

DAVENPORT CONSTANTS WITH GROWING BINARY RANK

CHAO LIU

ABSTRACT. We study the correction to the standard lower bound D^* for Davenport constants of finite abelian groups with a growing elementary two-component. For every fixed nontrivial abelian p -group H of odd order, we prove $D(H \oplus C_2^r) = D^*(H \oplus C_2^r) + (D(H) - 1) \log_2 r + O_H(1)$, with a uniform version for varying H . For $C_3 \oplus C_2^r$, we determine exact values on explicit infinite intervals of ranks. More generally, the correction is logarithmic or smaller precisely when the fixed group has at most one odd prime divisor. We show that the two-primary part affects the logarithmic coefficient: for $C_{24} \oplus C_2^r$, the ratio $(D - D^*)/\log_2 r$ has limsup at least $2.4933231 \dots > 2$, whereas for $C_3 \oplus C_2^r$ the limit is 2. These upper limiting coefficients are unbounded even with the odd prime fixed. The proofs use binary codes and finite-field Fourier analysis.

1. INTRODUCTION

For a finite abelian group G , the Davenport constant $D(G)$ is the least positive integer N such that every sequence of N elements of G contains a nonempty zero-sum subsequence. Repeated elements are allowed. If

$$G \cong C_{n_1} \oplus \cdots \oplus C_{n_s}, \quad 1 < n_1 \mid \cdots \mid n_s,$$

the standard construction gives

$$D^*(G) := 1 + \sum_{i=1}^s (n_i - 1) \leq D(G).$$

Equality holds for finite abelian p -groups by Olson's theorem [10]. We study $H \oplus C_2^r$, with particular attention to exact values, sharp logarithmic corrections, and the effect of the fixed group H on those corrections.

1.1. Sharp logarithmic corrections and exact values. We first determine the logarithmic correction for every fixed odd-primary label group.

Theorem 1.1 (Fixed odd p -groups). *Let p be an odd prime and H a fixed nontrivial finite abelian p -group. Then*

$$D(H \oplus C_2^r) = D^*(H \oplus C_2^r) + (D(H) - 1) \log_2 r + O_H(1). \quad (1)$$

Theorem 3.4 makes the estimate uniform in H . If $b = D(H) - 1$ and $r \geq 16b$, its remainder relative to $D^*(H \oplus C_2^r) + b \log_2(r/b)$ lies in $[-3b, 0)$. This also handles varying groups with $b = o(r)$.

For $C_3 \oplus C_2^r$, retaining signed Fourier information yields exact values on explicit infinite intervals of ranks. For $r \geq 1$, the standard lower bound for this group is $r + 5$.

Date: Working draft, revised October 28, 2026.

2020 Mathematics Subject Classification. 11B75, 20K01, 94B05, 68Q25.

Key words and phrases. Davenport constant, zero-sum sequence, binary linear code, Fourier sparsity, modular constraint, group program.

Theorem 1.2 (Infinite exact intervals). *For each integer $m \geq 2$, put*

$$a_m = 2^{m+1} - 2m - 2, \quad z_m = \left\lfloor \frac{2^{m+2}}{\sqrt{3}} \right\rfloor - 2m - 2.$$

For every integer $a_m \leq r \leq z_m$,

$$\mathsf{D}(C_3 \oplus C_2^r) = \mathsf{D}^*(C_3 \oplus C_2^r) + 2m - 4 = r + 2m + 1. \quad (2)$$

In particular, for every $m \geq 1$,

$$\mathsf{D}(C_3 \oplus C_2^{2^{m+1}-2m-2}) = 2^{m+1} - 1. \quad (3)$$

The case $m = 1$ in the last identity is simply $\mathsf{D}(C_3) = \mathsf{D}^(C_3) = 3$.*

The interval lengths are asymptotic to $(4/\sqrt{3} - 2)2^m$ and hence are proportional to their starting ranks. Section 5 gives integer refinements of both endpoints. The signed Fourier identities used for the upper bound retain information beyond a sphere-volume estimate.

Theorem 4.2 gives a complementary exact identity, expressing $\mathsf{D}(H \oplus C_2^r)$ through the minimum Fourier support of an H -valued function with a unique zero, for every odd-order abelian H . Appendix B localizes the remaining C_3 extremal parameters to two adjacent dimensions for all sufficiently large ranks; those two thresholds remain unevaluated.

1.2. Mixed-characteristic fibers. A zero-sum-free sequence gives a binary selection code: its binary projection must vanish, and the remaining H -valued sum has a unique zero on that kernel. When H has a two-primary part, the two-primary and odd-primary conditions have different natural representations. The former has bounded algebraic degree over $\mathbb{F}_2$; the latter has bounded Fourier sparsity in odd characteristic. The following theorem controls their intersection directly.

Theorem 1.3 (Mixed-characteristic intersection). *Let $\mathbb{K}$ be any field of characteristic different from two. Suppose $a : \mathbb{F}_2^d \rightarrow \mathbb{F}_2$ has algebraic degree at most $D \in \mathbb{Z}_{\geq 0}$, and $b : \mathbb{F}_2^d \rightarrow \mathbb{K}$ has Fourier sparsity at most S , where $S \geq 1$. If*

$$Z = \{x \in \mathbb{F}_2^d : a(x) = 1, b(x) \neq 0\}$$

is nonempty, then

$$|Z| \geq 2^{d-D} S^{-2^D}. \quad (4)$$

If Z is a singleton, then

$$d \leq D + 2^D \log_2 S. \quad (5)$$

Both conclusions remain valid on every binary affine restriction.

The proof extracts a fixed-dimensional linear space inside the nonzero-set of b , on which a low-degree binary polynomial cannot be a point mass. The bound is uniform in the field, including characteristic zero. It yields explicit estimates for every attainable fiber of a bounded-arity ordered product into $Q \times P$, where Q is a two-group and P is an odd p -group. Neither group need be abelian.

For any finite group K , write

$$t(K) = |\{p : p \text{ is an odd prime and } p \mid |K|\}|.$$

Theorem 1.4 (Logarithmic threshold). *Let H be a fixed finite abelian group. Then*

$$\mathsf{D}(H \oplus C_2^r) = \mathsf{D}^*(H \oplus C_2^r) + O_H(\log(r+2)) \iff t(H) \leq 1. \quad (6)$$

More precisely:

- (1) *If $t(H) = 0$, then $\mathsf{D}(H \oplus C_2^r) = \mathsf{D}^*(H \oplus C_2^r)$ for every r .*
- (2) *If $t(H) = 1$, then $\mathsf{D}(H \oplus C_2^r) = \mathsf{D}^*(H \oplus C_2^r) + \Theta_H(\log r)$.*

(3) If $t = t(H) \geq 2$, there is $c_H > 0$ such that, for all sufficiently large r ,

$$D(H \oplus C_2^r) \geq D^*(H \oplus C_2^r) + c_H \left(\frac{\log r}{\log \log r} \right)^t. \quad (7)$$

The multi-prime lower mechanism is the Barrington–Beigel–Rudich construction and its coding interpretation [1, 2]. The positive qualitative bound also follows from existing group-program results through the explicit reduction in Section 8. Our direct approach supplies constants and a common framework for the arithmetic and fiber statements.

1.3. Higher two-primary exponents. For comparing logarithmic coefficients, it is convenient to use

$$E_H(r) = D(H \oplus C_2^r) - D^*(H \oplus C_2^r), \quad \underline{\lambda}(H) = \liminf_{r \rightarrow \infty} \frac{E_H(r)}{\log_2 r}, \quad \bar{\lambda}(H) = \limsup_{r \rightarrow \infty} \frac{E_H(r)}{\log_2 r}.$$

Theorem 1.1 determines both coefficients for odd p -groups. Higher two-primary exponents can change them.

Theorem 1.5 (Two-primary dependence). *For $r \geq 512$,*

$$D(C_{24} \oplus C_2^r) \leq D^*(C_{24} \oplus C_2^r) + 32 \log_2 r + 3.$$

Moreover,

$$\frac{9}{5H_2(1/5)} \leq \bar{\lambda}(C_{24}) \leq 32, \quad \frac{9}{5H_2(1/5)} = 2.4933231062 \dots > 2, \quad (8)$$

where $H_2(u) = -u \log_2 u - (1-u) \log_2 (1-u)$ is binary entropy. For every fixed odd prime p and integer $a \geq 1$,

$$\bar{\lambda}(C_{p^{2^a}}) \geq \frac{1}{H_2(2^{-a})} \sim \frac{2^a}{a + \log_2 e} \quad (a \rightarrow \infty). \quad (9)$$

Thus these lower-bound coefficients are unbounded with p fixed.

The lower bound in (8) holds along an explicit sequence of ranks. It does not determine the exact Davenport constant, the optimal coefficient, or the existence of a coefficient limit. The underlying transfer, Theorem 10.2, converts finite zero-sum-free configurations in an abelian two-group into entropy lower bounds with a fixed elementary odd-primary target. Appendix A gives corresponding logarithmic-order conclusions for both small and large nonabelian Davenport constants.

1.4. Connections with earlier work. Logarithmic lower bounds for large elementary two-components have a history in zero-sum theory. For cyclic odd H , the lower coefficient $D(H) - 1$ is already contained in Liu [9, Theorem 4.3 and Corollary 4.4]. The simplex construction in Section 3 gives a direct form of this non-dispersive block method for arbitrary odd-order abelian label groups. Coding-theoretic approaches also appear in Plagne–Schmid [11]. Brakensiek, Gopi, and Guruswami [2] relate modular constraints on binary codes to sparse polynomial and weak-OR representations. We make the exact passage to Davenport constants explicit in Section 4.

The primary algebraic input is Olson’s group-ring method. The finite sphere-covering inequality in Corollary 3.2 also follows directly from Han–Zhang [6, Proposition 2.4], by taking the Hall subgroup to be C_2^r . We prove the stronger code-level covering-radius constraint and combine it with matching simplex constructions, uniform estimates, and signed Fourier identities for the exact C_3 intervals. Section 9.4 compares direct substitution into the same criterion for $C_{24} \oplus C_2^r$.

Idziak, Kawalek, Krzaczkowski, and Weiß [7] establish Boolean-conjunction lower bounds for programs over certain fixed groups and deduce polynomial lower bounds on nonempty solution densities. Section 8 constructs an explicit fixed wreath-product simulation of local maps on affine codes. It places our fixed nilpotent targets in their setting and recovers the qualitative fiber estimates and logarithmic Davenport upper bounds. The quantitative estimates here have independent proofs by Fourier support and primary group algebras.

1.5. Organization. Section 2 develops the selection-code and primary representations. Section 3 proves the sharp odd-primary and uniform estimates. Sections 4 and 5 give the exact Fourier transfer and the C_3 intervals. Sections 6–8 treat mixed-characteristic intersections, local fibers, and group programs. Section 9 proves the general threshold and the C_{24} upper bound. Section 10 gives the entropy construction, and Section 11 discusses its limitations and further questions. The appendices contain the nonabelian transfer and the large-rank C_3 localization.

AI tools developed by OpenAI were used in this work.

2. BINARY CODES AND PRIMARY REPRESENTATIONS

Unless specified otherwise, logarithms have base two. Write

$$V_b(L) = \sum_{j=0}^b \binom{L}{j},$$

with $\binom{L}{j} = 0$ for $j > L$. We set $D(1) = 1$, so that $D(1) - 1 = 0$. The algebraic degree of a binary function is the degree of its unique multilinear polynomial over $\mathbb{F}_2$. The zero function may be assigned degree $-\infty$.

2.1. The code correspondence.

Lemma 2.1. *For every fixed finite abelian group H , there is an integer c_H such that*

$$D^*(H \oplus C_2^r) = r + c_H$$

for all sufficiently large r .

Proof. For r sufficiently large, the rank of the two-primary component of $H \oplus C_2^r$ is at least the rank of every odd-primary component. Every nontrivial invariant factor is then even. Adding a further C_2 inserts one initial invariant factor equal to two, leaving all the others fixed. It increases D^* by one. $\square$

If $h_1, \dots, h_L \in H$, a weighted sum on a binary code is the map

$$\sigma_h(x) = \sum_{i=1}^L x_i h_i.$$

The bits are interpreted as the integers zero and one; this map is usually not a homomorphism from the binary additive group to H .

Proposition 2.2 (Selection kernels and realizations). *Let H be a finite abelian group.*

- (1) *If $((h_i, v_i))_{i=1}^L$ is zero-sum-free over $H \oplus C_2^r$, then the binary code*

$$V = \{x \in \mathbb{F}_2^L : \sum_i x_i v_i = 0\}$$

has dimension at least $L - r$, and $\sigma_h^{-1}(0) \cap V = \{0\}$.

