Uniform Distribution Theory ? (201?), no.?, 000–000

A WEIGHTED ZERO-SUM PROBLEM WITH QUADRATIC RESIDUES

David J. Grynkiewicz — François Hennecart

ABSTRACT. Given a ring R and a subset $A \subseteq R$, the A-weighted Davenport constant is the least integer $\mathsf{D}_A(R)$ such that any sequence of terms from R of length $\mathsf{D}_A(R)$ has a nontrivial subsequence $g_1 \cdot \ldots \cdot g_\ell$, where the $g_i \in R$ are the terms of the subsequence, such that $0 = a_1 g_1 + \ldots + a_\ell g_\ell$ for some $a_i \in A$.

Let $R = \mathbb{Z}/n\mathbb{Z}$ for an integer $n \geq 2$, regarded as a ring, let U_n be the set of units in R, and let $U_n^2 = \{u^2 : u \in U_n\}$ be the set of all squares of invertible elements. It is proved that the weighted Davenport constant $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z})$ is equal to $2\Omega(n) + 1$ when $\gcd(n, 10) = 1$ or $\gcd(n, 6) = 1$, extending a recent result of Chintamani and Moriya [CM] and another of Adhikari, David and Jiménez Urroz [ADJ]. Indeed, we show that $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) = 2\Omega(n) + \min\{\mathsf{v}_5(n), \mathsf{v}_3(n)\} + 1$ for odd n with either $\mathsf{v}_3(n) = 0$ or $\mathsf{v}_3(n) \geq \mathsf{v}_5(n)$. As part of the proof, we show how certain sequences of terms from an abelian group can be used to create a pairwise balanced design with $\lambda = 1$.

Communicated by

Dedicated to the memory of Pierre Liardet

1. Introduction

Given a ring R and a subset $A \subseteq R$, the A-weighted Davenport constant is the least integer $\mathsf{D}_A(R)$ such that any sequence of terms from R of length $\mathsf{D}_A(R)$ has a nontrivial subsequence $s_1 \cdot \ldots \cdot s_\ell$, where the $s_i \in R$ are the terms of the subsequence (we write sequences multiplicatively, following the notation of [Gr]

2000 Mathematics Subject Classification: primary 11B50, secondary 11B75.
Keywords: zero-sum, weighted Davenport constant, Erdős-Ginzburg-Ziv constant, Gao constant, pairwise balanced design, linear space.
The work of the second-named author is supported by 'ANR CAESAR' ANR-12-BS01-0011.

[GH]), such that $0 = a_1 s_1 + \ldots + a_\ell s_\ell$ for some $a_i \in A$, i.e., such that

$$0 \in \sum_{i=1}^{\ell} A s_i,$$

where $As_i = \{as_i : \ a \in A\}$. We define $\mathsf{E}_A(R)$ for R finite in a similar manner: the only difference is that we require the subsequence $s_1 \cdot \ldots \cdot s_\ell$ to have length exactly equal to $\ell = |R|$. We refer to $\mathsf{E}_A(R)$ as the weighted Gao constant.

By a result of [Gr, Chapter 16] [GMO] [YZ2] (extending the case when $R = \mathbb{Z}/n\mathbb{Z}$ [YZ1]), the two problems are in fact closely related: one has

$$\mathsf{E}_A(R) = \mathsf{D}_A(R) + |R| - 1. \tag{1}$$

This property was conjectured by Thangadurai in [Th] and confirmed the expectations of Adhikari et al. in [ADJ] and [AR], among others. It also extends the corresponding well-known identity for the usual Davenport and Gao constants due to Gao (see [Ga]). Indeed, it is from this now classical result of Gao that the name Gao constant is derived, distinguishing it from the Erdős-Ginzburg-Ziv constant, which is analogously defined but with $\exp(R)$ (the exponent of R regarded as an abelian group) replacing $|R|$ in the definition of $\mathsf{E}_A(R)$. The two names are sometimes interchanged and coincide when $R = \mathbb{Z}/n\mathbb{Z}$, which is the main ring/group of interest in this paper.

When $R = \mathbb{Z}/n\mathbb{Z}$, we let $U_n \subseteq \mathbb{Z}/n\mathbb{Z}$ denote the set of invertible elements modulo n. Then, letting $A = U_n^2 = \{u^2 : u \in U_n\}$, we have $\ell = \mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z})$ being the smallest integer such that, given any $s_1, \ldots, s_\ell \in \mathbb{Z}$, the equation

$$a_1^2 s_1 + \cdots + a_\ell^2 s_\ell \equiv 0 \bmod n$$

always has an integer solution $(a_1, \ldots, a_\ell) \in \mathbb{Z}^\ell$ that is non-zero modulo n and with either $\gcd(a_i, n) = 1$ or $a_i = 0$ for each i. In [CM] it has been proved that $\mathsf{E}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) = 2\Omega(n) + n$ (implying $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) = 2\Omega(n) + 1$ by (1)) for any integer n coprime to 30. The aim of this note is to extend this result (as well as Theorem 2 of [ADJ]) to allow $5 \mid n$ or $3 \mid n$.

Here, and in the rest of the paper, $\Omega(n)$ denotes the number of prime divisors (allowing repetition) of n, while $\omega(n)$ denotes the number of distinct prime divisors of n. Also, $\mathsf{v}_p(n) = d$ denotes the p-valuation of n, which is the maximal integer $d \geq 0$ such that $p^d \mid n$. Our main result is the following, nearly characterizing $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z})$ for odd n. Unfortunately, we were unable, in general, to combine the trick used to handle the case when $5 \mid n$ with the delicate argument used to handle $3 \mid n$. Perhaps the lower bound from Theorem 1.1.3 is the correct value in the remaining case when $0 < \mathsf{v}_3(n) < \mathsf{v}_5(n)$, as this would give a common generalization of parts 1 and 2 in Theorem 1.1 that agrees with the lower bound from part 3.

Theorem 1.1. *Let $n \geq 1$ be an odd integer.*

1. *If $3 \nmid n$, then $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) = 2\Omega(n) + 1$.*
2. *If $5 \nmid n$, then $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) = 2\Omega(n) + 1$.*
3. *In general,*

$$2\Omega(n) + 1 + \min\{\mathsf{v}_3(n), \mathsf{v}_5(n)\} \leq \mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) \leq 2\Omega(n) + 1 + \mathsf{v}_5(n).$$

Given an integer $m \geq 1$, a sequence $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell$ of terms from the ring R, and a subset $A \subseteq R$ with each $a \in A$ viewed as the map $x \mapsto ax$, we let

$$\Sigma_{\leq m}^{\cup}(A(S)) = \Big\{\sum_{i=1}^{r} a_i s_i : \ s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_r \text{ is a subsequence of } S \text{ of length } 1 \leq r \leq m \text{ and } a_i \in A\Big\},$$

$$\Sigma_{m}^{\cup}(A(S)) = \Big\{\sum_{i=1}^{m} a_i s_i : \ s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_m \text{ is a subsequence of } S \text{ of length } m \text{ and } a_i \in A\Big\}, \text{ and}$$

$$\sigma(A(S)) = \sum_{i=1}^{\ell} As_i = \Sigma_{|S|}^{\cup}(A(S)) = \Big\{\sum_{i=1}^{\ell} a_i s_i : \ a_i \in A\Big\} \subseteq R.$$

The notation is a special case of more general concepts from [Gr]. With this notation, $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z})$ (resp. $\mathsf{E}_{U_n^2}(\mathbb{Z}/n\mathbb{Z})$) is the least integer ℓ such that $0 \in \Sigma_{\leq \ell}^{\cup}(U_n^2(S))$ (resp. $0 \in \Sigma_n(U_n^2(S))$) for any sequence S of ℓ integers modulo n.

Since the lower bound on m required for Theorem 1.2 below always holds when $m = n$, we will deduce the upper bounds in Theorem 1.1 from the following more general result via (1).

Theorem 1.2. *Let $n \geq 3$ be an odd integer, let m be a positive integer and let S be a sequence of terms from $\mathbb{Z}/n\mathbb{Z}$.*

1. *If $3 \nmid n$, $m \geq 3\omega(n) + \min\{1, \mathsf{v}_5(n)\}$, and $|S| \geq m + 2\Omega(n)$, then $0 \in \Sigma_m^{\cup}(U_n^2(S))$.*
2. *If $3 \mid m$, $m \geq 4\Omega(n) + \omega(n) + \mathsf{v}_5(n) - 2$, and $|S| \geq m + 2\Omega(n) + \mathsf{v}_5(n)$, then $0 \in \Sigma_m^{\cup}(U_n^2(S))$.*

We notice that the main result in [CM], which is generalized by our results here, follows from Kneser's Theorem [Gr, Chapter 6] and it's special instances, the Cauchy-Davenport and Chowla Theorems. We obtain these improvements, in part, by use of explicit addition theorems derived using the discrete circle method. These explicit results are then combined with a combinatorial argument and some design theory to yield the final proof.

2. Notation

In this section, we present the basic notation for sequences and subsequence sums, found in the texts [Gr] [GH], that will be used in the remainder of the paper. This is done for the benefit of the reader less familiar with this notation.

All intervals will be discrete. Thus, given real numbers a and b, we let

$$[a, b] = \{x \in \mathbb{Z} : \ a \le x \le b\}.$$

Following the tradition in combinatorial number theory, *sequences* of terms from a set X are always *unordered* and finite in length, and we write them using multiplicative notation. The term multi-set would also be appropriate but is not used in the field. To make this formal, we use monoid theoretic notation arising from factorization theory. This means that a sequence S is written in the form

$$S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \tag{2}$$

with the $g_i \in X$ the terms of X. Repetition of terms is allowed, and, as our sequences are unordered, we have $S = g_{\tau(1)} \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_{\tau(\ell)}$ for any permutation τ of $[1, \ell]$. Formally, we view S as an element of the free abelian monoid $\mathcal{F}(X)$ with basis X and monoid operation denoted by $\boldsymbol{\cdot}$ (chosen to distinguish the monoid operation of sequence concatenation from ordinary ring or group theoretic multiplication). Of course, whenever we index the terms of S as in (2), we are implicitly ordering the terms of S. Normally this ordering is irrelevant, but sometimes it can be useful. If we have a fixed indexing/ordering of the terms of S as in (2), then we let

$$S(I) = \bullet_{i \in I} g_i$$

denote the subsequence of S consisting of those terms g_i with $i \in I$. As a matter of abbreviation, for $n \ge 0$, we let

$$g^{[n]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{n} \in \mathcal{F}(X)$$

denote a sequence consisting of the term g repeated n times. Likewise, if $T \in \mathcal{F}(X)$ is a sequence, then $T^{[n]} = \underbrace{T \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T}_{n}$ denotes the sequence consisting of the subsequence T repeated n times. In both cases, the bracket in the exponent is sometimes dropped when it leads to no confusion with other forms of multiplication.

Standard notation for monoids can be used to describe all the main properties of a sequence. In particular, for S given by (2),

$|S| = \ell$ is the *length* of the sequence S,

$\mathsf{v}_g(S) = \{i \in [1, \ell] : \ g_i = g\}$ is the *multiplicity* of the term g in S,
$\mathsf{h}(S) = \max\{\mathsf{v}_g(S) : g \in X\}$ is the *maximum multiplicity* of a term of S, and
$\mathrm{supp}(S) = \{g \in X : \ \mathsf{v}_g(S) > 0\}$ is the *support* of S.

The support is the set of all elements that occur as terms of S, i.e., $g \in \mathrm{supp}(S)$ if the sequence S contains the term g. Also, $T \mid S$ indicates that T is a subsequence of S, meaning $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in X$. The multiplicities $\mathsf{v}_g(S)$, for $g \in X$, completely characterize the sequence S, and an alternative way to write S, without involving an implicit ordering, is as

$$S = \bullet_{g \in X} g^{[\mathsf{v}_g(S)]}.$$

When $T \mid S$ is a subsequence of S, we use $T^{[-1]} \cdot S$ or $S \cdot T^{[-1]}$ to denote the subsequence of S obtained by removing the terms belonging to T, meaning $\mathsf{v}_g(T^{[-1]} \cdot S) = \mathsf{v}_g(S) - \mathsf{v}_g(T)$ for all $g \in X$. Also, $S \cdot T^{[-x]} = S \cdot (T^{[x]})^{[-1]}$ when $T^{[x]} \mid S$. Again, the brackets are sometimes dropped when this leads to no confusion.

Whenever addition is well-defined between the terms of S given by (2), we let

$$\sigma(S) = g_1 + \ldots + g_\ell$$

denote the sum of the terms of S. If $\varphi : X \to Y$ is a map, then $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_\ell) \in \mathcal{F}(Y)$ is the sequence over Y obtained by applying the map φ to each term of S. Note that $|\varphi(S)| = |S|$ always holds, regardless of the injectivity of φ.

3. Basic Setup

If G is a group and $H \le G$ is a subgroup, then $\phi_H : G \to G/H$ denotes the natural homomorphism. When $G = \mathbb{Z}/n\mathbb{Z}$ is cyclic and regarded as a ring, then all subgroups $H \le G$ are also ideals, and the map ϕ_H is a ring homomorphism. By the Chinese Remainder Theorem, there is a ring isomorphism

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_r^{n_r}\mathbb{Z}) \\ x &\mapsto (x \mod p_1^{n_1}, \ldots, x \mod p_r^{n_r}), \end{aligned}$$

where $p_1, \ldots, p_r$ are the distinct prime divisors of $n = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$. It will be more convenient to work with the isomorphic ring $G = (\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_r^{n_r}\mathbb{Z})$ rather than $\mathbb{Z}/n\mathbb{Z}$. When doing so, we have

$$U_G^2 = U_{p_1^{n_1}}^2 \times \ldots \times U_{p_r^{n_r}}^2,$$

where U_G denotes the units in the ring G. A sequence S of terms from $\mathbb{Z}/n\mathbb{Z}$ is then a U_n^2-weighted zero-sum precisely when the sequence of i-th coordinates forms a $U_{p_i^{n_i}}^2$-weighted zero-sum for each $i \in [1, r]$.

Let G be a ring isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and let $H \leq G$ be a subgroup. Then $H = dG$ for some $d \mid n$. Indeed, if $\mathsf{e}_G \in G$ is the identity of G, then H is generated (as a group) by $\mathsf{e}_H := d\mathsf{e}_G$. Moreover, H is a ring (though *not* a subring of G as it has no identity) if we redefine multiplication by setting $x\mathsf{e}_H \cdot y\mathsf{e}_H = xy\mathsf{e}_H$, where $x\mathsf{e}_H$, $y\mathsf{e}_H \in H$ are arbitrary elements with x, $y \in \mathbb{Z}$. One easily checks that this is well-defined and indeed makes H into a ring. Note we have used $\cdot$ to denote multiplication in the ring H, to distinguish it from multiplication in the ring R inherited to the ideal H. The two are clearly different in general. Let $\psi_d : G \to dG = H$ denote the multiplication by d map, so $\psi_d(x\mathsf{e}_G) = xd\mathsf{e}_G = x\mathsf{e}_H$, and let $\bar{\cdot} : H \to \mathbb{Z}/\frac{n}{d}\mathbb{Z}$ denote the map given by $\overline{x\mathsf{e}_H} = x + \frac{n}{d}\mathbb{Z}$, where $x \in \mathbb{Z}$. It is easily checked that both ψ_d and $\bar{\cdot}$ are ring homomorphisms, with the latter an isomorphism. Thus their composition map

$$\overline{\psi_d} : G \to \mathbb{Z}/\frac{n}{d}\mathbb{Z}$$

is also a ring homomorphism given by $\overline{\psi_d}(x\mathsf{e}_G) = \overline{\psi_d(x\mathsf{e}_G)} = x + \frac{n}{d}\mathbb{Z}$, where $x \in \mathbb{Z}$. From the above definitions, we have the following useful property:

$$gh = \psi_d(g) \cdot h \quad \text{for any } g \in G \text{ and } h \in H, \tag{3}$$

where multiplication in the left hand side is in the ring R and multiplication in the right hand side is in the ring H.

