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

WEIDONG GAO, JIANGTAO PENG AND QINGHAI ZHONG

ABSTRACT. Let K be an algebraic number field with non-trivial class group G and $\mathcal{O}_K$ be its ring of integers. For $k \in \mathbb{N}$ and some real $x \ge 1$, 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 prove, among other results, that $\mathsf{N}_1(C_{n_1} \oplus C_{n_2}) = n_1 + n_2$ for all integers n_1, n_2 with $1 < n_1 | n_2$.

1. Introduction

Let K be an algebraic number field, $\mathcal{O}_K$ its ring of integers and G 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 $|G| \ge 2$ and let $k \in \mathbb{N}$. In the 1960s P. Rémond and W. Narkiewicz initiated the study of the asymptotic behavior of counting functions associated with non-unique factorizations (for an overview and historical references see [17, 4]). Among others, the function

$$F_k(x) = \big|\{a\mathcal{O}_K : a \in \mathcal{O}_K \setminus \{0\}\,,\ (\mathcal{O}_K \colon a\mathcal{O}_K) \le x \text{ and } |\mathsf{Z}(a)| \le k\}\big|$$

was considered. It counts the number of principal ideals $a\mathcal{O}_K$ where $0 \ne a \in \mathcal{O}_K$ has at most k distinct factorizations and whose norm is bounded by x. In [15] it was proved that $F_k(x)$ behaves for $x \to \infty$ asymptotically like

$$x(\log x)^{1-1/|G|}(\log \log x)^{\mathsf{N}_k(\cdot)}\,.$$

This result was refined and extended in several ways: the asymptotics were sharpened in [10], the function field case was handled in [9], Chebotarev formations in [6] and non-principal orders in global fields in [5]. For more recent development see [4, Section 9.3] and [21, 14, 13, 11, 12]. In [16, 18], W. Narkiewicz and J. Śliwa showed that the exponents $\mathsf{N}_k(\cdot)$ depend only on the class group G, and they gave a combinatorial description of $\mathsf{N}_k(G)$ (see Definition 2.1). This description was used by the first author for a first detailed investigation of $\mathsf{N}_k(G)$ in [1]. In two recent papers [2] and [3], $\mathsf{N}_k(G)$ has been continued to investigated 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 $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$. Since $|G| \ge 2$, $\mathcal{O}_K$ 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

2010 *Mathematics Subject Classification.* 11R27, 11B30, 11P70, 20K01.

Key words and phrases. non-unique factorizations, Narkiewicz constants, zero-sum sequence.

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 $\mathsf N_1(G) \ge n_1 + \ldots + n_r$ (see Inequality 2.2), and in 1982 W. Narkiewicz and J. Śliwa stated the conjecture that 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 ([4, Theorem 6.2.8]). In this paper we shall determine $\mathsf N_1(G)$ for groups of rank two and obtain several related results. Our main results will be presented in the next section (see Theorems 2.3-2.6).

2. Notations and the main results

We denote by $\mathbb N$ the set of positive integers, by $\mathbb P \subseteq \mathbb N$ 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 $[a, b] = \{x \in \mathbb Z : a \le x \le b\}$. 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 $H_{\rm red} = H/H^\times = \{aH^\times : a \in H\}$ be the associated reduced monoid.

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

$$a = \prod_{p \in P} p^{\mathsf v_p(a)} \quad \text{with} \quad \mathsf v_p(a) \in \mathbb N_0 \quad \text{and} \quad \mathsf v_p(a) = 0 \quad \text{for almost all} \quad p \in P\,.$$

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

$$|a|_F = |a| = \sum_{p \in P} \mathsf v_p(a) \quad \text{the} \quad \textit{length} \text{ of } a\,.$$

The monoid $\mathsf Z(H) = \mathcal F(\mathcal A(H_{\rm red}))$ is the *factorization monoid* of H and $\pi \colon \mathsf Z(H) \to H_{\rm red}$ denotes the natural homomorphism given by mapping a factorization to the element it factorizes. Then the set $\mathsf Z(a) = \pi^{-1}(aH^\times) \subseteq \mathsf Z(H)$ is called the *set of factorizations* of a, and we say that a has *unique factorization* if $|\mathsf Z(a)| = 1$. The set $\mathsf L(a) = \{|z| \mid z \in \mathsf Z(a)\} \subseteq \mathbb N_0$ 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 $G_0 \subseteq G$ a subset. Then $\langle G_0 \rangle \subseteq G$ 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

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

If $I=[1,r]$ and $(e_1,\cdots,e_r)$ is independent, then we simply say that $e_1,\cdots,e_r$ 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 $\langle\{e_i : i\in I\}\rangle = G$. If $1<|G|<\infty$, then we have

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

where $r=\mathsf r(G)\in\mathbb N$ is the *rank* of G, $n_1,\cdots,n_r\in\mathbb N$ are integers with $1<n_1\mid\ldots\mid n_r$ 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 arithmetic of Krull monoids is studied by using two classes of auxiliary monoids: block monoids (in other words, monoids of zero-sum sequences) and type monoids (see [4, Sections 3.4 and 3.5]). We need both concepts for our investigations.

Monoid of zero-sum sequences. Let G be a finite additively written abelian group.

