-sum subsequence.

After renumbering if necessary, we may suppose that $i = 1$ and $j = 2$. A short zero-sum subsequence of $e_1^{p-1}e_2^{p-1}$ over $\varphi(G) \cong C_p \oplus C_p$ must be the form $e_1^{\epsilon_1}e_2^{\epsilon_2}$ with $\epsilon_1, \epsilon_2 \in [1, p-1]$ and $\epsilon_1 + \epsilon_2 \le p$. Moreover, if $\epsilon_1 + \epsilon_2 = p$, then it follows that $\epsilon_1(e_1 - e_2) = 0$ and hence $e_1 - e_2 = 0$, a contradiction. Thus $\epsilon_1 + \epsilon_2 < p$.

Let $u_1 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+1}, \ldots, S_{u_0+u_1}$ with the following properties.

- $S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1} \,|\, W_{e_1}W_{e_2}$.
- For every $\nu \in [1, u_1]$, $\overline{\varphi}(S_{u_0+\nu}) = {e_1}^{\epsilon_1}{e_2}^{\epsilon_2}$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We consider the type

$$W_0 = W(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1} = S(g_1 \cdot \ldots \cdot g_t S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}.$$

First, suppose that $\min\{\mathsf{v}_{e_1}(\overline{\varphi}(W_0)), \mathsf{v}_{e_2}(\overline{\varphi}(W_0))\} \ge p-1$. Then there are types T_1, T_2 dividing W_0 such that $\varphi(T_1)$ and $\varphi(T_2)$ are two short minimal zero-sum types which are not coprime. Thus Lemma 3.14 implies that S has two short minimal zero-sum subtypes which are not coprime, a contradiction.

Thus from now on, we may suppose that $\min\{\mathsf{v}_{e_1}(\overline{\varphi}(W_0)), \mathsf{v}_{e_2}(\overline{\varphi}(W_0))\} < p-1$. We obtain that

$$u_1 \geq \frac{\min\{\mathsf{v}_{e_1}(\overline{\varphi}(W)), \mathsf{v}_{e_2}(\overline{\varphi}(W))\} - (p-2)}{\max\{\epsilon_1, \epsilon_2\}} \geq \frac{(6p-6)(p-2)+1-(p-2)}{p-2}$$
$$> 6p-7.$$

Let $u_2 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+u_1+1}, \ldots, S_{u_0+u_1+u_2}$ with the following properties.

- $S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2} \mid S(S_1 \cdot \ldots \cdot S_{u_0+u_1})^{-1}$.
- For every $\nu \in [1, u_2]$, $\overline{\varphi}(S_{u_0+u_1+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

Since $\eta(\mathrm{Ker}(\varphi)) = 3m-2$, we infer that $u_0+u_1+u_2 \leq 3m-3$. Since $|S_{u_0+\nu}| \leq p-1$ for each $\nu \in [1, u_1]$ and $u_1 \geq 6p-6$, we obtain that

$$\begin{aligned}
&|S(g_1 \cdot \ldots \cdot g_t S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1} S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2})^{-1}| \\
&\quad \geq 3mp+1-t-(3m-3-u_0)p+6p-6 \\
&\quad \geq 3mp+1-(3m-3)p+6p-6 \geq 6p-5.
\end{aligned}$$

Again by using Lemma 3.14 we infer that S has two short minimal zero-sum subtypes which are not coprime, a contradiction.

Case 2. For every distinct $i, j \in [1, f]$ the sequence $e_i^{p-1} e_j^{p-1}$ has no short zero-sum subsequence.

We continue with the following four assertions on the structure of the types $W_{e_1}, \ldots, W_{e_k}$.

Assertion A2. Let $i \in [1, k]$ with $r_i \geq p+4$. Then $|\mathrm{supp}(\boldsymbol{\alpha}(W_{e_i}))| \leq 4$.
Assertion A3. Let $i \in [1, k]$ with $r_i \geq p+4$. Then $|\mathrm{supp}(\boldsymbol{\alpha}(W_{e_i}))| \leq 3$.
Assertion A4. Let $i \in [1, k]$ with $|W_{e_i}| \geq p+4$. Then $W_{e_i} = \xi_{i,1} \cdot \ldots \cdot \xi_{i,w_i} W_i'$ where $\boldsymbol{\alpha}(\xi_{i,1}) = \cdots = \boldsymbol{\alpha}(\xi_{i,w_i}) = \xi_i \in G$ and $|W_i'| \leq 4$.
Assertion A5. $|\,\mathrm{supp}(\sigma(\xi_1^p) \cdot \ldots \cdot \sigma(\xi_f^p))| \geq 3$.

Proof of Assertion A2. Assume to the contrary that $|\,\mathrm{supp}(\boldsymbol{\alpha}(W_{e_i}))| \geq 5$. Let $x_1, x_2, x_3, x_4, x_5 \in \mathrm{supp}(W_{e_i})$ such that $\boldsymbol{\alpha}(x_1), \ldots, \boldsymbol{\alpha}(x_5)$ are pairwise distinct, and let Z be a subtype of $W_{e_i}(x_1x_2x_3x_4x_5)^{-1}$ with $|Z| = p-1$. We set

$$W_1 = W \,\mathrm{lcm}(x_1 \cdot \ldots \cdot x_5 Z, W_{e_1}, W_{e_2})^{-1} \quad \text{and} \quad W_1' = W W_1^{-1}.$$

Let $u_1 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+1}, \ldots, S_{u_0+u_1}$ with the following properties.

- $S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1} \,|\, W_1$.
- For every $\nu \in [1, u_1]$, $\overline{\varphi}(S_{u_0+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

If $|W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}| \geq 6p-5$, then S has two short minimal zero-sum subtypes which are not coprime, a contradiction. Thus we may assume that

$$|W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}| \leq 6p-6.$$

Write $W_1' = (x_1 \cdot \ldots \cdot x_5 Z)TW_2$, where T is a subtype of W_1' with $\overline{\varphi}(T) = e_1^{4p-6}e_2^{4p-6}$. Now we apply (step by step) Lemma 3.13(a) (to the group $\varphi(G)$ and some types UV with $U \,|\, W_2, V \,|\, W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}$, $|V| = 2p-1$ and $\overline{\varphi}(U) = e_1^p e_2^p$) and Lemma 3.14 to obtain a maximal $u_2 \in \mathbb{N}_0$ such that there exist types $S_{u_0+u_1+1}, \ldots, S_{u_0+u_1+u_2}$ with the following properties.

- $S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2} \,|\, W_2 W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}$.
- For every $\nu \in [1, u_2]$, $\overline{\varphi}(S_{u_0+u_1+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, u_2]$, $\gcd(S_{u_0+u_1+\nu}, W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}) \neq 1$ and $\gcd(S_{u_0+u_1+\nu}, W_2) \neq 1$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

Let W_1'' (respectively, W_2'') be the remaining subsequence of $W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}$ (respectively, W_2) after the construction of these S_ν with $\nu \in [u_0+u_1+1, u_0+u_1+u_2]$. Then,

$$W_2 W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1} = S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2} W_1'' W_2''.$$

Clearly, $\max\{\mathsf{v}_{e_1}(\overline{\varphi}(S_\nu)), \mathsf{v}_{e_2}(\overline{\varphi}(S_\nu))\} \leq p-2$ holds for every $\nu \in [u_0+u_1+1, u_0+u_1+u_2]$. But $\min\{\mathsf{v}_{e_1}(\overline{\varphi}(W_2)), \mathsf{v}_{e_2}(\overline{\varphi}(W_2))\} - (p-1) \geq \min\{r_i \,|\, i \in [1,f]\} - (4p-6) - (p-1) \geq (6p-6)(p-2) + 1 - (4p-6) - (p-1) > (4p-4)(p-2) \geq \big(|W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}| - (2p-2)\big)(p-2)$. These show that if $|W_1''| \geq 2p-1$, then the construction of S_ν in the way above could be continued, a contraction to the maximality of u_2. Hence,

$$|W_1''| \leq 2p-2.$$

Let $u_3 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+u_1+u_2+1}, \ldots, S_{u_0+u_1+u_2+u_3}$ with the following properties.

- $S_{u_0+u_1+u_2+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3} \,|\, W_2''$.
- For every $\nu \in [1, u_3]$, $\overline{\varphi}(S_{u_0+u_1+u_2+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.