Let $G \cong \mathbb{Z}/n\mathbb{Z}$ and let $\varphi : G \to G'$ be a surjective ring homomorphism. Then $\ker\varphi = H \leq G$ is a subgroup, thus cyclic. Then $H = dG \cong \mathbb{Z}/\frac{n}{d}\mathbb{Z}$ and $G' \cong \mathbb{Z}/d\mathbb{Z}$ for some divisor $d \mid n$. Let $U_G \subseteq G$ and $U_{G'} \subseteq G'$ denote the units in the respective rings G and G'. Then we have

$$\varphi(U_G) = U_{G'}. \tag{4}$$

Indeed, recalling the short argument here, we see that, by composing the homomorphisms $\mathbb{Z}/n\mathbb{Z} \cong G \to G' \cong \mathbb{Z}/d\mathbb{Z}$, it suffices to prove (4) when $G = \mathbb{Z}/n\mathbb{Z}$ and $G' = \mathbb{Z}/d\mathbb{Z}$ with φ given by $x + n\mathbb{Z} \mapsto x + d\mathbb{Z}$. Now $U_G = U_n = \{x + n\mathbb{Z} : x \in \mathbb{Z}, \gcd(x, n) = 1\}$ and $U_{G'} = U_d = \{x + d\mathbb{Z} : \gcd(x, d) = 1\}$. Thus clearly $\varphi(U_G) \subseteq U_{G'}$. On the other hand, if $x \in \mathbb{Z}$ with $\gcd(x, d) = 1$, then $y = x + p_1 \cdots p_t d \in \mathbb{Z}$, where $p_1, \ldots, p_t$ are the distinct prime divisors of n that do not divide $\operatorname{lcm}(x, d)$, has $\varphi(y + n\mathbb{Z}) = x + d\mathbb{Z} \in U_d$ with $\gcd(y, n) = 1$ (the latter is easily seen by noting $\gcd(y, p) = 1$ for any prime $p \mid n$, distinguishing three disjoint cases depending on whether $p \mid x$, $p \mid d$ or $p \nmid \operatorname{lcm}(x, d)$), which shows that $U_{G'} = U_d \subseteq \varphi(U_n) = \varphi(U_G)$.

As one easy consequence of (4), we have

$$\phi_H\Big(\sigma(U_G^2(S))\Big) = \sigma\Big(\phi_H(U_G)^2(\phi_H(S))\Big) = \sigma\Big(U_{G/H}^2(\phi_H(S))\Big), \tag{5}$$

which allows us to argue inductively using factor rings G/H. In particular, $\mathsf{D}_{U_{G/H}^2}(G/H)$ is the minimal integer ℓ such that any sequence $S \in \mathcal{F}(G)$ with $|S| \ge \ell$ has a nontrivial subsequence $T \mid S$ with $H \cap \sigma(U_G^2(T)) \neq \emptyset$. As a second consequence, we have the following lemma, which allows us to apply Theorem 1.1 inductively to a subsequence whose terms are all from a proper *subgroup* $H \le G \cong \mathbb{Z}/n\mathbb{Z}$, even though H is not a *subring* of G.

Lemma 3.1. *Let G be a ring isomorphic to $\mathbb{Z}/n\mathbb{Z}$, let $H \le G$ be an additive subgroup of order $\frac{n}{d}$, and let $S \in \mathcal{F}(H)$ be a sequence of terms from H. Then*

$$\overline{\sigma(U_G^2(S))} = \sigma(U_{n/d}^2(\overline{S})),$$

where $H \cong \overline{H} = \mathbb{Z}/\frac{n}{d}\mathbb{Z}$ is the ring isomorphism described above. In particular, a sequence $S \in \mathcal{F}(H)$ is a U_G^2-weighted zero-sum in G if and only if $\overline{S} \in \mathcal{F}(\mathbb{Z}/\frac{n}{d}\mathbb{Z})$ is a $U_{n/d}^2$-weighted zero-sum in $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$.

P r o o f. Let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell$ with $s_i \in H$ and let

$$g = u_1^2 s_1 + \ldots + u_\ell^2 s_\ell \in \sigma(U_G^2(S))$$

be an arbitrary element, where $u_i \in U_G$. By (3), we have

$$g = \psi_d(u_1^2) \cdot s_1 + \ldots + \psi_d(u_\ell^2) \cdot s_\ell,$$

so that applying the ring isomorphism $\bar{\cdot}$ yields

$$\overline{g} \;=\; \overline{\psi_d}(u_1^2)\,\overline{s_1} + \ldots + \overline{\psi_d}(u_\ell^2)\,\overline{s_\ell} \in \sigma(U_{n/d}^2(\overline{S}))$$

where the inclusion follows from $\overline{\psi_d}(U_G^2) = \overline{\psi_d}(U_G)^2 = U_{n/d}^2$ (attained by applying (4) to the ring homomorphism $\overline{\psi_d}$). Thus $\overline{\sigma(U_G^2(S))} \subseteq \sigma(U_{n/d}^2(\overline{S}))$.

On the other hand, if $g' = v_1^2\,\overline{s_1} + \ldots + v_\ell^2\,\overline{s_\ell} \in \sigma(U_{n/d}^2(\overline{S}))$ is an arbitrary element, where $v_i \in U_{n/d} = \overline{\psi_d}(U_G)$, then each $v_i = \overline{\psi_d}(u_i) = \overline{\psi_d(u_i)}$ for some $u_i \in U_G$, in which case $g = u_1^2 s_1 + \ldots + u_\ell^2 s_\ell \in \sigma(U_G^2(S))$ has $\overline{g} = g'$ by the argument above, showing the reverse inclusion. □

The primes 3 and 5 need to be treated with extra care. If $G = \mathbb{Z}/n\mathbb{Z}$ with $n = 3^{n_3}$, then

$$U_{3^{n_3}}^2 = 1 + 3G.$$

If $n = 5^{n_5}$, then

$$U_{5^{n_5}}^2 = \{1, -1\} + 5G.$$

We also recall that $-1 \in U_p^2$, for an odd prime p, precisely when $p \equiv 1 \mod 4$.

Let G be an abelian group and let $S \in \mathcal{F}(G)$ be a sequence of terms from G. If $H \subseteq G$ is a subset, then we let $S_H \mid S$ denote the subsequence consisting of all terms from H. Thus $S = S_H \cdot S_{G\setminus H}$.

If $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell \in \mathcal{F}(G)$ with $G \cong \mathbb{Z}/n\mathbb{Z}$, then we generally have $\Sigma_m(U_G^2(S)) \neq \Sigma_m(U_G^2(S+g))$, where $g \in G$ and $S+g \in \mathcal{F}(G)$ denotes the translated sequence $(s_1+g)\cdot\ldots\cdot(s_\ell+g) \in \mathcal{F}(G)$. Moreover, $0 \in \Sigma_m(U_G^2(S+g))$ need not imply $0 \in \Sigma_m(U_G^2(S))$. As is often the case, the lack of translational invariance makes dealing with $\Sigma_m(U_G^2(S))$ more complicated. However, the following lemma gives one case when we are allowed to translate the terms of S.

Lemma 3.2. *Let n and m be positive integers, let $G \cong \mathbb{Z}/n\mathbb{Z}$, let $x \in G$ be an element with $\mathrm{ord}(x) = 3^\alpha$, where $\alpha \geq 0$, let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell \in \mathcal{F}(G)$ be a sequence of terms from G, and let $M = |\{i \in [1,\ell] : \mathsf{v}_3(\mathrm{ord}(s_i)) \geq \alpha\}|$ denote the number of terms s_i of S with $\mathsf{v}_3(\mathrm{ord}(s_i)) \geq \alpha$. Suppose $M \geq |S| - m + 1$ and $3 \mid m$. Then*

$$0 \in \Sigma_m(U_G^2(S+x)) \quad \textit{implies} \quad 0 \in \Sigma_m(U_G^2(S)),$$

where $S + x = (s_1+x)\cdot\ldots\cdot(s_\ell+x) \in \mathcal{F}(G)$.

P r o o f. If $3 \nmid n$, then $x = 0$ in view of $\mathrm{ord}(x) = 3^\alpha$, in which case the lemma is trivial. Therefore we may assume $3 \mid n$. Let

$$G = G_3 \times G_{p_1} \times \ldots \times G_{p_r} \cong \mathbb{Z}/n\mathbb{Z},$$

where $p_1, \ldots, p_r$ are the distinct prime divisors of n that are greater than 3, $G_3 = \mathbb{Z}/3^{n_3}\mathbb{Z}$, and each $G_{p_i} = \mathbb{Z}/q_i\mathbb{Z}$ with $q_i = p_i^{\mathsf{v}_{p_i}(n)}$ for $i = 1, \ldots, r$. By hypothesis, there exists a subsequence $s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_m \mid S$ and

$$u_i \in U_G = U_{3^{n_3}} \times U_{q_1} \times \ldots \times U_{q_r},$$

for $i = 1, \ldots, m$, such that

$$0 = u_1^2(s_1+x) + \ldots + u_m^2(s_m+x). \tag{6}$$

Since $\mathrm{ord}(x) = 3^\alpha$, we have $x \in G_3$, in which case we see that it suffices to show that

$$0 \in \sigma\Big(U_{3^{n_3}}^2(\pi(S))\Big),$$

where $\pi : G \to G_3 = \mathbb{Z}/3^{n_3}\mathbb{Z}$ is the projection map onto the first coordinate. To this end, we may w.l.o.g. assume $G = G_3 = \mathbb{Z}/3^{n_3}\mathbb{Z}$, in which case $U_G^2 = 1 + 3G$ and it remains to show

$$0 \in \sigma(U_G^2(S)). \tag{7}$$

Since $U_G^2 = 1 + 3G$, each $u_i^2 = 1 + 3v_i$ with $v_i \in G$, for $i = 1, \ldots, m$, and now (6) yields

$$0 \;=\; (1+3v_1)(s_1+x) + \ldots + (1+3v_m)(s_m+x)$$

$$= \quad \sigma(S) + 3\sum_{i=1}^{m} s_i v_i + \Big(m + 3\sum_{i=1}^{m} v_i\Big)x. \tag{8}$$

We may w.l.o.g. assume $\mathrm{ord}(s_1) = \max\{\mathrm{ord}(s_i) : \ i \in [1,m]\} = 3^{\beta}$, in which case

$$\langle s_1, \ldots, s_m\rangle = 3^{n_3-\beta}G \tag{9}$$

with $s_1 \in 3^{n_3-\beta}G \setminus 3^{n_3-\beta+1}G$. By hypothesis, $M \geq |S| - m + 1$, so that the pigeonhole principle ensures that $\mathrm{ord}(s_i) \geq 3^{\alpha}$ for some $i \in [1,m]$. Thus $\beta \geq \alpha$, so that

$$x \in 3^{n_3-\alpha}G \leq 3^{n_3-\beta}G. \tag{10}$$

Consequently, we see that (8), combined with (9), (10) and the hypothesis $3 \mid m$, yields

$$\sigma(S) = -3\sum_{i=1}^{m} s_i v_i - \Big(m + 3\sum_{i=1}^{m} v_i\Big)x \in 3^{n_3-\beta+1}G. \tag{11}$$

Since $U_G^2 = 1 + 3G$, it follows (in view of the definition of β and s_1) that

$$\sigma(U_G^2(S)) = \sum_{i=1}^{m}(1+3G)s_i = \sigma(S) + 3s_1G = \sigma(S) + 3^{n_3-\beta+1}G$$

is a $3^{n_3-\beta+1}G$-coset, which combined with equation (11) implies $0 \in 3^{n_3-\beta+1}G = \sigma(U_G^2(S))$, yielding (7) and completing the proof. □

Finally, we recall the following classical result from design theory [Kr, Section 12.1.6].

Theorem 3.3. *Let $\mathcal{H}$ be a hypergraph on v vertices such that any two vertices of $\mathcal{H}$ are contained in a unique edge of $\mathcal{H}$ (i.e., $\mathcal{H}$ is a pairwise balanced design with $\lambda = 1$). Let $K' \subseteq \mathbb{N}$ be a subset that contains all numbers that occur as a size of an edge of $\mathcal{H}$, and let $\beta(K') = \gcd\{k(k-1) : \ k \in K'\}$. Then*

$$v(v-1) \equiv 0 \mod \beta(K').$$

4. Representation Lemmas

In this section, we use the method of exponential or character sums to give precise information about which elements can be represented as a U_n^2-weighted sum for $n = p^{\alpha}$ an odd prime power. To this end, if $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_{\ell}$ is a sequence of integers, $t \in \mathbb{Z}$ and $q = p^{\alpha}$ is an odd prime power, then we let $N_q(t;S)$ to be

$$p^{-\alpha(|S|-1)+|S|}\big|\{(a_1, \ldots, a_{\ell}) \in U_n \times \ldots \times U_n : \ a_1^2 s_1 + \ldots + a_{\ell}^2 s_{\ell} \equiv -t \mod q\}\big|$$

and denote an appropriately scaled multiple of the number of representations modulo q in $\sigma(U_G^2(S))$ of $-t$. Thus $N_q(t;S) > 0$ precisely when $-t \in \sigma(U_q^2(S))$ modulo q.

The following lemmas will show that many elements of $\mathbb{Z}/q\mathbb{Z}$ can be represented as U_n^2-weighted subsequence sums of very short sequences $S \in \mathcal{F}(\mathbb{Z}/q\mathbb{Z})$ (of length 2, 3 or 4) provided the terms of S are *units*, i.e., generating elements for $\mathbb{Z}/q\mathbb{Z}$. They also give precise information about how many representations as a U_n^2-weighted subsequence sum each $-t \in \mathbb{Z}/q\mathbb{Z}$ has in terms of the quadratic character $\chi_p : U_q \to \{-1, 1\}$, which is the multiplicative group homomorphism that takes an element x from the multiplicative group U_q of units in $\mathbb{Z}/q\mathbb{Z}$ and assigns the value 1 or -1 to x according to whether x is a square or not. Thus, for $x \in \mathbb{Z}$ with $\gcd(x,p) = 1$, we have $\chi_p(x) = 1$ if $x \equiv y^2 \mod p$ for some $y \in \mathbb{Z}$, and $\chi_p(x) = -1$ otherwise.

