

SMALL-INDEX SUBSEQUENCES IN FINITE CYCLIC GROUPS

CHAO LIU

ABSTRACT. For $r \geq 1$, let $I_r(n)$ be the least length forcing a nonempty zero-sum subsequence of index at most r over the cyclic group C_n . We prove $I_r(n) \leq n^{1+o(1)}$ when $r \geq C[\omega(n) \log(2\omega(n))]^2$, and $I_1(p^k) \ll (k+1)p^k \log(2p^k)$ for prime powers. We also construct sequences showing that $I_r(n)/n$ is unbounded for every fixed r ; for $r = 1$, all terms may be generators.

1. INTRODUCTION AND MAIN RESULTS

Write C_n additively. A sequence over C_n is a finite multiset; repetitions are allowed. Fix a generator g and write $S = (a_1g) \cdots (a_\ell g)$ with $a_i \in [1, n] \cap \mathbb{Z}$. Its index is

$$\text{ind}(S) = \min_{u \in U(n)} \frac{1}{n} \sum_{i=1}^{\ell} [ua_i]_n, \quad U(n) = (\mathbb{Z}/n\mathbb{Z})^\times,$$

where $[x]_n$ is the least positive residue, so $[0]_n = n$. For $r \geq 1$, a sequence is *index- r -free* if it has no nonempty subsequence of index in $\{1, \dots, r\}$. Following [10], let $I_r(n)$ be the least integer such that every sequence of length at least $I_r(n)$ is not index- r -free. In particular, an index-one subsequence is a nonempty subsequence whose positive representatives sum to exactly n in one unit direction. A zero sum modulo n alone does not suffice.

The index-one problem originates in work of Lemke and Kleitman [9]. The proposed equality $I_1(n) = n$ fails for composite orders: Gao, Li, Peng, Plyley and Wang [6] gave counterexamples, and Liu [10, Theorem 1.5] proved, for fixed $d > 1$ and $r \geq 1$, that

$$(1.1) \quad I_r(n) \geq (1 + 1/d)n - O_{d,r}(\sqrt{n}) \quad (d \mid n, n \rightarrow \infty).$$

Subsequence sums of index-one-free sequences are also studied in [11]. We consider the forcing length for arbitrary sequences, including terms of proper additive order.

Our first result gives a near-linear forcing length once the allowed index exceeds a bound depending only on the number of distinct prime factors. Write $\omega(n)$ for this number. All constants below are independent of the prime factors and their exponents unless a dependence is displayed, and all logarithms are natural.

Theorem 1.1. *There is an absolute constant C such that, for every $\varepsilon > 0$, every $n \geq 2$ and every integer $r \geq 1$,*

$$(1.2) \quad r \geq C[\omega(n) \log(2\omega(n))]^2 \implies I_r(n) \ll_{\varepsilon} n^{1+\varepsilon}.$$

Moreover, for each integer $k \geq 1$, there is an integer R_k , depending only on k , such that

$$(1.3) \quad I_r(n) \ll_k n \log^{k+1}(2n) \quad (\omega(n) \leq k, r \geq R_k).$$

The implied constants depend only on ε in (1.2) and only on k in (1.3), uniformly in n and r .

2020 *Mathematics Subject Classification.* 11B30, 11B50, 11P70, 20K01.

Key words and phrases. Cyclic group, index of a sequence, zero-sum sequence, subsequence sum.

In particular, one fixed index R_2 gives

$$I_{R_2}(p^a q^b) \ll p^a q^b \log^3(2p^a q^b)$$

for all distinct primes p, q and all positive integers a, b , with no restriction on their relative sizes. This result is unconditional and includes sequences with terms of proper additive order. The proof combines an integer subset-sum interval with a choice of unit controlled by the Jacobsthal function, then sums reciprocal weights over all prime-power valuation classes.

For index one we obtain stronger bounds in several arithmetic families, including a conditional refinement under Dirichlet GRH. We also retain a uniform estimate for every allowed index r .

Theorem 1.2. *There is an absolute constant C with the following properties.*

(1) *For every prime p and every $k \geq 1$, with $n = p^k$,*

$$(1.4) \quad I_1(n) \leq C(k+1)n \log(2n).$$

In particular $I_1(n) \ll n \log^2(2n)$ uniformly on prime powers, and $I_1(p^k) \ll_k p^k \log(2p^k)$ for each fixed k .

(2) *For every $n \geq 2$ and every integer $r \geq 1$,*

$$(1.5) \quad n \leq I_r(n) \leq C \left(n + \frac{n^{3/2}}{\sqrt{r}} \right).$$

In particular $I_r(n) \ll n^{3/2}/\sqrt{r}$ for $1 \leq r \leq n$. For index one, writing $P^-(n)$ for the least prime divisor,

$$(1.6) \quad I_1(n) \leq C \min \left\{ n^{3/2}, n \log(2n) \left(1 + \frac{\sqrt{n}}{P^-(n)} \right) \right\}.$$

(3) *If $p \neq q$ are primes, $a \geq 1$, $P = p^a$ and $q \geq P$, then, for $n = Pq$,*

$$(1.7) \quad I_1(n) \leq Cn \log(2n) \left(a + 1 + \frac{1}{p} \sqrt{\frac{q}{P}} \right).$$

For every $\varepsilon > 0$ one also has

$$(1.8) \quad I_1(n) \ll_\varepsilon n^{4/3+\varepsilon}.$$

Under the Dirichlet generalized Riemann hypothesis,

$$(1.9) \quad I_1(n) \ll n \log^3(2n)$$

uniformly throughout this family.

(4) *For every prime p , with $n = 2p^2$,*

$$(1.10) \quad I_1(n) \leq Cn \log(2n).$$

This bound is unconditional and includes sequences with nonunit terms.

For example, (1.6) gives $O_{B,k}(n^{3/2-1/k} \log(2n))$ when n has $k \geq 2$ prime factors, counted with multiplicity, all in $[x, Bx]$. This gives exponent $7/6$ for balanced pqr and p^2q , and exponent $5/4$ for balanced p^2q^2 . Equation (1.7) gives $O((a+1)n \log(2n))$ throughout $p^a \leq q \leq p^{a+2}$. In particular the balanced semiprime bound is $O(n \log(2n))$. The family $2p^2$ in (1.10) is outside the larger-prime hypothesis for odd p . Its proof uses a parity-sensitive integer budget and reciprocal weights that sum all valuation classes with a convergent geometric series.

The conditional estimate (1.9) connects the forcing problem with uniform character-sum estimates for Dirichlet L -functions. It holds without an upper restriction on q/p^a . For example, for $n = 4q$ with $q \geq 5$ prime, our unconditional estimate is $O_\varepsilon(n^{4/3+\varepsilon})$, while Dirichlet GRH gives $O(n \log^3(2n))$. Its proof combines character orthogonality with smoothed prime-sum estimates in Section 4.4.

The estimate (1.5) is uniform in the allowed index r : it gives $I_r(n) = O(n)$ whenever r is bounded below by a fixed positive multiple of n . Exact large- r ranges also follow from known high-multiplicity theorems; see Corollary 2.3.

The lower bounds exhibit a different behavior for general composite orders. Put

$$P(d) = \prod_{p|d} (1 + 1/p), \quad s = \omega(d),$$

where the product and $\omega(d)$ count distinct prime factors.

Theorem 1.3. *Fix integers $d > 1$ and $r \geq 1$. For every sufficiently large multiple n of d , there is an index- r -free sequence over C_n of length*

$$(1.11) \quad |S| \geq P(d)n - O_{d,r}(n^{s/(s+1)}).$$

More explicitly, once $n > (rd^2)^{s+1}$ and $d \mid n$, one may take

$$(1.12) \quad |S| \geq P(d)n - (sP(d) + rd^2P(d) + d)n^{s/(s+1)}.$$

Consequently, for every $M > 0$ there exists $d > 1$, depending only on M , such that for every fixed $r \geq 1$, $I_r(n) > Mn$ for all sufficiently large multiples n of d .

When $d = p^a$ is a prime power, the leading coefficient $1 + 1/p$ and the error order in (1.11) agree with (1.1) applied with divisor p . For several prime divisors the coefficient multiplies: it is 2 for $d = 6$, $12/5$ for $d = 30$, and $96/35$ for $d = 210$. In particular the conclusion $I_1(n) \leq n + n/P^-(n)$ proposed in [10, Conjecture 4.1] fails on all sufficiently large multiples of 6. Section 5.1 gives a concrete index-one-free sequence of length 18000 over C_{12000} .

The next result shows that superlinear behavior persists even when every term is a generator. It is independent of Theorem 1.3.

Theorem 1.4. *There is a sequence $n_j \rightarrow \infty$ and index-one-free sequences S_j over C_{n_j} , all of whose terms have order n_j , such that*

$$(1.13) \quad \log \frac{|S_j|}{n_j} = \left(\frac{\log 6}{2} + o(1) \right) \frac{\log \log n_j}{\log \log \log n_j}.$$

Thus $I_1(n)$ has no absolute linear upper bound even on sequences consisting only of generators.

As a structural complement, we bound the length in terms of the maximum multiplicity. Write $\sigma_{-3/4}(n) = \sum_{d|n} d^{-3/4}$.

Theorem 1.5. *Let S be a nonempty index-one-free sequence over C_n , of length N and maximum multiplicity h . Then*

$$(1.14) \quad N \ll (nh)^{3/4} \sigma_{-3/4}(n),$$

with an absolute implied constant. For every fixed $k \geq 1$, if $\omega(n) \leq k$, then $N \ll_k (nh)^{3/4}$; in particular, $N \geq n$ forces $h \gg_k n^{1/3}$. Consequently every index-one-free sequence satisfies $|\text{supp}(S)| \leq n^{3/4+o(1)}$, and at prime-power orders $|\text{supp}(S)| \ll n^{3/4}$ with an absolute constant.

This applies to sequences of arbitrary length and multiplicities. The proof combines integer subset-sum theorems of Bringmann–Wellnitz [2] and Conlon–Fox–Pham [3] with an interval argument for repeated denominations. Section 6 proves the stronger bound obtained by keeping the maximum multiplicity in each exact-order class separately.

Section 2 develops the basic lemmas. Section 3 proves the near-linear small-index theorem. Section 4 proves the index-one upper bounds, including the GRH refinement. Section 5 gives the two lower constructions, and Section 6 proves the support and multiplicity bounds. The appendix proves the uniform index- r upper bound by integer descent.

The author acknowledges assistance from OpenAI tools in preparing this paper.

2. PRELIMINARIES

2.1. Integer intervals and truncated multiplicities. For a sequence S , let $c_x = v_x(S)$ be the multiplicity of x , and let $\Sigma_0(S)$ be its set of subsequence sums including the empty sum. When the entries are positive integers, $\Sigma_{0,\mathbb{Z}}(S)$ denotes their integer subsequence sums. Products of sequences mean concatenation. A nonempty zero-sum sequence is an *atom* if all its proper nonempty subsequences have nonzero sum. An index-one sequence is necessarily an atom: a proper zero sum would have a positive integer weight strictly between 0 and n in the same direction.

For $r \geq 1$, let $L_{U,r}(n)$ be the maximum length of an index- r -free sequence whose terms are units modulo n , and write $L_U(n) = L_{U,1}(n)$. These maxima are finite, since every type has multiplicity at most $n - 1$.

Lemma 2.1. *If $d \mid n$ and H is the subgroup of order d in C_n , then $\text{ind}_{C_n}(T) = \text{ind}_H(T)$ for every sequence T over H . Consequently, for every $r \geq 1$, an index- r -free sequence over C_n has length at most*

$$(2.1) \quad \sum_{\substack{d \mid n \\ d > 1}} L_{U,r}(d).$$

Proof. The reduction $U(n) \rightarrow U(d)$ is surjective. Indeed, lift a unit modulo d and impose residue 1 at each prime divisor of n not dividing d ; the Chinese remainder theorem supplies a lift coprime to n . For subgroup coordinates $x = (n/d)b$,

$$[u(n/d)b]_n = (n/d)[ub]_d.$$

The normalized weights and their minima therefore agree. Partition the terms by their exact additive order. The class of order d becomes a unit sequence in C_d , and is still index- r -free. The zero element cannot occur. This gives (2.1). $\square$

We use the classical short-zero-sum theorem: every sequence over C_n of length at least n has a nonempty zero-sum subsequence of length at most its maximum multiplicity; see [6, Lemma 3.1].

Lemma 2.2. *Every index- r -free sequence $S = \prod_a a^{c_a}$ over C_n satisfies*

$$(2.2) \quad \sum_a \min\{c_a, 2r + 1\} \leq n - 1.$$

Proof. For a zero-sum sequence T containing no zero term, in any unit direction u the two positive weights in directions u and $-u$ sum to $|T|n$. Their normalized weights are positive integers, so

$$\text{ind}(T) \leq \lfloor |T|/2 \rfloor.$$

Retain at most $2r + 1$ actual copies of each type. If their total length were at least n , the short-zero-sum theorem would give a zero sum of length at most $2r + 1$, hence of index at most r . A zero term is already an index-one singleton. This proves the bound. $\square$

The next exact ranges are direct consequences of known high-multiplicity results, stated here in terms of $I_r(n)$.

Corollary 2.3. *For every $n \geq 2$,*

$$I_r(n) = n \quad (r \geq \max\{1, \lfloor (n-1)/4 \rfloor\}).$$

For odd $n \geq 5$, the same equality holds already when $r \geq \max\{1, \lfloor (n-1)/6 \rfloor\}$.