- For every $\nu \in [1, u_3]$, $\overline{\varphi}(S_{u_0+u_1+u_2+\nu}) \in \{e_1^p, e_2^p\}$.
- The sequence $\overline{\sigma}(S_1)\cdot\ldots\cdot\overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1})\cdot\ldots\cdot\overline{\sigma}(S_{u_0+u_1+u_2+u_3}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set

$$W_2''' = W_2''(S_{u_0+u_1+u_2+1}\cdot\ldots\cdot S_{u_0+u_1+u_2+u_3})^{-1}.$$

If $\max\{\mathsf{v}_{e_1}(\overline{\varphi}(W_2''')), \mathsf{v}_{e_2}(\overline{\varphi}(W_2'''))\} \ge p+1$, then S has two short minimal zero-sum subtypes which are not coprime, a contradiction. Thus we obtain that $\max\{\mathsf{v}_{e_1}(\overline{\varphi}(W_2''')), \mathsf{v}_{e_2}(\overline{\varphi}(W_2'''))\} \le p$, which implies that $|W_2'''| \le 2p$. Now we have that

$$u_0+u_1+u_2+u_3 \ge u_0 + \frac{|S| - t - |W_2'''| - |W_1''| - |T| - |x_1\cdot\ldots\cdot x_5 Z|}{p} \ge 2m-1.$$

Since $\overline{\sigma}(S_1)\cdot\ldots\cdot\overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1})\cdot\ldots\cdot\overline{\sigma}(S_{u_0+u_1+u_2+u_3}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence, we infer that $|\operatorname{supp}(\overline{\sigma}(S_1)\cdot\ldots\cdot\overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1})\cdot\ldots\cdot\overline{\sigma}(S_{u_0+u_1+u_2+u_3}))| \ge 3$, and we can choose three distinct elements α, β, γ in this set. Since the elements $\boldsymbol{\alpha}(x_1+\sigma(Z)), \ldots, \boldsymbol{\alpha}(x_5+\sigma(Z))$ are pairwise distinct, we may assume — after renumbering if necessary — that $\boldsymbol{\alpha}(x_1+\sigma(Z)), \boldsymbol{\alpha}(x_2+\sigma(Z)) \notin \{\alpha,\beta,\gamma\}$. Since x_1Z and x_2Z are two short minimal zero-sum subtypes over $\varphi(G) \cong C_p \oplus C_p$ and S does not have two short minimal zero-sum subtypes, so we may assume that the sequence $\overline{\sigma}(S_1)\cdot\ldots\cdot\overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1})\cdot\ldots\cdot\overline{\sigma}(S_{u_0+u_1+u_2+u_3})\overline{\sigma}(x_1Z) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence. Now we have

$$|\operatorname{supp}(\overline{\sigma}(S_1)\cdot\ldots\cdot\overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1})\cdot\ldots\cdot\overline{\sigma}(S_{u_0+u_1+u_2+u_3})\overline{\sigma}(x_1Z))| \ge 4,$$

and we set $S_{u_0+u_1+u_2+u_3+1} = x_1Z$.

Again we apply (step by step) Lemma 3.13 (to the group $\varphi(G)$; note that $e_1^{p-1}e_2^{p-1}$ has no short zero-sum subsequence) and Lemma 3.14, to obtain a maximal $u_4 \in \mathbb{N}_0$ such that there exist types $S_{u_0+u_1+u_2+u_3+2}, \ldots, S_{u_0+u_1+u_2+u_3+u_4}$ with the following properties.

- $S_{u_0+u_1+u_2+u_3+2}\cdot\ldots\cdot S_{u_0+u_1+u_2+u_3+u_4} \,|\, TW_2'''W_1''(x_2x_3x_4x_5)$.
- For every $\nu \in [2, u_4]$, $\overline{\varphi}(S_{u_0+u_1+u_2+u_3+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [2, u_4]$, $\gcd(S_{u_0+u_1+u_2+u_3+\nu}, W_1''(x_2x_3x_4x_5)) \ne 1$ and $\gcd(S_{u_0+u_1+u_2+u_3+\nu}, TW_2''') \ne 1$.
- The sequence $\overline{\sigma}(S_1)\cdot\ldots\cdot\overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1})\cdot\ldots\cdot\overline{\sigma}(S_{u_0+u_1+u_2+u_3+u_4}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

Let T' (respectively, W_1''') be the remaining subtype of TW_2''' (respectively, $W_1''(x_2x_3x_4x_5)$) after the construction of these S_ν with $\nu \in [u_0+u_1+u_2+u_3+2, u_0+u_1+u_2+u_3+u_4]$. Then,

$$TW_2'''W_1''(x_2x_3x_4x_5) = S_{u_0+u_1+u_2+u_3+2}\cdot\ldots\cdot S_{u_0+u_1+u_2+u_3+u_4}T'W_1'''.$$

Obviously, for each $\nu \in [1, u_4']$ we have

$$\max\{\mathsf{v}_{e_1}(\overline{\varphi}(S_{u_0+u_1+u_2+u_3+\nu})), \mathsf{v}_{e_2}(\overline{\varphi}(S_{u_0+u_1+u_2+u_3+\nu}))\} \le p-2.$$

Note that $\overline{\varphi}(T) = e_1^{4p-6}e_2^{4p-6}$, $\overline{\varphi}(T') = e_1^c e_2^d$, and similarly to the argument for W_1'' we may assume that $|W_1'''| \le 2p-2$. Let $u_5 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+u_1+u_2+u_3+u_4+1}, \ldots, S_{u_0+u_1+u_2+u_3+u_4+u_5}$ with the following properties.

- $S_{u_0+u_1+u_2+u_3+u_4+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3+u_4+u_5} \,|\, T'$.
- For every $\nu \in [1, u_5]$, $\overline{\varphi}(S_{u_0+u_1+u_2+u_3+u_4+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, u_5]$, $\overline{\varphi}(S_{u_0+u_1+u_2+u_3+u_4+\nu}) \in \{e_1^p, e_2^p\}$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3+u_4+u_5}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set

$$T'' = T'(S_{u_0+u_1+u_2+u_3+u_4+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3+u_4+u_5})^{-1}.$$

Since S does not have two short minimal zero-sum subtypes which are not coprime, we infer that $\max\{\mathsf{v}_{e_1}(\overline{\varphi}(T'')), \mathsf{v}_{e_1}(\overline{\varphi}(T''))\} \le p$ and hence $|T''| \le 2p$. Since $|W_1'''T''| \le 4p-2$, it follows that

$$\begin{aligned} u_0 &+ u_1 + u_2 + u_3 + u_4 + u_5 \\ &\ge u_0 + \frac{|S| - t - |W_1'''T''|}{p} \ge u_0 + \frac{3mp + 1 - t - 4p + 2}{p} \\ &= 3m - 4 + \frac{u_0 p - t + 3}{p} = 3m - 4 + \frac{tp/2 - t + 3}{p} > 3m - 4. \end{aligned}$$

Now we have

$$|\operatorname{supp}(\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3+u_4+u_5}))| \ge 4,$$

and

$$|\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3+u_4+u_5})| \ge 3m - 3.$$

Thus Lemma 3.7 implies that the sequence

$$\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3+u_4+u_5})$$

has a short zero-sum subsequence, a contradiction. □

Proof of Assertion A3. By Assertion A2 we have $|\operatorname{supp}(\boldsymbol{\alpha}(W_{e_i}))| \le 4$, and hence there exists some element $y \in G$ with $\mathsf{v}_y(\boldsymbol{\alpha}(W_{e_i})) \ge \frac{p+4}{4} \ge 3$. Assume to the contrary that $|\operatorname{supp}(\boldsymbol{\alpha}(W_{e_i}))| = 4$, and let $y_1, y_2, y_3, y_4 \in \operatorname{supp}(W_{e_i})$ such that $\boldsymbol{\alpha}(y_1), \ldots, \boldsymbol{\alpha}(y_4)$ are pairwise distinct, and let y' and y'' be two distinct elements of $W_{e_i}(y_1y_2y_3y_4)^{-1}$ with $\boldsymbol{\alpha}(y') = \boldsymbol{\alpha}(y'') = y$. We can simply repeat the proof of Assertion A2: we only have to replace the sequence $x_1 \cdot \ldots \cdot x_5 Z$ by $y_1 \cdot \ldots \cdot y_4 Z' y' y''$, where Z' is a subtype of $W_{e_i}(y_1 \cdot \ldots \cdot y_4 y' y'')^{-1}$ of length $|Z'| = p - 2$. $\square$

Proof of Assertion A4. By Assertion A3 we have $|\mathrm{supp}(\boldsymbol{\alpha}(W_{e_i}))| \le 3$, and hence it suffices to prove that there exists at most one element $z \in G^\bullet \times \mathbb{N}$ with $\mathsf{v}_{\boldsymbol{\alpha}(z)}(\boldsymbol{\alpha}(W_{e_i}) \ge 3$. Assume to the contrary that there are two elements z_1 and z_2 such that $\boldsymbol{\alpha}(z_1)$ and $\boldsymbol{\alpha}(z_2)$ are distinct and $\mathsf{v}_{\boldsymbol{\alpha}(z_1)}(W_{e_i}) \ge \mathsf{v}_{\boldsymbol{\alpha}(z_2)}(W_{e_i})) \ge 3$. Let z_1', z_1'', z_2', z_2'' be four distinct elements of $W_{e_i}(z_1z_2)^{-1}$ with $\boldsymbol{\alpha}(z_1') = \boldsymbol{\alpha}(z_1'') = \boldsymbol{\alpha}(z_1)$ and $\boldsymbol{\alpha}(z_2') = \boldsymbol{\alpha}(z_2'') = \boldsymbol{\alpha}(z_2)$. Since $\gcd(m, 6) = 1$, the sums $\overline{\sigma}(z_1z_1'z_1''), \overline{\sigma}(z_1z_1''z_2), \overline{\sigma}(z_1z_2z_2')$ and $\overline{\sigma}(z_2z_2'z_2'')$ are distinct. Let z', z'' be two distinct elements of $W_{e_i}(z_1z_1'z_1''z_2z_2'z_2'')^{-1}$ with $\boldsymbol{\alpha}(z') = \boldsymbol{\alpha}(z'')$. Let Z'' be a subtype of $W_{e_i}(z_1z_1'z_1''z_2z_2'z_2''z'z'')^{-1}$ of length $|Z''| = p - 4$. Considering the type $z_1z_1'z_1''z_2z_2'z_2''z'z''Z''$ instead of $x_1 \cdot \ldots \cdot x_5 Z$, we can derive a contradiction as in the proof of Assertion A2. $\square$

Proof of Assertion A5. By using Lemma 3.14 repeatedly to the type $\prod_{i=1}^{f} \prod_{\nu=1}^{w_i} \xi_{i,\nu}$, we find a maximal $w \in \mathbb{N}_0$ such that there exist types $T_1, \ldots, T_w$ with the following properties.