Lemma 4.1. *Let $q = p^\alpha$ be an odd prime power, let $t \in \mathbb{Z}$ be an integer, let $x, y, z \in U_q$ be units in $\mathbb{Z}/q\mathbb{Z}$, and let $\chi = \chi_p$ be the quadratic character modulo p.*

1. *For $\gcd(p,t) = 1$, we have*

$$N_q(t; x \cdot y \cdot z) = (p-1)^3 + \chi(txyz)p^2 + (-1)^{(p-1)/2}(\chi(xy) + \chi(yz) + \chi(zx) + \chi(tx) + \chi(ty) + \chi(tz))p + 1.$$

2. *For $p \mid t$, we have*

$$N_q(t; x \cdot y \cdot z) = (p-1)^3 - (-1)^{(p-1)/2}(\chi(xy) + \chi(yz) + \chi(zx))(p-1)p - (p-1).$$

P r o o f. We set $e(x) = \exp(2\pi i x)$, where $i = \sqrt{-1}$ here. We will use the following Gauss sums:

$$G(h,d) = \sum_{u=1}^{d} e\left(\frac{hu^2}{d}\right) \quad \text{and} \quad G^*(h,d) = \sum_{\substack{u=1 \\ \gcd(u,d)=1}}^{d} e\left(\frac{hu^2}{d}\right).$$

Firstly, for $\beta \geq 2$ and $p \nmid h$, one has

$$G^*(h,p^\beta) = \sum_{\substack{u=1 \\ p \nmid u}}^{p^\beta} e\left(\frac{hu^2}{p^\beta}\right) = G(h,p^\beta) - \sum_{u=1}^{p^{\beta-1}} e\left(\frac{hu^2}{p^{\beta-2}}\right)$$

$$= G(h,p^\beta) - \sum_{v=1}^{p^{\beta-2}} \sum_{w=0}^{p-1} e\left(\frac{hv^2}{p^{\beta-2}}\right) = G(h,p^\beta) - pG(h,p^{\beta-2}),$$

where we have considered the change of variables $u = v + p^{\beta-2}w$. Secondly, still assuming $\beta \geq 2$ and using the change of variables $u = v + p^{\beta-1}w \in [1, p^\beta]$, where $w \in [0, p-1]$ and $v \in [1, p^{\beta-1}]$, for the first equality below, we have

$$\begin{aligned} G(h,p^\beta) &= \sum_{v=1}^{p^{\beta-1}} e\left(\frac{hv^2}{p^\beta}\right) \sum_{w=0}^{p-1} e\left(\frac{2hvw}{p}\right) = p \sum_{\substack{v=1 \\ p|v}}^{p^{\beta-1}} e\left(\frac{hv^2}{p^\beta}\right) = p \sum_{v=1}^{p^{\beta-2}} e\left(\frac{hv^2}{p^{\beta-2}}\right) \\ &= p\, G(h,p^{\beta-2}), \end{aligned}$$

where the second equality follows from the fact that sum of all p-th roots of unity is zero (along with the hypotheses p odd and $\gcd(p,h) = 1$); see [Gr, Chapter 1] or [Na, Chapter 2.7]. Hence

$$G^*(h,p^\beta) = 0 \quad \text{for } \beta \geq 2 \text{ and } p \nmid h. \tag{12}$$

Using the exponential sums $G^*(h,p^\beta)$ (see [Na, Chapter 2.7] or [Gr, Proposition 19.1] for the first equality), we may express $N_q(t; x \cdot y \cdot z)$ as

$$\begin{aligned} N_q(t;x\cdot y\cdot z) &= \frac{1}{p^{3\alpha-3}} \sum_{h=1}^{p^\alpha} G^*(hx,p^\alpha) G^*(hy,p^\alpha) G^*(hz,p^\alpha) e\Big(\frac{ht}{p^\alpha}\Big) \\ &= (p-1)^3 + \frac{1}{p^{3\alpha-3}} \sum_{\beta=1}^{\alpha} \sum_{\substack{h=1 \\ p\nmid h}}^{p^\beta} G^*(hxp^{\alpha-\beta},p^\alpha) G^*(hyp^{\alpha-\beta},p^\alpha) G^*(hzp^{\alpha-\beta},p^\alpha) e\Big(\frac{ht}{p^\beta}\Big) \\ &= (p-1)^3 + \frac{1}{p^{3\alpha-3}} \sum_{\beta=1}^{\alpha} p^{3(\alpha-\beta)} \sum_{\substack{h=1 \\ p\nmid h}}^{p^\beta} G^*(hx,p^\beta) G^*(hy,p^\beta) G^*(hz,p^\beta) e\Big(\frac{ht}{p^\beta}\Big), \end{aligned}$$

which gives, by (12),

$$\begin{aligned} N_q(t;x\cdot y\cdot z) &= (p-1)^3 + \sum_{h=1}^{p-1} G^*(hx,p) G^*(hy,p) G^*(hz,p) e\left(\frac{ht}{p}\right) \\ &= (p-1)^3 + \sum_{h=1}^{p-1} \big(G(hx,p)-1\big)\big(G(hy,p)-1\big)\big(G(hz,p)-1\big) e\left(\frac{ht}{p}\right). \end{aligned}$$

We know that $G(h,p)$, for $p \nmid h$, can be related to the usual Gauss sums $\tau(\chi) = \sum_{a=1}^{p-1} \chi(a)e(a/p)$:

$$G(h,p) = \sum_{a=1}^{p-1} \chi(a) e\left(\frac{ha}{p}\right) = \sum_{b=1}^{p-1} \chi(b)\overline{\chi(h)} e\left(\frac{b}{p}\right) = \overline{\chi(h)}\tau(\chi) = \chi(h)\tau(\chi),$$

where the $\bar{\cdot}$ used above refers to complex conjugation, so that $\chi(h) = \overline{\chi(h)} = \chi(h)^{-1} = \chi(h^{-1})$, and where the second equality follows by using the substitution $b = ah$. We now use the classical identity $\tau(\chi) = \sqrt{p}$ or $i\sqrt{p}$ according to $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$ (cf. [Ay, Theorem 4.15, p. 315]). We let E be the error term $E = N_q(t; x \cdot y \cdot z) - (p-1)^3$. Hence, for $p \equiv 1 \bmod 4$,

$$\begin{aligned} E &= \sum_{h=1}^{p-1} (\chi(hx)\sqrt{p} - 1)(\chi(hy)\sqrt{p} - 1)(\chi(hz)\sqrt{p} - 1) e\left(\frac{ht}{p}\right) \\ &= \big(p^{3/2}\chi(xyz) + \sqrt{p}(\chi(x) + \chi(y) + \chi(z))\big) \sum_{h=1}^{p-1} \chi(h) e\left(\frac{ht}{p}\right) \\ &\qquad - \big(p(\chi(xy) + \chi(yz) + \chi(zx)) + 1\big) \sum_{h=1}^{p-1} e\left(\frac{ht}{p}\right). \end{aligned}$$

If $p \nmid t$, then $\sum_{h=1}^{p-1} \chi(h) e\big(\frac{ht}{p}\big) = \chi(t)\sqrt{p}$ and $\sum_{h=1}^{p-1} e\big(\frac{ht}{p}\big) = -1$, whence

$$E = p^2\chi(xyzt) + p\big(\chi(xt) + \chi(yt) + \chi(zt) + \chi(xy) + \chi(yz) + \chi(zx)\big) + 1.$$

If $p \mid t$, then $\sum_{h=1}^{p-1} \chi(h) e\big(\frac{ht}{p}\big) = 0$ and $\sum_{h=1}^{p-1} e\big(\frac{ht}{p}\big) = p-1$, whence

$$E = -p(p-1)\big(\chi(xy) + \chi(yz) + \chi(zx)\big) - (p-1).$$

We argue similarly when $p \equiv 3 \bmod 4$. □

Consequently, if $p \mid t$, then $N_q(t; x\cdot y\cdot z) > 0$ when $p > 2 + (-1)^{(p-1)/2}(\chi(xy) + \chi(yz) + \chi(zx))$, which is always the case for $p > 5$. If $p \nmid t$, then we could observe that $N_q(t; x \cdot y \cdot z) = (p-1)^3 - p^2 + 1$ if $txyz$ is not a square modulo p, and $N_q(t; x \cdot y \cdot z) \geq (p-1)^3 + p^2 - 6p + 1$ if $txyz$ is a square modulo p. Hence $N_q(t; x \cdot y \cdot z) > 0$ if $p \geq 5$. Applying this to $p = 5$, one gets $U_{5^\alpha} \subseteq U_{5^\alpha}^2(x) + U_{5^\alpha}^2(y) + U_{5^\alpha}^2(z)$. Since $U_{5^\alpha}^2 = \{1,4\} + 5(\mathbb{Z}/5^\alpha\mathbb{Z})$, we deduce, when $5 \nmid xyzu$, that

$$\begin{aligned} &U_{5^\alpha}^2(x) + U_{5^\alpha}^2(y) + U_{5^\alpha}^2(z) + U_{5^\alpha}^2(u) \\ &\qquad = \{1,2,3,4\} + 5(\mathbb{Z}/5^\alpha\mathbb{Z}) + \{u, 4u\} + 5(\mathbb{Z}/5^\alpha\mathbb{Z}) = \mathbb{Z}/5^\alpha\mathbb{Z}. \end{aligned} \tag{13}$$

This property has been obtained in [CM] by using Kneser's Theorem.

For $p = 5$, our results are still unsatisfactory when $5 \mid t$. Hence we need an additional result.

Lemma 4.2. *Let $q = p^\alpha$ be an odd prime power, let $t \in \mathbb{Z}$ be an integer, let $x, y \in U_q$ be units in $\mathbb{Z}/q\mathbb{Z}$, and let $\chi = \chi_p$ be the quadratic character modulo p.*

1. *For $p \nmid t$, we have*
$$N_q(t; x \cdot y) = (p-1)^2 - (-1)^{(p-1)/2}(\chi(xy) + \chi(tx) + \chi(ty))p - 1.$$
2. *For $p \mid t$, we have*
$$N_q(t; x \cdot y) = ((-1)^{(p-1)/2}\chi(xy) + 1)p(p-1).$$

P r o o f. We argue as in the preceding lemma and consider only the case $p \equiv 1 \bmod 4$. We write $N_q(t; x \cdot y) = (p-1)^2 + E$, where
$$\begin{aligned} E &= \sum_{h=1}^{p-1} (\chi(hx)\sqrt{p} - 1)(\chi(hy)\sqrt{p} - 1) e\left(\frac{ht}{p}\right) \\ &= (p\chi(xy) + 1) \sum_{h=1}^{p-1} e\left(\frac{ht}{p}\right) - \sqrt{p}(\chi(x) + \chi(y)) \sum_{h=1}^{p-1} \chi(h) e\left(\frac{ht}{p}\right), \end{aligned}$$
and the result follows by distinguishing the cases $p \mid t$ and $p \nmid t$. □

We deduce from it that, if t is a multiple of $p \equiv 1 \bmod 4$, and if xy is square modulo p, then $t \in U_{p^\alpha}^2(x) + U_{p^\alpha}^2(y)$. Moreover, for each such $p > 5$, every invertible residue class modulo p^α is in $U_{p^\alpha}^2(x) + U_{p^\alpha}^2(y)$.

We now summarize the key points of the previous lemmas.

Lemma 4.3. *Let $q = p^\alpha$ be an odd prime power, let $G = \mathbb{Z}/q\mathbb{Z}$, and let $S \in \mathcal{F}(U_q)$ be a nontrivial sequence of units from G.*

1. *If $p \geq 7$ and $|S| \geq 3$, then $\sigma(U_q^2(S)) = G$.*
2. *If $p = 5$ and $|S| \geq 4$, then $\sigma(U_q^2(S)) = G$.*
3. *If $p = 5$ and $|S| = 3$, then $U_q \subseteq \sigma(U_q^2(S))$ and either $\sigma(U_q^2(S)) = G$ or the three terms of S are quadratically equivalent modulo 5 (so $\chi_5(x) = \chi_5(y) = \chi_5(z)$, where $S = x \cdot y \cdot z$). In the later case, we have $5G \subseteq \sigma(U_q^2(T))$ for any length two subsequence $T \mid S$.*
4. *If $p = 3$ and $\sigma(S) \in 3G$, then $\sigma(U_q^2(S)) = 3G$.*

P r o o f. Part 1 follows by Lemma 4.1 as explained after its proof. Part 2 follows as noted in (13). Part 3 follows from Lemmas 4.1 and 4.2. For Part 4, we have only to recall that $U_{3^\alpha}^2 = 1+3G$, so that $\sigma(U_q^2(S))$ is a $3G$-coset. More precisely, letting

$S = s_1 \cdot \ldots \cdot s_\ell$ with each $s_i \in U_q$ a unit, we have $U_q^2(s_i) = s_i + 3s_iG = s_i + 3G$ for each $i \in [1, \ell]$ (since the map $x \mapsto s_i x$ is an isomorphism of G). Thus $\sigma(U_q^2(S)) = \sum_{i=1}^{\ell} U_q^2(s_i) = \sum_{i=1}^{\ell}(s_i + 3G) = \sigma(S) + 3G = 3G$, with the final equality in view of the hypothesis $\sigma(S) \in 3G$. □

5. Stable Sequences and Pairwise Balanced Designs

For the proof of our main results, we will utilize an inductive structure that works in greater generality and which has nothing inherit to do with weighted subsequence sums. We present the ideas here.

Let G be a finite abelian group and let $\mathcal{S}_G$ be the set of subgroups of G. Let

$$f : \mathcal{S}_G \to \mathbb{Z}^+$$

be a function that assigns a positive integer to each subgroup of G. We say that f is *admissible* provided

A1. $f(H_1) \le f(H_2)$ for any subgroups $H_1 \le H_2 \le G$, and

A2. $f(H_1 + H_2) \le f(H_1) + f(H_2) - f(H_1 \cap H_2)$ for any subgroups H_1, $H_2 \le G$.

If the inequality in A1 is always strict when $H_1 < H_2$, then we say that f is *strictly admissible*. Given a finite abelian group G, an admissible function $f : \mathcal{S}_G \to \mathbb{Z}^+$, a sequence $S \in \mathcal{F}(G)$, and a subgroup $H \le G$, we say that H is *f-stable* in S provided

S1. $\langle \mathrm{supp}(S_H) \rangle = H$, and

S2. $|S_{H \setminus H'}| \ge f(H) - f(H') + 1$ for all proper subgroups $H' < H$.

We say that the sequence S is *f-stable* provided $\langle \mathrm{supp}(S) \rangle$ is f-stable in S. Note that S_H is f-stable when H is f-stable in S.

Finally, if f is admissible for G and $K \le G$ is a subgroup, then we can define another function $f_K : \mathcal{S}_G \to \mathbb{Z}^+$ by setting $f_K(H) = f(K + H)$. If $H_1 \le H_2 \le G$, then $K + H_1 \le K + H_2 \le G$, so A1 holding for f ensures that A1 holds for f_K. We also have

$$\begin{aligned} f_K(H_1 + H_2) &= f(K + H_1 + K + H_2) \\ &\le f(K + H_1) + f(K + H_2) - f((K + H_1) \cap (K + H_2)) \\ &\le f(K + H_1) + f(K + H_2) - f(K + (H_1 \cap H_2)) \\ &= f_K(H_1) + f_K(H_2) - f_K(H_1 \cap H_2), \end{aligned}$$

where the first inequality follows from A2 for f, and the second from A1 for f along with the inequality $K + (H_1 \cap H_2) \le (K + H_1) \cap (K + H_2)$. This shows that f_K is admissible for G. Also, observe that $f_K = f$ when K is trivial.