Proof. Suppose every length- n sequence of maximum multiplicity at least H has an index-one subsequence. For smaller multiplicity, the short-zero-sum theorem and unit reversal give a zero sum of index at most $\lfloor (H-1)/2 \rfloor$. Thus $I_r(n) \leq n$ for $r \geq \max\{1, \lfloor (H-1)/2 \rfloor\}$. Use $H = \lceil n/2 \rceil$ from [6, Theorem 1.3], and $H = \lceil n/3 \rceil$ for odd $n \geq 5$ from [13, Theorem 2.1]. The lower bound is the ordinary zero-sum-free sequence g^{n-1} for a generator g . $\square$

We use Kneser's addition theorem in its usual form: if A, B are finite nonempty subsets of an abelian group and H is the stabilizer of $A + B$, then $|A + B| \geq |A + H| + |B + H| - |H|$; see [4].

Lemma 2.4. *If $A \subseteq C_h$ contains 0, generates C_h , and $|A| = k$, then $\ell A = C_h$ for $\ell = \lceil 2h/k \rceil$.*

Proof. The case $h = 1$ is immediate. Otherwise suppose $\ell A \neq C_h$, and let H be its stabilizer, of size j . Write $t = |A + H|/j$. Since A generates the group, $t \geq 2$, and $k \leq tj$. Iterated Kneser in the quotient by H gives

$$\frac{|\ell A|}{j} \geq \ell(t-1) + 1 \geq \frac{2h(t-1)}{k} + 1 \geq \frac{h}{j} \frac{2(t-1)}{t} + 1 > \frac{h}{j},$$

a contradiction. The iteration is legitimate since a stabilizer of an intermediate sumset stabilizes the final sumset as well. $\square$

Lemma 2.5. *Let B be a set of k distinct positive integers, with $\gcd(B) = 1$ and $h = \max B$. Put*

$$\ell = \lceil 2h/k \rceil, \quad \rho = \ell + 1, \quad L = \ell h.$$

If $c_b \geq \rho$ for $b \in B$, then

$$(2.3) \quad [L, L + h + \sum_{b \in B} (c_b - \rho)b] \cap \mathbb{Z} \subseteq \Sigma_{0, \mathbb{Z}} \left(\prod_{b \in B} b^{c_b} \right).$$

Moreover $\rho \leq 4h/k$ and $L \leq 2h^2/k + h$.

Proof. Reduction of B modulo h has k distinct residues, contains 0 and generates C_h . By Lemma 2.4, every residue has an integer representation of weight at most ℓh , using at most ℓ entries of $B \setminus \{h\}$. For any integer $z \in [L, L + h]$, choose such a representation $w \equiv z \pmod{h}$, and add $(z - w)/h$ copies of h . This number lies between 0 and $\ell + 1$. Thus ρ copies of each denomination suffice for $[L, L + h]$. Each further copy of a denomination at most h extends the right endpoint by its value, since the interval and its translate overlap. The stated bounds follow from $k \leq h$. $\square$

Lemma 2.6. *For all sufficiently large integers n , put $H = \lfloor \sqrt{n}/16 \rfloor$. Let X be a multiset of primes in $(H/2, H]$, each of multiplicity at most $4\sqrt{n}$. If $|X| \geq 128\sqrt{n}$, then $n \in \Sigma_{0, \mathbb{Z}}(X)$.*

Proof. Let q have largest multiplicity M and put $\ell = \lfloor M/8 \rfloor$. If $M < 16$, then $|X| \leq 15H < \sqrt{n}$, a contradiction. Thus $M/16 \leq \ell \leq M/8$ and $2\ell + 3 \leq M/2$. Writing c_a for the other multiplicities, we have

$$\sum_{a \neq q} \min(c_a, \ell) \geq \frac{\ell}{M} (|X| - M) \geq \frac{|X| - M}{16} \geq q - 1.$$

Reserve $q - 1$ non- q copies, at most ℓ of each type, and $2\ell + 3$ copies of q . If d_a is the number of reserved copies of $a \neq q$, form $A_j = \{0\} \cup \{a \bmod q : d_a \geq j\}$ for $1 \leq j \leq \ell$. The nonzero residues in each layer are distinct, because the original window has width less than q . Cauchy–Davenport gives $A_1 + \dots + A_\ell = C_q$, since $\sum_j (|A_j| - 1) = q - 1$.

Each residue is therefore represented by reserved non- q copies with integer weight at most $L = \ell H$. Adding reserved q 's covers $[L, L + 2q] \cap \mathbb{Z}$; fewer than $2\ell + 3$ copies suffice because $H < 2q$. The width $2q$ exceeds every remaining denomination. Also $L \leq MH/8 \leq n/32$, whereas fewer than $3\sqrt{n}$ copies were reserved. For large n , $H \geq \sqrt{n}/32$, so the remaining weight is greater than

$$\frac{\sqrt{n}}{64} (128\sqrt{n} - 3\sqrt{n}) > n.$$

Adding the remaining copies one at a time extends the integer interval beyond n . $\square$

Proposition 2.7. *Every index-one-free unit sequence over C_n satisfies*

$$(2.4) \quad \sum_{x \in U(n)} \min\{c_x, \lfloor 4\sqrt{n} \rfloor\} \ll \varphi(n) \log(2n).$$

Every index-one-free sequence over C_n satisfies

$$(2.5) \quad \sum_{x \in \text{supp}(S)} \min\{c_x, \lfloor 4\sqrt{\text{ord}(x)} \rfloor\} \ll n \log(2n).$$

Proof. Truncate each unit multiplicity at $\lfloor 4\sqrt{n} \rfloor$, obtaining X . Use the prime window of Lemma 2.6, removing primes dividing n , and denote the remaining primes by $\mathcal{P}$. The prime number theorem gives $|\mathcal{P}| \gg \sqrt{n}/\log(2n)$ for large n : at most $\omega(n) \leq \log_2 n$ primes were removed. Quantitative versions of the required prime estimates are given in [5]. In every unit direction fewer than $128\sqrt{n}$ copies of X lie in $\mathcal{P}$, or the lemma gives an index-one subsequence. Averaging over $U(n)$, each unit type visits every allowed prime once, so

$$|\mathcal{P}||X| < 128\varphi(n)\sqrt{n}.$$

This proves (2.4). The finitely many small n are absorbed by increasing the absolute constant, using $c_x < n$. Apply this result to every exact-order class and use Lemma 2.1 and $\sum_{d|n} \varphi(d) = n$ to obtain (2.5). $\square$

2.2. Two-generator zero sums. The following elementary representation allows heights that need not be units.

Lemma 2.8. *Suppose $1^r b^s$ is a mixed atom over C_n , where $b \in U(n)$ and $b \neq 1$. If $s = 1$, it has index one. If $s > 1$, there are positive integers u, v such that*

$$(2.6) \quad 0 < u < s, \quad ru + sv = n, \quad v \equiv bu \pmod{n}, \quad \gcd(u, s) = 1.$$

Proof. Take $b \in [1, n-1]$. Write $r + bs = nt$. If a prime divides both t and s , it divides r , and division by that prime gives a proper zero sum. Thus $(t, s) = 1$. For $s > 1$, choose $0 < u < s$ with $tu \equiv 1 \pmod{s}$ and set $v = (n - ru)/s$. This is an integer and $bu - v = n(tu - 1)/s$ is a multiple of n . If $v < 0$, the counts $(-v, u)$ give a proper zero sum, since $-v < r$ and $u < s$. If $v = 0$, then $n \mid bu$, impossible since $u < s < n$. Hence $v > 0$. For $s = 1$, minimality gives $r + b = n$. $\square$

Proposition 2.9. *Let $\ell = P^-(n)$ and let a, b be distinct generators of C_n . If $a^A b^B$ is index-one-free but contains a nonempty zero sum, then*

$$(2.7) \quad A < n/\ell, \quad B < n/\ell.$$

Proof. Normalize a to 1. Any atom (r, s) contained in the sequence has index greater than one. In (2.6), u is therefore not a unit. A common prime factor of u and n divides v , so $u, v \geq \ell$ and $s > \ell$.

Consider

$$(2.8) \quad (r', s') = (r + v, s - u).$$

This is a positive zero sum and is itself an atom. Indeed, the vectors (r, s) and $(v, -u)$ form a basis of the lattice $\{(R, S) \in \mathbb{Z}^2 : R + bS \equiv 0 \pmod{n}\}$, since their determinant is $-n$. If a nonzero lattice point has $0 \leq R \leq r + v$ and $0 \leq S \leq s - u$, minimality of (r, s) forces $R > r$. The integer $\beta = (sR - rS)/n$ is positive. In the displayed basis write

$$R = kr + \beta v, \quad S = ks - \beta u.$$

Since $S \geq 0$, $k \geq 1$. Thus $R \geq r + v$, with equality only for $k = \beta = 1$. This proves minimality of (2.8). Moreover

$$\ell(r + v) \leq ru + sv = n.$$

If $A \geq n/\ell$, the neighboring atom remains in the original inventory: $r' \leq A$ and $1 \leq s' < s \leq B$. If it still has index greater than one, repeat. Its second count decreases strictly, so this process must reach an index-one atom, a contradiction. This proves $A < n/\ell$, and the other inequality follows by interchanging the two types. $\square$

Lemma 2.10. *Suppose either $n = p^k$, or $n = p^k q$ with distinct primes p, q and $q \geq p^k$. Every atom over C_n supported on at most two units has an index-one subsequence in its square.*

Proof. Single-type atoms and the case $s = 1$ in Lemma 2.8 are immediate. Use its positive heights u, v . In the mixed case $q \nmid u$: otherwise $q \mid v$ and $r + s \leq p^k \leq q$, whereas $s > u \geq q$. If u is a unit there is nothing to prove. Otherwise $p \mid u, v$, and $p \nmid r, s$ by $(u, s) = 1$ and the original zero-sum relation.

If $v > r$, set $R = r$ and $S = s$. The positive heights $(U_1, V_1) = (u + s, v - r)$ satisfy $rU_1 + sV_1 = n$ and $V_1 \equiv bU_1 \pmod{n}$, and avoid p . If $0 < v < r$ and $ru \geq n/2$, put

$$j = \lfloor (s - 1)/u \rfloor, \quad R = r + jv, \quad S = s - ju.$$

Then $1 \leq S < u$, $R < n/u \leq 2r$, $S \leq s$, and

$$(U_1, V_1) = (u - S, v + R), \quad RU_1 + SV_1 = n, \quad V_1 \equiv bU_1 \pmod{n}.$$

These heights again avoid p . If $sv > n/2$, use instead

$$j = \lfloor (r - 1)/v \rfloor, \quad R = r - jv, \quad S = s + ju, \quad (U_1, V_1) = (u + S, v - R).$$

Here $1 \leq R < v$, $S < n/v < 2s$, and the same identities hold. Equality $v = r$ is impossible because $p \mid v$ and $p \nmid r$. These cases already complete the proof for a prime power.

For $n = p^k q$, a further repair is needed only if $q \mid U_1, V_1$. In the translation case this forces $r + s \leq p^k \leq q$ and, from $U_1 = u + s < 2s$, gives $s > q/2$ and $r < q/2$. Replace the heights by $(u + hs, v - hr)$, choosing $h = 2$ for odd p and $h = 3$ for $p = 2$. They are positive: $V_1 \geq q$ and $(h - 1)r < q$. Their residues modulo p are nonzero, and modulo q are $(h - 1)s, -(h - 1)r$, also nonzero.

In the first shear case, $R + S \leq p^k \leq q$, and $r = (j + 1)R - jV_1 > 0$ implies $R > q/2$, hence $S < q/2$. Use $(u - hS, v + hR)$ with the same choice of h . Its first coordinate is positive because $U_1 \geq q > (h - 1)S$. Modulo p the two coordinates are $-hs, hr$, and modulo q they are $-(h - 1)S, (h - 1)R$. They are units. In the symmetric shear case, $s = (j + 1)S - jU_1 > 0$ gives $S > q/2$ and $R < q/2$; use $(u + hS, v - hR)$. The verification is identical with the roles exchanged. For $p = 2$, q is odd, so the factor $h - 1 = 2$ is nonzero modulo q .

In every case the final positive heights U, V satisfy $RU + SV = n$, $V \equiv bU \pmod{n}$, $(U, n) = 1$, with $R \leq 2r$ and $S \leq 2s$. The integer equality ensures $U, V < n$; they are the actual positive representatives, and the counts lie in the square of the original atom. $\square$

2.3. Short lattice coordinates. We first record the short-lattice argument in a form valid for arbitrary moduli. A vector is called primitive in a lattice if it is not a positive integer multiple of another vector of that lattice. Its integer coordinates need not be coprime.

Lemma 2.11. *Let $b \in \mathcal{U}(n)$, let $1 \leq m < n$, and suppose $m^2 > n$ and $1^m b^m$ has no nonempty zero sum. Set $Q = \lfloor n/m \rfloor$. The lattice*

$$\Lambda_b = \{(x, y) \in \mathbb{Z}^2 : y \equiv bx \pmod{n}\}$$

has a unique primitive positive vector (q, v) in $[1, Q]^2$. It can be completed to a basis $(q, v), (s, -r)$ with

$$(2.9) \quad 0 \leq s < q, \quad r > 0, \quad qr + vs = n.$$

If $D = (q, v)$, then

$$(2.10) \quad D \mid n, \quad (q, n) = (v, n) = D.$$

Proof. Place the $m + 1$ distinct representatives of $0, b, \dots, mb$ in m half-open intervals of length n/m . Two give a vector with $1 \leq q \leq m$ and $0 < |v| < n/m$. Negative v gives a forbidden zero sum, so $v > 0$. Shorten on the same lattice ray to a primitive vector; then $qv < n$. Complete it to a lattice basis, choose the determinant to be $-n$, and reduce the other first coordinate modulo q . This gives (2.9); $r > 0$ follows from $vs < qv < n$. If $q > n/m$, then $0 < r \leq n/q < m$ and $s < q \leq m$. Here $s = 0$ would force $n \mid r$, impossible. Thus $1^r b^s$ is a forbidden zero sum. Consequently $q \leq n/m$, and both coordinates are at most Q .