- $T_1 \cdot \ldots \cdot T_w \mid \prod_{i=1}^{f} \prod_{\nu=1}^{w_i} \xi_{i,\nu}$.
- For every $\nu \in [1, w]$, $\overline{\varphi}(T_\nu)$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, w]$, $\boldsymbol{\alpha}(T_\nu) \in \{\xi_1^p, \ldots, \xi_f^p\}$.
- The sequence $\overline{\sigma}(T_1) \cdot \ldots \cdot \overline{\sigma}(T_w) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set $R = \prod_{i=1}^{f} \prod_{\nu=1}^{w_i} \xi_{i,\nu}(T_1 \cdot \ldots \cdot T_w)^{-1}$, and observe that $\mathsf{v}_{\xi_i}(\boldsymbol{\alpha}(R)) \le p$ for every $i \in [1, f]$. Therefore,

$$\begin{aligned} w &\ge \frac{|S| - t - |\prod_{i=f+1}^{k} W_{e_i}| - |\prod_{i=1}^{f} W_i'| - fp}{p} \\ &\ge \frac{3mp + 1 - 3m - (p^2 - 1 - f)(6p - 6)(p - 2) - 4f - fp}{p} \\ &\ge 2m - 1. \quad \left(\text{Here we need that } m \ge \frac{33p^3}{4}.\right) \end{aligned}$$

Since $\overline{\sigma}(T_1) \cdot \ldots \cdot \overline{\sigma}(T_w) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence, we obtain that

$$|\,\mathrm{supp}(\sigma(\xi_1^p)\sigma(\xi_2^p) \cdot \ldots \cdot \sigma(\xi_f^p)| \ge 3. \qquad \square$$

Now we continue our proof by using the structural information obtained in Assertions A2–A5. We do not use any of the notations introduced in the proofs of Assertions A2–A5, but continue with the setting of (3.1)–(3.3).

After renumbering if necessary, we may suppose that $\sigma(\xi_1^p), \sigma(\xi_2^p)$ and $\sigma(\xi_3^p)$ are distinct. Let $u_1 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+1}, \ldots, S_{u_0+u_1}$ with the following properties.

- $S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1} \mid \prod_{i=4}^{k} W_{e_i}$.
- For every $\nu \in [1, u_1]$, $\overline{\varphi}(S_{u_0+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set

$$Q = \prod_{i=4}^{k} W_{e_i}(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1} \quad \text{and obtain that } |Q| \le 6p - 6.$$

We distinguish two cases.

Case 2.1: $e_1^{p-1}e_2^{p-1}e_3^{p-1} \in \mathcal{F}(\varphi(G))$ has no short zero-sum subsequence. We set $\boldsymbol{\alpha}(Q) = \theta_1 \cdot \ldots \cdot \theta_{u_2}$ with $u_2 = |Q| \le 6p - 6$. Since $\eta(C_p \oplus C_p) = 3p - 2$, for every $\nu \in [1, u_2]$, the sequence $e_1^{p-1}e_2^{p-1}e_3^{p-1}\theta_\nu$ has a short zero-sum subsequence containing θ_ν. Since each of r_1, r_2, r_3 is greater than or equal to $(6p-6)(p-2)+1$, we find (by using Lemma 3.14 step by step) u_2 types $S_{u_0+u_1+1}, \ldots, S_{u_0+u_1+u_2}$ with the following properties.

- $S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2} \mid QW_{e_1}W_{e_2}W_{e_3}$.
- For every $\nu \in [1, u_2]$, $\overline{\varphi}(S_{u_0+u_1+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, u_2]$, $\theta_\nu \mid \overline{\varphi}(S_{u_0+u_1+\nu}) \mid e_1^{p-1}e_2^{p-1}e_3^{p-1}\theta_\nu$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1})\overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set $Q' = QW_{e_1}W_{e_2}W_{e_3}(S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2})^{-1}$. Let $u_3 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+u_1+u_2+1}, \ldots, S_{u_0+u_1+u_2+u_3}$ with the following properties.

- $S_{u_0+u_1+u_2+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3} \mid Q'$.
- For every $\nu \in [1, u_3]$, $\overline{\varphi}(S_{u_0+u_1+u_2+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, u_3]$, $\overline{\varphi}(S_{u_0+u_1+u_2+\nu}) \in \{e_1^p, e_2^p, e_3^p\}$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0})\overline{\sigma}(S_{u_0+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1})\overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set $Q'' = Q'(S_{u_0+u_1+u_2+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3})^{-1}$ and observe that

$$\max\{\mathsf{v}_{e_1}(\overline{\varphi}(Q'')), \mathsf{v}_{e_3}(\overline{\varphi}(Q'')), \mathsf{v}_{e_3}(\overline{\varphi}(Q''))\} \le p,$$

which implies that $|Q''| \le 3p$. Therefore,

$$u_0 + u_1 + u_2 + u_3 \ge u_0 + \frac{|S| - t - |Q''|}{p} \ge 3m - 2 = \eta(\mathrm{Ker}(\varphi)),$$

a contradiction.

Case 2.2: $e_1^{p-1} e_2^{p-1} e_3^{p-1} \in \mathcal{F}(\varphi(G))$ has a short zero-sum subsequence. Let $e_1^{\ell_1} e_2^{\ell_2} e_3^{\ell_3}$ be a short minimal zero-sum subsequence of $e_1^{p-1} e_2^{p-1} e_3^{p-1}$, where $\ell_1, \ell_2, \ell_3 \in \mathbb{N}$ — recall that $e_i^{p-1} e_j^{p-1}$ has no short zero-sum subsequence for $i, j \in [1,3]$ — and $\ell_1 + \ell_2 + \ell_3 \in [3, p]$. According to Assertion A4 we have $W_{e_i} = \xi_{i,1} \cdot \ldots \cdot \xi_{i,w_i} W_i'$ where $|W_i'| \le 4$.

Applying Lemmas 3.13 and 3.14 to the types Q and $\prod_{\nu=1}^{w_1-\ell_1} \xi_{1,\nu} \prod_{\nu=1}^{w_2-\ell_2} \xi_{2,\nu}$, we find (step by step) a maximal $u_2 \in \mathbb{N}_0$ such that there exist types $S_{u_0+u_1+1}, \ldots, S_{u_0+u_1+u_2}$ with the following properties.

- $S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2} \mid Q \prod_{\nu=1}^{w_1-\ell_1} \xi_{1,\nu} \prod_{\nu=1}^{w_2-\ell_2} \xi_{2,\nu}$.
- For every $\nu \in [1, u_2]$, $\overline{\varphi}(S_{u_0+u_1+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, u_2]$, $\gcd(S_{u_0+u_1+\nu}, Q) \ne 1$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

After the construction of these S_ν for $\nu \in [1, u_2]$, let Q', W_{e_1}' and W_{e_2}' be the remaining subtypes of Q, $\prod_{\nu=1}^{w_1-\ell_1} \xi_{1,\nu}$ and $\prod_{\nu=1}^{w_2-\ell_2} \xi_{2,\nu}$, respectively. Then,

$$Q \prod_{\nu=1}^{w_1-\ell_1} \xi_{1,\nu} \prod_{\nu=1}^{w_2-\ell_2} \xi_{2,\nu} \left(S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2}\right)^{-1} = Q' W_{e_1}' W_{e_2}'.$$

We set

$$W_{e_3}' = \prod_{\nu=1}^{w_3-\ell_3-1} \xi_{3,\nu}.$$

Observe that $|Q'| \le 2p - 2$.

Applying Lemma 3.14 to $W_{e_1}' W_{e_2}' W_{e_3}'$, we find (step by step) a maximal $u_3 \in \mathbb{N}_0$ such that there exist types $S_{u_0+u_1+u_2+1}, \ldots, S_{u_0+u_1+u_2+u_3}$ with the following properties.