- (2) *Conversely, suppose $V \leq \mathbb{F}_2^L$ has dimension d and $\sigma_h^{-1}(0) \cap V = \{0\}$. A full-rank parity-check matrix B of V gives a zero-sum-free sequence $((h_i, B_i))_{i=1}^L$ over $H \oplus C_2^{L-d}$. For every $r \geq L - d$, padding by independent binary basis elements gives a zero-sum-free sequence of length $r + d$ over $H \oplus C_2^r$.*

Proof. A binary selection vector describes a subsequence, and its two components sum to zero exactly when it belongs to V and its H -sum vanishes. This proves both correspondences. In the second part, the appended basis elements use new binary coordinates, so a zero-sum selection cannot contain any of them. $\square$

For later use, if $T : \mathbb{F}_2^d \rightarrow \mathbb{F}_2^R$ is linear, the graph code $\{(x, Tx) : x \in \mathbb{F}_2^d\}$ has parity-check matrix $[T \mid I_R]$. It has length $d + R$, dimension d , and parity-check rank exactly R .

Lemma 2.3 (Binary minimum weight). *A nonzero binary polynomial of degree at most e in d variables has at least 2^{d-e} nonzero values.*

Proof. The assertion is immediate for a nonzero constant. Otherwise write $f(x', x_d) = g(x') + x_d h(x')$ with $h \neq 0$, after relabeling a variable on which f depends. The degree of h is at most $e - 1$. For every x' with $h(x') = 1$, the two values of f differ, so at least one is nonzero. Induction gives at least $2^{(d-1)-(e-1)} = 2^{d-e}$ such values. $\square$

2.2. Fourier support in characteristic different from two. For a field $\mathbb{K}$ with $\text{char } \mathbb{K} \neq 2$, put $\chi_u(x) = (-1)^{u \cdot x}$ and

$$f(x) = \sum_{u \in \mathbb{F}_2^d} \hat{f}(u) \chi_u(x), \quad \hat{f}(u) = 2^{-d} \sum_{x \in \mathbb{F}_2^d} f(x) \chi_u(x), \quad \text{sp}(f) = |\text{supp } \hat{f}|.$$

The characters form a basis over $\mathbb{K}$. Translation preserves sparsity. If $x = Az + c$ is an affine substitution, each character restricts to a scalar multiple of one character of z , so sparsity does not increase. Also

$$\text{sp}(fg) \leq \text{sp}(f) \text{sp}(g), \quad (10)$$

because Fourier support of a product is contained in the sumset of the two supports.

Lemma 2.4 (Finite-field uncertainty). *For every nonzero $f : \mathbb{F}_2^d \rightarrow \mathbb{K}$,*

$$|\text{supp } f| \text{sp}(f) \geq 2^d.$$

Proof. Let $\mathcal{T}_f$ be the linear span of all translates of f . Fourier diagonalization shows that its dimension is $\text{sp}(f)$: character averaging extracts each frequency with nonzero coefficient. Choose a basis of translates. Their supports cover $\mathbb{F}_2^d$, since otherwise every translate of f would vanish at a common point, forcing $f = 0$. Each basis function has support size $|\text{supp } f|$. The union bound proves the claim. No absolute values or positivity are used. $\square$

A multilinear polynomial of degree at most b in L binary coordinates has Fourier support at most $V_b(L)$. Indeed $x_i = (1 - \chi_{e_i})/2$, so only characters supported on at most b of the original coordinates occur. The same bound holds after affine restriction.

2.3. Primary group algebras. For a finite p -group R , write I_R for the augmentation ideal of $\mathbb{F}_p[R]$ and put

$$\kappa(R) = \max\{j : I_R^j \neq 0\}, \quad \kappa(1) = 0.$$

The ideal is nilpotent. One elementary proof is induction on $|R|$: choose a central element z of order p . The kernel of $\mathbb{F}_p[R] \rightarrow \mathbb{F}_p[R/\langle z \rangle]$ is the central ideal generated by $z - 1$, whose p th power vanishes. Nilpotence in the quotient therefore gives nilpotence in $\mathbb{F}_p[R]$. Jennings' theorem provides the exact general index [8].

If $R = \bigoplus_i C_{p^{a_i}}$ is abelian, the truncated-polynomial description gives

$$\mathbb{F}_p[R] \cong \mathbb{F}_p[T_1, \dots, T_s] / (T_1^{p^{a_1}}, \dots, T_s^{p^{a_s}}), \quad \kappa(R) = \sum_i (p^{a_i} - 1) = D(R) - 1. \quad (11)$$

Let $g_1, \dots, g_T$ be group-valued functions. In the relevant primary group algebra,

$$\prod_{j=1}^T [g_j(x)] = \prod_{j=1}^T (1 + ([g_j(x)] - 1)). \quad (12)$$

Every term with more than $\kappa(R)$ augmentation factors is zero. The expansion preserves the original order, including for nonabelian groups. Taking the coefficient of $[h]$ gives the exact indicator that the group product equals h .

3. SHARP ESTIMATES FOR ODD-PRIMARY LABEL GROUPS

3.1. A covering-radius constraint. For a binary linear code $C \subseteq \mathbb{F}_2^L$, its covering radius is

$$\rho(C) = \max_{w \in \mathbb{F}_2^L} \min_{c \in C} d_H(w, c),$$

where d_H is Hamming distance. We use the augmentation-ideal identity (11). In group-algebra formulas below, X^h denotes the basis element $[h]$.

Theorem 3.1 (Covering transfer). *Let H be a finite abelian p -group with p odd, and put $b = D(H) - 1$. For a sequence*

$$S = ((h_i, v_i))_{i=1}^L \quad \text{over } H \oplus \mathbb{F}_2^r,$$

define its binary character code by

$$C(S) = \{(\langle x, v_1 \rangle, \dots, \langle x, v_L \rangle) : x \in \mathbb{F}_2^r\} \subseteq \mathbb{F}_2^L.$$

If S is zero-sum free, then

$$\rho(C(S)) \leq b. \quad (13)$$

Proof. Let I be the augmentation ideal of $K[H]$, where $K = \mathbb{F}_p$. Fourier decomposition on the elementary two-component gives an injective algebra map

$$K[H \oplus \mathbb{F}_2^r] \longrightarrow \prod_{x \in \mathbb{F}_2^r} K[H], \quad X^{(h,v)} \longmapsto ((-1)^{\langle x, v \rangle} X^h)_x.$$

Indeed, the character matrix on $\mathbb{F}_2^r$ is invertible because 2 is invertible in K .

Suppose that a vector $w \in \mathbb{F}_2^L$ has distance at least $b+1$ from every codeword. Set $\varepsilon_i = (-1)^{w_i+1}$ and consider

$$F = \prod_{i=1}^L (1 - \varepsilon_i X^{(h_i, v_i)}).$$

In the component indexed by x , the factor at position i belongs to I whenever $w_i \neq \langle x, v_i \rangle$, since that factor is then $1 - X^{h_i}$. At least $b+1$ factors belong to I , so every component vanishes by (11). Hence $F = 0$. On the other hand, if S is zero-sum free, only the empty selection contributes to the coefficient of X^0 in F . That coefficient is 1, which is impossible. $\square$

Corollary 3.2 (Finite sphere-covering bound). *Every zero-sum-free sequence of length L over $H \oplus C_2^r$ satisfies*

$$2^{L-r} \leq V_b(L). \quad (14)$$

Consequently,

$$D(H \oplus C_2^r) \leq \min\{L \geq 1 : V_b(L) < 2^{L-r}\}. \quad (15)$$

Proof. Theorem 3.1 proves (14) by covering $\mathbb{F}_2^L$ with at most 2^r balls of size $V_b(L)$. Here is a direct algebraic verification as well. Let $A : \mathbb{F}_2^L \rightarrow \mathbb{F}_2^r$ have columns v_i and put $d = \dim \ker A \geq L - r$. Parameterize its kernel linearly by $x \in \mathbb{F}_2^d$, with coordinates $\ell_i(x) = \langle t_i, x \rangle \in \{0, 1\}$. For $\chi_t(x) = (-1)^{\langle t, x \rangle}$, one has $\ell_i = (1 - \chi_{t_i})/2$ in $\mathbb{F}_p$. Write $[X^0]$ for the coefficient at X^0 in $\mathbb{F}_p[H]$. Zero-sum freeness gives the identity

$$\delta_0(x) = [X^0] \prod_{i=1}^L (1 + \ell_i(x)(X^{h_i} - 1)).$$

Indeed, the product is $X^{\sum_i \ell_i(x) h_i}$, and its coefficient at X^0 is one precisely when $x = 0$. Expand the product. Every term involving more than b factors $X^{h_i} - 1$ vanishes by $I^{b+1} = 0$. Since $\ell_i = (1 - \chi_{t_i})/2$, the Fourier support of the remaining function is contained in

$$\left\{ \sum_{i \in J} t_i : J \subseteq \{1, \dots, L\}, |J| \leq b \right\},$$

which has at most $V_b(L)$ elements. On the other hand, every Fourier coefficient of δ_0 equals $2^{-d} \neq 0$ in $\mathbb{F}_p$. Consequently $2^{L-r} \leq 2^d \leq V_b(L)$, as required. For fixed r, b , the exponential term eventually exceeds the polynomial $V_b(L)$, so the minimum in (15) exists. $\square$

More precise lower bounds on the size of a covering code can be inserted in the same way. The transfer uses the covering radius of the particular code $C(S)$, and it allows zero columns and repeated columns in the projection matrix. Standard covering-code results, including those of Graham and Sloane [4], are therefore available after their individual hypotheses have been checked.

For later comparison with the standard lower bound, write an odd-order group as $H \cong \bigoplus_{j=1}^s C_{m_j}$ in invariant-factor form. Pairing its cyclic factors with s binary factors gives, for $r \geq s$,

$$D^*(H \oplus C_2^r) = r + 1 + 2 \sum_{j=1}^s (m_j - 1). \quad (16)$$

3.2. Simplex constructions. The next construction uses only that multiplication by a power of two is an automorphism of H .

Proposition 3.3 (Simplex blocks). *Let H be a nontrivial finite abelian group of odd order, and put $b = D(H) - 1$. For any positive integers $m_1, \dots, m_b$, set*

$$r_0 = \sum_{j=1}^b (2^{m_j} - 1 - m_j).$$

For every $r \geq r_0$,

$$D(H \oplus C_2^r) \geq r + 1 + \sum_{j=1}^b m_j. \quad (17)$$

In particular, if $r \geq b(2^m - 1 - m)$, then

$$D(H \oplus C_2^r) \geq r + bm + 1. \quad (18)$$

Proof. Choose a zero-sum-free sequence $h_1, \dots, h_b$ in H . Let $\mathcal{S}_m$ be the binary simplex code whose generator matrix has as columns all nonzero vectors of $\mathbb{F}_2^m$. Its length is $2^m - 1$, its dimension is m , and each nonzero word has weight 2^{m-1} .

Take the direct sum $\mathcal{K} = \bigoplus_{j=1}^b \mathcal{S}_{m_j}$, of length $N = \sum_j (2^{m_j} - 1)$ and dimension $\sum_j m_j$. Choose a quotient map $A : \mathbb{F}_2^N \rightarrow \mathbb{F}_2^{r_0}$ with kernel $\mathcal{K}$. For every position in block j , use the H -label $2^{-(m_j-1)}h_j$, where the inverse power denotes the inverse automorphism of H . Pair these labels with the columns of A .

A selection whose binary sum is zero has its indicator vector in $\mathcal{K}$. Each nonzero block contributes exactly h_j to its H -sum. If the selection is nonempty, this is a nonempty subsequence sum of $h_1, \dots, h_b$, hence is nonzero. Thus the resulting sequence is zero-sum free. Appending $r - r_0$ new independent binary basis vectors, with zero H -labels, preserves this property. Its total length is $N + r - r_0 = r + \sum_j m_j$. $\square$

For $r \geq b$, the choice $m = \lfloor \log_2(1 + r/b) \rfloor$ in (18) gives

$$D(H \oplus C_2^r) \geq r + b \lfloor \log_2(1 + r/b) \rfloor + 1 \geq r + b \log_2(r/b) - b + 1. \quad (19)$$

3.3. Uniform estimates.

Theorem 3.4 (Uniform second-order estimate). *Let H be any nontrivial finite abelian p -group, where p is odd, and put $b = D(H) - 1$ and $G = H \oplus C_2^r$. If $r \geq 16b$, then*

$$D(G) = D^*(G) + b \log_2(r/b) + \rho_H(r), \quad -3b \leq \rho_H(r) < 0. \quad (20)$$

More precisely,

$$D(G) \leq D^*(G) + \lceil b \log_2(r/b) \rceil - 1. \quad (21)$$

Consequently, for any sequence of such groups H_r , allowing their primes, ranks, and cyclic orders to vary, if $b_r = D(H_r) - 1 = o(r)$, then

$$D(H_r \oplus C_2^r) = D^*(H_r \oplus C_2^r) + (1 + o(1))b_r \log_2(r/b_r). \quad (22)$$

Moreover, $D(H_r \oplus C_2^r) \sim D^*(H_r \oplus C_2^r) \sim r$.

Proof of Theorem 3.4. Write $H = \bigoplus_{j=1}^s C_{p^{e_j}}$. By (11), $b = \sum_j (p^{e_j} - 1) \geq 2$. Since $s \leq b/2 \leq r$, (16) becomes

$$D^*(H \oplus C_2^r) = r + 2b + 1. \quad (23)$$

Subtracting this from (19) proves the lower bound in (20).