The elements of the free monoid $\mathcal F(G_0)$ are called *sequences* over G_0. Let

$$S=\prod_{g\in G_0} g^{\mathsf v_g(S)}\,,\quad \text{where } \mathsf v_g(S)\in\mathbb N_0 \text{ for all } g\in G_0 \text{ and } \mathsf v_g(S)=0 \text{ for almost all } g\in G_0\,,$$

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 $S_1\,|\,S$ 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 $|S|=l=\sum_{g\in G_0}\mathsf v_g(S)\in\mathbb N_0$ the *length* of S, $\operatorname{supp}(S)=\{g\in G_0\mid \mathsf v_g(S)>0\}\subset G_0$ the *support* of S, $\sigma(S)=\sum_{i=1}^{l} g_i=\sum_{g\in G_0}\mathsf v_g(S)g\in G$ the *sum* of S, and $\Sigma(S)=\{\sum_{i\in I} g_i : \emptyset\ne I\subseteq[1,l]\}$ 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.

We denote by $\mathcal B(G_0)=\{S\in\mathcal F(G_0):\sigma(S)=0\}$ 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

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

the *Davenport constant* of G_0. Every map of abelian groups $\varphi\colon G\to H$ extends to a homomorphism $\varphi\colon\mathcal F(G)\to\mathcal F(H)$ where $\varphi(S)=\varphi(g_1)\cdot\ldots\cdot\varphi(g_l)$. If φ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S)\in\operatorname{Ker}(\varphi)$.

For many zero-sum problems, the ordering of the elements of a sequence is not important. But when we count the number of subsequences with given property or consider so called unique factorization, we need to grant a sequence a ordering or label. There are two popular ways to label a sequence. One way is introduce the index set as doing by Narkiewicz in 1979 [16], and another way is using the concept of type as we doing in a recent paper [2]. In this paper we shall using the concept of type which was first introduced by Halter-Koch in 1992 [6].

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 satisfying

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

and let $\overline{\sigma} = \sigma \circ \boldsymbol{\alpha}\colon \mathcal{F}(G_0\times\mathbb{N}) \to G$. For a type $T \in \mathcal{F}(G_0\times\mathbb{N})$, $\boldsymbol{\alpha}(T) \in \mathcal{F}(G_0)$ is the associated (unlabeled) sequence. 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

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

the *monoid of zero-sum types* over G_0 (briefly, the *type monoid* over G_0). Type monoids were introduced by F. Halter-Koch in [8] and applied successfully in the analytic theory of so-called type-dependent factorization properties (see [4, Section 9.1], and [6, 7] for some early papers).

Every map of abelian groups $\varphi\colon G \to H$ extends to a unique homomorphism $\varphi\colon \mathcal{F}(G_0\times\mathbb{N}) \to \mathcal{F}(H\times\mathbb{N})$ satisfying $\varphi((g,n)) = (\varphi(g),n)$ for all $(g,n) \in G_0\times\mathbb{N}$. We denote by $\overline{\varphi} = \varphi\circ\boldsymbol{\alpha}\colon \mathcal{F}(G_0\times\mathbb{N}) \to \mathcal{F}(H)$ the unique homomorphism satisfying $\varphi((g,n)) = \varphi(g)$ for all $(g,n) \in G_0\times\mathbb{N}$.

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

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

For $S \in \mathcal{F}(G_0)$, we call $\tau(S)$ the *type associated with* S. The map $\boldsymbol{\beta} = \boldsymbol{\alpha}\mid_{\mathcal{T}(G_0)}\colon \mathcal{T}(G_0) \to \mathcal{B}(G_0)$ is a transfer homomorphism (see [4, Proposition 3.5.5]), and hence we have in particular that $\mathsf{L}(B) = \mathsf{L}\big(\tau(B)\big)$ for all $B \in \mathcal{B}(G^\bullet)$. Let T and T' be 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 $|\mathsf{Z}(T)| = |\mathsf{Z}(\tau(\boldsymbol{\alpha}(T)))|$. Let $T = (g_1,a_1)\cdot\ldots\cdot(g_l,a_l) \in \mathcal{F}(G\times\mathbb{N})$ be a type. For every $g \in G$, define $(g,0) + T = (g+g_1,a_1)\cdot\ldots\cdot(g+g_l,a_l)$.

The *greatest common divisor* of sequences $S, S' \in \mathcal{F}(G_0)$, denoted by $\gcd(S,S')$, is defined to be the greatest common subsequence of S and S' (i.e. it is always taken in the monoid $\mathcal{F}(G_0)$). Sequences S and S' are called *coprime* if $\gcd(S,S') = 1$. Similarly, the *greatest common divisor* of types $T, T' \in \mathcal{F}(G_0\times\mathbb{N})$, denoted by $\gcd(T,T')$, is defined to be the greatest common subtype of T and T' (i.e. it is always taken in $\mathcal{F}(G_0\times\mathbb{N})$). Types T and T' are called *coprime* if $\gcd(T,T') = 1$.

Narkiewicz constants. We start with the definition of the Narkiewicz constants (see [4, Definition 6.2.1]). Theorem 9.3.2 in [4] 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

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

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

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

has unique factorization, and hence

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

In [18], W. Narkiewicz and J. Śliwa conjectured that $\mathsf{N}_1(G)$ equals the above lower bound for all finite abelian groups.