- $S_{u_0+u_1+u_2+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3} \mid W_{e_1}' W_{e_2}' W_{e_3}'$.
- For every $\nu \in [1, u_3]$, $\overline{\varphi}(S_{u_0+u_1+u_2+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, u_3]$, $\boldsymbol{\alpha}(S_{u_0+u_1+u_2+\nu}) \in \{\xi_1^p, \xi_2^p, \xi_3^p\}$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set

$$Q'' = (W'_{e_1} W'_{e_2} W'_{e_3} (S_{u_0+u_1+u_2+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u-3})^{-1}) \cdot \left(\prod_{i=1}^{2} \left(W'_i \prod_{\nu=w_i-\ell_i+1}^{w_i} \xi_{i,\nu} \right) \right) W'_3 \prod_{\nu=w_3-\ell_3}^{w_3} \xi_{3,\nu},$$

and observe that, for $i \in [1,2]$,

$$\mathsf{v}_{e_i}(\bar{\varphi}(Q'')) \le p + \ell_i + 4 \quad \text{and} \quad \mathsf{v}_{e_3}(\bar{\varphi}(Q'')) \le p + \ell_i + 5,$$

which implies that

$$|Q''| \le 4p + 13.$$

Now we have

$$u_0 + u_1 + u_2 + u_3 \ge u_0 + \frac{|S| - t - |Q'| - |Q''|}{p} > 3m - 7,$$

and we set

$$u_4 = 3m - 3 - (u_0 + u_1 + u_2 + u_3) \in [0,3].$$

Using Lemmas 3.13 and 3.14, we find types $S_{u_0+u_1+u_2+u_3+1}, \ldots, S_{u_0+u_1+u_2+u_3+u_4}$ with the following properties.

- $S_{u_0+u_1+u_2+u_3+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3+u_4} \mid Q'Q''$.
- For every $\nu \in [1, u_4]$, $\overline{\varphi}(S_{u_0+u_1+u_2+u_3+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- $\boldsymbol{\alpha}(S_{u_0+u_1+u_2+u_3+1}) = \xi_1^{\ell_1} \xi_2^{\ell_2} \xi_3^{\ell_3}$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3+u_4}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

By definition of u_4, we have $u_0 + u_1 + u_2 + u_3 + u_4 = 3m - 3$, and thus Lemma 3.7 implies that

$$\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3+u_4}) = (p\xi_1)^{m-1} (p\xi_2)^{m-1} (p\xi_3)^{m-1}.$$

It follows that $\overline{\sigma}(\xi_1^{\ell_1} \xi_2^{\ell_2} \xi_3^{\ell_3}) = p\xi_\varepsilon$ for some $\varepsilon \in [1,3]$, and we set

$$\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) = (p\xi_1)^{s_1} (p\xi_2)^{s_2} (p\xi_3)^{s_3},$$

and

$$\overline{\sigma}(S_{u_0+u_1+u_2+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3}) = (p\xi_1)^{t_1} (p\xi_2)^{t_2} (p\xi_3)^{t_3}.$$

Then $s_\varepsilon + t_\varepsilon \ge m - 1 - u_4 \ge m - 4$, and we set $v' = \mathsf{v}_{\xi_\varepsilon}(\boldsymbol{\alpha}(W'_{e_\varepsilon}))$. Now by the construction of the types $S_{u_0+u_1+u_2+1}, \ldots, S_{u_0+u_1+u_2+u_3}$ we deduce that

$$s_\varepsilon + \frac{v' - p - \ell_\varepsilon}{p} + 1 \ge m - 4.$$

In a further step, instead of constructing $S_{u_0+u_1+u_2+1}, \ldots, S_{u_0+u_1+u_2+u_3}$, we apply Lemma 3.14 to $W'_{e_1} W'_{e_2} W'_{e_3}$ and find a maximal $w \in \mathbb{N}_0$ such that there exist types $V_1, \ldots, V_w$ with the following properties:

- $V_1 \cdot \ldots \cdot V_w \,|\, W'_{e_1} W'_{e_2} W'_{e_3}$.
- For every $\nu \in [1, w]$, $\overline{\varphi}(V_\nu)$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, w]$, $\boldsymbol{\alpha}(V_\nu)$ is of the form $\xi_1^{\ell_1} \xi_2^{\ell_2} \xi_3^{\ell_3}$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \overline{\sigma}(V_1) \cdot \ldots \cdot \overline{\sigma}(V_w) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

We set $Q''' = W'_{e_1} W'_{e_2} W'_{e_3} (V_1 \cdot \ldots \cdot V_w)^{-1}$, $v_\varepsilon = \mathsf{v}_{\xi_\varepsilon}(\boldsymbol{\alpha}(Q'''))$ and $w' = \lfloor \frac{v_\varepsilon - 1}{p} \rfloor$. Using Lemma 3.14 again we find w' types $V_{w+1}, \ldots, V_{w+w'}$ with the properties.

- $V_{w+1} \cdot \ldots \cdot V_{w+w'} \,|\, Q'''$.
- For every $\nu \in [1, w']$, $\overline{\varphi}(V_{w+\nu})$ is a short minimal zero-sum sequence over $\varphi(G)$.
- For every $\nu \in [1, w']$, $\boldsymbol{\alpha}(V_{w+\nu}) \in \{\xi_1^p, \xi_2^p, \xi_3^p\}$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S''_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \overline{\sigma}(V_1) \cdot \ldots \cdot \overline{\sigma}(V_w) \overline{\sigma}(V_{w+1}) \cdot \ldots \cdot \overline{\sigma}(V_{w+w'}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no short zero-sum subsequence.

Let

$$\tau = \min\left\{ \left\lfloor \frac{|W'_{e_1} - 1}{\ell_1} \right\rfloor, \left\lfloor \frac{|W'_{e_2} - \ell_2}{\ell_2} \right\rfloor, \left\lfloor \frac{|W'_{e_3} - \ell_3}{\ell_3} \right\rfloor \right\}.$$

Now we have that $p\xi_\varepsilon$ occurs in

$$\begin{aligned} &\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0}) \overline{\sigma}(S_{u_0+1}) \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \\ &\cdot \overline{\sigma}(V_1) \cdot \ldots \cdot \overline{\sigma}(V_w) \overline{\sigma}(V_{w+1}) \cdot \ldots \cdot \overline{\sigma}(V_{w+w'}) \end{aligned}$$

at least $s_\varepsilon + \tau + \frac{v' - \ell_\varepsilon \tau - p}{p} \ge m$ times, a contradiction.

Corollary 3.16. *For every $m \in \mathbb{N}$ there exists a positive integer $n \in m\mathbb{N}$ such that $\eta^*(C_n \oplus C_n) = 3n + 1$.*

Proof. Let $m = 2^{k_1} 3^{k_2} 5^{k_3} 7^{k_4} p_1 \cdot \ldots \cdot p_s$ where $s, k_1, \ldots, k_4 \in \mathbb{N}_0$ and $p_1, \ldots, p_s \in \mathbb{P}$ with $p_1 \le \cdots \le p_s$. We set $n = m 5^{k'_3} 7^{k'_4}$ with $k'_3, k'_4 \in \mathbb{N}_0$ such that $5^{k_3+k'_3} 7^{k_4+k'_4} \ge 33 p_s^3/4$ (in the case $s = 0$ set $k'_3 = k'_4 = 0$). Using Proposition 3.12 and Theorem 3.15(1)(a) and (1)(b), we infer that $\eta^*(C_k \oplus C_k) = 3k + 1$ holds for $k \in \{5^{k_3+k'_3} 7^{k_4+k'_4}, 5^{k_3+k'_3} 7^{k_4+k'_4} p_1, \ldots, 5^{k_3+k'_3} 7^{k_4+k'_4} p_1 \cdot \ldots \cdot p_s, n = 2^{k_1} 3^{k_2} 5^{k_3+k'_3} 7^{k_4+k'_4} p_1 \cdot \ldots \cdot p_s\}$. $\square$

4. On $\mathsf{N}_1(G)$ for Groups of Rank Two

The main aim of this section is to prove the following theorem.

Theorem 4.1. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 < n_1 \mid n_2$. Suppose that for every prime divisor p of n_1 we have $\eta^*(C_p \oplus C_p) = 3p + 1$ and that $\mathsf{N}_1(C_p \oplus C_p) = 2p$.*

(1) $\mathsf{N}_1(C_{n_1} \oplus C_{n_1}) = 2n_1$.
(2) *If* $\mathsf{D}(C_{n_1}^3) \le 3n_1 - 1$, *then* $\mathsf{N}_1(G) = n_1 + n_2$.

We analyze the above result. First, note that a main standing conjecture on the Davenport constant states that

$$\mathsf{D}(C_n^3) = \mathsf{d}^*(G) + 1 = 3n - 2 \quad \text{for all } n \in \mathbb{N}$$

(see [6, Conjecture 3.5]), and this holds true if n is a prime power (see [14, Theorem 5.5.9]). Let G be as in Theorem 4.1. Then

$$n_1 + n_2 \le \mathsf{N}_1(G) \le n_1 + n_2 - 2 + \mathsf{ol}(G),$$

where the left inequality is obvious (see inequality (2.2)) and the right inequality is the best upper bound known so far (see [14, Proposition 6.2.26]). Here $\mathsf{ol}(G)$ denotes the Olson constant of the group G (for recent progress, see [1, 10, 33]). Now Theorem 4.1 reduces the determination of the precise value of $\mathsf{N}_1(G)$ for general groups of rank two to the verification of the corresponding conjectures for groups $C_p \oplus C_p$ where p is prime. For small primes we have $\eta^*(C_p \oplus C_p) = 3p + 1$ by Proposition 3.12, and furthermore it is well known — due to the first author — that for all primes p with $p \le 151$, we have $\mathsf{N}_1(C_p \oplus C_p) = 2p$ (see [14, Proposition 6.2.11]). This result, in combination with Theorem 3.15(1)(b), Corollary 3.16 and with the following multiplicity result for $\mathsf{N}_1(G)$, provides further groups for which $\mathsf{N}_1(C_n \oplus C_n) = 2n$ holds, which are not covered by Theorem 4.1.