Any two vectors in this square have determinant of absolute value less than n , because $Q^2 < n$, and the determinant is a multiple of n . They lie on the same ray, giving uniqueness of the primitive vector. The basis determinant implies $D \mid n$. Since b is a unit, $(q, n) = (v, n)$; this common divisor divides D , and $D \mid n$ gives the reverse divisibility. This proves (2.10). $\square$

3. NEAR-LINEAR BOUNDS FOR SMALL INDICES

Let $J(n)$ be the least positive integer such that every block of $J(n)$ consecutive integers contains an integer coprime to n , and set $J(1) = 1$. Equivalently, $J(n) - 1$ is the maximal length of a block containing no integer coprime to n ; this additive-one convention does not affect the bound quoted below. Also put

$$\mathcal{A}(n) = \prod_{p^a \parallel n} (a + 6), \quad \sigma(n) = \sum_{d \mid n} d.$$

Here $\sigma(n)$ is the sum-of-divisors function. We prove the following quantitative form of Theorem 1.1.

Proposition 3.1. *There is an absolute constant C such that, for every $n \geq 2$ and every integer $r \geq 10^6 J(n)$,*

$$(3.1) \quad I_r(n) \leq C \sigma(n) \mathcal{A}(n) \log(2n).$$

We use Iwaniec's bound for the Jacobsthal function [7, Corollary, p. 226]:

$$(3.2) \quad J(n) \ll [\omega(n) \log(2\omega(n))]^2.$$

In particular, $J(n) \ll \log^4(2n)$. Also $J(d) \leq J(n)$ whenever $d \mid n$, since every block of $J(n)$ consecutive integers contains an integer coprime to n , hence to d .

3.1. Two-type atoms and short coordinates.

Lemma 3.2. *Suppose $\gcd(z, B, n) = 1$, with $B \neq 0$, and put $R = \prod_{p \mid n, p \nmid B} p$. Every block of $J(R)$ consecutive integers k contains one for which $z + Bk$ is coprime to n .*

Proof. If $p \mid B$ and $p \mid n$, then $p \nmid z$. For every prime $p \mid R$, the sole forbidden residue is $k \equiv -zB^{-1} \pmod{p}$. The Chinese remainder theorem translates these forbidden residues simultaneously into the condition that $k + \kappa$ be divisible by one of the primes dividing R . The definition of $J(R)$ now applies. The same assertion holds when $R = 1$. $\square$

Lemma 3.3. *Let $1^A b^B$ be a mixed atom over C_n , with $b \in \mathcal{U}(n)$ and $b \neq 1$. Its index is at most r if either $\min(A, B) \leq r$, or*

$$(3.3) \quad r \geq 4J(n), \quad AB \leq \frac{rn}{4(J(n) + 2)}.$$

Proof. Both counts are less than n . Normalize the type with the larger count to 1. The positive weight is a multiple of n strictly less than $(\min(A, B) + 1)n$, proving the first assertion.

Thus assume $A, B > r$. Lemma 2.8 supplies positive u, v with

$$Au + Bv = n, \quad v \equiv bu \pmod{n}, \quad (u, B) = 1.$$

Put $P = \prod_{p|n, p|B} p$. Choose $j \in [r/2, r]$ coprime to P ; this interval contains at least $J(P)$ consecutive integers. The conditions

$$x = ju + Bk > 0, \quad y = jv - Ak > 0$$

define an open interval of real k of length $jn/(AB) \geq 2(J(n) + 2)$. It contains a block of $J(n)$ consecutive integers. Since $\gcd(ju, B, n) = 1$, Lemma 3.2 gives such a k for which x is a unit modulo n . Then $y \equiv bx \pmod{n}$ is a unit as well, and

$$Ax + By = jn.$$

The inequalities $A, B > r \geq j$ imply $0 < x, y < n$. Hence these are the actual positive representatives in direction x , and the atom has index at most $j \leq r$. $\square$

For the remainder of this section, let $S = \prod_a a^{c_a}$ be an index- r -free unit sequence, where $r \geq 10^6 J(n)$. Define

$$(3.4) \quad T = 64\lceil\sqrt{n}\rceil, \quad \mathcal{H} = \{a : c_a \geq T\}, \quad Q = \lfloor n/T \rfloor.$$

If $T \geq n$, then $\mathcal{H}$ is empty. Otherwise every sequence $a^T b^T$ with distinct $a, b \in \mathcal{H}$ has no nonempty zero sum. Indeed, a zero sum would contain a mixed atom with counts $A, B \leq T$, since $T < n$. But

$$AB \leq T^2 \leq 16384n < \frac{rn}{4(J(n) + 2)},$$

so Lemma 3.3 gives a contradiction.

Lemma 2.11, applied with $m = T$, therefore gives unique lattice-primitive coordinates

$$(3.5) \quad q_{ab}a \equiv v_{ab}b \pmod{n}, \quad 1 \leq q_{ab}, v_{ab} \leq Q.$$

Reversing a, b interchanges the coordinates; take $(1, 1)$ on the diagonal. If $D = (q_{ab}, v_{ab})$, then

$$D \mid n, \quad (q_{ab}, n) = (v_{ab}, n) = D.$$

In particular, writing $(q_{ab}, v_{ab}) = (Dx, Ds_a)$ and $M = n/D$, we have $(x, s_a) = 1$ and $x, s_a \in \mathcal{U}(M)$.

We may henceforth assume that n exceeds an absolute threshold so that

$$(3.6) \quad 2Q^2 + Q < n, \quad 8Q < T, \quad J(n)Q < n/4.$$

The first two inequalities follow from (3.4), and the last follows from (3.2). The implied constant in (3.2) is absolute, so the finite exceptional set of moduli is independent of r . These moduli are absorbed into an absolute constant using $|S| \leq (n-1)\varphi(n)$.

3.2. An integer budget with an anchor. Fix $b \in \mathcal{H}$, $D \mid n$ with $1 < D \leq Q$, and $1 \leq x \leq K = \lfloor Q/D \rfloor$. Consider those $a \in \mathcal{H}$ whose coordinates relative to b are (Dx, Ds_a) , and put

$$F_D = \{p \mid n : p^{v_p(n)} \mid D\}.$$

Partition these types by the valuations $v_p(s_a)$ for $p \in F_D$. For a fixed valuation class, put $L = \prod_{p \in F_D} p^{v_p(s_a)}$ and partition further according to the unit

$$(3.7) \quad \gamma = (s_a/L)a^{-1} \pmod{n}.$$

Since $s_a \in \mathcal{U}(M)$, any prime $p \mid n$ dividing s_a does not divide $M = n/D$, so $p^{v_p(n)} \mid D$. Thus $p \in F_D$, and its full contribution to s_a is removed in L . Consequently s_a/L and γ are units modulo n . Also L is a unit modulo M , and all phases reduce to $xL^{-1}b^{-1} \pmod{M}$. Since $M \mid n$, the

Chinese remainder theorem shows that the reduction map $U(n) \rightarrow U(M)$ is surjective, so every fibre has $\varphi(n)/\varphi(M) \leq D$ elements. Thus there are at most D phases in each valuation class.

Lemma 3.4. *For every nonempty group $\mathcal{C}$ with fixed b, D, x , valuations and phase as above,*

$$(3.8) \quad \sum_{a \in \mathcal{C}} c_a s_a < 2M.$$

Proof. Let $g = \gcd_{a \in \mathcal{C}} s_a = Lg_0$ and $w_a = s_a/g$. Since $g_0 \mid s_a/L$ and s_a/L is coprime to n , both g_0 and $w_a = (s_a/L)/g_0$ are units modulo n . The distinct positive integers w_a have $\gcd 1$, and $(x, g) = 1$. The direction $u_0 = \gamma g_0^{-1} \pmod{n}$ gives the actual core heights w_a . Write $Y_0 = [u_0 b]_n$. The congruence $xa \equiv s_a b \pmod{M}$ implies

$$(3.9) \quad gY_0 = x + jM, \quad 0 \leq j < Dg.$$

Here $gY_0 - x > -M$, since $x \leq K < M$, and $gY_0 < gn = DgM$.

We claim $(j, Dg) = 1$. Set $h_a = (xa - s_a b)/M$, using integer representatives for a, b . Lattice primitivity implies $(h_a, D) = 1$: if a prime p divided both, then

$$n = DM \mid \frac{D}{p}(xa - s_a b),$$

so $(Dx/p, Ds_a/p)$ would be another lattice vector on the same positive ray, contradicting primitivity. Multiplying $Mh_a = xa - s_a b$ by u_0 , reducing modulo DM , and cancelling the integer factor M gives

$$u_0 h_a \equiv \frac{xw_a - s_a Y_0}{M} = -w_a j \pmod{D}.$$

Since u_0, w_a and h_a are units modulo D , this proves $(j, D) = 1$. Equation (3.9) and $(x, g) = 1$ also give $(j, g) = 1$. In particular $1 \leq j < Dg$.

Let $\lambda_0 \in [1, Dg - 1]$ be the inverse of j modulo Dg , and set $\sigma_0 = Dg - \lambda_0$. By Lemma 3.2, there is $t \in [0, J(n) - 1]$ such that

$$\lambda = \lambda_0 + tDg \in U(n), \quad 1 \leq k = t + 1 \leq J(n) \leq r.$$

Define the integers

$$(3.10) \quad \tau = \frac{M - x\sigma_0}{g}, \quad Y = \frac{M + \lambda x}{g}.$$

Their integrality follows by reducing $x + jM \equiv 0 \pmod{g}$ and $\lambda j \equiv 1 \pmod{Dg}$ modulo g . Moreover

$$(3.11) \quad D((D + 2)K^2 + K) \leq 2Q^2 + Q < n,$$

since $D \geq 2$ and $DK \leq Q$. Hence $\tau > 0$ and $1 \leq \sigma_0 < Dg \leq DK \leq Q < T$. The core heights in direction λu_0 satisfy

$$0 < \lambda w_a < J(n)Ds_a \leq J(n)Q < n.$$

The anchor height in that direction is exactly Y , because

$$g(\lambda Y_0 - Y) = M(\lambda j - 1) \in gn\mathbb{Z}, \quad 0 < Y < \frac{M}{g} + J(n)Dx \leq \frac{n}{2} + J(n)Q < n.$$

In particular, no inversion of the possibly nonunit integer g is being used. Since $\lambda + \sigma_0 = (t + 1)Dg$, the target identity is

$$(3.12) \quad \lambda\tau + \sigma_0 Y = \frac{(\lambda + \sigma_0)M}{g} = (t + 1)DM = kn.$$

Apply Lemma 2.5 to the denominations w_a . Write $h = \max w_a \leq K/g$ and let L_0 be its interval's left endpoint. At most $4K \leq 4Q < T/2$ copies of each type are reserved, and

$$gL_0 \leq 2K^2 + K < M - DK^2 < M - x\sigma_0 = g\tau$$

by (3.11). If the sum in (3.8) were at least $2M$, the unreserved weight would be at least

$$\frac{1}{2g} \sum_{a \in \mathcal{C}} c_a s_a \geq M/g > \tau.$$

The resulting integer interval therefore contains τ . Select actual core copies with total w -weight τ , and add σ_0 copies of b . This anchor is outside $\mathcal{C}$, since its diagonal coordinates have $D = 1$, and its available multiplicity is at least T . Equation (3.12) gives a nonempty subsequence of index at most $k \leq r$, a contradiction. $\square$

3.3. Reciprocal weights and summation over orders.

Proposition 3.5. *Under (3.4),*

$$(3.13) \quad W = \sum_{a \in \mathcal{H}} c_a \ll n\mathcal{A}(n) \log(2n).$$

Proof. Assume (3.6) and put $\alpha = 3/2$. For a pair with coordinates (Dx, Ds) define

$$w_{ab} = \frac{s}{x} \alpha^{\sum_{p \in F_D} (v_p(x) - v_p(s))}.$$

The reversed coordinates give $w_{ab}w_{ba} = 1$, and $w_{aa} = 1$. Fix an anchor b . For fixed $D > 1$, x , and valuations of s , Lemma 3.4 and the bound of D on the number of phases give total s -weight less than $2MD = 2n$. Write $x = x_0 \prod_{p \in F_D} p^{e_p}$, where $e_p = v_p(x)$ and x_0 is coprime to every prime in F_D . If $e_p > 0$, then $(x, s) = 1$ forces $v_p(s) = 0$; together with the factor p^{-e_p} from $1/x$, this contributes $(\alpha/p)^{e_p}$. If $e_p = 0$, summing over $v_p(s) = f \geq 0$ contributes $\sum_{f \geq 0} \alpha^{-f} = 3$. For each fixed exponent vector, the remaining sum of $1/x_0$ over $x_0 \leq K / \prod_{p \in F_D} p^{e_p}$ is at most H_K , where $K = \lfloor Q/D \rfloor$. Extending these nonnegative sums to all $e_p \geq 0$ gives

$$(3.14) \quad \begin{aligned} \sum_{a: (q_{ab}, v_{ab})=D} c_a w_{ab} &\leq 2nH_K \prod_{p \in F_D} \left(3 + \sum_{e \geq 1} (\alpha/p)^e \right) \\ &\leq 2n 6^{|F_D|} H_K. \end{aligned}$$

where $H_K = \sum_{j=1}^K 1/j$. Indeed, $3 + \alpha/(p - \alpha) \leq 6$ for every prime p , including $p = 2$.