And we need some other definitions:

Definition 2.2. 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 $|S| \ge \ell$ 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 $|S| \ge \ell$ has a short zero-sum subsequence (equivalently, S has a short minimal zero-sum subsequence).
- $\eta_g^*(G)$ the smallest integer $\ell \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G^\bullet)$ of length $|S| \ge \ell$ and with sum $\sigma(S) = g$ satisfies that S has two different short minimal zero-sum subsequences T_1 and T_2 such that $1 \ne \gcd(T_1, T_2)$. We set
$$\eta^*(G) = \max\{\eta_h^*(G) : h \in G\}\,.$$

Now we can state our main results

Theorem 2.3. *Let* $G = C_{n_1} \oplus C_{n_2}$ *with* $1 < n_1 \,|\, n_2$. *Then*
$$\mathsf{N}_1(G) = n_1 + n_2.$$

Theorem 2.4. *Let* $G = C_p \oplus C_p$, *where* p *is a prime and let* $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ *be a squarefree type of length* $|T| = 2p$. *If* T *does not have two minimal zero-sum subtypes which are not coprime, then there exists a basis* (e_1, e_2) *of* G *such that*

$$\boldsymbol{\alpha}(T) = e_1^p \prod_{i=1}^{p} (a_i e_1 + e_2),$$

where $\sum_{i=1}^{p} a_i \equiv 0 \pmod p$.

Theorem 2.5. *Let* $G = C_p \oplus C_p$, *where* p *is a prime. Let* $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ *be a squarefree type of length* $|S| = 3p$. *If* S *does not have two short minimal zero-sum subtypes which are not coprime, then there exists a basis* (e_1, e_2) *of* G *and* $a_1, a_2 \in [1, p-1]$ *such that* $\boldsymbol{\alpha}(S) = e_1^p e_2^p (a_1 e_1 + a_2 e_2)^p$.

Theorem 2.6. *Let* $G = C_n \oplus C_n$, *where* n *is a positive integer. Then* $\eta^*(G) = 3n + 1$.

3. PRELIMINARIES

In this section we first gather some known results needed in this paper, and then we employ group algebra as a tool to derive a result on subsequences sum (see Theorem 3.12), which will be crucial in the proof of Theorem 2.4 and might be of its own interesting.

Lemma 3.1. [4, Theorem 5.8.3] *Let* $G = C_{n_1} \oplus C_{n_2}$ *with* $1 \le n_1 \,|\, n_2$*. Then*

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

Lemma 3.2. [4, Proposition 5.7.7] *Let* $G = C_p \oplus C_p$*, where* p *is a prime. Suppose* $S \in \mathcal{F}(G)$ *is a sequence with* $|S| \ge 3p - 2$*. Then* S *has a zero-sum subsequence* $T \in \mathcal{F}(G)$ *of length* $|T| \in \{p, 2p\}$*.*

Lemma 3.3. [2, Lemma 2.2] *Let* G *be an abelian group with* $|G| > 1$ *and* $T \in \mathcal{T}(G^\bullet)$ *be a squarefree zero-sum type. Then the following statements are equivalent*:

(a) $|\mathsf{Z}(T)| = 1$.

(b) *If* $U, V \in \mathcal{T}(G)$ *with* $U \,|\, T$ *and* $V \,|\, T$*, then* $\gcd(U, V)$ *has sum zero.*

Lemma 3.4. [2, 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* $U_1, \cdots, U_r \in \mathcal{A}(\mathcal{T}(G^\bullet))$*.*

1. *If* $|\mathsf{Z}(T)| = 1$*, then* $\prod_{i=1}^r |U_i| \le |G|$*.*
2. *Let* $S_1, \cdots, S_t \in \mathcal{F}(G \times \mathbb{N})$ *such that* $S_1 \cdot \ldots \cdot S_t$ *is a zero-sum subtype of* T*.* *If* $|\mathsf{Z}(T)| = 1$*, then* $\tau\big(\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_t)\big)$ *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* $|\mathsf{Z}(T)| = 1$*.*

Lemma 3.5. [3, Theorem 1.2] $\mathsf{N}_1(C_p \oplus C_p) = 2p$*, where* p *is a prime.*

We need the following well known result

Lemma 3.6. *If* S *is a minimal zero-sum sequence over* C_n *of length* $|S| = n$*, then* $S = g^n$ *for some* $g \in C_n$*.*

Lemma 3.7. [2, Theorem 3.14(a)] *Let* $G = C_{mn} \oplus C_{mn}$ *with* $n, m \ge 2$*. If* $\eta^*(C_m \oplus C_m) = 3m + 1$ *and* $\eta^*(C_n \oplus C_n) = 3n + 1$ *then* $\eta^*(C_{mn} \oplus C_{mn}) = 3mn + 1$*.*

Lemma 3.8. [3, Lemma 4.4] *Let* $G = C_{n_1 p} \oplus C_{n_2 p}$ *with* $1 \le n_1 \,|\, n_2$ *and* p *being a prime. Suppose that* $\mathsf{N}_1(C_{n_1} \oplus C_{n_2}) = n_1 + n_2$ *for* $n_1 > 1$*, and suppose that* $\eta^*(C_p \oplus C_p) = 3p + 1$*. Then,* $\mathsf{N}_1(G) = n_1 p + n_2 p$*.*

Remark 3.9. If $n_1 = 1$ then $\mathsf{N}_1(C_{n_1} \oplus C_{n_2}) = \mathsf{N}_1(C_{n_2}) = n_2$ has been proved by Narkiewicz [16] (see also [4, Theorem 6.2.8] or [2, Theorem 5.1]). In [3], Lemma 3.8 is stated only for $n_1 > 1$, but the proof given there works also for the case of $n_1 = 1$.