The basic idea is as follows. Suppose one has a combinatorial invariant for certain finite abelian groups, like a weighted Davenport constant, that represents the minimal length so that all sequences of this length possess a desired property, e.g., contain a weighted zero-sum subsequence. If one wishes to show that the function f is an upper bound for this combinatorial invariant and is proceeding inductively, then the general procedure is to take a sequence $S \in \mathcal{F}(G)$ of length $|S| = f(G)$ with $\langle \mathrm{supp}(S) \rangle = G$ and assume S2 holds, else the theorem follows by applying an induction hypothesis to some subsequence $S_H \in \mathcal{F}(H)$ having $|S_H| = |S| - |S_{G\setminus H}| = f(G) - |S_{G\setminus H}| \ge f(H)$. Of course, one may not be able to effectively use the inductive hypothesis on certain subgroups $H \le G$, so it may be necessary to modify the function f to exclude these groups, hence the definition of f_K. This will be our general strategy for bounding $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z})$ in the next section. We now proceed with showing that there is always a certain underlying structure inherent when dealing with this general setup. Indeed, this structure will eventually allow us to define a pairwise balanced design with $\lambda = 1$ at the end of the section.

Lemma 5.1. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function, and let $S \in \mathcal{F}(G)$ be sequence of terms from G. Then there exists a minimal subgroup $H \le G$ such that*

$$|S_{G\setminus H}| \le f(G) - f(H).$$

Moreover, if $|S| \ge f(G) - f(H) + 1$, then $H = \langle \mathrm{supp}(S_H) \rangle$ is f-stable in S.

P r o o f. Let $G_0 = \langle \mathrm{supp}(S) \rangle$. Then $|S_{G\setminus G_0}| = 0 \le f(G) - f(G_0)$ in view of A1. Thus, since G is finite, there must exists a minimal subgroup $H \le G$ such that

$$|S_{G\setminus H}| \le f(G) - f(H).$$

If we also have $|S| \ge f(G) - f(H) + 1$, then S_H will be nontrivial. Thus, in view of A1, we must have $\langle \mathrm{supp}(S_H) \rangle = H$, else the subgroup $\langle \mathrm{supp}(S_H) \rangle$ would contradict the minimality of H. If S2 holds, then H is stable, as desired. Otherwise, there exists a proper subgroup $H' < H$ such that $|S_{H\setminus H'}| \le f(H) - f(H')$. However, in this case, we have

$$|S_{G\setminus H'}| = |S_{G\setminus H}| + |S_{H\setminus H'}| \le f(G) - f(H) + f(H) - f(H') = f(G) - f(H'),$$

so that H' contradicts the minimality of H. □

Lemma 5.2. *Let G be a finite abelian group G and let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \ge f(H_1) + \epsilon$ whenever $H_1 < H_2 \le G$,*

where $\epsilon \in \mathbb{Z}^+$. Let $S \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $\langle \mathrm{supp}(S)\rangle = G$, and let $K \le G$ be a subgroup.

If $H \le G$ is a subgroup with $|S_{G\setminus H}| \le f_K(G) - f_K(H) + \epsilon$, then $K \le H$.

P r o o f. Assume by contradiction that $H < H + K \le G$. Then $f(H + K) \ge f(H) + \epsilon$ by hypothesis, so that our other hypotheses give

$$|S_{G\setminus H}| \quad \le \quad f_K(G) - f_K(H) + \epsilon = f(G) - f(K + H) + \epsilon \le f(G) - f(H).$$

However, since $\langle \mathrm{supp}(S)\rangle = G$ by hypothesis, this contradicts that S is f-stable. □

Lemma 5.3. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be a strictly admissible function, let $S \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $\langle \mathrm{supp}(S)\rangle = G$, and let $K \le G$ be a subgroup.*

Suppose $T \mid S$ is a subsequence such that $|T| \le f_K(G) - f_K(H) + 1$, where $H = \langle \mathrm{supp}(S \cdot T^{[-1]})\rangle$. Then $K \le H$. Moreover, if $H < G$ is proper, then $S \cdot T^{[-1]} = S_H$.

P r o o f. By hypothesis, we have

$$|S_{G\setminus H}| \le |T| \le f_K(G) - f_K(H) + 1.$$

As as result, since f is strictly admissible, Lemma 5.2 yields $K \le H$. Now assume $H < G$ is proper.

If $|S_{G\setminus H}| \le f_K(G) - f_K(H) = f(G) - f(K + H) = f(G) - f(H)$, where the latter equality follows in view of $K \le H$, then this would contradict that S is f-stable with $\langle \mathrm{supp}(S)\rangle = G$. Therefore we may assume $|S_{G\setminus H}| \ge f_K(G) - f_K(H) + 1$, which forces equality to hold in our earlier estimate:

$$|S_{G\setminus H}| = |T| = f_K(G) - f_K(H) + 1.$$

Since $H = \langle \mathrm{supp}(S\cdot T^{[-1]})\rangle$, the only terms of S that can be from $G\setminus H$ are those from T. Consequently, the equality $|S_{G\setminus H}| = |T|$ is equivalent to $S \cdot T^{[-1]} = S_H$, as desired. □

Lemma 5.4. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \ge f(H_1) + \epsilon$ whenever $H_1 < H_2 \le G$, where $\epsilon \in \mathbb{Z}^+$, let $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S)\rangle = G$, and let $K \le G$ be a subgroup with $f(K) \ge \epsilon + 1$.*

Suppose $T = S(I) \mid S$ is a subsequence with $|T| \le f_K(G) - f_K(H) + \epsilon$ and $\mathrm{supp}(S \cdot T^{[-1]}) \subseteq H \le G$, where $I \subseteq [1, \ell]$. Then there exists a subsequence $U = S(J) \mid S$ such that

1. *$I \subseteq J$, so $T \mid U$,*

2. $K \le L \le H$, *where* $L = \langle \mathrm{supp}(S \cdot U^{[-1]}) \rangle$,
3. $|U| \le f_K(G) - f_K(L) + \epsilon$, *and*
4. $S \cdot U^{[-1]}$ *is* f_K*-stable.*

P r o o f. Since $f(H_2) \ge f(H_1) + \epsilon$ whenever $H_1 < H_2 \le G$, and since $|S_{G\setminus H}| \le |T|$ (in view of $\mathrm{supp}(S \cdot T^{[-1]}) \subseteq H$), Lemma 5.2 implies that $K \le H$. Let $S' = S \cdot T^{[-1]} \in \mathcal{F}(H)$ and apply Lemma 5.1 to the sequence $S' \in \mathcal{F}(H)$ using the admissible function f_K. Let $L \le H$ be the resulting subgroup and let $U = S'_{H\setminus L} \cdot T$, so that

$$S'_L = S' \cdot S'^{[-1]}_{H\setminus L} = S \cdot T^{[-1]} \cdot S'^{[-1]}_{H\setminus L} = S \cdot U^{[-1]}. \tag{14}$$

Then Lemma 5.1 and our hypothesis $|T| \le f_K(G) - f_K(H) + \epsilon$ yield

$$\begin{aligned} |S_{G\setminus L}| \le |U| = |S'_{H\setminus L}| + |T| &\le f_K(H) - f_K(L) + (f_K(G) - f_K(H) + \epsilon) \\ &= f_K(G) - f_K(L) + \epsilon. \end{aligned}$$

Consequently, since $f(H_2) \ge f(H_1) + \epsilon$ whenever $H_1 < H_2 \le G$, Lemma 5.2 implies that $K \le L$, whence

$$|S'| = |S| - |T| \ge f_K(H) - \epsilon \ge f_K(H) - f_K(K) + 1 \ge f_K(H) - f_K(L) + 1,$$

where the first inequality follows in view of the hypotheses $|S| = f(G) = f_K(G)$ and $|T| \le f_K(G) - f_K(H) + \epsilon$, the second from the hypothesis $f_K(K) = f(K) \ge \epsilon + 1$, and the third in view of $K \le L$ and A1. Thus Lemma 5.1 further implies that L is f_K-stable in S', implying that $S'_L = S \cdot U^{[-1]}$ (see (14)) is an f_K-stable sequence and that $L = \langle \mathrm{supp}(S'_L) \rangle = \langle \mathrm{supp}(S \cdot U^{[-1]}) \rangle$. Letting $T = S(I)$ and $U = S(J)$, with $I, J \subseteq [1, \ell]$, we clearly have $I \subseteq J$ in view of the definition of U, and all parts of the lemma have now been established. □

Lemma 5.5. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be a strictly admissible function, let $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \le G$ be a subgroup with $f(K) \ge 2$.*

Suppose $T_1 = S(I_1) \mid S$ and $T_2 = S(I_2) \mid S$, where $I_1, I_2 \subseteq [1, \ell]$, are subsequences such that, for $i = 1, 2$,

(a) $S \cdot T_i^{[-1]}$ *is f_K-stable and*

(b) $|T_i| \le f_K(G) - f_K(H_i) + 1$, *where* $H_i = \langle \mathrm{supp}(S \cdot T_i^{[-1]}) \rangle$.

If $I_1 \cap I_2 \ne \emptyset$, then there exists a subsequence $T = S(I) \mid S$, where $I \subseteq [1, \ell]$, such that

(i) $S \cdot T^{[-1]}$ *is f_K-stable,*

(ii) $|T| \le f_K(G) - f_K(H) + 1$, *where* $H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle$,
(iii) $I_1 \cup I_2 \subseteq I$ *and* $H \le H_1 \cap H_2$.

P r o o f. If $H_1 = G$, then (b) implies $|T_1| \le 1$. Hence, since $I_1 \cap I_2 \neq \emptyset$, this forces $I_1 \subseteq I_2$, so that the theorem holds with $I = I_2$, $T = T_2$ and $H = H_2$. Therefore we may assume $H_1 < G$ is proper. Likewise, we may assume $H_2 < G$ is proper. Consequently, Lemma 5.3 implies that

$$K \le H_1 \cap H_2 \quad \text{and} \quad S_{H_i} = S \cdot T_i^{[-1]} \quad \text{for } i = 1, 2. \tag{15}$$

Let $I' = I_1 \cup I_2$ and let $T' = S(I') \mid S$. Since $\mathrm{supp}(S \cdot T_i^{[-1]}) \subseteq H_i$, we have $\mathrm{supp}(S \cdot T'^{[-1]}) \subseteq H_1 \cap H_2$. Indeed, $S_{H_1 \cap H_2} = S \cdot T'^{[-1]}$.

If

$$|T'| = |I_1 \cup I_2| \le f_K(G) - f_K(H_1 \cap H_2) + 1, \tag{16}$$

then, since f is strictly admissible with $f(K) \ge 2$, we can apply Lemma 5.4 (with $\epsilon = 1$ and H taken to be $H_1 \cap H_2$) to the sequence T', resulting in the the desired subsequence $T = S(I) \mid S$ with $I_1 \cup I_2 = I' \subseteq I$. Therefore, we see that it suffices to show (16) holds to complete the proof.

From (b), we know

$$|I_1| = |T_1| \le f_K(G) - f_K(H_1) + 1 \ \text{ and } \ |I_2| = |T_2| \le f_K(G) - f_K(H_2) + 1. \tag{17}$$

Now $S \cdot S(I_1 \cap I_2)^{[-1]} = S_{H_1} \cdot S_{H_2} \cdot S_{H_1 \cap H_2}^{[-1]}$ follows in view of (15). Thus $S \cdot S(I_1 \cap I_2)^{[-1]} \mid S_{H_1 + H_2}$. Consequently, we must have

$$|I_1 \cap I_2| = |S(I_1 \cap I_2)| \ge f_K(G) - f_K(H_1 + H_2) + 1 = f(G) - f(H_1 + H_2) + 1, \tag{18}$$

where the latter equality follows in view of $K \le H_1 \cap H_2$. Indeed, if $H_1 + H_2 = G$, then (18) follows from the fact that $I_1 \cap I_2$ is nonempty by hypothesis. On the other hand, if $H_1 + H_2 < G$ is a proper subgroup and (18) fails, then $|S_{G \setminus (H_1 + H_2)}| \le |I_1 \cap I_2| \le f(G) - f(H_1 + H_2)$, contradicting that S is f-stable with $\langle \mathrm{supp}(S) \rangle = G$ by hypothesis. But now, combining (18) with (17), we obtain

$$\begin{aligned} |I_1 \cup I_2| &= |I_1| + |I_2| - |I_1 \cap I_2| \\ &\le (f_K(G) - f_K(H_1) + 1) + (f_K(G) - f_K(H_2) + 1) \\ &\qquad - (f_K(G) - f_K(H_1 + H_2) + 1) \\ &= f_K(G) - f_K(H_1) - f_K(H_2) + f_K(H_1 + H_2) + 1 \\ &\le f_K(G) - f_K(H_1 \cap H_2) + 1, \end{aligned}$$

where the final inequality follows from A2. This establishes (16), completing the proof as already remarked. □

Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be a strictly admissible function, let $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \le G$ be a subgroup with $f(K) \ge 2$.

Given these hypotheses, we can define an equivalence relation on the terms of the indexed sequence S by saying $s_x \sim s_y$, where $x, y \in [1, \ell]$, (formally, by saying $x \sim y$, since we regard *terms* of the indexed sequence as being distinct when their indices are distinct, regardless of whether $s_x = s_y$ as *elements* of G) provided there exists a subsequence $T = S(I) \mid S$, where $I \subseteq [1, \ell]$, such that

C1. $x, y \in I$,

C2. $S \cdot T^{[-1]}$ is f_K-stable

C3. $|T| \le f_K(G) - f_K(H) + 1$, where $H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle$.

The definition of $\sim$ is clearly symmetric. To show $\sim$ is reflexive, i.e., that $s_x \sim s_x$, apply Lemma 5.4 (with $\epsilon = 1$ and H taken to be G) to the subsequence $T = s_x$. Finally, transitivity of $\sim$ follows from Lemma 5.5. An equivalence class defined by $\sim$ will be called an *f_K-component* of S. Of course, since each f_K-component is an equivalence class, we have a factorization $S = T_1 \cdot \ldots \cdot T_r$, where the $T_i \in \mathcal{F}(G)$ are the f_K-components of S.

Lemma 5.6. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be a strictly admissible function, let $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \le G$ be a subgroup with $f(K) \ge 2$.*

Suppose $T \mid S$ is an f_K-component of S. Then T satisfies C2 and C3 and $K \le H$, where $H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle$.

P r o o f. This is a simple consequence of Lemma 5.5. The sequence T_x exhibiting that $s_x \sim s_x$, where s_x is a term of T, shows that there exists a nontrivial subsequence of T that satisfies C2 and C3. Thus let $T' = S(I') \mid T$ be a maximal length subsequence satisfying C2 and C3, where $I' \subseteq [1, \ell]$. If, by contradiction, there is some term s_z of $T \cdot T'^{[-1]}$, then let $T'' = S(I'')$ be a sequence exhibiting that $s_z \sim s_x$, where s_x is a term of T'. Then $x \in I' \cap I''$ and $z \in I'' \setminus I'$. Hence $|I' \cup I''| > |I'| = |T'|$ and $I' \cap I'' \neq \emptyset$. Applying Lemma 5.5 to T' and T'', we find a third subsequence $R = S(J) \mid S$ satisfying C2 and C3 with $I' \cup I'' \subseteq J$. All terms of R must be equivalent, implying $R \mid T$, so R contradicts the maximality of T' in view of $|I' \cup I''| > |T'|$. This shows that the f_K-component T must satisfy C2 and C3. Let $H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle$. Then $|S_{G \setminus H}| \le |T| \le f_K(G) - f_K(H) + 1$, so that Lemma 5.2 implies $K \le H$, completing the proof. □

Lemma 5.7. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be a strictly admissible function, let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \leq G$ be a subgroup with $f(K) \geq 2$.*

If $s_x \in \mathrm{supp}(S) \cap K$, then s_x is an f_K-component of S and $\langle \mathrm{supp}(S \boldsymbol{\cdot} s_x^{[-1]}) \rangle = G$.