Proposition 4.2. *Let $G = C_{mn} \oplus C_{mn}$ with $m, n \ge 2$. If $\mathsf{N}_1(C_m \oplus C_m) = 2m, \eta^*(C_n \oplus C_n) = 3n + 1$ and $\mathsf{N}_1(C_n \oplus C_n) = 2n$, then $\mathsf{N}_1(G) = 2mn$.*

Proof. By inequality (2.2) it suffices to prove that $\mathsf{N}_1(G) \le 2mn$. Let $\varphi\colon G \to G$ denote the multiplication by m. Then $\operatorname{Ker}(\varphi) \cong C_m^2$ and $\varphi(G) = mG \cong C_n^2$. Let $S \in \mathcal{T}(G^\bullet)$ be a squarefree type of length $|S| \ge 2mn + 1$, and without restrict we may assume that all labels are pairwise distinct (this implies in particular, that $\varphi(S)$ is squarefree too). We have to show that $|\mathsf{Z}(S)| > 1$. Assume to the contrary that $|\mathsf{Z}(S)| = 1$.

We set $S = g_1 \cdot \ldots \cdot g_l$, where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G^\bullet \times \mathbb{N}$, such that for some $t \in [0, l]$ we have $\overline{\varphi}(g_i) = 0$ for all $i \in [1, t]$ and $\overline{\varphi}(g_i) \ne 0$ for all $i \in [t+1, l]$. Suppose that $t \ge 2m+1$ and set $g_0 = (\overline{\sigma}(g_{2m+2} \cdot \ldots \cdot g_l), m_0)$, where $m_0 \in \mathbb{N}$ is chosen in such a way that $g_0 \nmid g_1 \cdot \ldots \cdot g_{2m+1}$. Then $\overline{\varphi}(g_0) = 0$ and $S' = g_0 \cdot \ldots \cdot g_{2m+1} \in \mathcal{T}(\operatorname{Ker}(\varphi))$ is squarefree. Since $|\mathsf{Z}(S)| = 1$, Lemma 3.9(2) (applied with $T = S, t = 2m + 2$,

$S_1 = g_1, \ldots, S_{2m+1} = g_{2m+1}$ and $S_{2m+2} = g_{2m+2} \cdot \ldots \cdot g_l$) implies that $|\mathsf{Z}(S')| = 1$, a contradiction to $|S'| > 2m = \mathsf{N}_1(\mathrm{Ker}(\varphi))$.

So we may suppose that $t \in [0, 2m]$, and we continue with the following assertion.

Assertion A. The type $g_1 \cdot \ldots \cdot g_t$ has a zero-sum free subtype T of length $|T| \geq \lceil \frac{t}{2} \rceil$.

Proof of Assertion A. If $t = 0$, then set $T = 1$. Suppose that $t \in [1, 2m]$. We write $g_1 \cdot \ldots \cdot g_t = U_0 U_1 \cdot \ldots \cdot U_f$ where $U_1, \ldots, U_f$ are minimal zero-sum types over $\mathrm{Ker}(\varphi)$ and U_0 zero-sum free. Since $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$, it follows that $|U_i| \geq 2$ for all $i \in [1, f]$. We choose an element $x_i \in \mathrm{supp}(U_i)$ for every $i \in [1, f]$. Since $|\mathsf{Z}(S)| = 1$, it follows that

$$g_1 \cdot \ldots \cdot g_t (x_1 \cdot \ldots \cdot x_f)^{-1} = U_0 (x_1^{-1} U_1) \cdot \ldots \cdot (x_f^{-1} U_f)$$

is zero-sum free, and obviously we have $|g_1 \cdot \ldots \cdot g_t (x_1 \cdot \ldots \cdot x_f)^{-1}| \geq \lceil \frac{t}{2} \rceil$. □

By Assertion A we may suppose without restriction that $g_1 \cdot \ldots \cdot g_{\lceil \frac{t}{2} \rceil}$ is zero-sum free, and we set $S_\nu = g_\nu$ for every $\nu \in [1, \lceil \frac{t}{2} \rceil]$. Let $u \in \mathbb{N}_0$ be maximal such that there exist types $S_{\lceil \frac{t}{2} \rceil + 1}, \ldots, S_u$ with the following properties.

- $S_{\lceil \frac{t}{2} \rceil + 1} \cdot \ldots \cdot S_u \mid S (S_1 \cdot \ldots \cdot S_{\lceil \frac{t}{2} \rceil})^{-1}$.
- For every $\nu \in [\lceil \frac{t}{2} \rceil + 1, u]$, $\overline{\varphi}(S_\nu)$ is a short zero sum sequence over $\varphi(G)$).
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is zero-sum free.

Since $\mathsf{D}(\mathrm{Ker}(\varphi)) = 2m - 1$, it follows that $u \leq 2m - 2$. We set $W = \gcd(S(S_1 \cdot \ldots \cdot S_u)^{-1}, g_{\lceil \frac{t}{2} \rceil + 1} \cdot \ldots \cdot g_l)$. Then W is the largest subtype of $S(S_1 \cdot \ldots \cdot S_u)^{-1}$ such that $\varphi(W) \in \mathcal{F}(G^\bullet \times \mathbb{N})$. Clearly, $\varphi(W)$ is squarefree, has sum zero and

$$\begin{aligned}
|\varphi(W)| &\geq |S| - |S_1 \cdot \ldots \cdot S_{\lceil \frac{t}{2} \rceil}| - |S_{\lceil \frac{t}{2} \rceil + 1} \cdot \ldots \cdot S_u| - \left(t - \left\lceil \frac{t}{2} \right\rceil \right) \\
&\geq (2mn + 1) - \left\lceil \frac{t}{2} \right\rceil - \left(u - \left\lceil \frac{t}{2} \right\rceil \right) n - \left(t - \left\lceil \frac{t}{2} \right\rceil \right) \\
&\geq \left(2m - u + \left\lceil \frac{t}{2} \right\rceil \right) n + 1 \geq (2m - u) n + 1.
\end{aligned}$$

We distinguish two cases.

Case 1: $u = 2m - 2$. Then $|W| \geq 2n + 1$. Since $\varphi(W) \in \mathcal{T}(\varphi(G)^\bullet)$ and $\mathsf{N}_1(\varphi(G)) = 2n$, Lemma 2.2 implies that W has two subtypes T_1 and T_2 such that $\varphi(T_1)$ and $\varphi(T_2)$ are two minimal zero-sum subtypes of $\varphi(W)$ which are not coprime. Let $\lambda \in [1, 2]$. Since $\mathsf{D}(\mathrm{Ker}(\varphi)) = 2m - 1$ and $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u)$ is zero-sum free, there exists a subset $I_\lambda \subset [1, u]$ such that $\overline{\sigma}(T_\lambda) \prod_{\nu \in I_\lambda} \overline{\sigma}(S_\nu)$ is a zero-sum sequence, and hence

$$T_\lambda V_\lambda, \quad \text{where } V_\lambda = \prod_{\nu \in I_\lambda} S_\nu,$$

is a zero-sum subtype of S. Since $|\mathsf{Z}(S)| = 1$, Lemma 2.2(c) implies that $\gcd(T_1V_1, T_2V_2) \in \mathcal{T}(G)$. Since $\gcd(T_i, V_j) = 1$ for all $i, j \in [1, 2]$, it follows that $\gcd(T_1V_1, T_2V_2) = \gcd(T_1, T_2)\gcd(V_1, V_2)$. Arguing as in the proof of Lemma 3.14, we infer that

$$\gcd(V_1, V_2) = \prod_{\nu \in I_1 \cap I_2} S_\nu \quad \text{and} \quad \overline{\sigma} \circ \varphi(\gcd(V_1, V_2)) = 0.$$

Thus we get

$$\begin{aligned} 0 &= \overline{\sigma}(\gcd(T_1V_1, T_2V_2)) = \varphi \circ \overline{\sigma}(\gcd(T_1V_1, T_2V_2)) \\ &= \overline{\sigma} \circ \varphi(\gcd(T_1V_1, T_2V_2)) = \overline{\sigma} \circ \varphi(\gcd(T_1, T_2)) = \overline{\sigma}(\gcd(\varphi(T_1), \varphi(T_2)). \end{aligned}$$

Since $\varphi(T_1)$ and $\varphi(T_2)$ are not coprime, their greatest common divisor is not trivial. But since it sums to zero, this is a contradiction to the minimality of $\varphi(T_1)$ and $\varphi(T_2)$.