For $D = 1$ the same row bound holds with the factor $6^{|F_D|} = 1$. To see this directly, fix $q_{ab} = x$. In direction xb^{-1} the corresponding heights are v_{ab} and the anchor height is x . Their union has gcd 1, since $(x, v_{ab}) = 1$, and all heights are at most Q . Include the anchor only once if it already occurs. Lemma 2.5 reserves fewer than $T/2$ copies per type and starts below $2Q^2 + Q < n$. Thus $\sum_{a: q_{ab}=x, (q_{ab}, v_{ab})=1} c_a v_{ab} < 2n$; otherwise its interval reaches n . Sum after division by x .

Consequently every row is at most

$$2nH_Q \sum_{D|n} 6^{|F_D|} = 2nH_Q \prod_{p^a \parallel n} (a + 6) = 2nH_Q \mathcal{A}(n).$$

For each prime power, the exponents $0, \dots, a-1$ in D have weight 1, while exponent a has weight 6, proving the product identity. Multiply each row by c_b and sum over b . The reciprocal relation and $z + z^{-1} \geq 2$ yield

$$W^2 \leq \sum_{a, b \in \mathcal{H}} c_a c_b w_{ab} \leq 2nH_Q \mathcal{A}(n) W.$$

Divide by W when it is positive. The bounded exceptional moduli are absorbed into the absolute constant as above. $\square$

Proof of Proposition 3.1. By Proposition 2.7, the types of multiplicity below T in a unit sequence contribute $O(\varphi(n) \log(2n))$, since

$$T \leq 32 \lfloor 4\sqrt{n} \rfloor, \quad c_a \leq 32 \min\{c_a, \lfloor 4\sqrt{n} \rfloor\} \quad (c_a < T).$$

Together with Proposition 3.5 this gives

$$L_{U,r}(n) \ll (\varphi(n) + n\mathcal{A}(n)) \log(2n).$$

For a general sequence, partition by exact additive order $d \mid n$. Lemma 2.1 applies, and $r \geq 10^6 J(d)$ because $J(d) \leq J(n)$. Since $\mathcal{A}(d) \leq \mathcal{A}(n)$,

$$\begin{aligned} I_r(n) - 1 &\ll \sum_{d \mid n} (\varphi(d) + d\mathcal{A}(d)) \log(2d) \\ &\leq (n + \sigma(n)\mathcal{A}(n)) \log(2n). \end{aligned}$$

This proves (3.1), after increasing the constant. $\square$

Proof of Theorem 1.1. Equation (3.2) makes the index hypothesis of Proposition 3.1 valid with an absolute constant in (1.2). For every $\varepsilon > 0$, $\mathcal{A}(n) \ll_\varepsilon n^\varepsilon$. Indeed, $a + 6 \leq 7^a$ for $a \geq 1$, so all sufficiently large primes satisfy $a + 6 \leq p^{\varepsilon a}$. For each of the finitely many smaller primes, $(a + 6)p^{-\varepsilon a}$ is bounded. Also $\sigma(n) \leq n(1 + \log n)$. Applying these estimates with a smaller ε proves (1.2).

If $\omega(n) \leq k$, then $\sigma(n)/n \ll_k 1$ and $\mathcal{A}(n) \ll_k \log^k(2n)$. The first follows by bounding $\prod_{p \mid n} (1 - 1/p)^{-1}$ by the product over the first k primes; the second follows from $a \leq \log n / \log 2$ for every $p^a \mid n$. Choose a fixed integer $R_k \geq C[k \log(2k)]^2$ and apply (3.1). This proves (1.3) for all $r \geq R_k$. $\square$

4. INDEX-ONE UPPER BOUNDS

4.1. A bound in terms of the least prime divisor.

Lemma 4.1. *Let S be an index-one-free unit sequence. Suppose A is a set of types of multiplicity at least $T \geq 8 \lfloor \sqrt{n} \rfloor$, and for each $a, b \in A$ there are coordinates satisfying*

$$q_{ab}a \equiv v_{ab}b \pmod{n}, \quad 1 \leq q_{ab}, v_{ab} \leq Q \leq \sqrt{n}/4,$$

with $(q_{ab}, v_{ab}) = 1$, both coordinates units, and $(q_{ba}, v_{ba}) = (v_{ab}, q_{ab})$. On the diagonal take $(1, 1)$. Then $W = \sum_{a \in A} c_a < 2nH_Q$, where $H_Q = \sum_{j=1}^Q 1/j$.

Proof. Fix b and a nonempty group of types with $q_{ab} = j$. In the unit direction jb^{-1} their distinct heights are v_{ab} , and the height of b is j . The union of these denominations has gcd 1. If b already belongs to the group, include it once. The interval of Lemma 2.5 requires at most $4Q \leq T/2$ copies of every type and starts below $2Q^2 + Q < n$. If $\sum_{a: q_{ab}=j} c_a v_{ab} \geq 2n$, the unreserved copies in the group have total weight at least n , so the interval reaches n . Therefore

$$\sum_{a: q_{ab}=j} c_a v_{ab} < 2n, \quad \sum_{a \in A} c_a \frac{v_{ab}}{q_{ab}} < 2nH_Q.$$

Multiply by c_b and sum over b . Reciprocal slopes on the reversed pair give

$$(4.1) \quad W^2 \leq \sum_{a, b \in A} c_a c_b \frac{v_{ab}}{q_{ab}} < 2nH_Q W.$$

Indeed, $x + x^{-1} \geq 2$ on each unordered pair, and the diagonal is unchanged. Divide by W if it is nonzero. $\square$

Proposition 4.2. *For every $n \geq 2$, with $\ell = P^-(n)$,*

$$(4.2) \quad L_U(n) \ll \log(2n) \left[n + \varphi(n) \left(1 + \frac{\sqrt{n}}{\ell} \right) \right].$$

Consequently the second term in (1.6) bounds $I_1(n)$.

Proof. For an index-one-free unit sequence choose the integer

$$T = \max\{8\lceil\sqrt{n}\rceil, 4n/\ell\}, \quad A = \{a : c_a \geq T\}.$$

If $T \geq n$, then A is empty. Otherwise Proposition 2.9 implies that every two-type sequence on A has no ordinary zero sum. Apply Lemma 2.11 with $m = T$. Its coordinates are at most $Q = \lfloor n/T \rfloor \leq \ell/4$, so neither is divisible by a prime factor of n . Equation (2.10) then makes their integer gcd 1. Reversing the pair exchanges the coordinates by uniqueness. Lemma 4.1 pays the entire high part by $O(n \log(2n))$.

Put $B_0 = \lfloor 4\sqrt{n} \rfloor$. For $c_a < T$,

$$c_a \leq \max\{1, T/B_0\} \min(c_a, B_0), \quad T/B_0 \ll 1 + \sqrt{n}/\ell.$$

Proposition 2.7 gives the remaining term in (4.2). This argument also covers $A = \emptyset$.

For a general sequence use (2.1), keeping the $\varphi(d)$ factor in the low part. Since $P^-(d) \geq \ell$ for $d \mid n$, its length is at most a constant times

$$\log(2n) \left[\sigma(n) + n + \frac{n\sqrt{n}}{\ell} \right].$$

Finally

$$\frac{\sigma(n)}{n} = \sum_{d \mid n} \frac{1}{d} \leq 1 + \frac{\tau(n) - 1}{\ell} \leq 1 + \frac{2\sqrt{n}}{\ell}.$$

This proves the assertion, including all terms of proper order. The extra 1 in passing from free length to forcing threshold is absorbed in the absolute constant. $\square$

4.2. Prime powers and a prime power times a larger prime. We now keep the short coordinates even when their gcd is nontrivial. Throughout this section let $n = p^k$, or $n = p^k q$ with distinct primes p, q and $q \geq p^k$. In the first case choose $T = 8\lceil\sqrt{n}\rceil$; in the second choose

$$(4.3) \quad T = \max\{8\lceil\sqrt{n}\rceil, \lceil 2q/p \rceil\}.$$

If $T \geq n$ there are no high types; all arguments concerning them are then omitted. Otherwise put

$$A = \{a : c_a \geq T\}, \quad m = \lfloor T/2 \rfloor, \quad Q = \lfloor n/m \rfloor, \quad B = \lfloor (n-1)/T \rfloor.$$

Here $m^2 > n$ and $Q \leq \sqrt{n}/4$. Lemma 2.10 shows that the sequence with multiplicities $\lfloor c_a/2 \rfloor$ contains no ordinary zero sum on at most two types. Thus Lemma 2.11 gives, for all distinct $a, b \in A$, unique primitive positive coordinates

$$(4.4) \quad q_{ab}a \equiv v_{ab}b \pmod{n}, \quad 1 \leq q_{ab}, v_{ab} \leq Q.$$

Use (1, 1) on the diagonal. The reversed coordinates are exchanged.

Lemma 4.3. *For the coordinates in (4.4),*

$$(4.5) \quad q_{ab}c_b < n, \quad v_{ab}c_a < n.$$

Consequently $q_{ab}, v_{ab} \leq B$. Their gcd D is a power of p . Writing $(q_{ab}, v_{ab}) = (Dr, Ds)$, both r, s are units modulo n .

Proof. Normalize b to 1 and a to a/b , and write $(\alpha, \beta) = (q_{ab}, v_{ab})$. Complete this vector to the basis $(\alpha, \beta), (s_0, -r_0)$ of Lemma 2.11. If $\alpha \geq n/c_b$, then $\alpha > 1$, $1 \leq r_0 \leq n/\alpha \leq c_b$, and $0 \leq s_0 < \alpha \leq Q < c_a$. The possibility $s_0 = 0$ would force $n \mid r_0$, impossible. If $D = 1$, α is a unit by (2.10), and $r_0\alpha + s_0\beta = n$ gives index one with available copies. If $D > 1$, then $p \mid \alpha, \beta$. In the mixed case $Q < q$, so D has no prime factor other than p . Since the first-coordinate projection of the lattice is $\mathbb{Z}$, the basis gives $(\alpha, s_0) = 1$, so $p \nmid s_0$. The positive direction $\alpha - s_0$ avoids p and, in the mixed case, is less than q . It is a unit. In this direction the heights are $\alpha - s_0$ and $\beta + r_0$, and

$$r_0(\alpha - s_0) + s_0(\beta + r_0) = n.$$

This is another forbidden certificate within the original counts. Thus $\alpha < n/c_b$; reversing the pair proves the other inequality. The diagonal follows from $c_a < n$.

The gcd assertion follows from (2.10) and $Q < q$ in the mixed case. If $D = p^e$ with $e < k$, the divided coordinates avoid p by (2.10). When $e = k$, which is possible only in the mixed case, (4.3) gives

$$r, s \leq B/p^k < p/2.$$

They again avoid p . All divided coordinates are less than the larger prime, so they avoid that prime as well. $\square$

The following local lemma is the step that removes the gcd loss. Its formulation concerns actual positive representatives in a single unit direction.

Lemma 4.4. *Let $D = p^e > 1$ with $D \mid n$, $D \leq B$, and put $M = n/D$ and $K = \lfloor B/D \rfloor$. In a unit direction suppose distinct core types have heights v_i , and a separate type has height $r + jM$, where*

$$(4.6) \quad 1 \leq r, v_i \leq K, \quad (r, n) = (v_i, n) = (r, v_i) = 1, \quad 1 \leq j < D, \quad (j, D) = 1.$$

Suppose all these multiplicities are at least T . If the sequence is index-one-free, then

$$(4.7) \quad \sum_i c_i v_i < 2n/D.$$

Proof. Let $g = \gcd_i v_i$, $x_i = v_i/g$, and $h = \max_i x_i$. Thus $(g, n) = (r, g) = 1$ and $\gcd_i x_i = 1$. The Chinese remainder theorem gives a unique $0 \leq \sigma < Dg$ satisfying

$$(4.8) \quad r\sigma \equiv M \pmod{g}, \quad j\sigma \equiv -1 \pmod{D}.$$

In particular $1 \leq \sigma < Dg \leq DK \leq n/T < T$ and $p \nmid \sigma$. Put

$$(4.9) \quad \tau = (M - r\sigma)/g, \quad \lambda = Dg - \sigma.$$

The integer $\lambda > 0$ avoids p . In the mixed case it is at most $B < q$, so it avoids the other prime too. Thus λg^{-1} is a legal change of direction modulo n .

We check the endpoints before using it. Since $D \geq 2$,

$$(4.10) \quad D((D+2)K^2 + K) \leq 2(DK)^2 + DK \leq 2n^2/T^2 + n/T < n.$$

Consequently $(D+2)K^2 + K < M$, and $r\sigma < DK^2$ implies $\tau > 0$. In the new direction the core heights are exactly λx_i : they lie in $(0, DK) \subset (0, n)$. The anchor height is exactly $Dr + \tau$. Indeed, (4.8) implies

$$\sigma(r + jM) + g\tau \equiv 0 \pmod{n},$$

and hence its residue after multiplying by λg^{-1} is $Dr + \tau$. This positive integer is less than n , as is also verified by the identity

$$(4.11) \quad \lambda\tau + \sigma(Dr + \tau) = Dg\tau + Dr\sigma = DM = n.$$

It remains to represent the integer τ with available core copies. If there are s core types, Lemma 2.5 supplies an interval starting at $L = \lceil 2h/s \rceil h$, using reserves $\rho = \lceil 2h/s \rceil + 1 \leq 4K < T/2$ per type. Moreover

$$gL \leq 2K^2 + K < M - DK^2 < M - r\sigma = g\tau.$$

If (4.7) fails, the unreserved normalized weight is at least $\frac{1}{2} \sum_i c_i x_i \geq M/g > \tau$. The interval therefore contains τ , represented by counts $d_i \leq c_i$. Take these core copies and $\sigma < T$ anchor copies in the new direction. Equation (4.11) gives total weight exactly n , contradicting freeness. No entry of height g or 1 has been added: g is used only to normalize integer denominations and to change a unit direction. $\square$

Proposition 4.5. *For the high types in this section,*

$$(4.12) \quad \sum_{a \in A} c_a \leq 2n(k+1)H_Q.$$

Proof. Fix $b \in A$. Pairs with $D = (q_{ab}, v_{ab}) = 1$ satisfy exactly the denomination-group estimate in the proof of Lemma 4.1, and contribute less than $2nH_Q$ to $\sum_a c_a v_{ab}/q_{ab}$.