Let F be a field, and let G be a finite abelian group. The group algebra $F[G]$ of G over F is a free F-module with basis $\{X^g, g \in G\}$ (built with a symbol X), where multiplication is defined by

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

Let p be a prime. From now on, let $F = F_p$ be the finite field of p elements. Let G be a finite abelian p-group. For any non-empty sequence $S = g_1 \cdot \ldots \cdot g_\ell \in \mathcal{F}(G)$, we define

$$\Pi(S) = \prod_{i=1}^{\ell}(1 - X^{g_i}) = \prod_{g\in G}(1 - X^g)^{\mathsf{v}_g(S)} \in F_p[G]$$

and

$$H_S = \{g \in G : (1 - X^g)\Pi(S) = 0 \in F_p[G]\}.$$

Then H_S is a subgroup of G.

Lemma 3.10. *Let p be a prime, G be a finite abelian p-group, and let $S \in \mathcal{F}(G^\bullet)$.*

1. *If $|S| \ge \mathsf{D}(G)$ then $\Pi(S) = 0 \in F_p[G]$.*
2. *If $|S| = \mathsf{D}(G) - 1$ and $\Pi(S) \ne 0$ then $G^\bullet \subseteq \Sigma(S)$.*
3. *If $H_S = G$ and $\Pi(S) \ne 0$ then $G^\bullet \subseteq \Sigma(S)$.*
4. *If $|S| = \mathsf{D}(G) - 2$ and $\Pi(S) \ne 0$ then there exists $h \in G$ such that $G^\bullet \setminus (\Sigma(S)) \subseteq h + H_S$.*

Proof. Let

$$\Pi(S) = \sum_{g\in G} a_g X^g.$$

1. See [19] or [4, Proposition 5.5.8].

2. See [4, Proposition 5.5.8].

3. If $H_S = G$ then for any element $h \in G$ we have $(1 - X^h)\sum_{g\in G} a_g X^g = \sum_{g\in G}(a_g - a_{g-h})X^g = 0$. It follows that $a_0 = a_{-h}$ for every $h \in G$. Thus $\alpha = a_0 \sum_{g\in G} g \ne 0$. This implies that $G^\bullet \subseteq \Sigma(S)$.

4. We only need to prove that for any $h_1,\ h_2 \in G^\bullet\setminus(\Sigma(S))$, $h_1 - h_2 \in H_S$. If $h_1 - h_2 \notin H_S$, then $(1 - X^{h_1-h_2})\Pi(S) \ne 0$ and $|(h_1 - h_2)S| = \mathsf{D}(G) - 1$. By Conclusion 3, $G^\bullet \subseteq \sum((h_1 - h_2)S)$. So there exists a subsequence $T|S$ such that $h_1 = (h_1 - h_2) + \sigma(T)$. It follows that $h_2 = \sigma(T) \in \Sigma(S)$, a contradiction. □

Let p be a prime, and let $G = C_p \oplus C_p$. Let $S \in \mathcal{F}(G)$ and let $A \subseteq G$. Define

- S_A to be the maximal subsequence of S such that $\operatorname{supp}(S_A) \subseteq A$;
- $\lambda(S) = \max\{|S_H| : H$ is a subgroup of G of order $p\}$;
- $\Lambda(S) = |\{H : H$ is a subgroup of G of order p and $S_H \ne 1\}|$.

Lemma 3.11. [20, Theorem 1] *Let $G = C_p \oplus C_p$ and $S \in \mathcal{F}(G^\bullet)$ with $p \le |S| \le 2p - 2$. If $\lambda(S) \le p - 1$ and $\Lambda(S) \le 2p - 1 - |S|$, then $\Pi(S) \ne 0 \in F_p[G]$.*

Theorem 3.12. *Let p be a prime, $G = C_p \oplus C_p$, and let $S \in \mathcal{F}(G^\bullet)$ with $|S| = 2p - 2$. If $\lambda(S) \le p - 1$ then there exists an element $g \in G$ such that $G \setminus \{g\} \subseteq \Sigma(S)$.*

Proof. Let

$$S = a_1 \cdots a_{2p-2}.$$

Assume to the contrary that, $G^\bullet \setminus \{g\} \not\subseteq \Sigma(S)$ holds for every $g \in G$. It follows that

$$G^\bullet \not\subseteq \Sigma(S).$$

Let $\Lambda(S) = t$ with $1 \le t \le p+1$. By renumbering if necessary we assume that

$$a_1, a_2, \cdots, a_t$$

are in distinct cyclic subgroups of G.

Let $S_0 = S(a_1a_2\cdots a_t)^{-1}$. Then $\lambda(S_0) \le \lambda(S) \le p-1$ and $\Lambda(S_0) \le t = 2p-2-|S_0| < 2p-1-|S_0|$. By Lemma 3.11, $\prod_{g|S_0}(1-X^g) \neq 0$. Let S_1 be the maximal subsequence of S such that $S_0\big|S_1$ and $\prod_{g|S_1}(1-X^g) \neq 0$.

If $|S_1| = 2p-2$, then $G^\bullet \subseteq \Sigma(S_1) \subseteq \Sigma(S)$ by Lemma 3.10, a contradiction.