P r o o f. Let $T = S(I) \mid S$ be the component of S that contains s_x, so $x \in I$, and then let $H = \langle \mathrm{supp}(S \boldsymbol{\cdot} T^{[-1]}) \rangle$. By Lemma 5.6, C2 and C3 hold for T. If $H = G$, then C3 implies that $|T| = 1$, in which case $T = s_x$ is itself a component, as desired. On the other hand, if $H < G$ is proper, then Lemma 5.3 implies that $S \boldsymbol{\cdot} T^{[-1]} = S_H$ with $K \leq H$. In other words, $\mathrm{supp}(T) \subseteq G \setminus H \subseteq G \setminus K$. However, this contradicts that s_x is a term of T from K. □

Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \geq f(H_1) + 2$ whenever $H_1 < H_2 \leq G$, let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \leq G$ be a subgroup with $f(K) \geq 3$. These are the same hypotheses needed to define f_K-components with the mild strengthening of now requiring $f(K) \geq 3$ and $f(H_2) \geq f(H_1) + 2$ instead of $f(K) \geq 2$ and $f(H_2) \geq f(H_1) + 1$.

A subsequence $T = S(I) \mid S$, where $I \subseteq [1, \ell]$, is called an *f_K-near-component* if

NC1. $S \boldsymbol{\cdot} T^{[-1]}$ is f_K-stable,

NC2. $f_K(T) \leq f_K(G) - f_K(H) + 2$, where $H = \langle \mathrm{supp}(S \boldsymbol{\cdot} T^{[-1]}) \rangle$, and

NC3. T is a maximal (by inclusion) subsequence of S such that NC1 and NC2 hold.

Lemma 5.8. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \geq f(H_1) + 2$ whenever $H_1 < H_2 \leq G$, let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \leq G$ be a subgroup with $f(K) \geq 3$.*

If $T \mid S$ is an f_K-near-component of S, then T contains terms from at least two distinct f_K-components of S and $K \leq H$, where $H = \langle \mathrm{supp}(S \boldsymbol{\cdot} T^{[-1]}) \rangle$. Furthermore, for any two terms s_x and s_y of S with $x, y \in [1, \ell]$ distinct, there exists an f_K-near-component $T = S(I) \mid S$ such that $x, y \in I$.

P r o o f. Let $T \mid S$ be an arbitrary f_K-near-component of S and let $H = \langle \mathrm{supp}(S \boldsymbol{\cdot} T^{[-1]}) \rangle$. In view of the hypothesis $f(H_2) \geq f(H_1) + 2$ for $H_1 < H_2 \leq G$ and Lemma 5.2, we have $K \leq H$. If, by contradiction, T does not contain terms from at least two distinct components, then T must be contained in a

single component of T, in which case the maximality condition NC3 forces T to be equal to this f_K-component. Thus $|S| = f_K(G) \geq f_K(G) - f_K(K) + 3 \geq f_K(G) - f_K(H) + 3$, where we have made use of the strengthened hypothesis $f_K(K) = f(K) \geq 3$ for the first inequality and A1 and $K \leq H$ for the second. Consequently, $S \cdot T^{[-1]}$ must contain at least two terms of S (in view of C3 for the component T). Let $g \in \mathrm{supp}(S \cdot T^{[-1]})$ and apply Lemma 5.4 with $\epsilon = 2$ to $T \cdot g$. Then the resulting sequence $U \mid S$ satisfies NC1 and NC2 with $g \cdot T \mid U$, contradicting the maximality condition NC3 for T.

Now assume s_x and s_y are terms from S with x, $y \in [1, \ell]$ distinct. Applying Lemma 5.4 (with $\epsilon = 2$ and H taken to be G) to the subsequence $s_x \cdot s_y$, we find a subsequence $T = S(I) \mid S$ that satisfies NC1 and NC2 with x, $y \in I$, meaning T is contained in a maximal subsequence satisfying NC1 and NC2, as desired. □

Lemma 5.9. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \geq f(H_1) + 2$ whenever $H_1 < H_2 \leq G$, let $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \leq G$ be a subgroup with $f(K) \geq 3$.*

If $T = S(I) \mid S$ is an f_K-near-component of S, then $T = U_1 \cdot \ldots \cdot U_r$, where each U_i, for $i \in [1, r]$, is an f_K-component of S. In particular, each $U_i = S(I_i)$ with $I_i \subseteq [1, \ell]$ and $I_1 \cup \ldots \cup I_r = I$ a disjoint union.

P r o o f. If the lemma is false, there must exist a component $U = S(J) \mid S$ such that $I \cap J \neq \emptyset$ and $J \nsubseteq I$ (recall that the components of S are equivalence classes, meaning they partition the terms of S). Let $H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle$ and $L = \langle \mathrm{supp}(S \cdot U^{[-1]}) \rangle$.

We have

$$|I| = |T| \leq f_K(G) - f_K(H) + 2 \text{ and } |J| = |U| \leq f_K(G) - f_K(L) + 1 \quad (19)$$

in view of NC2 and C3. Now $S \cdot S(I \cap J)^{[-1]} \mid (S \cdot T^{[-1]}) \cdot (S \cdot U^{[-1]})$, in turn implying $S \cdot S(I \cap J)^{[-1]} \mid S_H \cdot S_L$ (since $S \cdot T^{[-1]} \mid S_H$ and $S \cdot U^{[-1]} \mid S_L$), which ensures $S \cdot S(I \cap J)^{[-1]} \mid S_{H+L}$.

Consequently, we must have

$$|I \cap J| = |S(I \cap J)| \geq f_K(G) - f_K(H + L) + 1 = f(G) - f(H + L) + 1, \quad (20)$$

where the latter equality follows in view of $K \leq L$ (from Lemma 5.2). Indeed, if $H + L = G$, then (20) follows from the fact that we initially assumed $I \cap J$ to be nonempty. On the other hand, if $H + L < G$ is a proper subgroup and (20) fails, then $|S_{G \setminus (H+L)}| \leq f(G) - f(H + L)$, contradicting that S is f-stable with

$\langle \mathrm{supp}(S)\rangle = G$. But now, combining (19) with (20) and using A2, we obtain

$$|I \cup J| \le f_K(G) - f_K(H \cap L) + 2$$

by the same calculation used at the end of the proof of Lemma 5.5. Since $S{\cdot}T^{[-1]} \mid S_H$ and $S \cdot U^{[-1]} \mid S_L$, we have $S \cdot S(I \cup J)^{[-1]} \mid S_{H\cap L}$. Apply Lemma 5.4 (with $\epsilon = 2$ and H taken to be $H \cap L$) to the sequence $S(I \cup J)$. Let $W \mid S$ be the resulting sequence satisfying NC1 and NC2 with $S(I \cup J) \mid W$. Then $T = S(I) \mid W$ while $|W| \ge |I \cup J| > |I|$ in view of our initial assumption $J \nsubseteq I$. Thus W contradicts the maximality condition NC3 for the f_K-near-component $T = S(I)$, completing the proof. □

Lemma 5.10. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \ge f(H_1) + 2$ whenever $H_1 < H_2 \le G$, let $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S)\rangle = G$, and let $K \le G$ be a subgroup with $f(K) \ge 3$.*

If $T = S(I)$ and $T' = S(I')$ are distinct f_K-near-components of S (so $I \ne I'$) with $I \cap I' \ne \emptyset$, then $U = S(I \cap I')$ is an f_K-component of S.

P r o o f. Let $H = \langle \mathrm{supp}(S \cdot T^{[-1]})\rangle$ and let $H' = \langle \mathrm{supp}(S \cdot T'^{[-1]})\rangle$. By Lemma 5.9, we know that $U = S(I \cap I')$ is a union of f_K-components of S. Our goal is to show that it is a single f_K-component. By NC2, we have

$$|I| = |T| \le f_K(G) - f_K(H) + 2 \quad \text{and} \quad |I'| = |T'| \le f_K(G) - f_K(H') + 2. \tag{21}$$

Now $S \cdot S(I \cap I')^{[-1]} \mid (S \cdot T^{[-1]}) \cdot (S \cdot T'^{[-1]})$, in turn implying $S \cdot S(I \cap I')^{[-1]} \mid S_H \cdot S_{H'}$ (since $S \cdot T^{[-1]} \mid S_H$ and $S \cdot T'^{[-1]} \mid S_{H'}$), which ensures

$$S \cdot S(I \cap I')^{[-1]} \mid S_{H+H'}.$$

In view of Lemma 5.8, we have

$$K \le H \cap H'.$$

Suppose

$$|S(I \cap I')| \le f_K(G) - f_K(H + H') + 1.$$

Then we can apply Lemma 5.4 (with $\epsilon = 1$ and H taken to be $H + H'$) to the sequence $S(I \cap I')$ to conclude that $S(I \cap I')$ is contained in an f_K-component of S. However, since $S(I \cap I')$ is a union of f_K-components, this is only possible if $S(I \cap I')$ is actually equal to a single f_K-component, as desired. So we may instead assume that this inequality fails:

$$|S(I \cap I')| \ge f_K(G) - f_K(H + H') + 2. \tag{22}$$

Combining (22) and (21) and using A2, we find, as argued in Lemma 5.5 and Lemma 5.9, that

$$|I \cup I'| = |S(I \cup I')| \le f_K(G) - f_K(H \cap H') + 2.$$

Also, $\mathrm{supp}(S \cdot S(I \cup I')^{[-1]}) \subseteq \mathrm{supp}(S \cdot S(I)^{[-1]}) = \mathrm{supp}(S \cdot T^{[-1]}) \subseteq H$ and $\mathrm{supp}(S \cdot S(I \cup I')^{[-1]}) \subseteq \mathrm{supp}(S \cdot S(I')^{[-1]}) = \mathrm{supp}(S \cdot T'^{[-1]}) \subseteq H'$, so that $\mathrm{supp}(S \cdot S(I \cup I')^{[-1]}) \subseteq H \cap H'$. Thus we may apply Lemma 5.4 (with $\epsilon = 2$ and H taken to be $H \cap H'$) to $S(I \cup I')$. Let W be the resulting sequence satisfying NC1 and NC2 with $S(I \cup I') \mid W$. Then, since $|W| \ge |I \cup I'|$ with $I \ne I'$ (by hypothesis), this contradicts the maximality condition NC3 for either $T = S(I)$ or $T' = S(I')$, completing the proof. □

Lemma 5.11. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \ge f(H_1) + 2$ whenever $H_1 < H_2 \le G$, let $S = s_1 \cdot \ldots \cdot s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S) \rangle = G$, and let $K \le G$ be a subgroup with $f(K) \ge 3$.*

If $T \mid S$ is an f_K-near-component of S and $s_x \in \mathrm{supp}(T) \cap K$, then $T \cdot s_x^{[-1]}$ is an f_K-component of S.

P r o o f. Let $H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle$ and let $S' = S \cdot T^{[-1]}$. By Lemma 5.8, we have $K \le H$. From NC2, we have

$$|T \cdot s_x^{[-1]}| \le f_K(G) - f_K(H) + 1. \tag{23}$$

By NC1, we have

$$|(S' \cdot s_x)_{H \setminus L}| \ge |S'_{H \setminus L}| \ge f_K(H) - f_K(L) + 1$$

for any proper subgroup $L < H$. Moreover, since $s_x \in K \le H$, we have $\langle \mathrm{supp}(S' \cdot s_x) \rangle = \langle \mathrm{supp}(S') \rangle = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle = H$, so that $S' \cdot s_x = S \cdot T^{[-1]} \cdot s_x = S \cdot (T \cdot s_x^{[-1]})^{[-1]}$ is f_K-stable. Combined with (23), this shows that $T \cdot s_x^{[-1]}$ satisfies C2 and C3 and is thus contained in an f_K-component of S (as this shows all terms from $T \cdot s_x^{[-1]}$ are equivalent to each other under $\sim$).

By Lemma 5.7, we know s_x is an f_K-component of S. In consequence, Lemma 5.9 implies that $T \cdot s_x^{[-1]}$ is a union of f_K-components. However, since $T \cdot s_x^{[-1]}$ was just shown to be contained in an f_K-component of S, the only way this is now possible is if $T \cdot s_x^{[-1]}$ is itself an f_K-component of S, as desired. □

We now come to the crux of the section, showing that the above setup leads to a well-defined pairwise balanced design with $\lambda = 1$.

Theorem 5.12. *Let G be a finite abelian group G, let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be an admissible function such that $f(H_2) \ge f(H_1) + 2$ whenever $H_1 < H_2 \le G$,*

let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell \in \mathcal{F}(G)$ be sequence of terms from G that is f-stable with $|S| = f(G)$ and $\langle \mathrm{supp}(S)\rangle = G$, and let $K \le G$ be a subgroup with $f(K) \ge 3$.

Let $S = T_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T_r$, where the $T_i = S(I_i) \in \mathcal{F}(G)$ are the f_K-components of S. Let $\mathcal{H}$ be the hypergraph whose vertices are the f_K-components of S (formally, the integers from $[1, r]$) with edges corresponding to the f_K-near-components via Lemma 5.9, so $A \subseteq [1, r]$ is an edge when $S(\bigcup_{i\in A} I_i) = \bullet_{i\in A} T_i$ is an f_K-near-component of S. Then $\mathcal{H}$ is a pairwise balanced design with every pair of vertices contained in a unique edge.

P r o o f. In view of Lemma 5.9, the hypergraph $\mathcal{H}$ is well-defined. Moreover, Lemmas 5.9 and 5.8 ensure that any two components are contained in a common near-component. Finally, if two distinct components of S were contained in two distinct near-components $T = S(I)$ and $T' = S(I')$, then the intersection of these near-components would contain at least two components, contrary to Lemma 5.10. The theorem follows. □

6. Proof of Theorems 1.1 and 1.2

We begin with the lower bound.

Lemma 6.1. *Let $n \ge 1$ be an odd integer. Then*

$$\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) \ge 2\Omega(n) + 1 + \min\{\mathsf{v}_3(n), \mathsf{v}_5(n)\}.$$

P r o o f. Let $n_3 = \mathsf{v}_3(n)$ and let $n_5 = \mathsf{v}_5(n)$. Let

$$G = G_3 \times G_5 \times G_{p_1} \times \ldots \times G_{p_r} \cong \mathbb{Z}/n\mathbb{Z},$$

where $p_1, \ldots, p_r$ are the distinct prime divisors of n that are greater than 5, $G_3 = \mathbb{Z}/3^{n_3}\mathbb{Z}$, $G_5 = \mathbb{Z}/5^{n_5}\mathbb{Z}$, and each $G_{p_i} = \mathbb{Z}/q_i\mathbb{Z}$ with $q_i = p_i^{\mathsf{v}_{p_i}(n)}$ for $i = 1, \ldots, r$. It is easily seen that

$$\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) = \mathsf{D}_{U_G^2}(G) \ge \mathsf{D}_{U_H^2}(H) + \sum_{i=1}^{r} (\mathsf{D}_{U_{q_i}^2}(\mathbb{Z}/q_i\mathbb{Z}) - 1), \tag{24}$$

where $H = G_3 \times G_5$.