For $D = p^e > 1$, write $(q_{ab}, v_{ab}) = (Dr, Ds_a)$ with $(r, s_a) = 1$, and put $M = n/D$. Lemma 4.3 ensures all divided coordinates are units and at most $K = \lfloor B/D \rfloor$. Define

$$z_a = rab^{-1}s_a^{-1} \equiv 1 + t_a M \pmod{n}.$$

Primitivity in the original lattice implies $(t_a, D) = 1$. Indeed, if $p \mid t_a$, then

$$ra - s_a b \equiv t_a M s_a b \pmod{n}$$

implies $pM \mid ra - s_a b$, since $pM \mid n$. Hence $n \mid (D/p)(ra - s_a b)$, so $(Dr/p, Ds_a/p)$ would still belong to the original lattice, contrary to the primitivity of (Dr, Ds_a) . Fix r and a phase $t = t_a$. The unit direction

$$u_0 = (1 + tM)^{-1} r b^{-1}$$

makes all core heights exactly the distinct integers s_a . The anchor height is $r + jM$, with $j \equiv -r(1 + tM)^{-1}t \pmod{D}$, so $(j, D) = 1$. Lemma 4.4 applies to this group and yields

$$\sum_{a \text{ in the group}} c_a s_a < 2n/D.$$

There are at most $\varphi(D)$ phases. Dividing by r , summing over $r \leq \lfloor B/D \rfloor$, and then over $D = p^e > 1$, gives

$$\sum_{a: D > 1} c_a \frac{v_{ab}}{q_{ab}} \leq 2n \sum_{\substack{1 \leq e \leq k \\ p^e \leq B}} \frac{\varphi(p^e)}{p^e} H_{\lfloor B/p^e \rfloor} \leq 2nkH_Q.$$

Adding the $D = 1$ estimate, multiplying by c_b and using reciprocal pairing as in (4.1) proves (4.12). The anchor is used separately to prove each necessary inequality; certificates from different directions are never concatenated. $\square$

Proof of (1.4) and (1.7). For $n = p^k$, the low part has $c_a < T = 8\lceil \sqrt{n} \rceil$, so (2.4) bounds it by $O(\varphi(n) \log(2n))$. Proposition 4.5 gives

$$L_U(p^k) \ll (k+1)p^k \log(2p^k).$$

The finite cases with $T \geq n$ are absorbed in the constant. Sum over the exact-order classes p^j , $1 \leq j \leq k$. Since $\sum_{j=1}^k p^j \leq 2p^k$, Lemma 2.1 proves (1.4). Also $k \leq \log_2 n$, giving its uniform consequence.

For $n = p^k q$, the cutoff (4.3) and (2.4) give the low-part estimate

$$O\left(n \log(2n) \left(1 + \frac{1}{p} \sqrt{q/p^k}\right)\right).$$

Together with (4.12) this proves the corresponding unit bound. Apply it to the classes $p^j q$, $1 \leq j \leq a$, when the ambient order is $p^a q$. The necessary sums satisfy

$$\sum_{j=1}^a (j+1)p^j q \leq 2(a+1)p^a q, \quad \sum_{j=1}^a p^{j/2-1} q^{3/2} \ll \frac{p^a q}{p} \sqrt{q/p^a}.$$

The prime class q and the pure p -power classes are paid by (1.4). Lemma 2.1 now gives (1.7) for arbitrary sequences. $\square$

4.3. Twice a prime square. We prove (1.10). Throughout this section p is odd and $n = 2p^2$; the single order arising from $p = 2$ is absorbed into the absolute constant.

Lemma 4.6. *Every atom supported on at most two units of C_{2p^2} has an index-one subsequence in its sixth power.*

Proof. Only a mixed atom $1^r b^s$, with $s > 1$, requires proof. Lemma 2.8 gives positive heights u, v with

$$(4.13) \quad ru + sv = n, \quad v \equiv bu \pmod{n}, \quad (u, s) = (v, r) = 1.$$

For the second coprimality, a prime dividing v, r would divide n , then s from $r + bs \equiv 0$, and then u from $v \equiv bu$, a contradiction. The counts r, s have the same parity, as do u, v .

First suppose $p \mid u, v$, allowing any positive zero-sum counts and heights satisfying (4.13). Write $u = pA, v = pB$. Then

$$rA + sB = 2p, \quad p \nmid rs.$$

If u, v are even, then $A, B \geq 2$, $r + s \leq p$, and r, s are odd. The heights $(u + s, v - r)$ are positive units with the same counts. If u, v are odd and r, s are even, use these heights when $v > r$. Otherwise $r \geq p$ and $s < p \leq u$, so use $(u - s, v + r)$. These also are positive units with the same counts.

It remains that all four integers are odd. If $v > 2r$, use $(u + 2s, v - 2r)$; if $u > 2s$, use $(u - 2s, v + 2r)$. Otherwise $r \geq pB/2$ and $s \geq pA/2$ imply $AB \leq 2$. Thus $A = B = 1$, $r + s = 2p$, and $r, s \geq p/2$, with neither equal to p . For $r < p < s$, take

$$(R, S, U, V) = (r + p, s - p, r, r + 2p);$$

for $s < p < r$, take

$$(R, S, U, V) = (r - p, s + p, s + 2p, s).$$

In both cases $RU + SV = n$, $V \equiv bU \pmod{n}$, and U, V are positive units, while $R \leq 3r, S \leq 3s$. For example, the first choice follows from the neighboring counts $(r + v, s - u)$ and the height shift $(u - S, v + R)$. This proves a threefold repair whenever $p \mid u, v$.

If the original u is already a unit, finish. The only remaining case has u, v even and $p \nmid u$. Then r, s are odd. If $v > r$, use the unchanged counts and heights $(u + s, v - r)$. If $v < r$ and $ru \geq n/2$, put

$$j = \lfloor (s - 1)/u \rfloor, \quad R = r + jv, \quad S = s - ju, \quad (U, V) = (u - S, v + R).$$

Here $1 \leq S < u$, $R < n/u \leq 2r$ and $S \leq s$. The coprimality and zero-sum relations are preserved, since

$$(U, S) = (u, S) = (u, s) = 1, \quad (V, R) = (v, R) = (v, r) = 1, \\ R + bS = (r + bs) + j(v - bu) \equiv 0 \pmod{n}.$$

If $ru < n/2$, put instead

$$j = \lfloor (r - 1)/v \rfloor, \quad R = r - jv, \quad S = s + ju, \quad (U, V) = (u + S, v - R).$$

Then $1 \leq R < v$, $S < n/v < 2s$ and $R \leq r$. The same gcd equalities hold, and now $R + bS = (r + bs) - j(v - bu) \equiv 0 \pmod{n}$. Equality $v = r$ is excluded by parity. In every case the new

heights are positive odd integers, satisfy the same determinant and congruence identities, and obey $(U, S) = (V, R) = 1$. If they avoid p , finish; otherwise apply the preceding threefold repair. The resulting counts are at most $6r, 6s$. A positive identity of weight n makes both unit heights less than n , so they are the actual representatives. $\square$

The next lemma handles an even ordinary gcd without inverting it modulo $2p^2$.

Lemma 4.7. *Put $M = p^2$. Let $r, s_i \in [1, K]$ with the s_i distinct, $(r, s_i) = 1$, and r, s_i of opposite parity. Suppose all s_i have the same 2-adic valuation and*

$$2K < p, \quad 4K^2 + K < M.$$

Let b, a_i be actual unit types with $ra_i \equiv s_i b \pmod{M}$, each of multiplicity at least $T \geq 8K + 8$. In an index-one-free sequence their original multiplicities satisfy

$$(4.14) \quad \sum_i c_{a_i} s_i < 2M = n.$$

Proof. Let $g = (s_i : i)$ and $x_i = s_i/g$. The x_i are odd, have gcd 1, and have maximum $h \leq K/g$; also $(g, p) = (g, r) = 1$. Let u_0 be the odd lift modulo $2M$ of $rg^{-1}b^{-1} \pmod{M}$. It is a unit and $[u_0 a_i]_n = x_i$. Writing $y = [u_0 b]_n$ gives

$$gy = r + jM, \quad 1 \leq j < 2g, \quad (j, 2g) = 1.$$

Indeed g, r have opposite parity, so j is odd; any common divisor of j, g divides r . The anchor is separate from the core since $y > M/g > h$.

Take $1 \leq \lambda < 2g$ with $\lambda j \equiv 1 \pmod{2g}$, and put

$$\sigma = 2g - \lambda, \quad \tau = (M - r\sigma)/g, \quad Y = (M + \lambda r)/g.$$

These are integers. The number λ is odd and less than p , so λu_0 is a legal unit. The actual core heights and anchor height in this direction are respectively λx_i and Y , because

$$(4.15) \quad \lambda \tau + \sigma Y = 2M.$$

Here $r\sigma < 2K^2 < M$ makes $\tau > 0$, the identity gives $0 < Y < n$, and the anchor congruence follows from $\lambda j \equiv 1 \pmod{2g}$. Also $\sigma < 2g \leq 2K < T$.

Apply Lemma 2.5 to the denominations x_i . With k types, take $\ell = \lceil 2h/k \rceil$, $\rho = \ell + 1$ and $L = \ell h$. Its reserve satisfies $\rho \leq 4h < T/2$, while

$$gL \leq 2K^2 + K < M - 2K^2 < M - r\sigma = g\tau.$$

If (4.14) fails, the unreserved core has weight at least $M/g > \tau$. The interval therefore represents the integer τ using available copies. Combine it with σ anchor copies in direction λu_0 ; (4.15) gives weight exactly n , a contradiction. $\square$

Proof of (1.10). First consider a free unit sequence and set

$$T = 64\lceil\sqrt{n}\rceil, \quad m = \lfloor T/6 \rfloor, \quad Q = \lfloor n/m \rfloor, \quad K = \lfloor Q/2 \rfloor, \quad A = \{a : c_a \geq T\}.$$

If $T \geq n$, the high part is empty. Otherwise $m \geq T/7$, $m^2 > n$, and $Q \leq 7\sqrt{n}/64 < \sqrt{n}/8 < p/2$. Lemma 4.6 implies that every pair of types in A is ordinary-zero-sum-free in its m -by- m capacity box. Lemma 2.11 supplies unique primitive coordinates $(q_{ab}, v_{ab}) \in [1, Q]^2$; reverse pairs exchange coordinates. Their ordinary gcd D is 1 or 2 by (2.10). On the diagonal take $(1, 1)$.

If $D = 1$, both coordinates are odd units, and the denominator-group argument in Lemma 4.1 gives, for each fixed anchor b ,

$$(4.16) \quad \sum_{a:D=1} c_a v_{ab}/q_{ab} < 2nH_Q.$$

If $D = 2$, write $(q_{ab}, v_{ab}) = (2r_{ab}, 2s_{ab})$. The reduced coordinates are coprime and have opposite parity: if both were odd, $r_{ab}a - s_{ab}b$ would be even and divisible by the odd number M , contradicting

lattice primitivity. For fixed $r = r_{ab}$ and $e = v_2(s_{ab})$, the numerators s_{ab} are distinct. Indeed a reduced relation determines a modulo M , and a unit modulo M has a unique odd lift. Lemma 4.7 applies and gives

$$\sum_{a: r_{ab}=r, v_2(s_{ab})=e} c_a s_{ab} < n.$$

Choose $\alpha = 3/2$ and assign the positive rational pair weight

$$w_{ab} = \frac{v_{ab}}{q_{ab}} \alpha^{v_2(q_{ab}) - v_2(v_{ab})}.$$

It has $w_{ab}w_{ba} = 1$ and $w_{aa} = 1$; for $D = 1$ it is the unchanged slope. For $D = 2$ and odd r , the numerators have $e \geq 1$, so their total row cost is at most $nH_K \sum_{e \geq 1} \alpha^{-e} = 2nH_K$. For even $r = 2^f r_0$, the numerator is odd; summing over odd r_0 and $f \geq 1$ costs at most $nH_K \sum_{f \geq 1} (\alpha/2)^f = 3nH_K$. Thus every row has

$$\sum_{a \in A} c_a w_{ab} < 2nH_Q + 5nH_K \leq 7nH_Q.$$

Writing $W = \sum_{a \in A} c_a$, reciprocity gives

$$W^2 \leq \sum_{a, b \in A} c_a c_b w_{ab} < 7nH_Q W.$$

This pays all original high multiplicities with one harmonic sum. Proposition 2.7 pays the low part by $O(\varphi(n) \log(2n))$, since T is an absolute constant times $\sqrt{n}$. Hence $L_U(2p^2) \ll n \log(2n)$.

Finally the proper nonzero exact orders are $2, p, 2p, p^2$. The order-2 class has length at most one. The prime and prime-square classes have $O(d \log(2d))$ bounds from Section 4.2. For the order- $2p$ class, the elementary mixed estimate from that section gives $O(p^{3/2} \log(2p))$, already smaller than the required $O(p^2 \log(2p))$ ambient bound. Thus no sharper twice-prime estimate is needed. Lemma 2.1 includes every nonunit term with the same $O(n \log(2n))$ total cost. $\square$

4.4. Character estimates and the GRH bound. Let $M_{2,U}(d)$ be the maximum length of a unit sequence modulo d having no ordinary nonempty zero sum on at most two distinct types. At moduli where Lemma 2.10 holds, halving each multiplicity in an index-one-free sequence shows

$$(4.17) \quad L_U(d) \leq 2M_{2,U}(d) + \varphi(d).$$

A two-type atom in the halved sequence would have its square inside the original inventory, contradicting that lemma.