If $|S_1| \le 2p-4$, then there exist a_i, a_j with $1 \le i < j \le t$ such that $(1-X^{a_i})\prod_{g|S_1}(1-X^g) = (1-X^{a_j})\prod_{g|S_1}(1-X^g) = 0$. Therefore, $G = \langle a_i, a_j\rangle \subseteq H_{S_1} \subseteq G$. Hence, $H_{S_1} = G$. It follows from Lemma 3.10 that $G^\bullet \subseteq \Sigma(S_1) \subseteq \Sigma(S)$, again a contradiction. Therefore,

$$|S_1| = 2p-3.$$

By renumbering if necessary we can assume that $S = S_1a_1$. Since $\mathsf{D}(G)-2 = 2p-3$, $G^\bullet \not\subseteq \Sigma(S)$ and $a_1 \in H_{S_1}$, it follows from Lemma 3.10 that, there exists $h_1 \in G$ such that $G^\bullet \setminus (\Sigma(S_1)) \subseteq h_1 + \langle a_1\rangle$.

Let $S_0' = S(a_2,\cdots,a_t)^{-1}$. Then $\lambda(S_0') \le \lambda(S) \le p-1$ and $\Lambda(S_0') \le t = 2p-2-|S_0'|+1 = 2p-1-|S_0'|$. By Lemma 3.11, $\prod_{g|S_0'}(1-X^g) \neq 0$.

Let S_1' be the maximal subsequence of S such that $S_0'\big|S_1'$ and $\prod_{g|S_1'}(1-X^g) \neq 0$. In a similar way to above we deduce that $|S_1'| = 2p-3$ and there exists $h_2 \in G$ such that $G^\bullet \setminus (\Sigma(S_1)) \subseteq h_2 + \langle a_i\rangle$ for some $i \in [2,t]$.

Since $1 \neq i$ we have $|h_1 + \langle a_1\rangle \bigcap h_2 + \langle a_i\rangle| = 1$. Let $h_1 + \langle a_1\rangle \bigcap h_2 + \langle a_i\rangle = \{g\}$. Then,

$$G^\bullet \setminus (\Sigma(S)) \subseteq h_1 + \langle a_1\rangle \bigcap h_2 + \langle a_i\rangle = \{g\} \tag{3.1}$$

Since $\prod_{g|S}(1-X^g) = 0$, we have $0 \in \Sigma(S)$. This together with (3.1) gives that $G \setminus \{g\} \subseteq \Sigma(S)$. □

4. Proof of the main results

In this section we first generalize the concept on unique factorization to any square free type (not necessarily zero-sum).

Definition 4.1. Let G be an abelian group with $|G| > 1$ and $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a squarefree type. We say T has *unique factorization* if there is only one way to write T in the form $T = U_1 \cdots U_rU'$, where $U_1, \cdots, U_r$ are all minimal zero-sum types and U' is zero-sum free.

We have the following similar result to Lemma 3.3.

Lemma 4.2. *Let G be an abelian group with $|G| > 1$ and $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a squarefree type. Then the following statements are equivalent*:

(a) *T has unique factorization.*

(b) *If $U, V \in \mathcal{T}(G)$ with $U \,|\, T$ and $V \,|\, T$, then* $\gcd(U,V)$ *has sum zero.*

Lemma 4.3. *Let G be a finite abelian group and let $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a squarefree type of length $|T| = \mathsf{N}_1(G)$. If T has unique factorization then T is zero-sum.*

Proof. If $\sigma(\boldsymbol{\alpha}(T)) \neq 0$, there exists a squarefree type $T_1 \in \mathcal{T}(G^\bullet)$ such that $T_1 = Tw$, where $w \in G^\bullet \times \mathbb{N}$ and $\boldsymbol{\alpha}(w) = -\sigma(\boldsymbol{\alpha}(T))$. Since $|T_1| > \mathsf{N}_1(G)$, T_1 have two distinct factorizations:

$$T_1 = Z_1 Z_2 \cdots Z_r X_1 X_2 \cdots X_u = Z_1 Z_2 \cdots Z_r Y_1 Y_2 \cdots Y_v$$

where $Z_i, X_i,\ Y_k$ are all minimal zero-sum types, $X_i \neq Y_j$ for all $i \in [1,u]$ and $j \in [1,v]$, and $u, v \geq 2$. So, $X_1 X_2 \cdots X_u = Y_1 Y_2 \cdots Y_v$. It follows that there exist X_i and Y_j with $w \not| X_i, w \not| Y_j$ such that $\gcd(X_i, Y_j) \neq 1$, a contradiction to Lemma 4.2. □

We also need the following easy result.

Lemma 4.4. *Let $G = C_n$ with $n \neq 4$, and let $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a squarefree type of length $|T| = n$. If T has unique factorization then there exists $g \in G$ such that $\boldsymbol{\alpha}(T) = g^n$.*

Proof. By Lemma 4.3, we know that $T \in \mathcal{T}(G^\bullet)$. If T is a minimal zero-sum type then the result follows from Lemma 3.6. Otherwise $n \geq 5$ and $T = X_1 X_2 \cdots X_u$ with $u \geq 2$ and all X_i being minimal zero-sum subtypes of length not less than two. It follows that $|X_1||X_2| \cdots |X_u| > n$, a contradiction to Lemma 3.4. □

Proof of Theorem 2.4. We distinguish two cases:

CASE 1: $\lambda(\boldsymbol{\alpha}(T)) \geq p$.