Case 2: $u \le 2m - 3$. Then $|W| \ge 3n + 1 = \eta^*(\varphi(G))$. Thus W has two subtypes T_1 and T_2 such that $\varphi(T_1)$ and $\varphi(T_2)$ are two short minimal zero-sum types which are not coprime. Then Lemma 3.14 implies that S has two short minimal zero-sum subtypes which are not coprime, and hence $|\mathsf{Z}(S)| > 1$ by Lemma 2.2, a contradiction. □

Proof of Theorem 4.1. Theorem 3.15 implies that $\eta^*(C_{n_1} \oplus C_{n_1}) = 3n_1 + 1$. Thus the first statement follows from Proposition 4.2. Using the first statement and [14, Corollary 6.2.10] we obtain the second statement. □

5. On $\mathsf{N}_k(G)$ for Cyclic Groups and Elementary 2-Groups

In this section we establish two results. First, we show that in cyclic groups $\mathsf{N}_k(G)$ coincides with $\mathsf{N}_1(G)$ for large values of k (see Theorem 5.1). Second, we point out that this feature of cyclic groups is in sharp contrast to the behavior of the Narkiewicz constants in elementary 2-groups (see Theorem 5.3). Both proofs use ideas first developed in [5]. In the present paper we have the concept of type monoids at our disposal and, moreover, a result on the structure of long zero-sum free sequences which was recently established by Savchev and Chen in [36].

Theorem 5.1. *Let G be a cyclic group of order $n \ge 6$ and let $k \in \mathbb{N}$ with $k \le \frac{2 - \log_2 n + \sqrt{(\log_2 n)^2 + 2n - 18}}{2}$. Then $\mathsf{N}_k(G) = n$.*

We start with the the result by Savchev and Chen which we cite in a form given in [13, Theorem 5.1.8].

Lemma 5.2. *Let G be a cyclic group of order $n \ge 2$, and let S be a zero-sum free sequence over G of length $|S| = l \ge \frac{n+1}{2}$. Then there exists an element $g \in G$ with $\operatorname{ord}(g) = n$ such that*

$$S = (a_1 g) \cdot \ldots \cdot (a_l g),$$

where $1 = a_1 \le \cdots \le a_l \le n - 1$ and $\Sigma(S) = \{\nu g \mid \nu \in [1, a_1 + \cdots + a_l]\}$.

We will also need the following two elementary observations.

Lemma 5.3. *Let $A = a_1 \cdot \ldots \cdot a_\ell$ be a sequence of positive integers such that $a_1 + \cdots + a_\ell \le 2\ell - 1$. Then $\sum(A) = [1, a_1 + \cdots + a_\ell]$.*

Proof. For the proof we suppose that $1 \le a_1 \le \cdots \le a_\ell$ which implies that $a_1 = 1$. We proceed by induction on ℓ. If $\ell = 1$, then $A = 1$ and $\Sigma(A) = [1, 1]$. Suppose that $\ell \ge 2$. If $a_\ell = 1$, then $A = 1^\ell$ and $\Sigma(A) = [1, \ell]$. Suppose that $a_\ell \ge 2$, and set $A' = a_\ell^{-1} A$. Then $a_\ell \le \sigma(A') + 1$, $\sigma(A') \le 2\ell - 3$, and the induction hypothesis implies that $\Sigma(A') = [1, \sigma(A')]$. Therefore we obtain that

$$\begin{aligned}\Sigma(A) &= \Sigma(A') \cup \{a_\ell\} \cup (a_\ell + \Sigma(A')) \\ &= [1, \sigma(A')] \cup \{a_\ell\} \cup [a_\ell + 1, a_\ell + \sigma(A')] = [1, \sigma(A)].\end{aligned}$$

□

Lemma 5.4. *Let $n \ge 6$ and $A \in \mathcal{F}(\mathbb{N})$ be a sequence of positive integers of length $|A| = \ell \ge (n+2)/2$ and with $\sigma(A) < n$. Let $a \in \mathbb{N}$ denote the integer with $\mathsf{v}_a(A) = \max\{\mathsf{v}_g(A) \mid g \in \mathbb{N}\}$.*

(1) $\mathsf{v}_a(A) > n/6$.
(2) $a \in [1, 2]$.
(3) *If $x \in \Sigma(A)$ with $x \in [a+1, \sigma(A) - a]$, then $x = \sigma(aA')$ for some subsequence A' of A with $\mathsf{v}_a(A') \le \mathsf{v}_a(A) - 2$.*

Proof. (1) If $\mathsf{v}_a(A) \le n/6$, then

$$\begin{aligned}\sigma(A) &\ge \mathsf{v}_1(A) + 2\mathsf{v}_2(A) + 3(\ell - \mathsf{v}_1(A) - \mathsf{v}_2(A)) = 3\ell - 2\mathsf{v}_1(A) - \mathsf{v}_2(A) \\ &\ge 3\Big(\frac{n}{2}\Big) - 2\frac{n}{6} - \frac{n}{6} = n,\end{aligned}$$

a contradiction.

(2) If $a \ge 3$, then

$$\begin{aligned}\sigma(A) &\ge \mathsf{v}_1(A) + 2\mathsf{v}_2(A) + 3(\ell - \mathsf{v}_1(A) - \mathsf{v}_2(A)) = 3\ell - 2\mathsf{v}_1(A) - \mathsf{v}_2(A) \\ &= 2\ell + (\ell - \mathsf{v}_1(A) - \mathsf{v}_2(A)) - \mathsf{v}_1(A) \ge 2\ell + \mathsf{v}_a(A) - \mathsf{v}_1(A) \ge 2\ell \ge n,\end{aligned}$$

a contradiction.

(3) Since $n \ge 6$, we have $\mathsf{v}_a(A) \ge 2$, $|A| = \ell \ge 4$ and $\sigma(A) < n \le 2\ell - 2$. Therefore, $\sigma(Aa^{-2}) \le \sigma(A) - 2 \le 2\ell - 5 = 2(\ell - 2) - 1$, and Aa^{-2} satisfies the assumption of Lemma 5.3. Since $x - a \in [1, \sigma(A) - 2a] = \Sigma(Aa^{-2})$, it follows that $x - a = \sigma(A')$ for some subsequence A' of Aa^{-2}. □

We fix the notation which will be used in the subsequent lemmas and in the proof of Theorem 5.1. Let $k \in \mathbb{N}$, G be a finite abelian group with $|G| > 1$ and $T = g_1 \cdot \ldots \cdot g_l \in \mathcal{T}(G^\bullet)$ be squarefree with $|\mathsf{Z}(T)| = k$, where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G^\bullet \times \mathbb{N}$. For $\nu \in [1, k]$, let

$$z_\nu = U_{\nu,1} \cdot \ldots \cdot U_{\nu,r_\nu} \in \mathsf{Z}(T),$$

where, for all $\lambda \in [1, r_\nu]$,

$$U_{\nu,\lambda} = \prod_{i \in J_{\nu,\lambda}} g_i \in \mathcal{A}(\mathcal{T}(G^\bullet)) \quad \text{and} \quad [1, l] = J_{\nu,1} \uplus \ldots \uplus J_{\nu,r_\nu}.$$

Then $\mathsf{L}(T) = \{r_1, \ldots, r_k\}$, and we suppose that $r_1 = \max \mathsf{L}(T)$.

Lemma 5.5. *Let $k \in \mathbb{N}_{\ge 2}$ and $T \in \mathcal{T}(G^\bullet)$ be squarefree with $|\mathsf{Z}(T)| = k$. Then $\max \mathsf{L}(T) \le k - 1 + \log_2 |G|$.*

Proof. We assert that there exists a subset $\Lambda \subset [1, r_1]$ with $|\Lambda| \ge r_1 - k + 1$ such that

$$\prod_{\lambda \in \Lambda} U_{1,\lambda} \in \mathcal{T}(G)$$

has unique factorization. Suppose this holds true. Then Lemma 3.9(1) implies that

$$2^{|\Lambda|} \le \prod_{\lambda \in \Lambda} |U_{1,\lambda}| \le |G|.$$

Therefore we obtain $|\Lambda| \le \log_2 |G|$ and

$$\max \mathsf{L}(T) = r_1 \le |\Lambda| + k - 1 \le k - 1 + \log_2 |G|.$$

It remains to verify the existence of the set Λ. For every $i \in [2, k]$, there are $\alpha_i \in [1, r_1]$ and $\beta_i \in [1, r_i]$ such that $U_{1,\alpha_i} \ne U_{i,\beta_i}$. We set $\Lambda = [1, r_1] \setminus \{\alpha_i \mid i \in [2, k]\}$. Then $|\Lambda| \ge r_1 - (k - 1)$ and

$$\prod_{\lambda \in \Lambda} U_{1,\lambda} \in \mathcal{T}(G)$$

has unique factorization, since otherwise we would get $|\mathsf{Z}(T)| > k$. □

Lemma 5.6. *Let $k \in \mathbb{N}_{\ge 2}$ and $T \in \mathcal{T}(G^\bullet)$ be squarefree with $|\mathsf{Z}(T)| = k$. For $\nu \in [2, k]$ and for $\lambda \in [1, r_\nu]$, we define the set $I_\lambda = \{s \in [1, r_1] \mid J_{1,s} \cap J_{\nu,\lambda} \ne \emptyset\}$. Then the family $\{I_\lambda \mid \lambda \in [1, r_\nu]\}$ has a system of distinct representatives.*