For the upper bound, put $u = r/b \geq 16$ and

$$L = \lceil r + b \log_2 u + 2b \rceil.$$

The inequality $b \geq 2$ gives

$$\frac{L}{r} \leq 1 + \frac{\log_2 u + 5/2}{u} \leq \frac{45}{32}.$$

For the last inequality, $(\log_2 u + 5/2)/u$ is decreasing for $u \geq 16$ and equals $13/32$ at $u = 16$. For $1 \leq b \leq L$, setting $z = b/L \leq 1$ yields

$$z^b V_b(L) \leq (1 + z)^L \leq e^b, \quad V_b(L) \leq (eL/b)^b.$$

Using $e < 11/4$, we obtain

$$V_b(L) < \left(\frac{495}{128} \frac{r}{b} \right)^b < (4r/b)^b \leq 2^{L-r}.$$

Corollary 3.2 gives $D(H \oplus C_2^r) \leq L$. The rounding is exact:

$$L = r + 2b + \lceil b \log_2(r/b) \rceil = D^*(G) + \lceil b \log_2(r/b) \rceil - 1.$$

This proves (21). Since $\lceil y \rceil - 1 < y$ for every real y , it also gives $\rho_H(r) < 0$ in (20).

For the asymptotic assertion, $u_r = r/b_r \rightarrow \infty$ and $|\rho_{H_r}(r)| \leq 3b_r = o(b_r \log_2 u_r)$, proving (22). Furthermore, $b_r \log_2 u_r / r = \log_2 u_r / u_r \rightarrow 0$ and $(2b_r + 1)/r \rightarrow 0$, giving the stated first-order asymptotics. $\square$

Proof of Theorem 1.1. For fixed H , (20) already proves (1) with an explicitly bounded remainder. More precisely, for $r \geq 16b$ it gives

$$D(H \oplus C_2^r) = D^*(H \oplus C_2^r) + b \log_2 r + R_H(r), \quad -b \log_2 b - 3b \leq R_H(r) < -b \log_2 b. \quad \square$$

The factorial in the sphere volume gives a sharper explicit upper bound.

Proposition 3.5 (An explicit factorial bound). *Under the hypotheses of Theorem 3.4, assume only $r \geq 3b$ and define*

$$\varepsilon_b(r) = \frac{b(b \log_2 r + 3)}{r \ln 2 - b}.$$

Then

$$D(H \oplus C_2^r) \leq D^*(H \oplus C_2^r) + \lfloor b \log_2 r - \log_2(b!) + \varepsilon_b(r) \rfloor - 2b. \quad (24)$$

For fixed b , the displayed correction $\varepsilon_b(r)$ tends to zero.

Proof. Put $A = b \log_2 r - \log_2(b!)$, $\varepsilon = \varepsilon_b(r)$, and $L = r + \lfloor A + \varepsilon \rfloor + 1$. Let $c = L - r$. We have $A \geq 0$, $L \geq r \geq 3b$, and

$$A + \varepsilon < c \leq b \log_2 r + \varepsilon + 1.$$

Since $b!/j! \leq b^{b-j}$,

$$V_b(L) \leq \frac{L^b}{b!} \sum_{j=0}^b (b/L)^{b-j} \leq \frac{L^b}{b!(1 - b/L)}.$$

Write $\alpha = b/(r \ln 2) < 1$. The estimates $\log_2(1 + c/r) \leq c/(r \ln 2)$ and $-\log_2(1 - b/L) \leq 2b/(r \ln 2)$ give

$$\log_2 V_b(L) \leq A + \alpha c + 2\alpha \leq A + \alpha(b \log_2 r + \varepsilon + 3) = A + \varepsilon < c.$$

Here $b/L \leq 1/3$, so the second logarithmic estimate follows from $-\ln(1 - x) \leq 2x$ for $0 \leq x \leq 1/3$. Apply Corollary 3.2. $\square$

Example 3.6. Let $s_r = \lfloor r/(2 \log_2 r) \rfloor$ and

$$G_r = C_6^{s_r} \oplus C_2^{r-s_r}.$$

Its odd part is $C_3^{s_r}$, so $b_r = 2s_r \sim r/\log_2 r$. Therefore

$$D(G_r) = D^*(G_r) + (1 + o(1)) \frac{r \log_2 \log_2 r}{\log_2 r}, \quad D^*(G_r) = r + 4s_r + 1.$$

This follows from the uniform theorem even though the rank of the odd part tends to infinity.

3.4. A uniform bound for C_{2q}^r . The covering argument also applies when the odd and binary ranks grow together.

Corollary 3.7. *Let q be an odd prime power, and let $\lambda_q > 2(q-1)$ be the unique solution of*

$$\lambda_q \left[1 - H_2 \left(\frac{q-1}{\lambda_q} \right) \right] = 1, \quad (25)$$

where $H_2(u) = -u \log_2 u - (1-u) \log_2(1-u)$. For every integer $r \geq 1$,

$$D(C_{2q}^r) \leq \lfloor \lambda_q r \rfloor + 1 < 1.4162 D^*(C_{2q}^r). \quad (26)$$

Proof. Put $b = r(q-1)$ and $\Phi_q(x) = x[1 - H_2((q-1)/x)]$. On $x > 2(q-1)$, the derivative $\Phi_q'(x) = \log_2(2(1 - (q-1)/x))$ is positive, so Φ_q increases from zero to infinity. This proves existence and uniqueness in (25). Take $L = \lfloor \lambda_q r \rfloor + 1 > 2b$ and $z = b/(L-b)$. Then

$$V_b(L) \leq z^{-b}(1+z)^L = 2^{LH_2(b/L)} < 2^{L-r},$$

where the strict inequality follows from $L[1 - H_2(b/L)] = r\Phi_q(L/r) > r$. Corollary 3.2, with $H = C_q^r$, proves the first bound in (26).

For the numerical constant, put $c = 7081/5000 = 1.4162$ and $a = (q-1)/(2q-1) \in [2/5, 1/2]$. Define $F_c(a) = c[1 - H_2(a/c)] - (1-2a)$. Its derivative is $F_c'(a) = 2 - \log_2((c-a)/a) > 0$, because $c < 5a$. The endpoint inequality $F_c(2/5) > 0$ is equivalent to the exact integer comparison

$$2^{14081} 5^{6000} 5081^{5081} > 7081^{7081}.$$

Thus $\Phi_q(c(2q-1)) > 1$ and $\lambda_q < c(2q-1)$. Since $D^*(C_{2q}^r) = r(2q-1) + 1$ and $c > 1$, we obtain $\lfloor \lambda_q r \rfloor + 1 \leq \lambda_q r + 1 < c D^*(C_{2q}^r)$. $\square$

4. AN EXACT FOURIER FORMULATION

The code correspondence has a converse formulation that does not require H to be a p -group. Let H be a nontrivial finite abelian group of odd order. For $f : \mathbb{F}_2^d \rightarrow H$, define

$$\widehat{f}(t) = 2^{-d} \sum_{x \in \mathbb{F}_2^d} (-1)^{\langle t, x \rangle} f(x), \quad f(x) = \sum_{t \in \mathbb{F}_2^d} \widehat{f}(t) (-1)^{\langle t, x \rangle}.$$

These are identities in the additive group H : multiplication by 2^{-d} means applying the inverse of multiplication by 2^d .

Definition 4.1. For $d \geq 1$, let $\mu_H(d)$ be the minimum number of nonzero, nonconstant Fourier coefficients of a function $f : \mathbb{F}_2^d \rightarrow H$ such that

$$f(0) = 0, \quad f(x) \neq 0 \quad (x \neq 0).$$

Set $\mu_H(0) = 0$.

The minimum exists: there are finitely many functions, and the function taking a fixed nonzero value on $\mathbb{F}_2^d \setminus \{0\}$ is admissible.

Theorem 4.2 (Exact transfer). *For every nontrivial finite abelian odd-order group H and every $r \geq 0$,*

$$D(H \oplus C_2^r) = r + 1 + \max\{d \geq 0 : \mu_H(d) - d \leq r\}. \quad (27)$$

Proof. Take a zero-sum-free sequence $((h_i, v_i))_{i=1}^L$ and let $A : \mathbb{F}_2^L \rightarrow \mathbb{F}_2^r$ have columns v_i . Put $d = \dim \ker A$ and parameterize $\ker A$ injectively by $x \in \mathbb{F}_2^d$. Write its coordinate functions as $\ell_i(x) = \langle t_i, x \rangle \in \{0, 1\}$. Then

$$f(x) = \sum_{i=1}^L h_i \ell_i(x)$$

has zero set exactly $\{0\}$. Since $\ell_i = (1 - (-1)^{\langle t_i, x \rangle})/2$, it has at most L nonzero, nonconstant Fourier coefficients. Thus

$$\mu_H(d) - d \leq L - d = \text{rank } A \leq r, \quad L \leq r + d.$$

This gives the upper bound in (27).

Conversely, choose an admissible f with $s = \mu_H(d)$ nonconstant coefficients and let $E = \{t \neq 0 : \widehat{f}(t) \neq 0\}$. Since $f(0) = 0$,

$$f(x) = \sum_{t \in E} h_t \frac{1 - (-1)^{\langle t, x \rangle}}{2}, \quad h_t = -2\widehat{f}(t).$$

The set E spans $\mathbb{F}_2^d$: a nonzero vector orthogonal to all of E would give another zero of f . Hence the evaluation map

$$x \mapsto (\langle t, x \rangle)_{t \in E}$$

is injective. Its image $C_f \subseteq \mathbb{F}_2^s$ has dimension d . Let v_t be the images of the standard basis vectors under the quotient map $\mathbb{F}_2^s \rightarrow \mathbb{F}_2^s / C_f \cong \mathbb{F}_2^{s-d}$. The sequence $((h_t, v_t))_{t \in E}$ is zero-sum free: a nonempty selection with binary sum zero is a nonzero evaluation vector of some x , and its H -sum equals $f(x) \neq 0$.

If $s - d \leq r$, append $r - (s - d)$ independent binary basis vectors. This gives a zero-sum-free sequence of length $r + d$, proving the lower bound. It also proves that the maximum is finite, since $r + d \leq D(H \oplus C_2^r) - 1 \leq |H|2^r - 1$ for each feasible d . The case $d = 0$ uses the r independent binary basis vectors directly. $\square$

For $H = C_3 = \mathbb{F}_3$, it is convenient to include the constant Fourier coefficient. Define

$$\nu(d) = \min\{|\text{supp } \widehat{f}| : f : \mathbb{F}_2^d \rightarrow \mathbb{F}_3, f^{-1}(0) = \{0\}\} \quad (d \geq 1).$$

Multiplying f by a character preserves its zero set and translates its Fourier support. By moving a nonzero coefficient to the constant direction, one obtains

$$\mu_{C_3}(d) = \nu(d) - 1. \quad (28)$$

The reverse inequality follows because the full support has at most one more element than the nonconstant support. Consequently,

$$D(C_3 \oplus C_2^r) = r + 1 + \max(\{0\} \cup \{d \geq 1 : \nu(d) - 1 - d \leq r\}). \quad (29)$$

This is an exact structural formula. Evaluating its extremal parameter for every dimension is a further problem. Its sparse-representation language is related to the weak-OR formulation in [2, Section 4.3].

5. EXACT INTERVALS FOR THE ODD PART C_3

5.1. Signed Fourier coefficients. Let $f : \mathbb{F}_2^d \rightarrow \mathbb{F}_3$ have zero set $\{0\}$, and write

$$f(x) = \sum_{u \in S} a_u (-1)^{\langle u, x \rangle}, \quad a_u \in \{1, -1\}, \quad n = |S|.$$

The set S includes the constant direction when its coefficient is nonzero. Let P and Q count coefficients $+1$ and -1 , respectively.

Lemma 5.1 (Signed pair bound). *The support satisfies*

$$n \equiv 1 - (-1)^d \pmod{3}, \quad P - Q \equiv 0 \pmod{3}, \quad (30)$$

and

$$\binom{n}{2} \geq 2^d - 1. \quad (31)$$

If d is odd, then also

$$2(2^d - 1) \leq \binom{n}{2} + PQ, \quad 2^d \leq 1 + \frac{3n^2 - 2n - (P - Q)^2}{8}. \quad (32)$$

Proof. As an $\mathbb{F}_3$ -valued function, $f^2 = 1 - \delta_0$. The constant Fourier coefficient of the left side is $\sum_{u \in S} a_u^2 = n$; that of the right side is $1 - 2^{-d} = 1 - (-1)^d$ in $\mathbb{F}_3$. Also, $f(0) = \sum_u a_u = P - Q = 0$ in $\mathbb{F}_3$. This proves (30).

For each $t \neq 0$, let m_t count unordered pairs of distinct elements of S with sum t . The nonconstant coefficients of $f^2 = 1 - \delta_0$ give

$$2 \sum_{\substack{\{u,v\} \subseteq S \\ u+v=t}} a_u a_v = -2^{-d} \quad \text{in } \mathbb{F}_3. \quad (33)$$

In particular $m_t \geq 1$, and summing gives (31). If d is odd, the signed sum in (33) is -1 . Thus a direction represented by a unique pair must be represented by a pair of opposite signs.