There exists a subtype $T_1 \big| T$ of length $|T_1| = p$ such that $\boldsymbol{\alpha}(T_1)$ is a zero-sum sequence over some subgroup H of G with $H \cong C_p$. Since T_1 has unique factorization, by Lemma 4.4 there exists $e_1 \in G^\bullet$ such that $\boldsymbol{\alpha}(T_1) = e_1^p$. Now T_1 is a minimal zero-sum subtype of T of length $|T_1| = p$. From Lemma 3.4 we infer that TT_1^{-1} is also a minimal zero-sum type of T. We can assume that

$$\boldsymbol{\alpha}(T) = e_1^p \prod_{i=1}^{p} (a_i e_1 + b_i e_2)$$

for some basis (e_1, e_2) of G.

If $b_1 \cdots b_p$ is a minimal zero-sum sequence over C_p then $b_1 = \ldots = b_p$ by Lemma 3.6. Let $e_2' = b_1 e_2$. Then, (e_1, e_2') is also a basis of G and $\boldsymbol{\alpha}(T)$ has the desired form with the basis (e_1, e_2'). So, we may assume that $b_1 \cdots b_p$ is not minimal zero-sum. Then, there is a subset $I \subseteq [1,p]$ such that $\sum_{i \in I} b_i = 0$ and $1 \leq |I| < p$. Since TT_1^{-1} is a minimal zero-sum type, we have $\sum_{i \in I} a_i \neq 0 \in C_p$. Therefore,

$$e_1^{p - \sum_{i \in I} a_i} \prod_{i \in I} (a_i e_1 + b_i e_2)$$

is a zero-sum subsequence of $\boldsymbol{\alpha}(T)$ and $p - \sum_{i \in I} a_i \in [1, p-1]$. So, we can find two zero-sum types W_1 and W_2 of T such that $\boldsymbol{\alpha}(W_1) = \boldsymbol{\alpha}(W_2) = e_1^{p - \sum_{i \in I} a_i} \prod_{i \in I} (a_i e_1 + b_i e_2)$ and $\boldsymbol{\alpha}(\gcd(W_1, W_2)) = e_1$ has not zero-sum, a contradiction.

CASE 2: $\lambda(\boldsymbol{\alpha}(T)) \leq p - 1$.

Let T_2 be a minimal zero-sum subtype of T. It follows from $\lambda(\boldsymbol{\alpha}(T)) \le p-1$ that $|\text{supp}(\boldsymbol{\alpha}(T_2))| \ge 2$. Let $a, b \in G^\bullet \times \mathbb{N}$ such that $ab|T_2$ and $\boldsymbol{\alpha}(a) \ne \boldsymbol{\alpha}(b)$. Since $|\boldsymbol{\alpha}(T(ab)^{-1})| = 2p-2$, by $\lambda(\boldsymbol{\alpha}(T(ab)^{-1})) \le p-1$ and Theorem 3.12, $-\boldsymbol{\alpha}(a) \in \Sigma(\boldsymbol{\alpha}(T(ab)^{-1})$ or $-\boldsymbol{\alpha}(b) \in \Sigma(\boldsymbol{\alpha}(T(ab)^{-1})$. Without loss of generality, we can assume that $-\boldsymbol{\alpha}(a) \in \Sigma(\boldsymbol{\alpha}(T(ab)^{-1})$. It follows that there exists a minimal zero-sum subtype T_3 such that $a|T_3$ and $b \nmid T_3$, a contradiction. □

Proof of Theorem 2.5.

Clearly every subtype of S does not have two short minimal zero-sum subtypes which are not coprime. Since $|S| = 3p > 3p-2$, by Lemma 3.2 S has a zero-sum subtype $T \in \mathcal{T}(G^\bullet)$ of length $|T| \in \{p, 2p\}$. We distinguish two cases.

CASE 1: S has a zero-sum subtype $T \in \mathcal{T}(G^\bullet)$ of length $|T| = 2p$.

Since T does not have two short minimal zero-sum subtypes which are not coprime, by Theorem 2.4, $T = T_1T_2$ with T_1, T_2 are minimal zero-sum subtypes of length p.

Choose $x, y \in G^\bullet \times \mathbb{N}$ with $x|T_1$ and $y|T_2$. Since $|Sx^{-1}y^{-1}| = 3p-2$, by Lemma 3.2 $Sx^{-1}y^{-1}$ has a zero-sum subtype $T' \in \mathcal{T}(G^\bullet)$ of length $|T'| \in \{p, 2p\}$.

If $|T'| = 2p$, then again by Theorem 2.4 we know that $T' = T_1'T_2'$ with T_1', T_2' are minimal zero-sum subtypes of length p. So $T_1T_2T_1'T_2'|S$, yielding a contradiction.

If $|T'| = p$, then $\gcd(T_1, T') = \gcd(T_2, T') = 1$. Thus $S = T_1T_2T'$. Since T_1T_2, T_1T' and T_2T' are zero-sum subtypes of length $2p$, by using Theorem 2.4 repeatedly, we infer that there exists a basis (e_1, e_2) of G such that $\boldsymbol{\alpha}(S) = e_1^p e_2^p \prod_{i=1}^p (a_ie_1 + b_ie_2)^p$. Now in a similar way to the proof of Theorem 2.4 we deduce that $a_1 = \ldots = a_p$ and $b_1 = \ldots = b_p$.

CASE 2: S does not have a zero-sum subtype of length $2p$.