Let p be a prime and let $K = \mathbb{Z}/q\mathbb{Z}$ with $q = p^m$. We say that $k, \tilde{k} \in K$ are quadratically equivalent (resp. inequivalent) modulo p if $k\tilde{k}$ is a non zero square (resp. is not a square) modulo p. We first assume that $p \ge 7$. Let S be a sequence of length $2\Omega(p^m) = 2m$ consisting of two terms $p^i k_i, p^i \tilde{k}_i$ from $p^i K \setminus p^{i+1}K$, for $i = 0, 1, \ldots, m-1$, such that $k_i, \tilde{k}_i$ are either quadratically equivalent modulo p (if $p \equiv -1 \mod 4$) or quadratically inequivalent modulo p

(if $p \equiv 1 \mod 4$). Suppose $T \mid S$ is a U_K^2-weighted zero-sum. Let $j \in [0, m-1]$ be the minimal integer such that T contains a term from $p^jK \setminus p^{j+1}K$. Then, by construction of S, it follows that T contains either a single unit (i.e., generator) from $K' = \langle \mathrm{supp}(T) \rangle = p^jK$ or else exactly two units $p^jk_j, p^j\tilde{k}_j$ from K', such that $k_j, \tilde{k}_j$ are either quadratically equivalent modulo p (if $p \equiv -1 \mod 4$) or quadratically inequivalent modulo p (if $p \equiv 1 \mod 4$). It is then clear from Lemma 4.2 that T cannot be a U_K^2-weighted zero-sum. So we instead conclude that S is free of U_K^2-weighted zero-sums, implying

$$\mathsf{D}_{U_q^2}(\mathbb{Z}/q\mathbb{Z}) \ge |S| + 1 = 2m + 1 \text{ for any prime } p \ge 7 \text{ and } q = p^m \text{ with } m \ge 0. \quad (25)$$

Let $m = \min\{n_3, n_5\}$ and let $M = \max\{n_3, n_5\}$. If $n_5 > n_3$, let

$$h_i = (0, 5^{n_5-m-i}g_i),$$
$$\tilde{h}_i = (0, 5^{n_5-m-i}\tilde{g}_i) \in \{0\} \times 5^{n_5-m-i}G_5 \setminus 5^{n_5-m-i+1}G_5 \subseteq H, \text{ for } i = 1, 2, \ldots, n_5 - m = n_5 - n_3 = M - m,$$

be two elements such that $g_i, \tilde{g}_i$ are quadratically inequivalent modulo 5 (say $g_i = 1$ and $\tilde{g}_i = 2$). If $n_5 < n_3$, let

$$h_i = (3^{n_3-m-i+1}g_i, 0),$$
$$\tilde{h}_i = (3^{n_3-m-i+1}\tilde{g}_i, 0) \in 3^{n_3-m-i}G_3 \setminus 3^{n_3-m-i+1}G_3 \times \{0\} \subseteq H, \text{ for } i = 1, 2, \ldots, n_3 - m = n_3 - n_5 = M - m,$$

be two elements such that $g_i, \tilde{g}_i$ are quadratically equivalent modulo 3 (say $g_i = \tilde{g}_i = 1$).

Set

$$S = (3^{n_3-1}, 5^{n_5-1})^{[5]} \cdot (3^{n_3-2}, 5^{n_5-2})^{[5]} \cdot \ldots \cdot (3^{n_3-m}, 5^{n_5-m})^{[5]} \cdot \bullet_{i=1}^{M-m}(h_i \cdot \tilde{h}_i) \in \mathcal{F}(G_3 \times G_5).$$

Observe that $|S| = 5m + 2(M - m) = 2M + 3m = 2n_3 + 2n_5 + m = 2\Omega(|H|) + \min\{n_3, n_5\}$. Suppose $T \mid S$ is a nontrivial U_H^2-weighted zero-sum subsequence. Similar to the case when $p \ge 7$, Lemma 4.2 ensures that T cannot contain either h_{M-m} nor $\tilde{h}_{M-m}$, in which case Lemma 4.2 further implies T cannot contain either h_{M-m-1} nor $\tilde{h}_{M-m-1}$. Continuing in this fashion, we see that Lemma 4.2 ensures that T cannot contain any of the terms h_i nor $\tilde{h}_i$ for $i = 1, \ldots, M - m$. Thus

$$T \mid (3^{n_3-1}, 5^{n_5-1})^{[5]} \cdot (3^{n_3-2}, 5^{n_5-2})^{[5]} \cdot \ldots \cdot (3^{n_3-m}, 5^{n_5-m})^{[5]}. \quad (26)$$

Let $j \in [1, m]$ be the maximal integer such that $h := (3^{n_3-j}, 5^{n_5-j}) \in \mathrm{supp}(T)$. Thus h is a unit modulo both 5 and 3 in

$$H' = \langle \mathrm{supp}(T) \rangle = H'_3 \times H'_5,$$

where

$$H'_3 = 3^{n_3-j}G_3 \cong \mathbb{Z}/3^j\mathbb{Z} \quad \text{and} \quad H'_5 = 5^{n_5-j}G_5 \cong \mathbb{Z}/5^j\mathbb{Z},$$

i.e., $\pi_2(h) = 5^{n_5-j}$ is a generator of $H'_5 \cong \mathbb{Z}/5^j\mathbb{Z}$ and $\pi_1(h) = 3^{n_3-j}$ is a generator of $H'_3 \cong \mathbb{Z}/3^j\mathbb{Z}$, where

$$\pi_1 : G_3 \times G_5 \to G_3 \quad \text{and} \quad \pi_2 : G_3 \times G_5 \to G_5$$

are the i-th coordinate projection homomorphisms. Moreover, any term of T that is unit modulo either 5 or 3 in H' must be equal to h.

Since $T \in \mathcal{F}(H')$ is a U^2_H-weighted zero-sum sequence (and thus also a $U^2_{H'}$-weighted zero-sum by Lemma 3.1) and $U^2_{H'} = U^2_{H'_3} \times U^2_{H'_5}$, it follows that $\pi_1(T) \in \mathcal{F}(H'_3)$ is also a $U^2_{H'_3}$-weighted zero-sum sequence. Since $U^2_{H'_3} = 1 + 3H'_3$, the only way this is possible is if $\pi_1(\sigma(T)) \in 3H'_3 = 3^{n_3-j+1}G_3$. In view of the definition of j and (26), this is only possible if the term $h = (3^{n_3-j}, 5^{n_3-j})$ occurs with multiplicity a multiple of 3 in T, forcing $\mathsf{v}_g(T) = 3$. Since T is a $U^2_{H'}$-weighted zero-sum sequence and $U^2_{H'} = U^2_{H'_3} \times U^2_{H'_5}$, it follows that $\pi_2(T) \in \mathcal{F}(H'_5)$ is also a $U^2_{H'_5}$-weighted zero-sum sequence. However, since $\mathsf{v}_g(T) = 3$, we see that $\pi_2(T)$ contains exactly 3 units (i.e, generators) $5^{n_5-j}g, 5^{n_5-j}g', 5^{n_5-j}g''$ from $H'_5 = 5^{n_5-j}G_5 \cong \mathbb{Z}/5^j\mathbb{Z}$, all of them equal to $\pi_2(h)$, implying that g, g', g'' are all quadratically equivalent, contrary to Lemma 4.1. So we instead conclude that S contains no U^2_H-weighted zero-sum, implying

$$\mathsf{D}_{U^2_H}(H) \geq |S| + 1 = 2\Omega(|H|) + 1 + \min\{n_3, n_5\}. \tag{27}$$

Combining (24), (25), and (27), the desired lower bound follows. □

Next, we finish the case when $3 \nmid n$.

Proof of Theorem 1.1.1 and Theorem 1.2.1. The case $n = 1$ in Theorem 1.1.1 is trivial, so let $n \geq 3$ be an odd integer with $\gcd(n, 3) = 1$ and let

$$G = G_{p_1} \times \ldots \times G_{p_r} \cong \mathbb{Z}/n\mathbb{Z},$$

where $p_1, \ldots, p_r$ are the distinct prime divisors of n and each $G_{p_i} = \mathbb{Z}/p_i^{n_i}\mathbb{Z}$ with $n_i = \mathsf{v}_{p_i}(n)$. If a prime $p \nmid n$, then set G_p to be the trivial group. The lower bound for Theorem 1.1.1 follows from Lemma 6.1. As explained in the

introduction, the upper bound for Theorem 1.1.1 follows from Theorem 1.2.1. Thus it remains to prove the upper bound for Theorem 1.2.1. To that end, let

$$m \ge 3\omega(n) + \min\{1, \mathsf{v}_5(n)\}$$

be an integer. For a sequence $S \in \mathcal{F}(G)$ with $|S| \ge m + 2\Omega(n)$, we need to show that $0 \in \Sigma_m^{\cup}(U_G^2(S))$.

Clearly, we may assume $\mathsf{v}_0(S) \le m-1$, else the desired conclusion is trivial. Thus, if $n = p \ge 7$ is a prime, then there are at least $2\Omega(n)+1 = 3 = 3\omega(n)$ units in S, in which case $0 \in G = \Sigma_m^{\cup}(U_G^2(S))$ follows from Lemma 4.3.1 in view of $m \ge 3$. Likewise, if $n = 5$, then there are at least $2\Omega(n)+1 = 3 = 3\omega(n)$ units in S. If this inequality is strict, then $0 \in G = \Sigma_m^{\cup}(U_G^2(S))$ follows from Lemma 4.3.2 in view of $m \ge 4$. If it holds with equality, then Lemma 4.3.3 instead implies either $0 \in G = \Sigma_m^{\cup}(U_G^2(S))$ (if the three units are not quadratically equivalent modulo 5) or $0 \in 5G \subseteq \Sigma_m^{\cup}(U_G^2(S \cdot g^{[-1]})) \subseteq \Sigma_m(U_G^2(S))$ (if they are quadratically equivalent), where $g \in \mathrm{supp}(S)$ is a unit. In all cases, we obtain the desired result. So we may assume $\Omega(n) \ge 2$ and proceed by induction assuming the theorem known for all proper subgroups of $G \cong \mathbb{Z}/n\mathbb{Z}$.

Since G is cyclic, the subgroups of G are in 1–1 correspondence with the divisors $d \mid n$. Let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be the function given by $f(H) = f(|H|) = m + 2\Omega(|H|)$. Observe that $f(\mathrm{lcm}(d_1,d_2)) = f(d_1) + f(d_2) - f(\gcd(d_1,d_2))$ for any divisors $d_i \mid n$. Thus the function f is admissible with

$$f(H_2) \ge f(H_1) + 2 \quad \text{whenever } H_1 < H_2 \le G. \tag{28}$$

Let $K = G_5 \le G$ be the subgroup of order $5^{\mathsf{v}_5(n)}$. Then

$$f(K) \ge f(\{0\}) = m \ge 3\omega(n) + \min\{1, \mathsf{v}_5(n)\} \ge 3.$$

Let $S = s_1 \cdot \ldots \cdot s_{|S|} \in \mathcal{F}(G)$ be a sequence with

$$|S| = f(G) = m + 2\Omega(n)$$

that, by contradiction, does not have $0 \in \Sigma_m(U_G^2(S))$. We may assume that $\langle \mathrm{supp}(S)\rangle = G$, else $0 \in \Sigma_m(U^2_{|H|}(\overline{S_H})) = \overline{\Sigma_m(U_G^2(S))}$ follows by induction and Lemma 3.1, where $H = \langle \mathrm{supp}(S)\rangle$, contradicting that S contains no U_G^2-weighed zero-sum of length m. Likewise, we must have $|S_H| \le f(H) - 1$ for any proper subgroup $H < G$, for otherwise applying the induction hypothesis to $\overline{S_H}$ again yields $0 \in \Sigma_m(U^2_{|H|}(\overline{S_H})) = \overline{\Sigma_m(U_G^2(S))}$, contradicting via Lemma 3.1 that S contains no U_G^2-weighted zero-sum of length m, as before. As a result, we have

$$|S_{G\setminus H}| \ge |S| - f(H) + 1 = f(G) - f(H) + 1 \ge 3 \tag{29}$$

for any an proper subgroup $H < G$. In particular, we see that S is f-stable and now have all the needed hypotheses to talk of f_K-components.

If $5 \nmid n$, then let $W \mid S$ be a subsequence with $|W| = m$ and $|W_{G\setminus pG}| \geq 3$ for each prime $p \mid n$ (i.e., W contains at least 3 units modulo p). Such a subsequence W exists in view of (29) and $|S| \geq m \geq 3\omega(n)$. Applying Lemma 4.3.1 to W, it follows that $0 \in G = \Sigma_m(U_G^2(W)) \subseteq \Sigma_m(U_G^2(S))$, contrary to assumption. Therefore, we may now assume $5 \mid n$, so that $5G < G$ is a proper subgroup.

If (29) is strict for $H = 5G$, then let $W \mid S$ be a subsequence with $|W| = m$, $|W_{G\setminus 5G}| \geq 4$ and $|W_{G\setminus pG}| \geq 3$ for each prime $p \mid n$. Such a subsequence W exists in view of (29) and $|S| \geq m \geq 3\omega(n) + 1$. Applying Lemmas 4.3.1 and 4.3.2 to W, it follows that $0 \in G = \Sigma_m(U_G^2(W)) \subseteq \Sigma_m(U_G^2(S))$, contrary to assumption. Therefore, we instead assume $|S_{G\setminus 5G}| = 3$.

If the three terms of $S_{G\setminus 5G}$ are not quadratically equivalent modulo 5, then let $W \mid S$ be a subsequence with $|W| = m$ and $|W_{G\setminus pG}| \geq 3$ for each prime $p \mid n$. Applying Lemmas 4.3.1 and 4.3.3 to W, it follows that $0 \in G = \Sigma_m(U_G^2(W)) \subseteq \Sigma_m(U_G^2(S))$, contrary to assumption. So we may w.l.o.g now assume

$$S_{G\setminus 5G} = s_1 \cdot s_2 \cdot s_3$$

consists of three terms all quadratically equivalent to each other modulo 5.

Let $T = S(I)$, where $I \subseteq [1, f(G)]$, be the f_K-component containing s_1, so $1 \in I$, and let

$$H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle.$$

By Lemma 5.6, we have $K \leq H$ with $S \cdot T^{[-1]}$ f_K-stable and

$$|S \cdot T^{[-1]}| = |S| - |T| \geq f_K(H) - 1 = f(H) - 1 = m + 2\Omega(|H|) - 1 \geq m + 1. \quad (30)$$

We cannot have $S_{G\setminus 5G} = s_1 \cdot s_2 \cdot s_3 \mid T$, as then $\mathrm{supp}(S \cdot T^{[-1]})$ contains no generator modulo 5, making $\langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle = H$ impossible in view of $G_5 = K \leq H$. This leaves us with two cases.

Case 1:

$I \cap [1, 3] = \{1\}$. In this case, $s_2 \cdot s_3 \mid S \cdot T^{[-1]}$. Since $S' = S \cdot T^{[-1]}$ is f_K-stable with $K = G_5 \leq H$ (so that $K + pH = pH$ for $p \neq 5$), we have

$$|S'_{G\setminus pH}| \geq f_K(H) - f_K(pH) + 1 = f(H) - f(pH) + 1 \geq 3$$

for any prime divisor $p \geq 7$ of $|H|$, where the final inequality comes from (28). Thus, in view of $m \geq 3\omega(n) + 1 \geq 3\omega(|H|)$ and (30), let $W \mid S'$ be a subsequence with $|W| = m$, with $s_2 \cdot s_3 \mid W$, and with $|W_{H\setminus pH}| \geq 3$ for any prime divisor $p \geq 7$ of $|H|$. Since s_2 and s_3 are quadratically equivalent modulo 5, applying Lemmas 4.3.1 and 4.3.3 to W yields $0 \in 5G \subseteq \Sigma_m(U_G^2(W)) \subseteq \Sigma_m(U_G^2(S))$, contrary to assumption.