Lemma 4.8. *Suppose $2 \leq m \leq \lfloor (d-1)/2 \rfloor$, and let A_m be the set of types having multiplicity at least m in such a two-type-zero-sum-free sequence. Write $K = |A_m|$ and $\Phi = \varphi(d)$. For a nonnegative weight w supported on $1 \leq h \leq m$, set*

$$W = \sum_{(h,d)=1} w(h), \quad B_\chi = \sum_{h \leq m} w(h) \chi(h), \quad \lambda = \max_{\chi(-1)=-1} |B_\chi|^2.$$

Then $K \leq \Phi \lambda / (W^2 + \lambda)$ whenever $W > 0$.

Proof. There are no equations $ha + jb = 0$ with $a, b \in A_m$ and positive unit counts $h, j \leq m$. This includes $a = b$, because $h + j < d$. Character orthogonality on $U(d)$ gives

$$0 = K^2 W^2 + \sum_{\chi \neq \chi_0} \chi(-1) |B_\chi|^2 \left| \sum_{a \in A_m} \chi(a) \right|^2.$$

Discard the even nonprincipal terms, which are nonnegative, and use Parseval to bound the remaining sum of squared coefficients by $\Phi K - K^2$. Thus $K^2 W^2 \leq \lambda(\Phi K - K^2)$. $\square$

Proposition 4.9. *Uniformly for d having at most two distinct prime divisors,*

$$M_{2,U}(d) \ll_{\varepsilon} d^{4/3+\varepsilon}.$$

Under the Dirichlet generalized Riemann hypothesis,

$$M_{2,U}(d) \ll d + \varphi(d) \log^3(2d).$$

Proof. Every multiplicity is less than d . Any two distinct multiplicities have sum at most $d - 1$: otherwise the progressions $\{0, a, \dots, c_a a\}$ and $\{0, -b, \dots, -c_b b\}$ intersect at a nonzero residue, giving a forbidden zero sum. Thus at most one type has multiplicity exceeding $\lfloor (d-1)/2 \rfloor$, and its tail costs less than d . It suffices to sum the layer bounds of Lemma 4.8 up to this cutoff; finitely many small layers cost $O(d)$.

For the unconditional bound use $w(h) = (1 - h/m)^2$ for $h \leq m$. For every nonprincipal character the Mellin identity is

$$B_{\chi} = \frac{1}{2\pi i} \int_{(2)} L(s, \chi) m^s \frac{2}{s(s+1)(s+2)} ds.$$

Petrov and Young [12, Theorem 1.1] prove, for every primitive character of conductor f ,

$$(4.18) \quad L(1/2 + it, \chi) \ll_{\delta} (f(1 + |t|))^{1/6+\delta}.$$

An induced character adds at most two bounded Euler factors on $\Re s = 1/2$. Shifting the integral there, its cubic denominator gives

$$|B_{\chi}| \ll_{\delta} \sqrt{m} d^{1/6+\delta}, \quad \lambda \ll_{\delta} m d^{1/3+2\delta}.$$

Inclusion–exclusion over at most two primes gives $W = m\varphi(d)/(3d) + O(1)$, uniformly. Since $\varphi(d)/d \geq 1/3$, $W \gg m$ above an absolute constant. Thus $K \ll_{\delta} d^{4/3+2\delta}/m$. Summing the layers and absorbing the harmonic logarithm into d^{ε} proves the first assertion.

For the conditional assertion use the von Mangoldt weight

$$w(h) = \Lambda(h) \frac{h}{m} \left(1 - \frac{h}{m}\right) \quad (1 \leq h \leq m).$$

We give the uniform estimates, including the passage to induced characters. Only odd characters occur in the maximum in Lemma 4.8; their primitive inducing characters are nonprincipal and odd as well.

First let ψ be primitive and odd, of conductor f . Mellin inversion with kernel $1/((s+1)(s+2))$ gives

$$(4.19) \quad B_{\psi} = \frac{1}{2\pi i} \int_{(2)} -\frac{L'}{L}(s, \psi) \frac{m^s}{(s+1)(s+2)} ds.$$

Shift to $\Re s = -1/2$, taking horizontal edges at a sequence of heights avoiding zeros. The crossed poles are precisely the nontrivial zeros, counted with multiplicity: $L(s, \psi)$ has no pole, its first trivial zero is at -1 , and the kernel poles $-1, -2$ lie to the left of the new line. On that line the functional equation and the absolutely convergent logarithmic derivative at $3/2 - it$ imply

$$\left| \frac{L'}{L}(-1/2 + it, \psi) \right| \ll \log(f(2 + |t|)).$$

The kernel has quadratic decay there. The remaining integral is therefore $O(m^{-1/2} \log(2f))$, with an absolute constant, and

$$(4.20) \quad B_{\psi} = - \sum_{\rho} \frac{m^{\rho}}{(\rho+1)(\rho+2)} + O(m^{-1/2} \log(2f)).$$

This is the usual explicit-formula contour argument; see [8, Section 2] for the completed-function framework.

Here is an explicit uniform bound for the zero sum. Set

$$\mathcal{L}(s, \psi) = (f/\pi)^{(s+1)/2} \Gamma((s+1)/2) L(s, \psi).$$

Let b_ψ be the coefficient of s in the exponential factor of the Hadamard product for $\mathcal{L}(s, \psi)$. The functional equation gives, also for complex ψ ,

$$\Re b_\psi + \sum_{\rho} \Re \frac{1}{\rho} = 0;$$

see [8, (2.3)–(2.4)]. Taking real parts of the logarithmic derivative and using GRH therefore gives at $s = 2$

$$\begin{aligned} \sum_{\rho=1/2+i\gamma} \frac{3/2}{(3/2)^2 + \gamma^2} &= \Re \frac{\mathcal{L}'}{\mathcal{L}}(2, \psi) \\ &= \frac{1}{2} \log(f/\pi) + \frac{1}{2} \frac{\Gamma'}{\Gamma}(3/2) + \Re \frac{L'}{L}(2, \psi) \ll \log(2f). \end{aligned}$$

The last logarithmic derivative is absolutely bounded, since $|L'/L(2, \psi)| \leq \sum_{h \geq 2} \Lambda(h)/h^2 < \infty$. Moreover $|\rho + 1| |\rho + 2| \gg 1 + \gamma^2$. Consequently

$$(4.21) \quad \sum_{\rho} \frac{1}{|(\rho + 1)(\rho + 2)|} \ll \log(2f), \quad |B_\psi| \ll \sqrt{m} \log(2f).$$

Now let χ modulo d be induced by ψ . Their weighted sums differ only at powers of primes dividing d but not f . Because $0 \leq t(1-t) \leq 1/4$ on $[0, 1]$ and $\omega(d) \leq 2$,

$$(4.22) \quad |B_\chi - B_\psi| \leq \frac{1}{4} \sum_{\substack{\ell|d, \ell \text{ prime} \\ \ell \nmid f}} \log \ell \left\lfloor \frac{\log m}{\log \ell} \right\rfloor \leq \frac{1}{2} \log m.$$

Since $f \mid d$ and $m < d$, this proves

$$(4.23) \quad |B_\chi| \ll \sqrt{m} \log(2d), \quad \lambda \ll m \log^2(2d)$$

uniformly over all the odd characters in question.

Finally, the principal mass is uniformly large. The prime number theorem and partial summation give

$$\sum_{h \leq m} \Lambda(h) \frac{h}{m} \left(1 - \frac{h}{m}\right) = \frac{m}{6} + o(m).$$

Removing prime powers whose primes divide d costs at most $\omega(d) \log m/4 \leq \frac{1}{2} \log m$, by the same estimate as (4.22). Thus $W \geq m/12$ for all $m \geq m_0$, where m_0 is absolute and independent of d . Lemma 4.8 and (4.23) now yield

$$|A_m| \ll \frac{\varphi(d) \log^2(2d)}{m} \quad (m \geq m_0).$$

Summing these layers contributes $O(\varphi(d) \log^3(2d))$. The layers $m < m_0$ cost $O(d)$, as does the single-type tail already isolated above. This proves the conditional assertion with an absolute implied constant. $\square$

Proof of (1.8) and (1.9). Every divisor of $p^a q$ is either p^j or $p^j q$, and $q \geq p^j$. Thus Lemma 2.10 and (4.17) apply to each exact-order class. With $\alpha = 4/3 + \varepsilon$, $\sum_{d|p^a q} d^\alpha \ll_\varepsilon (p^a q)^\alpha$. For the conditional bound use $\sum_{d|p^a q} d \leq 3p^a q$ and $\sum_{d|p^a q} \varphi(d) = p^a q$. Lemma 2.1 and Proposition 4.9 complete both proofs. $\square$

5. LOWER BOUNDS

5.1. A construction on all large multiples of a fixed integer.

Proposition 5.1. *Let $d \geq 2$, $r \geq 1$ and $Q \geq 1$ be integers with $\text{rad}(Q) \mid d$. Let $m > rdQ$ and set $n = dm$, $H = m - rdQ$. Then*

$$(5.1) \quad S = \prod_{a|Q} \prod_{\substack{0 \leq i < d \\ (i,a)=1}} (im + a)^{\lfloor H/a \rfloor}$$

is index- r -free over C_n , and

$$(5.2) \quad |S| = \sum_{a|Q} \frac{d\varphi(a)}{a} \left\lfloor \frac{H}{a} \right\rfloor.$$

Here $(0, 1) = 1$, so all d lifts with $a = 1$ are included. There is no requirement that Q divide m or n .

Proof. All displayed types lie in $[1, n - 1]$ and are distinct: $a \leq Q < m$, so reduction modulo m determines a , then determines i . Fix any $u \in U(n)$ and write their actual heights as

$$w_{a,i} = [u(im + a)]_n = ua + m(iu - dk_{a,i}), \quad k_{a,i} \in \mathbb{Z}.$$

Every prime dividing a divides d but divides neither i nor u . Thus $(iu - dk_{a,i}, a) = 1$. The rational numbers

$$\frac{w_{a,i}/a - u}{m} = \frac{iu - dk_{a,i}}{a}$$

are reduced. Equality of two normalized heights $w_{a,i}/a$ first forces equality of their positive reduced denominators, and then $d \mid u(i - j)$, so the types are equal. Since $a \mid Q$, the numbers

$$y_{a,i} = Qw_{a,i}/a$$

are distinct positive integers, all congruent to Qu modulo m . At most one lies in $(0, m)$. For every other type,

$$(5.3) \quad w_{a,i} \geq am/Q.$$

Suppose actual counts $e_{a,i} \leq \lfloor H/a \rfloor$ give an integer sum jn , $1 \leq j \leq r$. Reduction modulo m , and $(u, m) = 1$, show that $B = \sum e_{a,i}a$ is a positive multiple of m . If no copy of the possible exceptional type with $y < m$ is selected, (5.3) gives $B \leq jdQ < m$, a contradiction. Otherwise its strictly positive height makes the contribution of all other types satisfy $B_{\text{high}} < jdQ \leq rdQ$. The one exceptional type contributes at most $a \lfloor H/a \rfloor \leq H = m - rdQ$. Hence again $B < m$, a contradiction. This rules out every sum $n, 2n, \dots, rn$ in every unit direction, and is equivalent to index- r -freeness.

The number of allowed i for a fixed a is $d\varphi(a)/a$: coprimality depends only on $\text{rad}(a)$, which divides d . This proves (5.2). $\square$

Proof of Theorem 1.3. Define

$$F(Q) = \sum_{a|Q} \frac{\varphi(a)}{a^2}, \quad G(Q) = \sum_{a|Q} \frac{\varphi(a)}{a}.$$

Proposition 5.1 and $\lfloor x \rfloor \geq x - 1$ give

$$(5.4) \quad |S| \geq (n - rd^2Q)F(Q) - dG(Q), \quad G(Q) \leq Q.$$

If $Q = \prod_{p|d} p^{k_p}$, multiplicativity yields

$$F(Q) = \prod_{p|d} \left(1 + \frac{1}{p} - \frac{1}{p^{k_p+1}} \right).$$

Set $X = n^{1/(s+1)}$, $k_p = \lfloor \log_p X \rfloor$. Then $Q \leq X^s$, and $n > (rd^2)^{s+1}$ ensures $n > rd^2Q$, as required. Since $p^{k_p+1} > X$,

$$0 \leq P(d) - F(Q) \leq P(d) \sum_{p|d} p^{-k_p-1} \leq sP(d)/X.$$

Substitution in (5.4) gives (1.12) and hence (1.11).

Finally the numbers $P(d)$ are unbounded. For d the product of the primes at most z ,

$$P(d) = \prod_{p \leq z} (1 - p^{-2}) \prod_{p \leq z} (1 - p^{-1})^{-1} \geq \frac{1}{2} \sum_{j \leq [z]} \frac{1}{j} \rightarrow \infty.$$

Here the first product is at least $\prod_{j=2}^{\infty} (1 - j^{-2}) = 1/2$, and the finite Euler product contains all reciprocals $1/j$ with $j \leq z$. Given M , choose d with $P(d) > M$, independently of r , and then let its multiples tend to infinity. Since $I_r(n) > |S|$, the final assertion follows. $\square$

Example 5.2. Take $d = 6$, $Q = 6$, $r = 1$, and $m = 2000$. Formula (5.1) gives the following index-one-free sequence over C_{12000} :

$$\prod_{i=0}^5 (2000i + 1)^{1964} \prod_{i \in \{1,3,5\}} (2000i + 2)^{982} \cdot \prod_{i \in \{1,2,4,5\}} (2000i + 3)^{654} \prod_{i \in \{1,5\}} (2000i + 6)^{327}.$$

Its length is $6 \cdot 1964 + 3 \cdot 982 + 4 \cdot 654 + 2 \cdot 327 = 18000$. Thus $I_1(12000) \geq 18001$, contradicting the proposed bound $n + n/P^-(n) = 18000$ at this order. This example is a direct instance of the proof, with no exhaustive computation needed.