Let U be the number of uniquely represented nonzero directions. Then

$$\binom{n}{2} = \sum_{t \neq 0} m_t \geq U + 2(2^d - 1 - U), \quad U \leq PQ.$$

These give the first inequality in (32). Substituting $PQ = (n^2 - (P - Q)^2)/4$ gives the second. $\square$

Corollary 5.2 (Odd-dimensional support bound). *For every integer $s \geq 1$,*

$$\nu(2s+1) > \frac{4}{\sqrt{3}} 2^s. \quad (34)$$

Proof. Write $n = \nu(2s+1)$. Equation (31) gives $n \geq 5$. If $n \leq (4/\sqrt{3})2^s$, then (32) would imply

$$2^{2s+1} \leq 1 + \frac{3n^2 - 2n}{8} \leq 2^{2s+1} + 1 - \frac{n}{4} < 2^{2s+1},$$

a contradiction. $\square$

If a zero-sum-free sequence over $C_3 \oplus C_2^r$ has length L and $L - r \geq d \geq 1$, choose a d -dimensional subspace of the binary projection kernel. Its label-sum function is admissible, as in Theorem 4.2, and its full Fourier support has size at most $L + 1$. We will use this even when the full kernel is larger than d .

5.2. Proof of the explicit intervals.

Proof of Theorem 1.2. For the lower bound, take two simplex blocks of dimension m in Proposition 3.3. Their binary quotient dimension is $a_m = 2(2^m - 1 - m)$. Hence for every $r \geq a_m$,

$$D(C_3 \oplus C_2^r) \geq r + 2m + 1.$$

Suppose $m \geq 2$ and a zero-sum-free sequence of length $L = r + 2m + 1$ exists with $r \leq z_m$. Put $T = 2^m$. Restrict its label-sum function to a $(2m+1)$ -dimensional kernel subspace. It has Fourier support size $n \leq L + 1 \leq 4T/\sqrt{3}$, contradicting Corollary 5.2. This proves the upper bound. The case $m = 1$ is $r = 0$ and follows from $D(C_3) = 3$. $\square$

The isolated values (3) also have a short proof using only the sphere volume. At $L = 2^{m+1} - 1$,

$$V_2(L) = 2^{2m+1} - 2^m + 1 < 2^{2m+1} = 2^{L-a_m}.$$

This gives the upper bound directly from Corollary 3.2.

5.3. An integer refinement. For odd $d \geq 1$, let λ_d be the least positive integer n satisfying

$$n \equiv 2 \pmod{3}, \quad 3n^2 - 2n - 9\mathbf{1}_{\{n \text{ odd}\}} \geq 8(2^d - 1). \quad (35)$$

This is an explicit arithmetic bound, not an unknown Fourier extremum. For instance, set

$$R_e(d) = \frac{1 + \sqrt{24 \cdot 2^d - 23}}{3}, \quad R_o(d) = \frac{1 + \sqrt{24 \cdot 2^d + 4}}{3}.$$

Then

$$\lambda_d = \min \left\{ 2 + 6 \left\lceil \frac{R_e(d) - 2}{6} \right\rceil, 5 + 6 \left\lceil \frac{R_o(d) - 5}{6} \right\rceil \right\}. \quad (36)$$

By (30), when n is odd the integer $P - Q$ is odd and divisible by three, so $(P - Q)^2 \geq 9$. Lemma 5.1 therefore proves $\nu(d) \geq \lambda_d$.

Proposition 5.3 (Refined exact intervals). *Put*

$$\ell_m = 2^{m+1} - 2m - 3 + \mathbf{1}_{\{m \text{ odd}\}}, \quad u_m = \lambda_{2m+1} - 2m - 3.$$

For every $m \geq 1$ and every integer $\ell_m \leq r \leq u_m$,

$$D(C_3 \oplus C_2^r) = r + 2m + 1. \quad (37)$$

Proof. On $\mathbb{F}_2^m \oplus \mathbb{F}_2^m$, consider

$$f(x, y) = (1 - \delta_0(x)) + (1 - \delta_0(y)) \quad \text{in } \mathbb{F}_3.$$

Its only zero is $(0, 0)$: elsewhere its value is one or two. There are $2(2^m - 1)$ nonconstant Fourier coefficients. The constant coefficient is $2 - 2^{1-m}$, which is zero for even m and nonzero for odd m . Thus the full support has size

$$B_{2m} = 2^{m+1} - 2 + \mathbf{1}_{\{m \text{ odd}\}}.$$

Translate this support by a character so it contains a nonzero constant coefficient. Equations (28) and (29) then give the lower bound for $r \geq B_{2m} - 1 - 2m = \ell_m$.

For the upper bound, a zero-sum-free sequence of length $r + 2m + 1$ would yield, on a $(2m + 1)$ -dimensional kernel subspace, an admissible function of support size at most

$$r + 2m + 2 \leq \lambda_{2m+1} - 1.$$

This contradicts $\nu(2m + 1) \geq \lambda_{2m+1}$. $\square$

6. A MIXED-CHARACTERISTIC INTERSECTION THEOREM

We first extract a linear space from the support of a Fourier-sparse function. The dimension required for this extraction will depend only on the degree of the binary condition.

Lemma 6.1 (A flat in a sparse support). *Suppose $b : \mathbb{F}_2^d \rightarrow \mathbb{K}$ satisfies $b(0) \neq 0$ and $\text{sp}(b) \leq S$. If an integer $t \geq 0$ satisfies*

$$d > t + 2^t \log S, \tag{38}$$

then $\text{supp } b$ contains a linear subspace of dimension $t + 1$.

Proof. Start from $U = \{0\}$. Suppose a j -dimensional subspace $U \subseteq \text{supp } b$ has been constructed. Define

$$H_U(x) = \prod_{u \in U} b(x + u).$$

It is nonzero at zero, and (10) gives $\text{sp}(H_U) \leq S^{2^j}$. Hence

$$|\text{supp } H_U| \geq 2^d S^{-2^j}$$

by Lemma 2.4. If $d > j + 2^j \log S$, this support is larger than $|U|$. Choose $v \in \text{supp } H_U \setminus U$. Then $v + U \subseteq \text{supp } b$, and $U \cup (v + U)$ is a $(j + 1)$ -dimensional linear subspace in $\text{supp } b$. The function $j + 2^j \log S$ is nondecreasing, so (38) permits all the required extensions. $\square$

Proof of Theorem 1.3. First suppose Z is a singleton. Translate its point to zero. If (5) failed, Lemma 6.1 with $t = D$ would give a $(D + 1)$ -dimensional subspace $U \subseteq \text{supp } b$. On U , the binary function a is one at zero and zero elsewhere. In basis coordinates it is $\prod_{i=1}^{D+1} (1 + x_i)$, whose degree is $D + 1$. Affine substitution cannot increase degree, a contradiction.

For general nonempty Z , translate a point of Z to zero and choose an inclusion-maximal linear subspace W with $W \cap Z = \{0\}$. Put $k = \dim W$. The singleton bound on W gives $k \leq D + 2^D \log S$. Every coset of W meets Z : a missing coset $v + W$ would make $W \cup (v + W)$ a larger isolating subspace. Therefore

$$|Z| \geq 2^{d-k} \geq 2^{d-D} S^{-2^D}.$$

All ingredients are stable under affine restriction, as required. $\square$

Remark 6.2. The theorem is not obtained by multiplying separate lower bounds for $\{a = 1\}$ and $\{b \neq 0\}$; two sets of large density can have a very small intersection. The argument instead uses the algebraic degree of one condition and the translation structure of the other. Section 11.1 shows that the coefficient of $\log S$ in the singleton bound cannot universally be replaced by one, even when $D = 3$ and b takes only the values zero and one.

7. FIBERS OF LOCAL GROUP-VALUED PRODUCTS

Let $V \subseteq \mathbb{F}_2^L$ be an affine code of dimension d . Fix scopes $S_j \subseteq [L]$, with $|S_j| \leq \beta$, and maps $g_j : \mathbb{F}_2^{S_j} \rightarrow K$. We consider the ordered product

$$F(x) = g_1(x|_{S_1}) \cdots g_T(x|_{S_T}), \quad x \in V. \quad (39)$$

The arity $\beta \geq 1$ is fixed; the scopes may overlap arbitrarily. The order in (39) is part of the data.

Theorem 7.1 (Explicit local fibers). *Let Q be a finite two-group and P a finite odd p -group, and take $K = Q \times P$. Define*

$$D_0 = \beta \kappa(Q), \quad W = \sum_{j=0}^{\kappa(P)} 2^{\beta j} \binom{T}{j}.$$

Every attainable $h \in K$ satisfies

$$\frac{|F^{-1}(h) \cap V|}{|V|} \geq 2^{-D_0} W^{-2^{D_0}}. \quad (40)$$

If a fiber is a singleton, then

$$d \leq D_0 + 2^{D_0} \log W. \quad (41)$$

Proof. Write $h = (h_Q, h_P)$ and parametrize V by $\mathbb{F}_2^d$. First work in $\mathbb{F}_2[Q]$. Before restriction to V , each local augmentation-valued function $[g_j^Q(x)] - 1$ has a multilinear representation of degree at most β with coefficients in I_Q . By (12), terms with more than $\kappa(Q)$ such factors vanish. Thus the coefficient of $[h_Q]$ in the ordered product is a binary polynomial a of degree at most D_0 . It is the exact Q -target indicator. The degree bound persists after the affine parametrization over $\mathbb{F}_2$.

Now work in $\mathbb{F}_p[P]$. A surviving term in the augmentation expansion has its factors indexed by $J \subseteq [T]$ with $|J| \leq \kappa(P)$. It depends on at most $\beta|J|$ original binary coordinates. On V , those coordinates are affine linear forms, so any scalar coefficient of this term has Fourier support in a space of at most $2^{\beta|J|}$ characters. Summing over J shows that the exact P -target indicator b has $\text{sp}(b) \leq W$. The desired fiber is precisely $\{a = 1, b \neq 0\}$. Apply Theorem 1.3. $\square$

Corollary 7.2 (Search consequences). *For fixed Q, P, β , existence of a target preimage in (39) can be tested in randomized polynomial time with one-sided error. A preimage can be found with the same error guarantee. Deterministic search and emptiness certification take time $\exp(O_{Q,P,\beta}((\log(T+2))^2))$, in addition to polynomial input-reading and linear-algebra costs.*

Proof. Project V onto the union of the scopes. Its dimension is at most βT , and projection has equal-size fibers, preserving the density of every target fiber. Uniform sampling succeeds with inverse polynomial probability by (40). Every sampled candidate is checked directly; in an empty fiber the algorithm never outputs a witness.

For deterministic search, identify the projected code with $\mathbb{F}_2^{d_0}$. Choose a solution z of minimum Hamming weight k . The coordinate subspace on its support contains no other solution: every other point has fewer than k nonzero coordinates. Applying (41) to that subspace gives $k = O_{Q,P,\beta}(\log(T+2))$. Enumerating all vectors up to this weight gives the asserted running time, including when no solution exists. A projected witness can be lifted to V by linear algebra. $\square$

7.1. Sharper estimates for weighted abelian sums. Let Q be abelian of two-power order and P abelian of odd prime-power order, allowing either group to be trivial. Set $b_Q = D(Q) - 1$ and $b_P = D(P) - 1$.

Corollary 7.3 (Weighted fibers). *For labels $h_i \in Q \oplus P$ on an affine binary code V of dimension d and length L , every attainable weighted sum has at least*

$$2^{d-b_Q} V_{b_P}(L)^{-2^{b_Q}} \quad (42)$$

preimages. In particular, a singleton fiber implies

$$d \leq b_Q + 2^{b_Q} \log V_{b_P}(L). \quad (43)$$

Proof. The Q indicator has binary degree at most b_Q . For the odd part, expand

$$\prod_{i=1}^L (1 + x_i([h_i^P] - 1)) \quad \text{in } \mathbb{F}_p[P].$$

Its target coefficient is a multilinear polynomial of degree at most b_P in the original bits. It therefore has Fourier support at most $V_{b_P}(L)$, also after affine restriction. Theorem 1.3 gives the claim. $\square$

When $Q = 1$, the singleton bound is just $d \leq \log V_{b_P}(L)$, and the density bound also follows directly from Lemma 2.4. The mixed intersection argument is what controls a simultaneous nontrivial two-primary condition.

8. A CONNECTION WITH PROGRAMS OVER FIXED GROUPS

This section gives a second, qualitative route to the preceding fiber bounds. A program over a fixed finite group G is an ordered list of instructions, each of which chooses one of two group elements according to one input bit. An accepting subset of G specifies the Boolean output. Constants can be inserted as instructions with equal choices. Let $\gamma_G(n)$ denote the minimum program length representing an n -variable singleton indicator, with value infinity if no such program exists.

We use the following consequence of existing results. By [7, Theorem 17], if

$$G \leq N \times (R \rtimes A), \quad (44)$$

where N is finite nilpotent, R is a finite p -group, and A is finite abelian, then $\gamma_G(n) \geq 2^{c_G n}$ for all sufficiently large n , with $c_G > 0$. Their Proposition 9 converts this into an inverse-polynomial lower bound for every nonempty accepting set of a program of length m .