Case 2:

$I \cap [1,3] = \{1,2\}$ or $I \cap [1,3] = \{1,3\}$. In this case, we may w.l.o.g assume $I \cap [1,3] = \{1,2\}$. Let $T' = T \cdot s_3$. Then T' contains the only three terms s_1, s_2 and s_3 that are generators modulo 5. Consequently, $H' = \langle \mathrm{supp}(S \cdot T'^{[-1]}) \rangle < H$ since $K = G_5 \le H$ and $\mathrm{supp}(S \cdot T'^{[-1]})$ contains no generators modulo 5. Hence

$$|S_{G \setminus H'}| \le |T'| = |T| + 1 \le f_K(G) - f_K(H) + 2 \le f_K(G) - f_K(H'),$$

where the first inequality follows by C3 for the f_K-component T (cf. Lemma 5.6), and the second from $H' < H$ and (28), contradicting that S is f_K-stable. □

Finally, we finish with the case when $3 \mid n$.

Proof of Theorem 1.1.2, Theorem 1.1.3 and Theorem 1.2.2. It is clear that Theorem 1.1.2 follows from Theorem 1.1.3. The lower bound for Theorem 1.1.3 follows from Lemma 6.1. As the upper bound for Theorem 1.1.3 follows from Theorem 1.2.2 as explained in the introduction, it remains to prove Theorem 1.2.2.

The case when $3 \nmid n$ in Theorem 1.1.2 follows from the already established Theorem 1.1.1. Therefore we may assume $n \ge 3$ is an odd integer with $3 \mid n$. Let

$$G = G_{p_1} \times \ldots \times G_{p_r} \cong \mathbb{Z}/n\mathbb{Z},$$

where $p_1, \ldots, p_r$ are the distinct prime divisors of n and each $G_{p_i} = \mathbb{Z}/p_i^{n_i}\mathbb{Z}$ with $n_i = \mathsf{v}_{p_i}(n)$. Let

$$m \ge 4\Omega(n) + \omega(n) + \mathsf{v}_5(n) - 2 \tag{31}$$

be an integer with $3 \mid m$. For a sequence $S \in \mathcal{F}(G)$ with $|S| \ge m + 2\Omega(n) + \mathsf{v}_5(n)$, we need to show that $0 \in \Sigma_m^{\cup}(U_G^2(S))$. Observe that (31) implies

$$m \ge 5\omega(n) - 2 + \min\{1, \mathsf{v}_5(n)\} \quad \text{and} \tag{32}$$

$$m \ge 4\Omega(n) + \mathsf{v}_5(n) - 2\mathsf{v}_3(n) + 1. \tag{33}$$

If $\Omega(n) = 1$, then, since $3 \mid n$, we must have $G = \mathbb{Z}/3\mathbb{Z}$, in which case $U_G^2 = \{1\}$. Then $|S| \ge m + 2\Omega(n) + \mathsf{v}_5(n) = m + 2 = m - 1 + |G|$, in which case $0 \in \Sigma_m^{\cup}(U_G^2(S))$ follows from repeated application of the Erdős-Ginzburg-Ziv Theorem [Gr, Theorem 10.1] in view of $3 \mid m$ and $|G| = 3$. Therefore, we may assume $\Omega(n) \ge 2$ and proceed by induction assuming the theorem known for all proper subgroups of $G \cong \mathbb{Z}/n\mathbb{Z}$.

Since G is cyclic, the subgroups of G are in 1–1 correspondence with the divisors $d \mid n$. Let $f : \mathcal{S}_G \to \mathbb{Z}^+$ be the function given by

$$f(H) = f(|H|) = m + 2\Omega(|H|) + \mathsf{v}_5(|H|)$$

and let $g : \mathcal{S}_G \to \mathbb{Z}^+$ be the function given by

$$g(H) = g(|H|) = m - 2\Omega(n) + 2\mathsf{v}_3(n) + 4\Omega(|H|) + \mathsf{v}_5(|H|) - 2\mathsf{v}_3(|H|).$$

Observe that $m \geq 2\Omega(n) + 1$ in view of (31), so that $g(H) \geq 1$ holds for all $H \leq G$. Also observe that $f(\mathrm{lcm}(d_1, d_2)) = f(d_1) + f(d_2) - f(\gcd(d_1, d_2))$ for any divisors $d_i \mid n$, and likewise for g. Thus the functions f and g are strictly admissible with

$$f(H_2) \geq f(H_1) + 2 \quad \text{whenever } H_1 < H_2 \leq G. \tag{34}$$

Let $K = G_3 \leq G$ be the subgroup of order $3^{\mathsf{v}_3(n)}$. Then

$$f(K) \geq f(\{0\}) = m \geq 3.$$

Let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_{|S|} \in \mathcal{F}(G)$ be a sequence with

$$|S| = f(G) = g(G) = m + 2\Omega(n) + \mathsf{v}_5(n)$$

that, by contradiction, does not have $0 \in \Sigma_m(U_G^2(S))$. We may assume that $\langle \mathrm{supp}(S) \rangle = G$, else $0 \in \Sigma_m(U_{|H|}^2(\overline{S_H})) = \overline{\Sigma_m(U_G^2(S))}$ follows by induction and Lemma 3.1, where $H = \langle \mathrm{supp}(S) \rangle$, contradicting that S contains no U_G^2-weighed zero-sum of length m. Likewise, we must have $|S_H| \leq f(H) - 1$ for any proper subgroup $H < G$, for otherwise applying the induction hypothesis to $\overline{S_H}$ again yields $0 \in \Sigma_m(U_{|H|}^2(\overline{S_H})) = \overline{\Sigma_m(U_G^2(S))}$, contradicting via Lemma 3.1 that S contains no U_G^2-weighted zero-sum of length m, as before. As a result, S is f-stable and

$$|S_{G \setminus H}| \geq |S| - f(H) + 1 = f(G) - f(H) + 1 \geq 3 \tag{35}$$

for any proper subgroup $H < G$. Consequently, we now have all the needed hypotheses to apply the machinery of Section 5. However, before doing so, we need to establish two additional claims.

Claim A

Our next goal is to show that—replacing, if need be, S by $S - x$ for some $x \in G$ such that $0 \in \Sigma_m(U_G^2(S - x))$ implies $0 \in \Sigma_m(U_G^2(S))$—we may assume

$$\mathsf{v}_0(S) \geq g(\{0\}) = m - 2\Omega(n) + 2\mathsf{v}_3(n). \tag{36}$$

Since $|S| = g(G) \geq g(G) - g(\{0\}) + 1$, we can apply Lemma 5.1 to S using the admissible function $g : \mathcal{S}_G \to \mathbb{Z}^+$. Indeed, we can apply Lemma 5.1 using the admissible function g to any translated sequence $S - x$, so long as $x \in G$ is an element such that $0 \in \Sigma_m(U_G^2(S - x))$ implies $0 \in \Sigma_m(U_G^2(S))$. Over all such potential $x \in G$, suppose $x \in G$ is one such that $S - x$ has the resulting subgroup $H \leq G$ from the application of Lemma 5.1 being minimal, and replacing S by $S - x$, w.l.o.g. assume $x = 0$.

From Lemma 5.1, we have that $H \le G$ is g-stable in S with

$$\begin{aligned} |S_H| &= |S| - |S_{G\setminus H}| \ge g(|H|) \\ &= m - 2\Omega(n) + 2\mathsf{v}_3(n) + 4\Omega(|H|) + \mathsf{v}_5(|H|) - 2\mathsf{v}_3(|H|). \end{aligned} \tag{37}$$

If H is trivial, then (36) follows, as claimed, so instead assume $H \le G$ is non-trivial. Let $W' \mid S_H$ be a minimal length subsequence such that

$$\begin{aligned} &|W'_{H\setminus 3H}| \ge g(H) - g(3H) + 1 = 3 \quad \text{if } 3 \mid |H|, \\ &|W'_{H\setminus 5H}| \ge g(H) - g(5H) + 1 = 6 \quad \text{if } 5 \mid |H|, \quad \text{and} \\ &|W'_{H\setminus pH}| \ge g(H) - g(pH) + 1 = 5 \quad \text{for any prime } p \mid |H| \text{ with } p \ge 7. \end{aligned} \tag{38}$$

Since S_H is g-stable (as H is g-stable in S by the application of Lemma 5.1), it follows that (38) holds with $W' = S_H$, so W' exists. Moreover, we clearly have

$$\begin{aligned} 3 \le |W'| &\le 5\omega(|H|) - 2\min\{1, \mathsf{v}_3(|H|)\} + \min\{1, \mathsf{v}_5(|H|)\} \\ &\le 5\omega(n) - 2 + \min\{1, \mathsf{v}_5(n)\}, \end{aligned} \tag{39}$$

where for the latter inequality we have made use of the fact that $3 \mid n$ (to ensure that $H < G$ is proper when $\mathsf{v}_3(|H|) = 0$). As a result, (32) ensures that

$$|W'| \le m. \tag{40}$$

From (37) and (33), we have

$$\begin{aligned} |S_H| &\ge 2\Omega(n) + \mathsf{v}_5(n) + 1 + 4\Omega(|H|) + \mathsf{v}_5(|H|) - 2\mathsf{v}_3(|H|) \\ &\ge 2\Omega(n) + \mathsf{v}_5(n) + \min\{1, \mathsf{v}_5(|H|)\} + 5\omega(|H|) - 2\Omega(|H|) - \mathsf{v}_5(|H|) \\ &= \Big(5\omega(|H|) - 2 + \min\{1, \mathsf{v}_5(|H|)\}\Big) + \Big(2\Omega(|G/H|) + \mathsf{v}_5(|G/H|)\Big) + 2 \\ &\ge \Big(5\omega(|H|) - 2 + \min\{1, \mathsf{v}_5(|H|)\}\Big) + \Big(\mathsf{D}_{U^2_{G/H}}(G/H) - 1\Big) + 2, \end{aligned} \tag{41}$$

where the final inequality follows by applying the induction hypothesis to G/H (possible, since H is assumed non-trivial). Additionally, (37) and (33) give

$$\begin{aligned} |S_H| &\ge 2\Omega(n) + \mathsf{v}_5(n) + 1 + 4\Omega(|H|) + \mathsf{v}_5(|H|) - 2\mathsf{v}_3(|H|) \\ &\ge 2\Omega(n) + \mathsf{v}_5(n) + 2. \end{aligned} \tag{42}$$

Next, we wish to extend the sequence $W' \mid S_H$, which has $|W'| \le m$ in view of (40), to a subsequence $W \mid S$ such that

$$W' \mid W, \quad |W| = m, \quad \sigma(U^2_G(W_{G\setminus H})) \cap H \ne \emptyset \tag{43}$$

and, moreover,

$$|S_H \cdot W_H^{[-1]}| \ge 2 \quad \text{if } 3 \mid |H|. \tag{44}$$

To do this, we iteratively pull off subsequences $T_1 \cdot \ldots \cdot T_s \mid S_{G\setminus H}$ that have $\sigma(U^2_G(T_i)) \cap H \ne \emptyset$ and $|T_i| \le \mathsf{D}_{U^2_{G/H}}(G/H)$. This can be done in view of (5)

(and the comments thereafter) until either $|W' \cdot T_1 \cdot \ldots \cdot T_s \cdot T_{s+1}| \geq m+1$ or $|S_{G\setminus H} \cdot (T_1 \cdot \ldots \cdot T_s)^{[-1]}| \leq \mathsf{D}_{U^2_{G/H}}(G/H) - 1$.

In the former case, assuming $s+1$ is the minimal index such that $|W' \cdot T_1 \cdot \ldots \cdot T_s \cdot T_{s+1}| \geq m+1$, we then have

$$m - \mathsf{D}_{U^2_{G/H}}(G/H) + 1 \leq m + 1 - |T_{s+1}| \leq |W' \cdot T_1 \cdot \ldots \cdot T_s| \leq m.$$

Consequently, in view of (39) and (41), we see that we can extend $W' \cdot T_1 \cdot \ldots \cdot T_s$ to a subsequence W satisfying (43) and (44) by simply adding an appropriate number of terms from $S_H \cdot W'^{[-1]}$.

In the latter case, we have

$$\begin{aligned} |S_{G\setminus H} \cdot (T_1 \cdot \ldots \cdot T_s)^{[-1]}| &\leq \mathsf{D}_{U^2_{G/H}}(G/H) - 1 \leq 2\Omega(|G/H|) + \mathsf{v}_5(|G/H|) \\ &\leq 2\Omega(n) + \mathsf{v}_5(n) - 2 \leq |S| - m - 2, \end{aligned}$$

where the second and third inequalities follow in view of the induction hypothesis applied to G/H and $H \leq G$ being nontrivial. Hence $|S_H \cdot T_1 \cdot \ldots \cdot T_s| \geq m+2$. Thus, since $|W' \cdot T_1 \cdot \ldots \cdot T_s| \leq m$ (else the former case holds), we can again simply add an appropriate number of terms from $S_H \cdot W'^{[-1]}$ to result in the sequence W satisfying (43) and (44). As a result, we see that in either case we arrive at the subsequence $W \mid S$ with the desired properties (43) and (44).

In view of (43), let $\alpha \in \sigma(U^2_G(W_{G\setminus H})) \cap H$. If $\sigma(W_H) + \alpha \in 3H$, then—in view of $W' \mid W$, (38) and (43)—we can apply Lemma 4.3 to conclude that $0 \in 3H \subseteq \sigma(U^2_G(W)) = \Sigma_m(U^2_G(W)) \subseteq \Sigma_m(U^2_G(S))$, contrary to assumption. So we can assume otherwise. In particular, we must have $3 \mid |H|$, in which case (44) assures us that there are at least two terms from S_H outside W.

If $x \cdot y \mid S_H \cdot W_H^{[-1]}$ and $x' \cdot y' \mid W_H$, then we can swap x for x', or y for y', or $x \cdot y$ for $x' \cdot y'$ to result in a new sequence $V = W \cdot x'^{[-1]} \cdot x$ or $V = W \cdot y'^{[-1]} \cdot y$ or $V = W \cdot (x' \cdot y')^{[-1]} \cdot x \cdot y$ that can miss at most two terms from W' (in the event that one or both of the terms being swapped out of W were from W'). Thus (38) implies

$$\begin{aligned} &|V_{H\setminus 3H}| \geq 1 \quad \text{if } 3 \mid |H|, \\ &|V_{H\setminus 5H}| \geq 4 \quad \text{if } 5 \mid |H|, \text{ and} \\ &|V_{H\setminus pH}| \geq 3 \quad \text{for any prime } p \mid |H| \text{ with } p \geq 7. \end{aligned} \tag{45}$$

In particular, $\langle \mathrm{supp}(V) \rangle = \langle \mathrm{supp}(W) \rangle = H$ and $V_{G\setminus H} = W_{G\setminus H}$.