Let $T_1, T_2, \cdots, T_r$ be the all zero-sum subtypes of S of length p. We show next that

$$\gcd(T_1, T_2, \cdots, T_r) = 1. \tag{4.1}$$

Assume to the contrary that $x \mid \gcd(T_1, T_2, \cdots, T_r)$ for some $x \in G^\bullet \times \mathbb{N}$. Consider Sx^{-1}. Since $|Sx^{-1}| = 3p-1$, by Lemma 3.2 we have Sx^{-1} has a zero-sum subtype $T' \in \mathcal{T}(G^\bullet)$ of length $|T'| \in \{p, 2p\}$. Since S does not have a zero-sum subtype of length $2p$, we have $|T'| = p$. But T' is different from all of $T_1, T_2, \cdots, T_r$, a contradiction to that $T_1, T_2, \cdots, T_r$ are the all of the zero-sum subtypes of S of length p. This proves that $\gcd(T_1, T_2, \cdots, T_r) = 1$. It follows that

$$r \ge 2$$

Clearly $|\mathsf{Z}(T_1)| = \ldots = |\mathsf{Z}(T_r)| = 1$. Since S does not have a zero-sum subtype of length $2p$, we infer that $|\gcd(T_i, T_j)| \ne 1$ for all $i, j \in [1, r]$. Therefore,

$$\gcd(T_i, T_j) \text{ is a nonempty zero-sum type}$$

for all $i, j \in [1, r]$.
This together with $r \ge 2$ shows that each T_i is not a minimal zero-sum type. Hence,

$$p \ge 5.$$

If $p = 5$, then $T_i = X_1^{(i)}X_2^{(i)}$ for each $i \in [1, r]$, where $|X_1^{(i)}| = 2$, $|X_2^{(i)}| = 3$, and $X_1^{(i)}, X_2^{(i)}$ are both minimal zero-sum types. From (4.1) we know that there exist $i, j \in [1, r]$ such that $X_1^{(i)} \ne X_1^{(1)}$ and $X_2^{(j)} \ne X_1^{(2)}$. So $X_1^{(1)}X_1^{(i)}X_2^{(1)}X_2^{(j)}$ is a zero-sum type of T of length $10 = 2 \times 5$, a contradiction.

Let $p = 7$. If there exists $T_i = X_1X_2$ such that $|X_1| = 2$, $|X_2| = 5$, where X_1, X_2 are minimal zero-sum types, then from (4.1) we know that there exists $T_j = X_1X_3$ such that $\gcd(T_j, X_2) = 1$, where X_3 is a zero-sum type. Let $W = X_1X_2X_3$, then $|\mathsf{Z}(W)| = 1$ by Lemma 3.4. But $|X_1||X_2||X_3| = 50 > 49$, a contradiction to Lemma 3.4.

Otherwise for every i, $T_i = X_1^{(i)}X_2^{(i)}$, where $|X_1^{(i)}| = 3$, $|X_2^{(i)}| = 4$, $X_1^{(i)}$ is a minimal zero-sum type and $X_2^{(i)}$ is a zero-sum types. If $X_2^{(i)}$ is a minimal zero-sum type for each $i \in [1, r]$, then similarly to the case of $p = 5$ we infer that there exist $i, j \in [1, r]$ such that $X_1^{(i)} \neq X_1^{(1)}$ and $X_2^{(j)} \neq X_1^{(2)}$. So $X_1^{(1)}X_1^{(i)}X_2^{(1)}X_2^{(j)}$ is a zero-sum type of T of length $14 = 2 \times 7$, a contradiction.

So, $X_2^{(i)} = Y_1Y_2$ for some $i \in [1, r]$, where $|Y_1| = |Y_2| = 2$, and both Y_1 and Y_2 are minimal zero-sum types. Without loss of generality, we assume that $i = 1$. From (4.1) we know that there exists some $i \in [1, r]$ such that $X_1^{(i)} \neq X_1^{(1)}$. If there is some $j \in [2, r]$ such that $X_2^{(j)}$ is a minimal zero-sum type . Then, $X_1^{(1)}Y_1Y_2X_1^{(i)}X_2^{(j)}$ is a zero-sum type of length $14 = 2\times 7$, a contradiction. Therefore, for every $j \in [2, r]$, $X_2^{(j)}$ is a product of two minimal zero-sum types each of length two. Again from (4.1) we know that there exist some $j \in [2, r]$ such that T_j has a minimal zero-sum subtype Z such that $|Z| = 2$ and $\gcd(Z, T_1) = 1$. So, $T_1X_1^{(i)}Z = X_1^{(1)}Y_1Y_2X_1^{(i)}Z$ has unique factorization by Lemma 3.4. But $|X_1^{(1)}||Y_1||Y_2||X_1^{(i)}||Z| = 72 > 49$, a contradiction. So we can assume that

$$p \geq 11.$$

SUBCASE 2.1: There exists $i \in [1, r]$ such that T_i has a minimal zero-sum subtype X_1 with $|X_1| \geq \frac{p+1}{2}$.