Proposition 8.1 (Fixed wreath-product simulation). *Fix $K = Q \times P$ and β as in Theorem 7.1. There is a fixed finite group W satisfying (44) such that, after parametrizing the relevant projection of V , each target condition $F(x) = h$ in (39) is recognized by a W -program of length $O_\beta(T^2)$. The simulation preserves the fraction of satisfying inputs.*

Proof. Let $A = \mathbb{F}_2^\beta$ and use the regular translation action on K^A . Write

$$W = K^A \rtimes A, \quad (f, u)(g, v) = (f \tau_u g, u + v), \quad (\tau_u g)(a) = g(a + u).$$

Multiplication in K^A is pointwise and ordered.

Project the code onto the coordinates that occur in a scope, and parametrize it by $z \in \mathbb{F}_2^{d_0}$, where $d_0 \leq \beta T$. Each local scope is an affine map $y_j(z) \in A$; append unused coordinates when its size is smaller than β . Regard the local table as $f_j \in K^A$. The cursor $(1, y_j(z))$ can be computed with at most d_0 bit-dependent translation instructions and one constant instruction. Consequently

$$(1, y_j(z))(f_j, 0)(1, y_j(z))^{-1} = (\tau_{y_j(z)} f_j, 0) \quad (45)$$

is a program of length at most $2d_0 + 3$. At coordinate $a = 0$, the right-hand side has value $g_j(y_j(z))$. The product of these conjugates has cursor zero, and its base coordinate at zero is exactly $F(x)$. Take the accepting subset

$$\{(f, 0) \in W : f(0) = h\}.$$

This gives length at most $T(2d_0 + 3)$ and the desired accepting condition.

Finally the diagonal cursor map embeds W into

$$(Q^A \rtimes A) \times (P^A \rtimes A). \quad (46)$$

The first factor is a two-group and hence nilpotent; the second is an odd p -group extended by the abelian group A . Thus (44) applies. Uniform binary parameters give uniform points of the projected affine code, and projection has equal-size fibers, so all accepting fractions are preserved. $\square$

Corollary 8.2 (Qualitative density from group programs). *For every fixed Q, P, β there is $C = C(Q, P, \beta)$ such that every nonempty fiber in Theorem 7.1 has density at least $(T + 2)^{-C}$.*

Proof. Apply the program density consequence above to Proposition 8.1. Its length is polynomial in T , and its group is fixed. The resulting density is the original fiber density. $\square$

The explicit estimate (40) and this reduction serve different quantitative purposes. The former gives an exponent in terms of primary augmentation indices and applies a field-uniform intersection theorem. The latter explains why the qualitative phenomenon is compatible with fixed-group satisfiability theory. Thus the polynomial-density and search consequences can be obtained through this fixed-group connection, while the direct Fourier argument also provides the explicit estimates needed below.

9. LOGARITHMIC DAVENPORT CORRECTIONS

9.1. One odd prime: explicit upper bounds. Let $H = Q \oplus P$, where Q is a fixed abelian two-group and P a fixed abelian odd p -group. Put

$$b_Q = D(Q) - 1, \quad b_P = D(P) - 1, \quad A_H(L) = b_Q + 2^{b_Q} \log V_{b_P}(L).$$

Proposition 9.1 (A finite-rank bound). *If $r \geq 1$ and $\lfloor A_H(2r) \rfloor \leq r - 1$, then*

$$D(H \oplus C_2^r) \leq r + 1 + \lfloor A_H(2r) \rfloor. \quad (47)$$

Consequently

$$D(H \oplus C_2^r) \leq r + 2^{b_Q} b_P \log r + O_H(1). \quad (48)$$

Proof. If a zero-sum-free sequence has length L , its selection kernel in Proposition 2.2 has dimension at least $L - r$. The zero fiber of its H -sum is a singleton. Thus

$$L - r \leq A_H(L) \quad (49)$$

by Corollary 7.3. Take $L = r + 1 + \lfloor A_H(2r) \rfloor \leq 2r$. Then $L - r = 1 + \lfloor A_H(2r) \rfloor > A_H(2r) \geq A_H(L)$, contradicting (49). This proves (47).

For fixed $b_P > 0$, $\log V_{b_P}(2r) = b_P \log r + O_H(1)$, so the finite condition holds for all sufficiently large r and yields (48). If $b_P = 0$, the same conclusion holds with a bounded correction, and Olson's formula gives the exact value $D(H \oplus C_2^r) = r + D(H)$. $\square$

Remark 9.2. Corollary 8.2 gives the qualitative conclusion of Proposition 9.1 by the same selection-kernel argument. If its unique fiber has dimension d , its density 2^{-d} must be at least $L^{-O_H(1)}$. Hence $L - r \leq d = O_H(\log L)$, which implies $L = r + O_H(\log r)$. The elementary proof above identifies an explicit coefficient.

9.2. Lower bounds and the odd-prime threshold. We first record the standard simplex-block argument in the form needed for the logarithmic lower bound.

Corollary 9.3 (Logarithmic simplex lower bound). *For every nontrivial fixed finite abelian group H of odd order,*

$$D(H \oplus C_2^r) \geq r + (D(H) - 1) \log r - O_H(1).$$

In particular, for every odd prime p ,

$$D(C_p \oplus C_2^r) \geq r + (p - 1) \log r - O_p(1). \quad (50)$$

Proof. Apply (19) with $b = D(H) - 1$ fixed. $\square$

If an odd prime p divides $|H|$, then $C_p \leq H$, so (50) and Lemma 2.1 give $E_H(r) \gg_H \log r$.

Lemma 9.4 (Composite-modulus construction). *Let H be a fixed finite abelian group with $t = t(H) \geq 2$. Then (7) holds for all sufficiently large r .*

Proof. Choose the distinct odd primes $p_1, \dots, p_t$ dividing $|H|$ and set $M = \prod_i p_i$. For a large integer B , let Q_i be the largest power of p_i not exceeding $B + 1$, and set $d = \prod_i Q_i - 1$. Thus $d \gg_H B^t$.

For $q = p^k$, the polynomial

$$u_q(x) = \sum_{j=0}^{q-1} (-1)^j e_j(x) \quad \text{over } \mathbb{F}_p \quad (51)$$

is the indicator of $q \mid \text{wt}(x)$ on any binary cube; e_j denotes the elementary symmetric polynomial and $e_0 = 1$. To verify this, at weight $w \geq 1$ use

$$\sum_{j=0}^{q-1} (-1)^j \binom{w}{j} = (-1)^{q-1} \binom{w-1}{q-1}.$$

Since q is odd, the sign is positive, and Lucas's theorem makes the last binomial coefficient equal to one modulo p precisely when $q \mid w$, and zero otherwise. At $w = 0$, the sum is one.

By the Chinese remainder theorem, combine the polynomials $1 - u_{Q_i}$ into one polynomial f over $\mathbb{Z}/M\mathbb{Z}$ of degree at most B . Its zero set on $\mathbb{F}_2^d$ is exactly $\{0\}$: the simultaneous conditions $Q_i \mid \text{wt}(x)$ force $\prod_i Q_i \mid \text{wt}(x)$, while $0 \leq \text{wt}(x) \leq d$. This is the symmetric composite-modulus mechanism of [1], used in the sparse-polynomial/code setting in [2].

Because two is invertible modulo M , expand f in parity characters. At most $V_B(d)$ frequencies occur. The identity $f(0) = 0$ gives

$$f(x) = \sum_{u \neq 0} c_u (\chi_u(x) - 1) = \sum_{u \neq 0} (-2c_u) \ell_u(x),$$

where $\ell_u(x) = u \cdot x \pmod{2}$ is regarded as a bit. Use one coordinate for each nonzero coefficient c_u . The resulting linear map to a binary code is injective: a vector in its kernel would also be a zero of f . The code has dimension d and length $L \leq V_B(d) - 1$, with a unique zero for its weighted C_M -sum.

Now $\log V_B(d) = O_H(B \log B)$. For each sufficiently large r , choose $B = \lfloor \varepsilon_H \log r / \log \log r \rfloor$, where $\varepsilon_H > 0$ is a sufficiently small fixed constant. Then $L \leq r$, and Proposition 2.2 gives a zero-sum-free sequence of length $r + d$ in $C_M \oplus C_2^r$. The subgroup $C_M \leq H$ and $D^*(H \oplus C_2^r) = r + O_H(1)$ finish the proof. $\square$

The same construction has a finite form, useful without an unspecified asymptotic constant.

Proposition 9.5 (Finite composite-modulus bound). *Let $M = p_1 \cdots p_t$ be a product of distinct odd primes, with $t \geq 1$. Choose $Q_i = p_i^{a_i}$, with $a_i \in \mathbb{Z}_{\geq 0}$, and put $Q = \prod_i Q_i$ and $d_0 = \max_i (Q_i - 1)$. Then*

$$D(C_M \oplus C_2^r) \geq r + Q \quad \text{whenever} \quad r \geq V_{d_0}(Q - 1) - Q. \quad (52)$$

Proof. Combine the polynomials $1 - u_{Q_i}$ in (51) by CRT on the cube of dimension $Q - 1$. For $Q_i = 1$, set $u_1 = 1$. The resulting polynomial has a unique zero and degree at most d_0 , so $\mu_{C_M}(Q - 1) \leq V_{d_0}(Q - 1) - 1$. Theorem 4.2 now applies. If $Q = 1$, the same conclusion follows from $\mu_{C_M}(0) = 0$. $\square$

Example 9.6. For $M = 15$, take $Q_1 = 3^a$ and $Q_2 = 5^b$. On the cube of dimension $3^a 5^b - 1$, the polynomial is explicitly

$$f = 10 \sum_{j=1}^{3^a-1} (-1)^{j+1} e_j + 6 \sum_{j=1}^{5^b-1} (-1)^{j+1} e_j \pmod{15}.$$

Its only zero is the origin, and its degree is at most $\max(3^a, 5^b) - 1$. Both prime components test the same Boolean weight, over a range of length $3^a 5^b$.

Proposition 9.7 (An explicit bound at every large rank). *Let H be fixed and abelian, with distinct odd prime divisors $p_1, \dots, p_t$, where $t \geq 2$, and put $M = \prod_i p_i$. For $r \geq 4$, set*

$$R = \log_2 r, \quad d = \left\lfloor \frac{R}{(t-1) \log_2 R + t + 2} \right\rfloor, \quad Q_i = p_i^{\lfloor \log_{p_i}(d+1) \rfloor}.$$

Whenever $d \geq 1$,

$$D(H \oplus C_2^r) \geq r + \prod_i Q_i > r + \frac{(d+1)^t}{M}. \quad (53)$$

In particular,

$$D(H \oplus C_2^r) \geq D^*(H \oplus C_2^r) + \left(\frac{1}{M(t-1)^t} + o_H(1) \right) \left(\frac{\log_2 r}{\log_2 \log_2 r} \right)^t. \quad (54)$$

Proof. The group H contains C_M . The largest allowed powers satisfy $(d+1)/p_i < Q_i \leq d+1$, whence $Q = \prod_i Q_i > (d+1)^t/M$. Put $k = Q - 1$ and $d_0 = \max_i(Q_i - 1) \leq d$. If $k \geq d \geq 1$, the binomial estimate used in the proof of Theorem 3.4 gives

$$\begin{aligned} V_{d_0}(k) &\leq V_d(k) \leq (ek/d)^d \\ &\leq (e2^t d^{t-1})^d < 2^{d((t-1)\log_2 R + t + 2)} \leq 2^R = r. \end{aligned}$$

Here $k < (d+1)^t \leq 2^t d^t$, $d \leq R$, and $e < 4$. If $k < d$, use $V_{d_0}(k) \leq 2^k \leq 2^d \leq r$ instead. Proposition 9.5 proves (53). Finally $d \sim R/((t-1)\log_2 R)$, and Lemma 2.1 absorbs the fixed difference between $D^*(H \oplus C_2^r)$ and r in the $o_H(1)$ term. $\square$

Corollary 9.8 (Sublinear corrections for cyclic odd parts). *For every fixed odd integer $M \geq 3$, as $r \rightarrow \infty$,*

$$D(C_M \oplus C_2^r) = D^*(C_M \oplus C_2^r) + O_M\left(\frac{r}{\log r}\right). \quad (55)$$

In particular,

$$\frac{E_{C_{15}}(r)}{\log r} \rightarrow \infty, \quad \frac{E_{C_{15}}(r)}{r} \rightarrow 0.$$

Proof. Brakensiek–Gopi–Guruswami [2, Corollary 4.24, preprint version] show that a binary linear subspace $U \leq \mathbb{F}_2^N$ in which zero is the only word of weight divisible by M satisfies $\dim U = O_M(N/\log(N+2))$, assuming bounded-torsion PFR. That hypothesis is supplied by Gowers–Green–Manners–Tao [3, Theorem 1.1].