Now, if some such swap results in a sequence V with $\sigma(V_H) + \alpha \in 3H$, then applying Lemma 4.3 yields $0 \in 3H \subseteq \sigma(U^2_G(V)) = \Sigma_m(U^2_G(V)) \subseteq \Sigma_m(U^2_G(S))$, a contradiction as before. So may instead assume we always have $\sigma(V_H) \in -\alpha + 1 + 3H$ or $\sigma(V_H) \in -\alpha - 1 + 3H$ (note that $H/3H \cong \mathbb{Z}/3\mathbb{Z}$ as $3 \mid |H|$ with H

cyclic). It is easily seen that this is only possible if all but at most one term of S_H is from the same $3H$-coset. Indeed, if this assertion fails and there does not exist some $g \in \mathrm{supp}(S_H)$ such that $|\mathrm{supp}(S_H \cdot g^{[-1]})| = 1$, then it is possible to choose $x \cdot y \mid S_H \cdot W_H^{[-1]}$ and $x' \cdot y' \mid W_H$ such that $x - x' \notin 3H$ and $y - y' \notin 3H$ (since $|W'| \geq 2$ and since there are at least two terms from S_H outside W), in which case $\sigma(V_H)+\{0, x-x'\}+\{0, y-y'\}+3H$ represents the possible values for $\sigma(V_H)$ modulo $3H$ when we allow V to be obtained from W by either not swapping any terms (so $V = W$), swapping x for x' (so $V = W \cdot x'^{[-1]} \cdot x$), swapping y for y' (so $V = W \cdot y'^{[-1]} \cdot y$), or swapping $x \cdot y$ for $x' \cdot y'$ (so $V = W \cdot (x' \cdot y')^{[-1]} \cdot x \cdot y$). However, applying the Cauchy-Davenport Theorem ([Gr, Theorem 6.2]), we find that $\sigma(V_H) + \{0, x - x'\} + \{0, y - y'\} + 3H = H$, which means that at least one of these four possible ways to define V has $\sigma(V_H) + \alpha \in 3H$, contradicting that this should fail for all of them as noted above. In summary, we have just shown that all but at most one term from S_H is from the same $3H$-coset, say $x + 3H$ with $x \in G_3$ (we may assume $x \in G_3$ as G_3 contains a full set of $3H$-coset representatives).

We cannot have $x + 3H = 3H$, as then $|S_{H \setminus 3H}| \leq 1$, contrary to (38). Therefore, we may instead assume $x \in H \setminus 3H$, so that $\mathrm{ord}(x) = 3^\alpha$ (in view of $x \in G_3$) with $\alpha = \mathsf{v}_3(|H|)$. In view of (42), we have at least $2\Omega(n)+\mathsf{v}_5(n)+1 = |S|-m+1$ terms s_i of S with $\mathsf{v}_3(\mathrm{ord}(s_i)) = \alpha$ (namely, all but at most one term of S_H). Thus we can invoke Lemma 3.2 to conclude that $0 \in \Sigma_m(U_G^2(S-x))$ implies $0 \in \Sigma_m(U_G^2(S))$. Since the latter is assumed to fail, this means $0 \notin \Sigma_m(U_G^2(S-x))$. By removing at most one additional term from $S_H - x$, we find that all remaining terms are from $3H < H$. But this means that if we apply Lemma 5.1 to $S - x$, then the resulting minimal subgroup H' will have $H' \leq 3H < H$, contradicting the minimality assumption assumed for $H \leq G$ at the beginning of Claim A, which completes the proof of the claim.

As already established, we have all the needed hypotheses to apply the machinery of Section 5 to the f-stable sequence S using the admissible function f_K. In view of Claim A and (33), we have $\mathsf{v}_0(S) \geq 2\Omega(n) + \mathsf{v}_5(n) + 1$. Thus

$$W = S \cdot 0^{[-2\Omega(n)-\mathsf{v}_5(n)]}$$

is a subsequence of S with $|W| = m$.

Claim B

If $T \mid W$ is a subsequence such that $S \cdot T^{[-1]}$ is f_K-stable and $|T| \leq 2\Omega(n) + \mathsf{v}_5(n)$, then $\sigma(W \cdot T^{[-1]}) \notin 3H$, where $H = \langle \mathrm{supp}(S \cdot T^{[-1]}) \rangle$.

Let $W' = W \cdot T^{[-1]} \cdot 0^{[|T|]}$. In view of $|T| \le 2\Omega(n) + \mathsf{v}_5(n)$, we have $W' \mid S$. Since $S' = S \cdot T^{[-1]}$ is f_K-stable, and since all terms outside W are zero, it follows that $\langle \mathrm{supp}(W')\rangle = \langle \mathrm{supp}(S \cdot T^{[-1]})\rangle = H$, that $|W'_{H\setminus pH}| = |S'_{H\setminus pH}| \ge f_K(H) - f_K(pH) + 1 = 3$ for any prime $p \mid |H|$ with $p \ge 7$, and that $|W'_{H\setminus 5H}| = |S'_{H\setminus 5H}| \ge f_K(H) - f_K(5H) + 1 = 4$ if $5 \mid |H|$. Thus, if $\sigma(W \cdot T^{[-1]}) \in 3H$ were to hold by contradiction, then applying Lemma 4.3 to W' yields $0 \in \sigma(U_G^2(W')) = \Sigma_m(U_G^2(W')) \subseteq \Sigma_m(U_G^2(S))$ in view of $W' \mid S$, which is contrary to assumption, completing the claim.

Since S is f-stable, and thus also f_K-stable, we can apply Claim B taking T be the trivial sequence and thereby conclude that

$$\pi(\sigma(W)) \equiv x \mod 3G_3 \quad \text{for some } x \in G_3 \setminus 3G_3, \tag{46}$$

where $\pi : G \to G_3$ denotes the projection homomorphism onto the 3-component $G_3 = \mathbb{Z}/3^{n_3}\mathbb{Z}$.

Let $T \mid S$ be an arbitrary f_K-component of S with $T \mid W$ and let $H = \langle \mathrm{supp}(S \cdot T^{[-1]})\rangle$. Then Lemma 5.6 implies that $K \le H$, that $S \cdot T^{[-1]}$ is f_K-stable, and that

$$\begin{aligned} |T| &\le f_K(G) - f_K(H) + 1 = 2\Omega(n) - 2\Omega(|H|) + \mathsf{v}_5(n) - \mathsf{v}_5(|H|) + 1 \\ &\le 2\Omega(n) - 2\Omega(|K|) + \mathsf{v}_5(n) - \mathsf{v}_5(|K|) + 1 \le 2\Omega(n) + \mathsf{v}_5(n) - 1, \end{aligned}$$

where we have made free use of $\{0\} \ne G_3 = K \le H \le G$. Since $G_3 = K \le H$, we have $G_3 \le H = \langle \mathrm{supp}(S \cdot T^{[-1]})\rangle$. Consequently, if $\pi(\sigma(T)) \equiv x \mod 3G_3$, then (46) implies that $\sigma(W \cdot T^{[-1]}) \in 3H$, contrary to Claim B. Therefore we instead conclude that

$$\pi(\sigma(T)) \equiv 0 \text{ or } -x \mod 3G_3 \tag{47}$$

for any f_K-component T with $T \mid W$ (note that $G_3/3G_3 \cong \mathbb{Z}/3\mathbb{Z}$, so any nonzero residue class not equal to x must be equal to $-x$).

Let $T \mid S$ be an arbitrary f_K-near-component of S with $T \mid W$ and let $H = \langle \mathrm{supp}(S \cdot T^{[-1]})\rangle$. Then Lemma 5.8 implies that $K \le H$, while NC1 and NC2 imply that $S \cdot T^{[-1]}$ is f_K-stable and that

$$\begin{aligned} |T| &\le f_K(G) - f_K(H) + 2 = 2\Omega(n) - 2\Omega(|H|) + \mathsf{v}_5(n) - \mathsf{v}_5(|H|) + 2 \\ &\le 2\Omega(n) - 2\Omega(|K|) + \mathsf{v}_5(n) - \mathsf{v}_5(|K|) + 2 \le 2\Omega(n) + \mathsf{v}_5(n), \end{aligned}$$

where we have made free use of $\{0\} \ne G_3 = K \le H \le G$. Since $G_3 = K \le H$, we have $G_3 \le H = \langle \mathrm{supp}(S \cdot T^{[-1]})\rangle$. Consequently, if $\pi(\sigma(T)) \equiv x \mod 3G_3$,

then (46) implies that $\sigma(W \cdot T^{[-1]}) \in 3H$, contrary to Claim B. Therefore, as before, we instead conclude that

$$\pi(\sigma(T)) \equiv 0 \text{ or } -x \mod 3G_3 \tag{48}$$

for any f_K-near-component T with $T \mid W$.

In view of Lemma 5.7, we know that any term of S equal to $0 \in K$ is itself anf_K-component of S. Thus, since all terms of S outside W are equal to 0, it follows that $S \cdot W^{[-1]}$ is a union of f_K-components, implying that W is likewise a union of f_K-components. In particular, if $T \mid S$ is a component such that $T \nmid W$, then $T = 0$ and $\pi(\sigma(T))) \equiv 0 \mod 3G_3$. Since all terms of $S \cdot W^{[-1]}$ are equal to $0 \in K$, Lemma 5.11 implies that any f_K-near-component T with $T \nmid W$ can contain at most one f_K-component dividing W.

In view of (47), let $W = T_1 \cdot \ldots \cdot T_v \cdot U_1 \cdot \ldots \cdot U_s$, where the T_i are the components of S with $\pi(\sigma(T_i)) \equiv -x \mod 3G_3$ and the U_i are the components of S dividing W with $\pi(\sigma(U_i)) \equiv 0 \mod 3G_3$. Then (in view of (46))

$$x \equiv \pi(\sigma(W)) \equiv \sum_{i=1}^{v} \pi(\sigma(T_i)) \equiv -vx \mod 3G_3,$$

implying that

$$v \equiv -1 \mod 3. \tag{49}$$

If $T \mid S$ is an f_K-near-component of S that contains at least two f_K-components T_i and T_j with $\pi(\sigma(T_i)) \equiv \pi(\sigma(T_j)) \equiv -x \mod 3G_3$, then $T \mid W$ (as shown in the previous paragraph), whence (48) gives $\pi(\sigma(T)) \equiv -x$ or $0 \mod 3G_3$. Clearly, $\pi(\sigma(T)) \equiv -e_T x \mod 3G_3$, where e_T is the number of f_K-components U that divide T and have $\pi(\sigma(U)) \equiv -x \mod 3G_3$, which means that

$$e_T \equiv 1 \text{ or } 0 \mod 3$$

for any near-component T containing at least two components T_i and T_j with $\pi(\sigma(T_i)) \equiv \pi(\sigma(T_j)) \equiv -x \mod 3G_3$.

By Theorem 5.12, the hypergraph $\mathcal{H}$ whose vertices correspond to the f_K-components of S and whose edges correspond to the f_K-near-components of S is a pairwise balanced design with $\lambda = 1$. Let $\mathcal{H}'$ be the sub-hypergraph induced by all those vertices (i.e., components) T_i such that $\pi(\sigma(T_i)) \equiv -x \mod 3G_3$ (discarding all edges of size 1). In other words, the vertices of $\mathcal{H}'$ are those $T_1, \ldots, T_r$ defined in the previous paragraph, and the edges of $\mathcal{H}'$ correspond to those near-components $T \mid W$ that contain at least two distinct components T_i and T_j. Then $\mathcal{H}'$ is also a pairwise balanced design with $\lambda = 1$. Moreover, as shown in the previous paragraph, the number of vertices in $\mathcal{H}'$ is equal to $v \equiv -1 \mod 3$, and each edge $T \mid W$ contains $e_T \equiv 1$ or $0 \mod 3$ vertices. Thus, $\mathcal{H}'$ is a pairwise balanced design on $v \equiv -1 \mod 3$ vertices such that any edge E of $\mathcal{H}'$

has $|E| \in K' := (1 + 3\mathbb{N}) \cup 3\mathbb{N}$. Now $\beta(K') := \gcd\{k(k-1) : \ k \in K'\} = 6$, but $v(v-1) \equiv -1 \mod 3$, so that $v(v-1) \not\equiv 0 \mod 6$. This contradicts Theorem 3.3, completing the proof. □

7. Concluding remarks

Let $G \cong \mathbb{Z}/n\mathbb{Z}$ and let $S \in \mathcal{F}(G)$ be a sequence of terms from G. In the scope of the standard Gao constant problem, it is clear that 0 can be written as the sum of n elements of S if it can be written similarly with n elements of $S - x$, for any $x \in G$. We may ask the following question: what is the least integer $\ell(n)$ such that, if $|S| \geq \ell(n)$, then

$$0 \in \Sigma_n(U_G^2(S)) \quad \text{implies} \quad 0 \in \Sigma_n(U_G^2(S-x)) \text{ for all } x \in G?$$

Let $S = s_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} s_\ell$ be a sequence of $\mathsf{E}_{U_G^2}(G) - 1$ terms such that $0 \notin \Sigma_n(U_G^2(S))$. Then

$$\sum_{x=1}^{n} |(S+x)_{U_G}| = \sum_{i=1}^{\ell} \sum_{\substack{x=1 \\ \gcd(s_i+x,n)=1}}^{n} 1 = |S|\varphi(n), \tag{50}$$

where φ denotes the Euler totient function. Hence there exists some x such that $|(S+x)_{U_G}| \geq \varphi(n)|S|/n > \varphi(n)$. For n large enough, we get $|(S+x)_{G \setminus pG}| \geq 4$ for any prime $p \mid n$, whence Lemma 4.3 gives $0 \in \mathbb{Z}/n\mathbb{Z} = \Sigma_n(U_G^2(S+x))$ when $\gcd(n,6) = 1$. It follows that the integer $\ell(n)$ defined above is equal to $\mathsf{E}_{U_G^2}(G)$ in this case.

REFERENCES

[Ay] R. Ayoub: *An introduction to the analytic theory of numbers*. Mathematical Surveys, No. 10, American Mathematical Society, Providence, R.I., 1963

[ADJ] S.D. Adhikari; C. David; J. Jiménez Urroz: Generalizations of some zero-sum theorems, *Integers* **8** (2008), A52.

[AR] S.D. Adhikari; P. Rath: Davenport constant with weights and some related questions, *Integers* **6** (2006), A30.

[CM] M.N. Chintamani; B.K. Moriya: Generalizations of some zero sum theorems, *Proc. Indian Acad. Sci. Math. Sci.* **122** (2012), 15–21.

[Ga] W. Gao: Addition theorems for finite abelian groups, *J. Number Theory* **53** (1995), 241–246.

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

[Gr] D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30, Springer (2013).

[GMO] D.J. Grynkiewicz; L.E. Marchan; O. Ordaz: A weighted generalization of two theorems of Gao, *Ramanujan J.* **28** (2012), 323–340.

[Na] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, Harrisonburg, VA (1996).

[Kr] *Handbook of Discrete and Combinatorial Mathematics*, Ed. Kenneth H. Rosen, CRC Press, New York (2000).

[Th] R. Thangadurai: A variant of Davenport's constant, *Proc. Indian Acad. Sci. Math. Sci.* **117** (2007), 147–158.

[YZ1] P. Yuan; X. Zeng: Davenport constant with weights, *European J. Combin.* **31** (2010), 677–680.

[YZ2] P. Yuan; X. Zeng, Weighted Davenport's constant and the weighted EGZ Theorem, *Discrete Mathematics*, 311 (2011), n. 17, 1940–1947.

Received 0.0.0000
Accepted 0.0.0000

David J. Grynkiewicz
Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152
USA
E-mail: diambri@hotmail.com

François Hennecart
Institut Camille Jordan
Université Jean-Monnet Saint-Étienne
23, rue du Docteur Paul Michelon
42023 Saint-Etienne Cedex 02
France
E-mail: francois.hennecart@univ-st-etienne.fr