5.2. Long free sequences consisting only of generators. For a real $K \geq 2$ let $\mathcal{P}(K) = \prod_{\ell \leq K, \ell \text{ prime}} \ell$. The first observation uses a gap in the small positive units and a multiplicative subgroup of the unit group.

Lemma 5.3. *Let $n = AK$ with integers $A, K \geq 2$. Let T be a nontrivial multiplicative subgroup of $U(n)$ such that*

- (1) *every $a \in T$ is congruent to 1 modulo A ;*
- (2) *$U(n) \cap [1, K] = \{1\}$ in positive representatives;*
- (3) *every nonidentity representative of T is greater than $n/2$.*

Put $\delta = \min_{a \in T \setminus \{1\}} (n - [a]_n)$. For every $1 \leq c < \delta$, $\prod_{a \in T} a^c$ is index-one-free. At $c = \delta$ it has an index-one subsequence.

Proof. An index-one certificate in direction u has a number of terms divisible by A , since every term is congruent to u modulo A . It therefore uses at least A copies. If uT does not contain the representative 1, every height is a unit greater than K , giving weight at least $A(K+1) > n$. If $1 \in uT$, then $u \in T$ and multiplication by u permutes the uniform sequence. A sum n now uses either only 1's, requiring n copies, or one nonidentity height $a > n/2$, requiring $n - a \geq \delta$ copies of 1. Neither is available when $c < \delta$. At $c = \delta$, an element attaining the minimum together with δ copies of 1 gives weight n . $\square$

To construct many subgroup elements at heights greater than $n/2$, we first represent the sixth roots of unity by small positive costs.

Lemma 5.4. *For every prime $p \equiv 1 \pmod{3}$, $p > 64$, there are positive integers x, y such that*

$$p = x^2 - xy + y^2, \quad x/2 < y < 2x.$$

Set $\lambda = (x + y)^{-1} \pmod{p}$ and

$$E_p = \{0, 3x, 3y, 2(x + y), 2y - x, 2x - y\}.$$

These six distinct integers lie in $[0, p)$, and $\{1 - \lambda e : e \in E_p\}$ is exactly the sixth-root subgroup of $\mathbb{F}_p^\times$. Its only zero cost is $e = 0$, and $\max E_p = 2(x + y) \leq 4\sqrt{p}$.

Proof. Let $\omega = e^{2\pi i/3}$. The norm on $\mathbb{Z}[\omega]$ is $N(a + b\omega) = a^2 - ab + b^2$. Rounding both real coordinates in the basis $1, \omega$ gives error norm at most $3/4$, proving the Euclidean algorithm and principality of ideals. A nontrivial cubic root in $\mathbb{F}_p$ defines a surjection $\mathbb{Z}[\omega] \rightarrow \mathbb{F}_p$. Its kernel has index p , so a generator has norm p . Multiply it by a complex unit to put its argument in $[\pi/6, \pi/2]$. Its coordinates are then $x, y > 0$ with $x/2 \leq y \leq 2x$. Equality would give a norm three times a square, impossible for $p > 3$.

Modulo p , $(x + y)^2 = 3xy$. Thus $r_1 = 1 - 3\lambda x$ and $r_2 = 1 - 3\lambda y$ have sum -1 and product 1 , and are the two nontrivial cubic roots. They are distinct, since $x = y$ would give $p = x^2$. The six roots $1, r_1, r_2, -1, -r_1, -r_2$ have the listed costs. Their positive costs follow from $x/2 < y < 2x$. Finally $p = (x + y)^2 - 3xy \geq (x + y)^2/4$, so the maximum cost is at most $4\sqrt{p} < p$. Distinct roots then imply distinct integer costs. $\square$

Proposition 5.5. *Choose distinct primes $p_i \equiv 1 \pmod{3}$, $p_i > 64$, with cost sets E_i and coefficients λ_i as above, such that*

$$(5.5) \quad \sum_{i=1}^s \frac{\max E_i}{p_i} < \frac{1}{2}.$$

Put $K = \prod_i p_i$, $d_i = K/p_i$, $A_0 = \mathcal{P}(K)/K$. Choose a positive integer c satisfying

$$(5.6) \quad A_0 c d_i \equiv \lambda_i \pmod{p_i} \quad (1 \leq i \leq s),$$

and $A = A_0 c \geq 2K$. Set $n = AK$. For $e = (e_i) \in \prod_i E_i$, put $B(e) = \sum_i d_i e_i$ and define

$$a_0 = 1, \quad a_e = n - AB(e) + 1 \quad (e \neq 0).$$

These 6^s types form a multiplicative subgroup of $U(n)$. Writing $e_i^+ = \min(E_i \setminus \{0\})$, the sequence with each type repeated

$$(5.7) \quad c_* = n \min_i (e_i^+ / p_i) - 2$$

times is index-one-free, and has length at least $6^s(n / \max_i p_i - 2)$.

Proof. Since $(A_0, K) = 1$, the Chinese remainder theorem gives (5.6); all its residues for c are units, so $(A, K) = 1$. Adding a multiple of K to c ensures $A \geq 2K$. By (5.5), $0 < B(e) < K/2$ for $e \neq 0$. Thus $a_e \in (n/2, n)$, and every a_e is 1 modulo A . Modulo p_i , it is $1 - \lambda_i e_i$. Hence the types are distinct, are units, and form under CRT the subgroup $\{1\} \times \prod_i \mu_6(\mathbb{F}_{p_i})$ in $U(A) \times \prod_i \mathbb{F}_{p_i}^\times$. Every prime at most K divides n , so the small-unit condition of Lemma 5.3 holds. Its minimum complementary height is

$$\delta = A \min_i (d_i e_i^+) - 1 = n \min_i (e_i^+ / p_i) - 1.$$

Use that lemma with $c_* = \delta - 1$. This is a positive integer, and $e_i^+ \geq 1$ gives the claimed length estimate. $\square$

Proof of Theorem 1.4. For sufficiently large s , choose s distinct primes in $[256s^2, 512s^2]$ satisfying $p_i \equiv 1 \pmod{3}$. The prime number theorem in this fixed progression supplies more than s choices; for explicit estimates sufficient here see [1]. Lemma 5.4 gives

$$\sum_i \frac{\max E_i}{p_i} \leq \sum_i \frac{4}{\sqrt{p_i}} \leq \frac{1}{4},$$

so Proposition 5.5 applies. Take the least positive CRT solution $1 \leq c < K$. For large s , $A_0 c \geq 2K$ automatically, by the prime number theorem.

Let $n_s = \mathcal{P}(K)c$. Then

$$\log K = (2 + o(1))s \log s, \quad \log n_s = \vartheta(K) + \log c = (1 + o(1))K.$$

The exact capacity (5.7) is at least $n_s/(512s^2) - 2$ and less than n_s , so $\log(|S_s|/n_s) = s \log 6 + O(\log s)$. Also

$$\frac{\log \log n_s}{\log \log \log n_s} = (2 + o(1))s.$$

This proves (1.13). $\square$

6. SUPPORT AND MULTIPLICITY BOUNDS

We first state precisely the external integer subset-sum input. For a nonempty positive-integer multiset X , write $m = |X|$, $M = \max X$, $\mu = \max_t v_t(X)$ and $W = \sum X$. It is δ -dense if $m^2 \geq \delta \mu M$. An integer $d > 1$ is an α -almost divisor if at most $\alpha \mu W/m^2$ actual entries are not divisible by d .

Lemma 6.1 (Bringmann–Wellnitz [2], Theorems 4.1–4.2). *If $\delta \geq 1$, $\delta \geq 16\alpha$ and X is δ -dense, some $d \geq 1$ makes $Y = \{x/d : x \in X, d \mid x\}$ δ -dense, without an α -almost divisor, and with $|Y| \geq 3m/4$. Furthermore, put*

$$D(m, \mu) = 1699200 \log_2(2m) \log_2^2(2\mu), \quad A(\mu) = 42480 \log_2(2\mu), \quad B(\mu) = 169920 \log_2(2\mu).$$

If X is $D(m, \mu)$ -dense and has no $A(\mu)$ -almost divisor, then its integer subsequence sums contain every integer in

$$[\lambda, W - \lambda], \quad \lambda = B(\mu) \mu M W / m^2.$$

Using base-two logarithms only enlarges the numerical sufficient thresholds from the source. We use no algorithmic running-time assertion.

Lemma 6.2. *Let a generator sequence over C_q have maximum multiplicity at most h . Suppose one unit direction has m actual copies with heights at most $M < q$. Set $L = \log_2(2h)$, $D = 1699200 \log_2(2m) L^2$ and $B = 169920 L$. An index-one subsequence exists if*

$$(6.1) \quad m \geq 4\sqrt{hq}, \quad m^2 \geq DhM, \quad \frac{4}{3}BhM^2/m \leq q.$$

Proof. Select exactly m such copies and apply the first part of Lemma 6.1 to their heights X , with $\delta = D$ and $\alpha = 42480L$. The numerical condition $D \geq 16\alpha$ holds. For the resulting divided multiset Y , put $t = |Y| \geq 3m/4$ and $V = \sum Y$. Sorting positive integers of multiplicity at most h gives

$$(6.2) \quad V \geq t^2/(2h) \geq 9m^2/(32h) \geq (9/2)q.$$

In particular the division has not reduced the total below the target. The second part of Lemma 6.1 applies to Y , since its parameters and logarithmic thresholds are no larger. Also

$$\lambda_Y \leq BhM^2/(d^2t) \leq \frac{4}{3}BhM^2/m \leq q.$$

Thus $q \in [\lambda_Y, V - \lambda_Y]$ is an actual integer sum in Y . Every retained height was a unit modulo q , so $(d, q) = 1$. If u was the original direction, ud^{-1} is a legal unit and has actual representatives x/d for precisely those retained copies. Their selected integer sum q is the required certificate. $\square$

Proposition 6.3. *Every index-one-free set of generators of C_q has cardinality $O(q^{3/4})$, with an absolute implied constant.*

Proof. Let K be its cardinality. For all sufficiently large q we have $4^{\omega(q)} \leq q$. Put $m = \lceil 4\sqrt{q} \rceil \leq 5\sqrt{q}$ and suppose $K > Cq^{3/4}$, with C a sufficiently large absolute constant. Then $K > 4m$. Set $M = \lceil 2qm/K \rceil$, so $m \leq M < q$ and $M \leq 4qm/K$. Inclusion–exclusion and $K \leq \varphi(q)$ give

$$R_q(M) := |U(q) \cap [1, M]| \geq M\varphi(q)/q - 2^{\omega(q)}, \quad \frac{KR_q(M)}{\varphi(q)} \geq 2m - 2^{\omega(q)} \geq m.$$

Thus some unit direction has at least m distinct heights at most M . With $B_0 = 169920$, we have

$$\frac{m^2}{M} \geq \frac{K}{\sqrt{q}}, \quad \frac{4}{3}B_0M^2/m \leq \frac{320}{3}B_0q^{5/2}/K^2.$$

For sufficiently large C and then sufficiently large q , these inequalities imply all the conditions of Lemma 6.2 with $h = 1$. This contradicts freedom. The finitely many remaining orders are absorbed into the constant using $K \leq q$. $\square$

We also use a set version of the integer subset-sum theorem.

Lemma 6.4 (Conlon–Fox–Pham [3, Theorem 6.1]). *There are absolute constants $C_0, C_1, C_2 > 0$ such that the following holds. If $X \subseteq [1, M] \cap \mathbb{Z}$ has $m \geq C_0\sqrt{M}$ elements, some integer $g \geq 1$ makes*

$$Y = \{x/g : x \in X, g \mid x\}, \quad |Y| \geq m - C_1(\log^3(2M) + M/m).$$

The integer subset sums of Y contain at least M consecutive integers, with first point at most $C_2M^2/(gm)$.

The cited theorem represents every point of the interval using at most C_2M/m distinct elements of Y . Since each is at most M/g , this also gives the asserted bound on its first point. Reserving one copy of every element of Y therefore suffices for all these representations.

Proposition 6.5. *Let $S = \prod_a a^{c_a}$ be an index-one-free generator sequence over C_q , and let $K_H = |\{a : c_a \geq H\}|$ for each integer $H \geq 1$. Then*

$$(6.3) \quad K_H \ll q^{3/4}H^{-1/4}.$$

Consequently, if h is its maximum multiplicity, then

$$(6.4) \quad |S| \ll (qh)^{3/4}.$$

Both implied constants are absolute.

Proof. There is nothing to prove for $H \geq q$, since q copies of a generator have index one. The case $H = 1$ follows from Proposition 6.3, applied to one copy of each type. That same proposition, together with $2^{\omega(q)} = q^{o(1)}$ and $q/\varphi(q) = q^{o(1)}$, gives, uniformly for every H ,

$$(6.5) \quad \frac{K_H 2^{\omega(q)}}{\varphi(q)} \ll q^{-1/4+o(1)} \leq 1$$

for all sufficiently large q . This uses only the already proved set bound.