From (4.1) we know that there exists some $j \in [1, r] \setminus \{i\}$ such that $\gcd(T_j, X_1) = 1$. It follows that $|\gcd(T_i, T_j)| \leq \frac{p-1}{2}$. Let $T_i = A_1 \cdots A_tX_1 \cdots X_u$ and $T_j = A_1 \cdots A_tY_1 \cdots Y_v$, where $A_1, \cdots, A_t$, $X_1, \cdots, X_u, Y_1, \cdots, Y_v$ are different minimal zero-sum subtypes of S. Let

$$T = A_1 \cdots A_tX_1 \cdots X_uY_1 \cdots Y_v.$$

Clearly $|T| < 2p$. Since T does not have two short minimal zero-sum subtypes which are not coprime, by Lemma 3.4.(3) we infer that $|\mathsf{Z}(T)| = 1$. Since $p \geq 11$ and $2 \leq |A_1| + \cdots + |A_t| \leq \frac{p-1}{2}$, it follows from Lemma 3.4(1) that $p^2 \geq |A_1| \cdots |A_t||X_1| \cdots |X_u||Y_1| \cdots |Y_v| \geq (|A_1| + \ldots + |A_t|)(|X_1|+\ldots+|X_u|)(|Y_1|+\ldots+|Y_v|) = (|A_1|+\ldots+|A_t|)(p-(|A_1|+\ldots+|A_t|))^2 \geq 2(p-2)^2 > p^2$, a contradiction.

SUBCASE 2.2: For every $i \in [1, r]$ and every minimal zero-sum subtype X of T_i, we have $|X| \leq \frac{p-1}{2}$.

Since $|T_1| = p$ and p is an odd prime, we infer that T_1 contains a minimal zero-sum subtype X_1 of length $|X_1| \geq 3$. From (4.1) we know that there exists some $i \in [2, r]$ such that $\gcd(T_i, X_1) = 1$. It follows that $|\gcd(T_1, T_i)| \leq p - 3$. Let $T_1 = A_1 \cdots A_tX_1 \cdots X_u$ and $T_i = A_1 \cdots A_tY_1 \cdots Y_v$, where $A_1, \cdots, A_t, X_1, \cdots, X_u, Y_1, \cdots, Y_v$ are different minimal zero-sum subtypes of S. Let

$$T = A_1 \cdots A_tX_1 \cdots X_uY_1 \cdots Y_v.$$

Clearly $|T| < 2p$. Since T does not have two short minimal zero-sum subtypes which are not coprime, by Lemma 3.4.(3) we infer that $|\mathsf{Z}(T)| = 1$. By Lemma 3.4(1),

$$\begin{aligned} p^2 &\geq |A_1| \cdots |A_t||X_1| \cdots |X_u||Y_1| \cdots |Y_v| \\ &\geq |A_1| \cdots |A_t||X_1||X_2| \cdots |X_u|(|Y_1| + \ldots + |Y_v|) \\ &= |A_1| \cdots |A_t||X_1||X_2| \cdots |X_u|(|X_1| + \ldots + |X_u|) \\ &\geq \begin{cases} 3 \cdot \dfrac{p-1}{2}\dfrac{p-5}{2} \cdot 3 > p^2 & \text{If } |X_1| + \ldots + |X_u| = 3 \text{ and } p \geq 11, \\ 2 \cdot \dfrac{p-1}{2}\dfrac{p-3}{2} \cdot 4 > p^2 & \text{If } |X_1| + \ldots + |X_u| > 3 \text{ and } p \geq 11, \end{cases} \end{aligned}$$

yielding a contradiction. □

Proof of Theorem 2.6. By Lemma 3.7, it suffices to show that the theorem is true for $n = p$ is a prime. Now the result follows from Theorem 2.5. □

Proof of Theorem 2.3. Since $\mathsf{N}_1(C_1 \oplus C_n) = \mathsf{N}_1(C_n) = n$ for every integer n and $\mathsf{N}_1(C_p \oplus C_p) = 2p$ for every prime number p, the result follows from Theorem 2.6 and Lemma 3.8 by induction. □

Acknowledgments. We would like to thank the referee for his/her very useful suggestions. This work has been supported by the PCSIRT Project of the Ministry of Science and Technology, and the National Science Foundation of China.

References

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

[2] W. Gao, A. Geroldinger, and Q. Wang, *A quantitative aspect of non-unique factorizations: the Narkiewicz constants*, International Journal of Number Theory, Volume: 7, Issue: 6(2011) pp. 1463-1502.

[3] W. Gao, Y. Li, and J. Peng, *A quantitative aspect of non-unique factorizations: the Narkiewicz constants II*, Colloq. Math. **124** (2011), 205-218.

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

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

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

[7] ______, *Relative types and their arithmetical applications*, PU.M.A., Pure Math. Appl. **3** (1992), 81 – 92.

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

[9] 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.

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

[11] ______, *Irreducible algebraic integers in short intervals*, Math. Ann. **345** (2009), 47 – 71.

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

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

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

[15] W. Narkiewicz, *Numbers with unique factorizations in an algebraic number field*, Acta Arith. **21** (1972), 313 – 322.

[16] ______, *Finite abelian groups and factorization problems*, Colloq. Math. **42** (1979), 319 – 330.

[17] ______, *Elementary and Analytic Theory of Algebraic Numbers, 3rd ed.*, Springer, 2004.

[18] W. Narkiewicz and J. Śliwa, *Finite abelian groups and factorization problems II*, Colloq. Math. **46** (1982), 115 – 122.

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

[20] C. Peng, *Addition theorems in elementary abelian groups I*, J. Number Theory **27** (1987), 46 – 57.

[21] M. Radziejewski, *Oscillations of error terms associated with certain arithmetical functions*, Monatsh. Math. **144** (2005), 113 – 130.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: wdgao_1963@yahoo.com.cn

College of Science, Civil Aviation University of China, Tianjin 300300, P.R. China
E-mail address: jtpeng1982@yahoo.com.cn

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: zhongqinghai@yahoo.com.cn