Let a zero-sum-free sequence of length L over $C_M \oplus C_2^r$ have cyclic labels $h_i \in \{0, \dots, M-1\}$. Its binary selection kernel V has dimension $d \geq L - r$, and $\sum_i h_i x_i = 0 \pmod{M}$ has the unique solution $x = 0$ on V . Replace coordinate x_i by h_i copies, omitting it if $h_i = 0$. This linear map T has target length $N = \sum_i h_i \leq (M-1)L$ and is injective on V : if $Tx = 0$, its weighted label sum is zero, so $x = 0$. Moreover $\text{wt}(Tx) \equiv \sum_i h_i x_i \pmod{M}$. Applying the cited code bound to $T(V)$ gives

$$L - r \leq d = O_M\left(\frac{N}{\log(N+2)}\right) = O_M\left(\frac{L}{\log(L+2)}\right).$$

This first gives $L \leq 2r$ for all sufficiently large L , and then $L \leq r + O_M(r/\log r)$. The standard lower bound proves (55). For $M = 15$, combine this upper bound with Proposition 9.7 and $D^*(C_{15} \oplus C_2^r) = r + 29$. $\square$

Proof of Theorem 1.4. If $t(H) = 0$, then $H \oplus C_2^r$ is a two-group and Olson's formula applies. If $t(H) = 1$, Proposition 9.1 gives the logarithmic upper bound, and Corollary 9.3 in a subgroup gives the logarithmic lower bound. For $t(H) \geq 2$, Lemma 9.4 applies; its lower bound divided by $\log r$ tends to infinity. $\square$

Corollary 9.9 (Elementary two-primary parts). *For every odd prime p and fixed $u \geq 0$,*

$$E_{C_2^u \oplus C_p}(r) = (p-1) \log r + O_{p,u}(1).$$

In particular the coefficient limit exists and equals $p-1$.

Proof. Absorb C_2^u into the growing binary rank. The case $Q = 1$ of Proposition 9.1 gives an upper coefficient $p-1$, and Corollary 9.3 gives the same lower coefficient. The standard lower bound differs from the binary rank by a fixed constant, and $\log(r+u) = \log r + O_u(1/r)$. $\square$

Corollary 9.10 (Nilpotent fiber threshold). *For a fixed finite nilpotent group K , the following are equivalent:*

- (1) $t(K) \leq 1$;
- (2) *for every fixed β , all nonempty fibers of all products (39) on all binary affine codes have density at least $(T+2)^{-c_{K,\beta}}$, with an exponent independent of the code, scopes, maps, and target.*

Proof. If $t(K) \leq 1$, the Sylow decomposition is $K = Q \times P$ with Q, P as in Theorem 7.1; either that theorem or Corollary 8.2 applies. If $t(K) = t \geq 2$, the Sylow direct product contains a cyclic subgroup of order M , the product of its distinct odd prime divisors. The weighted codes in Lemma 9.4 give one-bit local factors with a singleton identity fiber. Its density is 2^{-d} , while $d \gg B^t$ and $\log(T+2) = O(B \log B)$. Hence $d/\log(T+2) \rightarrow \infty$, contradicting any uniform polynomial density bound. $\square$

The last equivalence concerns solution density. It does not by itself assert computational hardness when the density bound fails.

9.3. An explicit upper bound for C_{24} . For $C_{24} \cong C_8 \oplus C_3$, the general coefficient in (48) is $2^7 \cdot 2 = 256$. A preliminary mod-four extraction reduces the binary degree needed in the final intersection step.

Lemma 9.11 (A mod-four zero subcode). *Let $V \leq \mathbb{F}_2^L$ have dimension d , and let $q(x) = \sum_i q_i x_i \pmod{4}$. There is a subcode $U \leq V$ with $q|_U = 0$ and*

$$\dim U \geq \max\{0, \lfloor (d-2)/2 \rfloor\}.$$

Proof. Suppose $v_1, \dots, v_j$ span a zero subcode. To extend it impose

$$q(x) = 0 \pmod{4}, \quad 2 \sum_i q_i x_i (v_s)_i = 0 \pmod{4} \quad (1 \leq s \leq j).$$

These are weighted binary constraints into $C_4 \oplus C_2^j$. Their common zero indicator has binary degree at most $3+j$ by (11) and the group-algebra expansion. It is one at zero. Lemma 2.3 gives at least $2^{d-(3+j)}$ points in its support. If $d > 3+2j$, this is larger than the old span, so an extending vector exists. The identity

$$q(x \oplus y) = q(x) + q(y) - 2 \sum_i q_i x_i y_i \pmod{4}$$

shows that the enlarged span is again zero. Iteration gives the stated dimension. $\square$

Lemma 9.12 (The residual cubic). *Let $q(x) = \sum_i q_i x_i \pmod{8}$ on a binary linear code U . If every value is divisible by four, then $q/4 : U \rightarrow \mathbb{F}_2$ has algebraic degree at most three.*

Proof. In basis coordinates z on U , every original bit is a parity. Its integer multilinear coefficient on a monomial of size j is divisible by 2^{j-1} . Consequently q has a multilinear representation modulo eight with no terms of degree at least four. Since all its values are divisible by four, integer Möbius inversion shows that all its coefficients are divisible by four modulo eight. Divide by four and reduce modulo two. $\square$

Theorem 9.13 (Explicit C_{24} bounds). *For any weighted C_{24} -sum on a binary affine code of length L and dimension d , every attainable fiber has at least*

$$\frac{2^d}{512 V_2(L)^{16}} \quad (56)$$

points. A singleton fiber implies

$$d \leq 9 + 16 \log V_2(L). \quad (57)$$

For every $r \geq 512$,

$$D(C_{24} \oplus C_2^r) \leq r + 10 + \lfloor 16 \log(2r^2 + r + 1) \rfloor, \quad (58)$$

$$E_{C_{24}}(r) \leq 32 \log r + 3. \quad (59)$$

Proof. First suppose the zero fiber on a linear code is $\{0\}$. Apply Lemma 9.11 to the reduction modulo four of its C_8 -sum. On a subcode U of dimension $k \geq \max\{0, \lfloor (d-2)/2 \rfloor\}$, the remaining C_8 zero indicator is a binary polynomial of degree at most three, by Lemma 9.12. The C_3 zero indicator has Fourier support at most $V_2(L)$. Theorem 1.3 gives $k \leq 3 + 8 \log V_2(L)$. Since $d \leq 2k + 3$, apart from the harmless case $d \leq 3$, this proves (57).

Translate an arbitrary attained affine target to zero. Toggling a bit x_i about a fixed solution replaces its weight by $(-1)^{(x_0)_i} h_i$ and subtracts the target. Thus the singleton bound is stable under every affine restriction. The maximal isolating-subspace argument in the proof of Theorem 1.3 gives (56).

Use the proof of Proposition 9.1 with $A(L) = 9 + 16 \log V_2(L)$. Now $V_2(2r) = 2r^2 + r + 1$, and the necessary finite cutoff holds for $r \geq 512$. Indeed $A(2r) \leq 41 + 32 \log r$, and $r - 42 - 32 \log r$ is positive at 512 and increasing thereafter. This proves (58). Finally

$$16 \log(2r^2 + r + 1) \leq 32 \log r + 16 + 16 \log(1 + 1/r) < 32 \log r + 17$$

in this range. Since $D^*(C_{24} \oplus C_2^r) = r + 24$, (59) follows. $\square$

9.4. Direct comparison with a covering criterion. Han–Zhang’s covering criterion [6, Proposition 2.4], applied with odd primary part C_3 and complementary group $C_8 \oplus C_2^r$, requires

$$8 2^r \sum_{j=0}^2 \binom{N}{j} 7^{N-j} < 8^N. \quad (60)$$

At $N = r + O(\log r)$ even the $j = 0$ term prevents this inequality: its ratio to 8^N has binary logarithm $3 + r - N \log(8/7)$, which tends to infinity. Thus this direct substitution does not give (59). This observation concerns that substitution, not a non-implication claim about every possible use of the criterion. The alternative qualitative derivation through fixed-group programs was established in Section 8.

10. ENTROPY LOWER BOUNDS FROM FINITE CONFIGURATIONS

We now turn from fiber lower bounds to constructions of singleton fibers. The following exact identity permits the internal prime-power scale to grow while the odd target group remains fixed.

10.1. An exact prime-power detector. For $U \subseteq [n]$, write $\ell_U(x) = \bigoplus_{i \in U} x_i \in \{0, 1\}$ and $\chi_U(x) = (-1)^{\ell_U(x)}$.

Lemma 10.1 (Truncated Fourier detector). *Let p be an odd prime, $k \in \mathbb{Z}_{\geq 1}$, and $A \in \mathbb{Z}_{\geq 2}$. Set $t = p^k$ and $n = At - 1$. Define $b(x) = \mathbf{1}_{t|\text{wt}(x)}$ on $\mathbb{F}_2^n$, with values in $\mathbb{F}_p$. Then*

$$b(x) = \sum_{\substack{U \subseteq [n] \\ |U| < t}} \chi_U(x). \quad (61)$$

Every displayed Fourier coefficient is exactly one; all others are zero. Moreover

$$2 \sum_{\substack{U \subseteq [n] \\ 1 \leq |U| < t}} \ell_U(x) = 1 - b(x) \quad \text{in } \mathbb{F}_p. \quad (62)$$

Proof. Fix a frequency U of size j , and write $j = qt + s$ with $0 \leq s < t$. The unnormalized Fourier coefficient of b is the sum of all coefficients whose exponent is divisible by t in the polynomial

$$(1 - z)^j (1 + z)^{n-j}.$$

In characteristic p , Frobenius gives the factorization

$$(1 - z^t)^q (1 + z^t)^{A-q-1} (1 - z)^s (1 + z)^{t-1-s}.$$

The final factor has degree $t - 1$ and constant term one. Only its constant term can contribute to exponents divisible by t . The sum of the desired coefficients is therefore

$$(1 - y)^q (1 + y)^{A-q-1} \Big|_{y=1} = \begin{cases} 2^{A-1}, & q = 0, \\ 0, & q \geq 1. \end{cases}$$

After normalization, the nonzero coefficient is $2^{A-1-n} = 2^{A(1-t)} = 1$ in $\mathbb{F}_p$, since $p - 1 \mid t - 1$. This proves (61).

Evaluating at zero gives $\sum_{j=1}^{t-1} \binom{n}{j} = 0$ in $\mathbb{F}_p$. Substitute $\chi_U = 1 - 2\ell_U$ into (61) to obtain (62). $\square$

The output in (62) is always zero or one in the same fixed field $\mathbb{F}_p$. The growing number $t = p^k$ is a weight-divisibility scale, not the order of the target group.

10.2. The configuration transfer theorem. Let Q be a finite abelian two-group. A finite list $(q_i, a_i)_{i=1}^s$, with $q_i \in Q$ and $a_i \in \mathbb{Z}_{\geq 1}$, will be called an admissible configuration if, for all $(z_1, \dots, z_s) \in \mathbb{Z}^s$,

$$0 \leq z_i \leq a_i \ (1 \leq i \leq s), \quad \sum_i z_i q_i = 0 \implies z_1 = \dots = z_s = 0. \quad (63)$$

Equivalently, the multiset with a_i copies of each q_i is zero-sum-free. The same label may occur in more than one block.

Theorem 10.2 (Transfer from a finite configuration). *Let $P = C_p^v$, where p is an odd prime and $v \in \mathbb{Z}_{\geq 1}$, and suppose $(q_i, a_i)_{i=1}^s$ is admissible in Q , with $1 \leq s \leq v(p - 1)$. For each $k \in \mathbb{Z}_{\geq 1}$, put*

$$A_i = a_i + 1, \quad t = p^k, \quad n_i = A_i t - 1, \quad d_k = \sum_i n_i, \quad R_k = \sum_{i=1}^s \sum_{j=1}^{t-1} \binom{n_i}{j}.$$

There is a zero-sum-free sequence of length $R_k + d_k$ over $Q \oplus P \oplus C_2^{R_k}$. Consequently

$$\bar{\lambda}(Q \oplus P) \geq \frac{\sum_i A_i}{\max_i \{A_i H_2(1/A_i)\}}. \quad (64)$$

Proof. Choose $h_1, \dots, h_s \in P$ forming a zero-sum-free sequence. This is possible by taking a subsequence of the standard sequence with $p-1$ copies of each of v independent generators.

Take independent binary blocks $x^{(i)} \in \mathbb{F}_2^{n_i}$. For each i and every nonempty $U \subseteq [n_i]$ with $|U| < t$, introduce a parity coordinate $y_{i,U} = \ell_U(x^{(i)})$. The resulting graph code

$$V_k = \{(x, Tx) : x \in \mathbb{F}_2^{d_k}\} \subseteq \mathbb{F}_2^{d_k + R_k}$$

has full-rank parity-check matrix $B = [T \mid I_{R_k}]$. Give a systematic coordinate from block i the label $(q_i, 0)$ in $Q \oplus P$, and a parity coordinate from block i the label $(0, 2h_i)$. Attach the corresponding column of B to each label, obtaining a sequence in $Q \oplus P \oplus C_2^{R_k}$.

If a selection has zero binary sum, its parity bits are $y = Tx$. Its odd component is, by Lemma 10.1,

$$\sum_i h_i(1 - b_i(x^{(i)})), \quad b_i(x^{(i)}) = \mathbf{1}_{t|\text{wt}(x^{(i)})}.$$

Each coefficient is zero or one. Since the sequence (h_i) is zero-sum-free, vanishing forces every coefficient to be zero. Thus $\text{wt}(x^{(i)}) = tz_i$ with $0 \leq z_i \leq a_i$. The Q component is $t \sum_i z_i q_i$. Multiplication by the odd integer t is invertible on Q , so (63) gives $z_i = 0$ for every i . Hence $x = 0$ and then $y = 0$. The sequence is zero-sum-free.