Fix $A = 16$ and a sufficiently large absolute B , depending on the constants of Lemma 6.4. Suppose $2 \leq H < q$ and

$$K := K_H > BK_0, \quad K_0 = q^{3/4}H^{-1/4}.$$

Set $t = \sqrt{q/H}$, $m = \lceil At \rceil$ and $M = \lceil 2qm/K \rceil$. Since $t \geq 1$ and $K_0/t = (qH)^{1/4}$, sufficiently large q gives $At \leq m \leq 2At$ and $K > 4m$. Hence $m \leq M < q$ and $M \leq 4qm/K$. Averaging the K distinct types over unit directions and using (6.5) gives

$$\frac{KR_q(M)}{\varphi(q)} \geq KM/q - 1 \geq 2m - 1 \geq m.$$

Choose exactly m types in such a direction u , with heights $X \subseteq [1, M]$, and retain H actual copies of each. The parameters satisfy

$$(6.6) \quad \frac{M^2}{m} \leq \frac{32Aq}{B^2}, \quad \frac{m^2}{M} \geq \frac{mK}{4q}.$$

Whenever we retain heights divisible by an integer g , that integer is coprime to q . In direction ug^{-1} , the retained heights are exactly x/g , still positive and less than q .

Low multiplicity: $2 \leq H \leq q^{1/3}$. Here $m \geq Aq^{1/3}$ and

$$\frac{m^2}{M} \geq \frac{AB}{4} q^{1/4} H^{-3/4} \geq \frac{AB}{4}.$$

Choose B so that $m \geq C_0 \sqrt{M}$ and $C_1 M/m \leq m/4$. For sufficiently large q , also $C_1 \log^3(2M) \leq m/4$. Lemma 6.4 therefore retains $s \geq m/2$ divided types Y , each with H actual copies. Reserve one copy of every retained type. Their subset sums contain at least M consecutive integers with first point at most

$$C_2 M^2 / (gm) \leq 32AC_2 q / B^2 \leq q.$$

Each remaining copy has value at most $M/g \leq M$, so adjoining these copies extends the interval without an integer gap. Their total weight is at least

$$(H-1) \frac{s(s+1)}{2} \geq \frac{(H-1)m^2}{8} \geq \frac{A^2 q}{16} \geq q.$$

Thus the extended interval contains q , giving an index-one subsequence in the single direction ug^{-1} .

High multiplicity: $q^{1/3} \leq H < q$. Put $g = \gcd(X)$, $Y = X/g$ and $v = \max Y \leq M$. Apply Lemma 2.5 to these m distinct denominations. Since $HK > Bq$, its reserved multiplicity satisfies

$$\rho \leq 4v/m \leq 16q/K \leq 16H/B \leq H/2.$$

Its interval starts at

$$L \leq 2v^2/m + v \leq 3M^2/m \leq 96Aq/B^2 \leq q.$$

The unreserved copies have total weight at least

$$(H-\rho) \sum_{y \in Y} y \geq \frac{H}{2} \frac{m(m+1)}{2} \geq \frac{A^2 q}{4} \geq q.$$

The resulting integer interval again contains q in direction ug^{-1} . Both cases contradict freedom.

All choices of constants precede the lower bound on q . The finitely many omitted orders are absorbed uniformly in H , since $H < q$ and $K_H \leq q$. This proves (6.3). Finally,

$$|S| = \sum_{H=1}^h K_H \ll q^{3/4} \sum_{H=1}^h H^{-1/4} \ll (qh)^{3/4},$$

proving (6.4). □

Proposition 6.6. *Let S be a nonempty index-one-free sequence over C_n . For each $d \mid n$, $d > 1$, let h_d be the largest multiplicity of an element of exact order d , taking $h_d = 0$ if that class is empty. Then*

$$(6.7) \quad |S| \ll \sum_{\substack{d \mid n \\ d > 1}} (dh_d)^{3/4}.$$

In particular, if h is the maximum multiplicity, then

$$(6.8) \quad |S| \ll (nh)^{3/4} \quad \text{when } n \text{ is a prime power.}$$

All implied constants are absolute. For each fixed $\varepsilon > 0$, all copies of types whose original multiplicity is at most $n^{1/3-\varepsilon}$ contribute only $o(n)$ terms.

Proof. By Lemma 2.1, the exact-order- d class is an index-one-free generator sequence over C_d . Applying (6.4) to each nonempty class gives (6.7). Since $h_d \leq h$,

$$|S| \ll h^{3/4} \sum_{d|n} d^{3/4} = (nh)^{3/4} \sigma_{-3/4}(n).$$

If $\omega(n) \leq k$, then

$$\sigma_{-3/4}(n) \leq \prod_{p|n} (1 - p^{-3/4})^{-1} \leq (1 - 2^{-3/4})^{-k}.$$

This proves (6.8) and the length and inverse-multiplicity assertions of Theorem 1.5. Retaining one copy of every type and using $\sigma_{-3/4}(n) \leq \tau(n) = n^{o(1)}$ proves its support assertions, where $\tau(n)$ counts the positive divisors of n . Finally, apply the same estimate to the actual subsequence consisting of all copies of types with original multiplicity at most $n^{1/3-\varepsilon}$. Its length is at most $n^{1-3\varepsilon/4+o(1)} = o(n)$. $\square$

APPENDIX A. AN INTEGER DESCENT AND THE GENERAL BOUND

We prove the uniform index- r bound (1.5). The descent retains one denomination of maximum multiplicity; this ensures that the final divisor is a unit in the group application.

Lemma A.1. *Let $X = \prod_{a \in B} a^{c_a}$ be an integer multiset with distinct denominations $B \subset (H/2, H] \cap \mathbb{Z}$, length N , and maximum multiplicity M . If $N \geq 2048H$, there are a submultiset X' and an integer D dividing all its entries and one original denomination of multiplicity M , such that $|X'| \geq 15N/16$ and $\Sigma_{0,\mathbb{Z}}(X'/D)$ contains an integer interval $[L, V]$ satisfying*

$$(A.1) \quad L \leq 65MH^2/N + 1, \quad V - L > N^2/(32M).$$

Proof. Fix q_0 of multiplicity M and $\ell = \lceil 64MH/N \rceil$. Since $N \leq MH$ and $N \geq 2048H$,

$$M \geq 2048, \quad 64MH/N \leq \ell \leq 65MH/N, \quad \ell \leq M/16, \quad 2\ell + 3 \leq M/4.$$

At a descent step, let the already divided common factor be D_i , $H_i = H/D_i$, and $q_i = q_0/D_i$. All current denominations lie in $(H_i/2, H_i]$, and all M anchor copies are retained. For $a \neq q_i$ put $d_a = \min(\lfloor c_a/4 \rfloor, \ell)$ and

$$A_j = \{0\} \cup \{a \bmod q_i : d_a \geq j\}, \quad 1 \leq j \leq \ell.$$

The nonzero residues within each layer are distinct. If their sumset is proper in C_{q_i} , let its stabilizer be $J = d_i\mathbb{Z}/q_i\mathbb{Z}$ with $d_i \mid q_i$ and $d_i \geq 2$. Iterated Kneser gives

$$\sum_{a: d_i \nmid a} d_a = \sum_j |A_j \setminus J| \leq \sum_j (|A_j + J| - |J|) < q_i.$$

For each type $d_a \geq (\ell/M)c_a - 1$. There are at most H_i denominations, so fewer than $(M/\ell)(q_i + H_i) \leq 2MH_i/\ell$ copies have denomination not divisible by d_i . Delete these and divide all retained entries by d_i . The anchor is retained. Each H_i decreases at least by half, so the total loss over the whole descent is at most

$$\sum_i 2MH_i/\ell \leq 4MH/\ell \leq N/16.$$

The descent terminates, since q_i is a decreasing positive integer and the residue cover holds when $q_i = 1$.

At termination reserve the d_a copies of each nonanchor type and $2\ell + 3$ anchor copies. This reserves at most $|X'|/4 + M/4 \leq |X'|/2$ copies. The layer cover gives each residue an integer representation of weight at most ℓH_i . As in the prime window argument, the anchor extends these

to $[\ell H_i], [\ell H_i] + 2q_i] \cap \mathbb{Z}$. The width exceeds H_i , so every remaining copy extends this interval. At least $R \geq |X'|/2 \geq 15N/32 > N/4$ copies remain. Distinct positive integer denominations with at most M copies each have total weight at least $R^2/(2M)$. Adding these copies increases the interval width by their full integer weight. Thus $V - L > N^2/(32M)$, while the left is at most $\ell H_i + 1 \leq 65MH^2/N + 1$. All divided factors divide the original anchor, as required. $\square$

Proof of (1.5). First let S be an index- r -free unit sequence over C_d , where $1 \leq r \leq d/2$, and write $W = |S|$. Set

$$H = \lfloor \sqrt{rd} \rfloor, \quad E(d) = 2^{\omega(d)} d / \varphi(d).$$

Inclusion-exclusion gives

$$|\mathcal{U}(d) \cap (H/2, H]| \geq H\varphi(d)/(2d) - 2^{\omega(d)+1}.$$

There is an absolute bound $E(d) \ll d^{1/4}$: for primes $p \geq 23$, $2p/(p-1) \leq p^{1/4}$, and the finitely many smaller primes contribute an absolute constant. Thus for all sufficiently large d , uniformly in r , one has $H \geq 8E(d)$. The window contains at least $H\varphi(d)/(4d)$ units. If N_u actual copies lie in the window in direction u , averaging gives

$$\frac{1}{\varphi(d)} \sum_{u \in \mathcal{U}(d)} N_u \geq WH/(4d).$$

Suppose some $N_u \geq 2048d$. Since $H < d$, Lemma A.1 applies, with maximum multiplicity $M < d$. Its divisor D divides an actual unit denomination, so $(D, d) = 1$. In the single legal direction uD^{-1} the divided integers are exactly the positive representatives of the retained original copies. The covered integer interval satisfies

$$L \leq 65rd/2048 + 1 < rd, \quad V - L > \frac{(2048d)^2}{32d} > d.$$

Consequently it contains a positive multiple jd with $1 \leq j \leq r$. The corresponding actual submultiset is a zero sum of index at most j , contrary to freedom. Therefore every $N_u < 2048d$, and

$$(A.2) \quad L_{U,r}(d) \ll d^2/H \ll d^{3/2}/\sqrt{r} \quad (1 \leq r \leq d/2).$$

The finitely many smaller d are absorbed into the absolute constant: their unit sequences have length at most $(d-1)\varphi(d)$, and there are only finitely many admissible pairs (d, r) .

Now take an arbitrary index- r -free sequence over C_n . By Lemma 2.2, all copies of types with $c_a \leq 2r+1$ have total length at most $n-1$. Every remaining type has additive order $d > 2r+1$, since a type of order d has multiplicity less than d . Partition these remaining copies by exact order. Lemma 2.1 identifies each class with an index- r -free unit sequence over C_d , and (A.2) applies because $r < d/2$. Hence

$$|S| \leq n-1 + \frac{C}{\sqrt{r}} \sum_{\substack{d|n \\ d > 2r+1}} d^{3/2} \leq n-1 + \frac{3Cn^{3/2}}{\sqrt{r}}.$$

Here $\sum_{d|n} (d/n)^{3/2} \leq \sum_{k \geq 1} k^{-3/2} \leq 3$. This proves the upper bound in (1.5); the lower bound is g^{n-1} . At $r = 1$ it supplies the $O(n^{3/2})$ term of (1.6), completing Theorem 1.2. $\square$

REFERENCES

- [1] M. A. Bennett, G. Martin, K. O'Bryant and A. Rechnitzer, *Explicit bounds for primes in arithmetic progressions*, Illinois J. Math. **62** (2018), 427–532. arXiv:1802.00085.
- [2] K. Bringmann and P. Wellnitz, *On near-linear-time algorithms for dense subset sum*, in Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA), 2021, 1777–1796. doi:10.1137/1.9781611976465.107. Full version: arXiv:2010.09096 (2020), Theorems 4.1–4.2.

- [3] D. Conlon, J. Fox and H. T. Pham, *Subset sums, completeness and colorings*, J. Eur. Math. Soc., to appear. arXiv:2104.14766 (2021), Theorem 6.1.
- [4] M. DeVos, *A short proof of Kneser's addition theorem for abelian groups*, preprint (2013). arXiv:1303.3539.
- [5] P. Dusart, *Estimates of some functions over primes without $R.H.$* , preprint (2010). arXiv:1002.0442.
- [6] W. Gao, Y. Li, J. Peng, C. Plyley and G. Wang, *On the index of sequences over cyclic groups*, Acta Arith. **148** (2011), 119–134. doi:10.4064/aa148-2-2.
- [7] H. Iwaniec, *On the problem of Jacobsthal*, Demonstratio Math. **11** (1978), 225–232. doi:10.1515/dema-1978-0121.
- [8] Y. Lamzouri, X. Li and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp. **84** (2015), 2391–2412. arXiv:1309.3595.
- [9] P. Lemke and D. Kleitman, *An addition theorem on the integers modulo n* , J. Number Theory **31** (1989), 335–345.
- [10] C. Liu, *On the index- r -free sequences over finite cyclic groups*, Int. J. Number Theory **14** (2018), 1627–1636. doi:10.1142/S1793042118500987.
- [11] J. Peng, S. Yuan and Y. Li, *On subsequence sums of index-1-free sequences over cyclic groups*, Discrete Math. **349** (2026), no. 4, Paper No. 114918. doi:10.1016/j.disc.2025.114918.
- [12] I. Petrow and M. P. Young, *The fourth moment of Dirichlet L -functions along a coset and the Weyl bound*, Duke Math. J. **172** (2023), 1879–1960. arXiv:1908.10346.
- [13] X. Zeng, Y. Li and P. Yuan, *On a conjecture of Lemke and Kleitman*, Acta Arith. **168** (2015), 289–300. doi:10.4064/aa168-3-5.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MISSISSIPPI, USA

Email address: chaoliuac@gmail.com