Proof. Assume to the contrary that this does not hold. Then, by Hall's Theorem, there is a subset $\Omega \subset [1, r_\nu]$ such that for

$$I_\Omega = \bigcup_{\omega \in \Omega} I_\omega \quad \text{we have } |I_\Omega| < |\Omega|.$$

By definition of the sets I_λ, we get

$$\bigcup_{\omega \in \Omega} J_{\nu,\omega} \subset \bigcup_{i \in I_\Omega} J_{1,i},$$

and we set $J = \bigcup_{i \in I_\Omega} J_{1,i} \setminus \bigcup_{\omega \in \Omega} J_{\nu,\omega}$. Then it follows that

$$T = \left(\prod_{i \in J} g_i \right) \prod_{\omega \in \Omega} \left(\prod_{i \in J_{\nu,\omega}} g_i \right) \prod_{\lambda \in [1, r_1] \setminus I_\Omega} \left(\prod_{i \in J_{1,\lambda}} g_i \right)$$

is a product of at least $r_1 - |I_\Omega| + |\Omega| > r_1$ minimal zero-sum types, a contradiction to $r_1 = \max \mathsf{L}(T)$. $\square$

Lemma 5.7. *Let $T \in \mathcal{T}(G^\bullet)$ be squarefree with $|\mathsf{Z}(T)| = 2$. Then $|T| < \max \mathsf{L}(T) + \mathsf{D}(G)$.*

Proof. Let $\{I_\lambda \,|\, \lambda \in [1, r_2]\}$ be as in Lemma 5.6 and $(s_\lambda)_{\lambda \in [1,r_2]}$ be a system of distinct representatives. Then for every $\lambda \in [1, r_2]$ we have $J_{1,s_\lambda} \cap J_{2,\lambda} \neq \emptyset$, and for every $i \in [1, r_1]$ there is an $u_i \in J_{1,i}$ such that $u_{s_\lambda} \in J_{1,s_\lambda} \cap J_{2,\lambda}$. Now we set $\Lambda = [1, l] \backslash \{u_1, \ldots, u_{r_1}\}$. By construction, no non-empty subset $\Lambda' \subset \Lambda$ is a union of sets $J_{1,\lambda}$ with $\lambda \in [1, r_1]$, or of sets $J_{2,\lambda}$ with $\lambda \in [1, r_2]$. Since $|\mathsf{Z}(T)| = 2$, this implies that $\prod_{\lambda \in \Lambda} g_\lambda$ is zero-sum free and hence $|\Lambda| < \mathsf{D}(G)$. Thus we obtain that

$$|T| = l = |\Lambda| + r_1 < \mathsf{D}(G) + \max \mathsf{L}(T). \qquad \square$$

Proof of Theorem 5.1. Assume to the contrary that $\mathsf{N}_k(G) \neq n$. Since $n = \mathsf{N}_1(G) \le \cdots \le \mathsf{N}_k(G)$, we may set $\mathsf{N}_k(G) = n + 1 + t$ with $t \in \mathbb{N}_0$. We choose a squarefree $T \in \mathcal{T}(G^\bullet)$ with $|\mathsf{Z}(T)| \le k$ and $|T| = \mathsf{N}_k(G)$. Since $\mathsf{N}_1(G) = n$, it follows that $|\mathsf{Z}(T)| = k' \in [2, k]$. Then $\mathsf{N}_{k'}(G) = \mathsf{N}_k(G)$, and thus, after replacing k by k' if necessary, we may suppose that $|\mathsf{Z}(T)| = k$.

For $\lambda \in [1, r_2]$, we set $I_\lambda = \{s_\lambda \in [1, r_1] \,|\, J_{1,s_\lambda} \cap J_{2,\lambda} \neq \emptyset\}$, and by Lemma 5.6 we may choose a system of distinct representatives $(s_\lambda)_{\lambda \in [1,r_2]}$. Then for every $i \in [1, r_1]$ there is an $u_i \in J_{1,i}$ such that $u_{s_\lambda} \in J_{1,s_\lambda} \cap J_{2,\lambda}$. Therefore there is a subset $I \subset [1, l]$ with $|I| = r_1 + r_3 + \cdots + r_k$ such that $I \cap J_{\nu,j} \neq \emptyset$ for all $\nu \in [1, k]$ and all $j \in [1, r_\nu]$. Now we set $\Lambda = [1, l] \backslash I$. Since $|\mathsf{Z}(T)| = k$, the type $U = \prod_{\lambda \in \Lambda} g_\lambda$ is zero-sum free. Using Lemma 5.5 we obtain that

$$\begin{aligned} n - |U| = n - |\Lambda| &= n - (n + 1 + t - |I|) \le |I| - 1 = r_1 + r_3 + \cdots + r_k - 1 \\ &\le (k-1)r_1 - 1 \le (k-1)(k - 1 + \log_2 |G|) - 1 \\ &\le (\text{by our assumption on } k) \frac{n-11}{2}. \end{aligned}$$

Let R be a zero-sum free subsequence of $\boldsymbol{\alpha}(T)$ having maximal length. Then $|R| \ge |U| \ge \frac{n+11}{2}$, and we set $r = |R|$ and $s = |T| - r = n + 1 + t - r$. By Lemma 5.2 we may write

$$\boldsymbol{\alpha}(T) = (a_1 g) \cdot \ldots \cdot (a_r g)(b_1 g) \cdot \ldots \cdot (b_s g),$$

where $g \in G$ with $\operatorname{ord}(g) = n$, $a_i, b_j \in [1, n-1]$ and $\Sigma(A) = [1, \sigma(A)] \subset [1, n-1]$ with $A = a_1 \cdot \ldots \cdot a_r \in \mathcal{F}(\mathbb{N})$. Let $a \in \mathbb{N}$ with $\mathsf{v}_a(A) = \max\{\mathsf{v}_{a_i}(A) \,|\, i \in [1, r]\}$. By Lemma 5.4, we obtain that

$$a \in [1, 2] \quad \text{and} \quad \mathsf{v}_a(A) \ge \frac{n}{6} > k.$$

Assume to the contrary that $n - b_j \in [a+1, \sigma(A) - 2a]$. Then Lemma 5.4 implies that $n - b_j = a + \sigma(A')$ for some subsequence A' of A with $\mathsf{v}_a(A') \le \mathsf{v}_a(A) - 2$, and thus

$$b_j + (\mathsf{v}_a(A') + 1)a + \sigma(A' a^{-\mathsf{v}_a(A')}) = n. \tag{5.1}$$

Since $2 \le \mathsf{v}_a(A') + 1 \le \mathsf{v}_a(A) - 1$, we can choose the $(\mathsf{v}_a(A') + 1)a$'s in the left-hand side of (5.1) in at least $\binom{\mathsf{v}_a(A)}{\mathsf{v}_a(A')+1} \ge \mathsf{v}_a(A) \ge n/6 > k$ ways, a contradiction to $|\mathsf{Z}(T)| = k$. Therefore,

$$b_j \in [n-a, n-1] \cup [1, n - \sigma(A) + 2a].$$

If $b_{j_1}, b_{j_2} \in [1, n - \sigma(A) + 2a]$ for $j_1 \ne j_2$, then $2 \le b_{j_1} + b_{j_2} \le 2(n - \sigma(A) + 2a) \le n - 3 < n - a$. Arguing as above we can infer that $b_{j_1} + b_{j_2} \in [2, n - \sigma(A) + 2a]$. Repeating this argument we finally obtain

$$\sum_{j \in [1,s], b_j \le n - \sigma(A) + 2a} b_j \le n - \sigma(A) + 2a,$$

and hence

$$\sum_{i=1}^{r} a_i + \sum_{j \in [1,s], b_j \le n - \sigma(A) + 2a} b_j \le n + 2a. \tag{5.2}$$

Now we distinguish two cases.

Case 1: $a = 1$. If $b_j = n - 1$ for some $j \in [1, s]$, then T has at least $\mathsf{v}_1(A) \ge n/6 > k$ distinct factorizations, a contradiction. Therefore, $b_j \le n - \sigma(A) + 2$ holds for every $j \in [1, s]$, and (5.2) implies that $\sum_{i=1}^{r} a_i + \sum_{j=1}^{s} b_j \le n + 2$. Since $r + s \ge n + 1$, it follows that $\sum_{i=1}^{r} a_i + \sum_{j=1}^{s} b_j \in [n+1, n+2]$, a contradiction to $\overline{\sigma}(T) = 0$.