For a fixed integer $A \geq 2$, Stirling's formula gives

$$\log \left(\sum_{j=1}^{t-1} \binom{At-1}{j} \right) = At H_2(1/A) + o(t). \quad (65)$$

For $A > 2$, bound the sum between its largest term and At times that term and apply Stirling's formula. For $A = 2$, the sum equals $2^{2t-2} - 1$, giving the same estimate. Since the number of blocks is fixed,

$$d_k = t \sum_i A_i + O(1), \quad \log R_k = t \max_i \{A_i H_2(1/A_i)\} + o(t).$$

The sequence length gives $D(Q \oplus P \oplus C_2^{R_k}) \geq R_k + d_k + 1$. Subtract $D^* = R_k + O_{Q,P}(1)$ and divide by $\log R_k$. This proves (64). $\square$

Definition 10.3 (Finite entropy bound). For a positive integer b , define

$$\mathcal{B}_b(Q) = \max \left(\{0\} \cup \left\{ \frac{\sum_{i=1}^s (a_i + 1)}{\max_i \{(a_i + 1) H_2(1/(a_i + 1))\}} : \begin{array}{l} 1 \leq s \leq b, \\ (q_i, a_i)_{i=1}^s \text{ admissible in } Q \end{array} \right\} \right).$$

This is a finite maximum: every admissible list satisfies $\sum_i a_i \leq D(Q) - 1$, and the labels are chosen in a fixed finite group. Theorem 10.2 gives

$$\bar{\lambda}(Q \oplus C_p^v) \geq \mathcal{B}_{v(p-1)}(Q). \quad (66)$$

This parameter packages a family of lower bounds; it is not asserted to equal the Davenport coefficient.

Example 10.4 (Elementary two-groups). For $Q = C_2^u$, every admissible list has $a_i = 1$ and linearly independent labels. Thus $\mathcal{B}_b(C_2^u) = \min\{u, b\}$. On the other hand, the weighted odd-primary bound and v independent simplex constructions give

$$E_{C_2^u \oplus C_p^v}(r) = v(p-1) \log r + O_{p,u,v}(1).$$

For the lower bound, use $p-1$ simplex blocks in each independent C_p coordinate; their total dimension is $v(p-1)m$, and $m = \log r + O_{p,v}(1)$. For the upper bound absorb C_2^u into the binary rank and use $b_P = v(p-1)$ in Corollary 7.3. In particular (66) need not be sharp.

10.3. The C_{24} family and unbounded coefficient growth.

Corollary 10.5 (An explicit C_{24} lower family). *For each integer $k \geq 1$, put $t = 3^k$ and*

$$n_1 = 5t - 1, \quad n_2 = 4t - 1, \quad R_k = \sum_{j=1}^{t-1} \left(\binom{n_1}{j} + \binom{n_2}{j} \right).$$

Then

$$E_{C_{24}}(R_k) \geq 9 \cdot 3^k - 25, \quad (67)$$

and

$$\bar{\lambda}(C_{24}) \geq \frac{9}{5H_2(1/5)}. \quad (68)$$

Proof. In $Q = C_8$, let q be a generator and take two blocks with $(q_1, q_2) = (q, q)$ and $(a_1, a_2) = (4, 3)$. If $0 \leq z_1 \leq 4$ and $0 \leq z_2 \leq 3$, then $0 \leq z_1 + z_2 \leq 7$. Hence the configuration is admissible. Take $P = C_3$ and $h_1 = h_2$ a generator. Theorem 10.2 gives a zero-sum-free sequence of length $R_k + 9t - 2$. Since $D^*(C_{24} \oplus C_2^{R_k}) = R_k + 24$, this proves (67). The larger of the two entropy exponents is $5H_2(1/5)$, which proves (68). $\square$

Here is the sequence without matrix notation. Let g have order 24, and let $e_{i,U}$, with $i = 1, 2$ and $\emptyset \neq U \subseteq [n_i]$, $|U| < t$, be independent elements of order two. Take the terms

$$9g + \sum_{U \ni j} e_{i,U} \quad (1 \leq j \leq n_i), \quad 8g + e_{i,U} \quad (1 \leq |U| < t), \quad i = 1, 2. \quad (69)$$

The residues 9 and 8 correspond to $(1, 0)$ and $(0, 2)$ under $C_{24} \cong C_8 \oplus C_3$. If the binary sum vanishes, the second type of term is selected exactly according to the relevant parity of the first type. The odd component forces the two block weights to have the form $w_1 = tz_1$ and $w_2 = tz_2$, with $0 \leq z_1 \leq 4$ and $0 \leq z_2 \leq 3$. The C_8 component gives $t(z_1 + z_2) \equiv 0 \pmod{8}$. Since $t = 3^k$ is invertible modulo eight, $z_1 + z_2 \equiv 0 \pmod{8}$. Now $0 \leq z_1 + z_2 \leq 7$ forces $z_1 = z_2 = 0$, and hence both weights vanish.

For orientation, the finite lower estimates are:

k	d_k	$\log_2 R_k$	$9 \cdot 3^k - 25$	$(9 \cdot 3^k - 25) / \log_2 R_k$
2	79	27.932222	56	2.004853
3	241	91.980460	218	2.370069
4	727	286.127990	704	2.460437
5	2185	870.104755	2162	2.484758

These entries illustrate the explicit family; its asymptotic coefficient follows from (65).

Corollary 10.6 (Growing two-primary exponent). *For every odd prime p and integer $a \geq 1$,*

$$\bar{\lambda}(C_{p2^a}) \geq \frac{1}{H_2(2^{-a})}. \quad (70)$$

Proof. Take one block in $Q = C_{2^a}$ with a generator q_1 and $a_1 = 2^a - 1$. This is admissible, and Theorem 10.2 with $P = C_p$ gives (70). The expansion $H_2(\varepsilon) = \varepsilon \log_2(1/\varepsilon) + \varepsilon \log_2 e + O(\varepsilon^2)$ gives (9). $\square$

Proof of Theorem 1.5. Combine Corollary 10.5 with Theorem 9.13 for (8). Corollary 10.6 proves (9). $\square$

Together with Corollary 9.9, the C_{24} example rules out a coefficient formula depending only on the odd primary part. In particular no constant depending on C_8 and C_3 can make $E_{C_{24}}(r) = 2 \log_2 r + O(1)$.

11. LIMITATIONS AND FURTHER QUESTIONS

For $C_3 \oplus C_2^r$, Theorem 1.2 gives numerical equalities on infinitely many explicit rank intervals. Theorem B.1 gives a structural identity at every sufficiently large rank, with two Fourier thresholds still to be evaluated. These are different levels of determination. For general odd p -groups, Theorem 1.1 identifies the logarithmic coefficient $b = D(H) - 1$, but an exact bounded remainder must retain the discrete dependence on r . Indeed, if $D(H \oplus C_2^r) - D^*(H \oplus C_2^r) - b \log_2 r$ converged, its limit along $r = 2^j$ would be an integer, whereas along $r = \lfloor 2^{j+1/(2b)} \rfloor$ it would be a half-integer.

11.1. A necessary loss in degree–sparsity intersection bounds. Theorem 1.3 has a large dependence on D . Some dependence on the binary degree is unavoidable even with a fixed odd output field.

Proposition 11.1 (A cubic obstruction). *There is no constant C such that every pair $a : \mathbb{F}_2^d \rightarrow \mathbb{F}_2$, $b : \mathbb{F}_2^d \rightarrow \mathbb{F}_3$ with $\deg a \leq 3$ and $\{a = 1, b \neq 0\} = \{0\}$ satisfies $d \leq \log_2 \text{sp}(b) + C$. This remains false if b is restricted to the values zero and one.*

Proof. Take $t = 3^k$, $d = 4t - 1$, and let $b(x) = \mathbf{1}_{t|\text{wt}(x)}$. Define the binary polynomial $a(x) = (1 + e_1(x))(1 + e_2(x))$. The functions e_1, e_2 give the lowest two binary digits of $\text{wt}(x)$, so $a(x) = 1$ exactly when $4 \mid \text{wt}(x)$, and $\deg a \leq 3$. The common condition implies $4t \mid \text{wt}(x)$ and therefore $x = 0$. Lemma 10.1 gives

$$\text{sp}(b) = \sum_{j=0}^{t-1} \binom{d}{j}, \quad \frac{\log_2 \text{sp}(b)}{d} \rightarrow H_2(1/4) < 1.$$

Thus $d - \log_2 \text{sp}(b) \rightarrow \infty$. □

More generally, taking the indicator of weight divisible by 2^a gives binary degree at most $2^a - 1$ and sparsity exponent $H_2(2^{-a})$. Thus any universal singleton estimate

$$d \leq C_D \log_2 \text{sp}(b) + O_D(1)$$

must satisfy

$$C_{2^a-1} \geq \frac{1}{H_2(2^{-a})} \quad (a \geq 2).$$

The upper coefficient 2^D and this necessary lower dependence leave a substantial gap. Its study is independent of whether a specific group-valued fiber has extra structure.

11.2. Coefficient limits and optimal constructions. For fixed H with $t(H) = 1$, the threshold theorem places $\underline{\lambda}(H)$ and $\bar{\lambda}(H)$ between positive finite constants. It does not show that they are equal. Theorem 10.2 supplies families along the prime-power scales $t = p^k$; no assertion of a single coefficient limit is needed for these lower bounds.

Three questions arise naturally. First, does the limit $E_H(r)/\log_2 r$ exist for every such H ? Second, how closely does the finite configuration bound $\mathcal{B}_{v(p-1)}(Q)$ approximate the upper limiting coefficient for $H = Q \oplus C_p^v$? Third, can the degree–sparsity intersection bound incorporate more of the two-primary algebra and the odd weight detector, leading to matching upper bounds?

The first concrete case is C_{24} , where the present results give

$$2 \leq \underline{\lambda}(C_{24}) \leq \bar{\lambda}(C_{24}) \leq 32, \quad \bar{\lambda}(C_{24}) \geq 2.4933231062 \dots$$

The lower bound two for the liminf comes from the simplex construction. The larger limsup bound proves that the formula with coefficient two is false, without deciding whether the normalized excess converges.

11.3. More than one odd prime. When $t(H) \geq 2$, the composite-modulus construction proves superlogarithmic growth. Corollary 9.8 gives a sublinear upper bound for cyclic odd H , but matching bounds remain open. The fixed-group program used in Proposition 8.1 then has a normal base involving several odd primes, so the specific class (44) no longer applies through that decomposition. The elementary intersection theorem also controls only one odd-characteristic Fourier condition at a time. A quantitative principle for several odd characteristics would need to account for the composite-modulus singleton constructions.

APPENDIX A. A TRANSFER TO NONABELIAN DAVENPORT CONSTANTS

For a finite group G , let $\mathbf{d}(G)$ be the maximum length of a product-one-free sequence, where selected terms may be reordered. Let $\mathbf{D}(G)$ be the maximum length of an atom in the monoid of product-one sequences. In the abelian case $\mathbf{D}(G) = \mathbf{d}(G) + 1$.

Proposition A.1. *Let K be any fixed finite group whose prime divisors lie in $\{2, p\}$, with p odd. Then*

$$\mathbf{d}(K \times C_2^r) = r + O_K(\log(r+2)), \quad \mathbf{D}(K \times C_2^r) = r + O_K(\log(r+2)).$$

If $p \mid |K|$, both corrections to r are $\Theta_K(\log r)$. No nilpotence assumption on K is needed.

Proof. Define the fixed abelian certificate group

$$B_K = \bigoplus_{g \in K \setminus \{1\}} C_{\text{ord}(g)}.$$

Replace the K -label g of a term by the generator of its own cyclic summand of B_K ; give the identity label certificate zero. A zero-sum subsequence of the certificates uses each nonidentity g a multiple of $\text{ord}(g)$ times. Its K terms can therefore be grouped into identity blocks. If its binary sum vanishes, it is product-one in $K \times C_2^r$. Consequently

$$\mathbf{d}(K \times C_2^r) + 1 \leq \mathbf{D}(B_K \oplus C_2^r).$$

Proposition 9.1 bounds the right-hand side by $r + O_K(\log(r+2))$. The trivial lower bound for the small constant is r , and the subgroup $C_p \leq K$, when present, gives the logarithmic lower bound by Corollary 9.3.

For the large constant, the general inequality

$$\mathbf{d}(G) + 1 \leq \mathbf{D}(G) \leq \mathbf{d}(G) + 2|G'| - 1$$

uses the upper bound of [5, Theorem 3.1]. Since $(K \times C_2^r)' = K'$, the gap is bounded independently of r , proving the remaining assertions. $\square$

APPENDIX B. AN EXACT STRUCTURE FORMULA FOR ALL SUFFICIENTLY LARGE RANKS

The exact transfer can be localized to two adjacent dimensions. The construction needed for this localization is uniform in all sufficiently large even dimensions. The result below retains two unevaluated extremal thresholds; it is not a closed evaluation for all ranks.