Case 2: $a = 2$. If $b_j = n - 2$ for some $j \in [1, s]$, then T has at least $\mathsf{v}_2(A) \ge n/6 > k$ distinct factorizations, a contradiction. If $b_j = b_i = n - 1$ for some $i \ne j \in [1, s]$, then T has at least $\mathsf{v}_2(A) \ge n/6 > k$ distinct factorizations, a contradiction. Thus after renumbering if necessary, we may suppose that $b_j \le n - \sigma(A) + 4$ holds for every $j \in [1, s-1]$. It follows from (5.2) that $\sum_{i=1}^{r} a_i + \sum_{j=1}^{s-1} b_j \le n + 4$. If $b_s \le n - \sigma(A) + 4$, then, as in Case 1, we derive a contradiction to $\overline{\sigma}(T) = 0$. Therefore, we get that $b_s = n - 1$. But from $r + s - 1 \ge n$ and $\sum_{i=1}^{r} a_i + \sum_{j=1}^{s-1} b_j \le n + 4$ we obtain that 1 occurs with multiplicity at least $n - 8 > k$ times in $a_1 \cdot \ldots \cdot a_r b_1 \cdot \ldots \cdot b_{s-1}$. Since $b_s + 1 = n$, T has at least as many factorizations as the above multiplicity of 1, a contradiction to $|\mathsf{Z}(T)| = k$. □

We end this section with a result on elementary 2-groups which is in contrast to Theorem 5.1.

Theorem 5.8. *Let G be an elementary 2-group of rank $r \in \mathbb{N}$ and let $k \in \mathbb{N}$. Then $\mathsf{N}_k(G) = 2r$ if and only if $k \in [1, 2]$.*

Proof. By inequality (2.2), we have $2r \le \mathsf{N}_1(G) \le \mathsf{N}_2(G)$. First, we show that $\mathsf{N}_2(G) \le 2r$. Let $T \in \mathcal{T}(G^\bullet)$ be squarefree with $|\mathsf{Z}(T)| = 2$ and $\max \mathsf{L}(T) = r_1$.

Then Lemma 5.7 implies that $\mathsf{D}(G)+r_1-1 \geq |T| \geq 2r_1$. This implies $r_1 \leq \mathsf{D}(G)-1$ and thus $|T| \leq 2\mathsf{D}(G)-2 = 2r$.

Second, we verify that $\mathsf{N}_3(G) > 2r$. Let $(e_1, \ldots, e_r)$ be a basis of G and $B = e_1^4 e_2^2 \cdot \ldots \cdot e_r^2$. Then

$$\tau(B) = (e_1,1)(e_1,2)(e_1,3)(e_1,4)\prod_{i=2}^{r}(e_i,1)(e_i,2) \quad \text{and} \quad \mathsf{Z}(\tau(B)) = \{z_1, z_2, z_3\},$$

where

$$z_1 = ((e_1,1)(e_1,2))((e_1,3)(e_1,4))\prod_{i=2}^{r}((e_i,1)(e_i,2)),$$

$$z_2 = ((e_1,1)(e_1,3))((e_1,2)(e_1,4))\prod_{i=2}^{r}((e_i,1)(e_i,2)),$$

$$z_3 = ((e_1,1)(e_1,4))((e_1,2)(e_1,3))\prod_{i=2}^{r}((e_i,1)(e_i,2)).$$

This shows that $\mathsf{N}_3(G) \geq |\tau(B)| = 2r+2$. □

Acknowledgments

The first and third authors were supported by the PCSIRT Project of the Ministry of Science and Technology, and the National Science Foundation of China. The second author was supported by the Austrian Science Fund FWF, Project No. P21576-N18. A part of this paper was written during a stay of the second author at the Center for Combinatorics, Nankai University. He would like to thank them for the excellent working conditions and for all the hospitality. Furthermore, we would like to thank the referee for their careful reading. They have observed various inaccuracies and their list of comments has helped a lot to improve the clarity of the presentation.

Note Added in Proof. W. Gao, Y. Li and J. Peng proved that $\mathsf{N}_1(C_p \oplus C_p) = 2p$ for all primes p (their paper "A quantitative aspect of non-unique factorizations: The Narkiewicz constants II" has been accepted for publication in *Colloq. Math.*). Thus one of the two assumptions in Theorem 4.1 has been verified.

References

[1] G. Bhowmik and J.-C. Schlage-Puchta, An improvement on Olson's constant for $\mathbb{Z}_p \oplus \mathbb{Z}_p$, *Acta Arith.* **141** (2010) 311–319.

[2] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham, Zero-sum problems in finite abelian groups and affine caps, *Q. J. Math.* **58** (2007) 159–186.

[3] Y. Fan, W. Gao and Q. Zhong, On the Erdős–Ginzburg–Ziv constant of finite abelian groups of high rank, *J. Number Theory* **131** (2011) 1864–1874.

[4] E. Fogels, Zur Arithmetik quadratischer Zahlkörper, *Univ. Riga. Wiss. Abh. Kl. Math. Abt.* **1** (1943) 23–47.

[5] W. Gao, On a combinatorial problem connected with factorizations, *Colloq. Math.* **72** (1997) 251–268.

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

[7] W. Gao, A. Geroldinger and D. J. Grynkiewicz, Inverse zero-sum problems III, *Acta Arith.* **141** (2010) 103–152.

[8] W. Gao, A. Geroldinger and W. A. Schmid, Inverse zero-sum problems, *Acta Arith.* **128** (2007) 245–279.

[9] W. Gao, Q. H. Hou, W. A. Schmid and R. Thangadurai, On short zero-sum subsequences II, *Integers* **7** (2007) Paper A21, 1–22.

[10] W. Gao, I. Ruzsa and R. Thangadurai, Olson's constant for the group $\mathbb{Z}_p \oplus \mathbb{Z}_p$, *J. Combin. Theory Ser. A* **107** (2004) 49–67.

[11] W. Gao and R. Thangadurai, A variant of Kemnitz conjecture, *J. Combin. Theory Ser. A* **107** (2004) 69–86.

[12] A. Geroldinger, Factorization of natural numbers in algebraic number fields, *Acta Arith.* **57** (1991) 365–373.

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

[14] A. Geroldinger and F. Halter-Koch, *Non-unique Factorizations*, *Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, Vol. 278 (Chapman & Hall/CRC, 2006).

[15] A. Geroldinger, F. Halter-Koch and J. Kaczorowski, Non-unique factorizations in orders of global fields, *J. Reine Angew. Math.* **459** (1995) 89–118.

[16] F. Halter-Koch, Chebotarev formations and quantitative aspects of non-unique factorizations, *Acta Arith.* **62** (1992) 173–206.

[17] ———, Relative types and their arithmetical applications, *Pure Math. Appl.* **3** (1992) 81–92.

[18] ———, Typenhalbgruppen und Faktorisierungsprobleme, *Result. Math.* **22** (1992) 545–559.

[19] F. Halter-Koch and W. Müller, Quantitative aspects of non-unique factorization: A general theory with applications to algebraic function fields, J. *Reine Angew. Math.* **421** (1991) 159–188.

[20] H. Harborth, Ein Extremalproblem für Gitterpunkte, *J. Reine Angew. Math.* **262** (1973) 356–360.

[21] J. Kaczorowski, Some remarks on factorization in algebraic number fields, *Acta Arith.* **43** (1983) 53–68.

[22] ———, Irreducible algebraic integers in short intervals, *Math. Ann.* **345** (2009) 297–305.

[23] ———, A note on algebraic integers with prescribed factorization properties in short intervals, *Funct. Approx. Comment. Math.* **40** (2009) 151–154.

[24] ———, On the distribution of irreducible algebraic integers, *Monatsh. Math.* **156** (2009) 47–71.

[25] J. Kaczorowski, G. Molteni and A. Perelli, Unique factorization results for semigroups of L-functions, *Math. Ann.* **341** (2008) 517–527.

[26] A. Kemnitz, Extremalprobleme für Gitterpunkte, Ph.D. thesis, Technische Universität Braunschweig (1982).

[27] ———, On a lattice point problem, *Ars Combin.* **16-B** (1983) 151–160.

[28] W. Narkiewicz, On algebraic number fields with non-unique factorizations, *Colloq. Math.* **12** (1964) 59–67.

[29] ______, Numbers with unique factorizations in an algebraic number field, *Acta Arith.* **21** (1972) 313–322.
[30] ______, Finite abelian groups and factorization problems, *Colloq. Math.* **42** (1979) 319–330.
[31] ______, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd edn. (Springer, 2004).
[32] W. Narkiewicz and J. Śliwa, Finite abelian groups and factorization problems II, *Colloq. Math.* **46** (1982) 115–122.
[33] O. Ordaz, A. Philipp, I. Santos and W. A. Schmid, On the Olson and the strong Davenport constants, to appear in *J. Théor. Nombres Bordeaux*.
[34] M. Radziejewski, Oscillations of error terms associated with certain arithmetical functions, *Monatsh. Math.* **144** (2005) 113–130.
[35] C. Reiher, A proof of the theorem according to which every prime number possesses property B, to appear in *J. Lond. Math. Soc.*
[36] S. Savchev and F. Chen, Long zero-free sequences in finite cyclic groups, *Discrete Math.* **307** (2007) 2671–2679.
[37] W. A. Schmid, Restricted inverse zero-sum problems in groups of rank two, to appear in *Q. J. Math.*
[38] ______, Inverse zero-sum problems II, *Acta Arith.* **143** (2010) 333–343.