Theorem B.1 (Two-threshold localization). *Let $r \geq 15 \cdot 2^{63} - 133$ be an integer, and put*

$$m = \left\lfloor \log_2 \left(\frac{8}{15} (r + 2 \log_2 r) \right) \right\rfloor.$$

Then

$$\begin{aligned} \mathbf{D}(C_3 \oplus C_2^r) &= r + 2m + 1 \\ &\quad + \mathbf{1}_{\{\nu(2m+1) \leq r+2m+2\}} \\ &\quad + \mathbf{1}_{\{\nu(2m+2) \leq r+2m+3\}}. \end{aligned} \tag{71}$$

The indicators retain two unevaluated extremal thresholds. Their sum is zero, one, or two, and each determines the exact feasible increment. The sufficient cutoff is explicit and is not optimized. The proof uses a construction valid in every sufficiently large even dimension.

Theorem B.2 (Uniform even-dimensional construction). *For every integer $M \geq 66$, there is a function $f : \mathbb{F}_2^{2M} \rightarrow \mathbb{F}_3$ whose zero set is $\{0\}$ and whose nonzero Fourier coefficients are all equal to one, with*

$$|\text{supp } \widehat{f}| = 15 \cdot 2^{M-3}.$$

In particular, $\nu(2M) \leq 15 \cdot 2^{M-3}$.

B.1. A construction from finite-field lines. For a finite subset T of a binary vector space, put

$$U_T(x) = \sum_{t \in T} (-1)^{\langle t, x \rangle} \quad \text{in } \mathbb{F}_3.$$

We will use finite sets T satisfying

$$U_T(x) \neq 0 \quad \text{for every character } x. \quad (72)$$

Singletons satisfy (72), as do translates of $W \setminus \{0\}$ when W has odd dimension. Indeed, the latter character sums, up to sign, are $2^{\dim W} - 1$ and -1 , both nonzero modulo three. Cartesian products and translations preserve (72).

Lemma B.3 (Extension using finite-field lines). *Let $j \in \mathbb{Z}_{\geq 1}$ and $q = 2^j$. Suppose $S \subseteq V$ has $U_S^{-1}(0) = \{0\}$ and admits a disjoint partition into $q + 1$ sets $T_0, \dots, T_q$ satisfying (72). Then there is such a support in dimension $\dim V + 2j$ of size $q|S|$.*

Proof. Let $L_0, \dots, L_q$ be the one-dimensional $\mathbb{F}_q$ -subspaces of $\mathbb{F}_q^2$, viewed as binary j -spaces, and set

$$S' = \bigsqcup_{i=0}^q (T_i \times L_i).$$

The annihilators $L_i^\perp$ also partition the nonzero dual vectors. Indeed, distinct L_i span $\mathbb{F}_q^2$, so their annihilators meet only at zero; counting $(q+1)(q-1) = q^2 - 1$ nonzero vectors proves the claim. At a character $(x, 0)$ the sum is $qU_S(x)$. At (x, y) with $y \neq 0$, exactly one annihilator contains y , and the sum is $qU_{T_i}(x)$. Since q is invertible in $\mathbb{F}_3$, the unique zero is $(0, 0)$. The partition is disjoint because the T_i are disjoint. $\square$

B.2. An eight-dimensional example. Take independent binary three-spaces X, Y , and a binary two-space Z with distinct nonzero vectors ℓ_0, ℓ_1, ℓ_2 . In $X \oplus Y \oplus Z$ put

$$S = \{0, \ell_0\} \sqcup \{x, x + \ell_1 : 0 \neq x \in X\} \sqcup \{y, y + \ell_2 : 0 \neq y \in Y\}.$$

This set has thirty points, and U_S vanishes only at zero: apply Lemma B.3 with $q = 2$ to $X \cup Y$, partitioned as $\{0\}, X \setminus 0, Y \setminus 0$. The character sum of $X \cup Y$ is $8\mathbf{1}_{x=0} + 8\mathbf{1}_{y=0} - 1$, which has precisely one zero modulo three.

The sets $Y \setminus 0$ and $(Y \setminus 0) + \ell_2$ are disjoint seven-point sets in S satisfying (72). Let $V_X = X \oplus \langle \ell_1 \rangle$. For a basis x_1, x_2, x_3 of X , define

$$E = (\langle x_1, x_2 \rangle \setminus 0) \sqcup (\langle x_3, \ell_1 \rangle \setminus 0).$$

The character sum of this six-point set vanishes only at zero in V_X , since it equals $4\mathbf{1}_{\xi=0} + 4\mathbf{1}_{\eta=0} - 2$. It contains ℓ_1 , whereas $S \cap V_X = V_X \setminus \{\ell_1\}$. Thus $T = V_X \setminus E$ is a ten-point subset of S . It satisfies (72): at the trivial restricted character its sum is $16 - 6 = 10$, and elsewhere its sum is $-U_E \neq 0$. The two seven-point sets and T leave six singleton points. We have therefore partitioned S into nine parts, each satisfying (72), of sizes

$$10, 7, 7, 1, 1, 1, 1, 1, 1.$$

B.3. Refining the partition and covering all large even dimensions. Suppose $q = 2^j$, with $j \geq 3$ odd, and $U_S^{-1}(0) = \{0\}$. Assume S has a partition into $q + 1$ parts satisfying (72), including distinct parts T_a, T_b, T_c of sizes seven, seven, and ten. The extension in Lemma B.3 admits partitions into both $4q + 1$ and $16q + 1$ parts satisfying (72). The three parts $T_a \times \{0\}, T_b \times \{0\}, T_c \times \{0\}$ remain in each partition.

For the first transition, initially partition each product into

$$T_i \times \{0\}, \quad T_i \times (L_i \setminus 0).$$

These satisfy (72) because j is odd, and there are $2(q + 1)$ pieces. Choose a three-space $W \subseteq L_a$ and replace the nonzero layer of T_a by $T_a \times (W \setminus 0)$ and the $q - 8$ translates $T_a \times \{z\}$ for $z \in L_a \setminus W$; this adds $q - 8$ pieces. Replace the nonzero layer of T_c by its $q - 1$ translates, adding $q - 2$ pieces, and split one ten-point translate into singletons, adding nine. The total is

$$2(q + 1) + (q - 8) + (q - 2) + 9 = 4q + 1.$$

For the second transition, start with the same $2(q + 1)$ pieces. Refine $T_i \times (L_i \setminus 0)$ for $i = a, b, c$ into translates, obtaining $5q - 4$ pieces. There are $2(q - 1)$ seven-point translates and $q - 1$ ten-point translates. Split

$$N_7 = \frac{11q - 4}{6}$$

of the seven-point translates and one ten-point translate into singletons. Here N_7 is an integer because $q \equiv 2 \pmod{6}$, and $0 \leq N_7 \leq 2(q - 1)$ because $q \geq 8$. The resulting count is

$$5q - 4 + 6N_7 + 9 = 16q + 1.$$

In both cases, $T_a \times \{0\}, T_b \times \{0\}, T_c \times \{0\}$ remain intact. Every operation preserves (72) for each part and preserves disjointness.

Starting with the eight-dimensional example and $j_0 = 3$, the next extension exponent can consequently be chosen as $j_i + 2$ or $j_i + 4$. After $k \geq 1$ extensions the attainable half-dimensions are exactly

$$\left\{ M : k^2 + 2k + 4 \leq M \leq 2k^2 + k + 4, \quad M \equiv k \pmod{2} \right\}.$$

Indeed,

$$M = k^2 + 2k + 4 + 2 \sum_{i=0}^{k-2} (k - 1 - i) \epsilon_i, \quad \epsilon_i \in \{0, 1\},$$

and the subset sums of $1, \dots, k - 1$ fill the interval from zero to $k(k - 1)/2$. The step-two intervals for k and $k + 2$ meet once

$$(2k^2 + k + 4) + 2 - ((k + 2)^2 + 2(k + 2) + 4) = (k - 6)(k + 1) \geq 0.$$

They cover every even $M \geq 52$ and every odd $M \geq 67$, hence every $M \geq 66$. Each extension multiplies the support size by 2^j and increases the half-dimension by j . The final size is therefore $30 \cdot 2^{M-4} = 15 \cdot 2^{M-3}$. This proves Theorem B.2.

B.4. Proof of the large-rank formula. We first record the monotonicity used to pass from feasibility of a dimension to feasibility of the preceding one. For $d \geq 2$, choose f attaining $\nu(d)$. Then $f^2 = 1 - \delta_0$. Every nonconstant Fourier coefficient of this square equals $-2^{-d} \neq 0$, so the support of $\hat{f}$ contains a pair differing by any prescribed nonzero direction h . Upon restriction to $h^\perp$, the coefficients indexed by u and $u + h$ are replaced by their sum. At least one pair of nonzero coefficients is thereby replaced by at most one nonzero coefficient. The restricted function still has zero set $\{0\}$. Hence

$$\nu(d - 1) \leq \nu(d) - 1, \quad t_{d-1} \leq t_d, \quad t_d = \nu(d) - d - 1.$$

Put

$$A_m = \frac{15}{8}2^m - 2m - 1.$$

The sequence A_m is strictly increasing for $m \geq 5$. For integer $r \geq A_{66}$ the unique integer $m \geq 66$ with $A_m \leq r < A_{m+1}$ is

$$m = \left\lfloor \log_2 \left(\frac{8}{15}(r + 2 \log_2 r) \right) \right\rfloor.$$

Here is a direct check of the rounding. The function $r + 2 \log_2 r$ is increasing. For $m \geq 5$, $A_m \geq (49/32)2^m > \sqrt{2}2^m$, so $A_m + 2 \log_2 A_m \geq (15/8)2^m$. On the other side, $A_m - 1 < 2^{m+1}$ implies

$$A_m - 1 + 2 \log_2(A_m - 1) < (15/8)2^m.$$

These two inequalities identify every integer boundary exactly.

Theorem B.2 makes dimension $2m$ feasible in (29). Dimension $2m+3$ is impossible: Corollary 5.2, with $s = m+1$, gives

$$\nu(2m+3) > \frac{8}{\sqrt{3}}2^m,$$

whereas integer $r < A_{m+1}$ implies $r + 2m + 4 \leq (15/4)2^m$. Monotonicity excludes all higher dimensions. The feasible maximum thus belongs to $\{2m, 2m+1, 2m+2\}$, and the last dimension is feasible only if the preceding one is feasible. Consequently

$$D(C_3 \oplus C_2^r) = r + 2m + 1 + \mathbf{1}_{\{\nu(2m+1) \leq r+2m+2\}} + \mathbf{1}_{\{\nu(2m+2) \leq r+2m+3\}}.$$

This proves Theorem B.1. The two indicators retain the unevaluated extremal thresholds; the formula is an exact structural identity, and the construction does not assert equality in $\nu(2M) \leq 15 \cdot 2^{M-3}$.

REFERENCES

- [1] D. A. M. Barrington, R. Beigel, and S. Rudich, *Representing Boolean functions as polynomials modulo composite numbers*, Comput. Complexity **4** (1994), 367–382. doi:10.1007/BF01263424.
- [2] J. Brakensiek, S. Gopi, and V. Guruswami, *Constraint satisfaction problems with global modular constraints: algorithms and hardness via polynomial representations*, SIAM J. Comput. **51** (2022), no. 3, 577–626. doi:10.1137/19M1291054. Preprint version: arXiv:1902.04740v1.
- [3] W. T. Gowers, B. Green, F. Manners, and T. Tao, *Marton’s conjecture in abelian groups with bounded torsion*, preprint, 2024. arXiv:2404.02244v2.
- [4] R. L. Graham and N. J. A. Sloane, *On the covering radius of codes*, IEEE Trans. Inform. Theory **31** (1985), no. 3, 385–401. Author’s copy.
- [5] D. J. Gryniewicz, *The large Davenport constant II: general upper bounds*, preprint, 2012. arXiv:1211.2614.
- [6] D. Han and H. Zhang, *Davenport constants of finite abelian groups*, preprint, 2026. arXiv:2610.15102v1.
- [7] P. M. Idziak, P. Kawałek, J. Krzaczkowski, and A. Weiß, *Satisfiability problems for finite groups*, in 49th International Colloquium on Automata, Languages, and Programming (ICALP 2022), LIPIcs **229**, article 127, 127:1–127:20. doi:10.4230/LIPIcs.ICALP.2022.127.
- [8] S. A. Jennings, *The structure of the group ring of a p -group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175–185. doi:10.2307/1989916.
- [9] C. Liu, *On the lower bounds of Davenport constant*, J. Combin. Theory Ser. A **171** (2020), article 105162. doi:10.1016/j.jcta.2019.105162.
- [10] J. E. Olson, *A combinatorial problem on finite Abelian groups, I*, J. Number Theory **1** (1969), 8–10. doi:10.1016/0022-314X(69)90021-3.
- [11] A. Plagne and W. A. Schmid, *An application of coding theory to estimating Davenport constants*, Des. Codes Cryptogr. **61** (2011), 105–118. arXiv:1007.0259.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MISSISSIPPI
 Email address: chaoliuac@gmail.com