hexagon:2611.00889v2

# Integral zero-sum incidence identities and Davenport constants in rank three

Claudiu G. Pop* George C. Rad George C. Ţurcaş†

November 22, 2026

**Abstract**

We study the Davenport constant of finite abelian groups through signed identities among zero-sum subsequences. An integral incidence identity of degree $t$ for a sequence assigns integer weights to its nonempty zero-sum subsequences so that the weights add up to one, while those of the subsequences containing any given nonempty set of at most $t$ terms add up to zero. Over a finite abelian $p$-group $H$, the zero-sum subsequences of a sequence of any length have an indicator polynomial of degree at most $\mathsf{D}(H)-1$, and this gives a transfer principle: if, for each $t \ge 0$, every sequence of $L(t)$ terms over $Q$ admits such an identity of degree $t$, then $\mathsf{D}(Q \oplus H) \le L(\mathsf{D}(H)-1)$ for every finite abelian $p$-group $H$. For $m \in \{2,3,4\}$ we construct integral identities at length $L(t) = m(t+3)-2$ over $C_m^3$, and prove that these thresholds are sharp over fields of characteristic zero or characteristic not dividing $m$. For a prime $p \nmid m$ and $0 \le a \le b \le c$, we prove that

$$\mathsf{D}(C_{mp^a} \oplus C_{mp^b} \oplus C_{mp^c}) = m(p^a + p^b + p^c) - 2.$$

In particular $\mathsf{D}(C_{15}^3) = 43$ and $\mathsf{D}(C_{20}^3) = 58$, which are the two smallest cases of the conjecture $\mathsf{D}(C_n^3) = 3n-2$ left open in the literature. The proofs of the base cases for $m \in \{3,4\}$ are computer-assisted. All of the results in this paper have been formalised in Lean 4.

## 1 Introduction

Let $G$ be a finite abelian group, written additively. A *sequence* over $G$ is a finite list of elements of $G$ in which repetitions are allowed, and the *Davenport constant* $\mathsf{D}(G)$ is the least integer $L$ such that every sequence of $L$ terms over $G$ has a nonempty subsequence with sum zero. If

$$G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}, \qquad 1 < n_1 \mid \cdots \mid n_r,$$

then $n_i - 1$ copies of each basis element form a zero-sum free sequence, so

$$\mathsf{D}(G) \;\ge\; \mathsf{D}^*(G) := 1 + \sum_{i=1}^{r} (n_i - 1).$$

Olson proved that equality holds for $p$-groups and for groups of rank at most two [16, 17]. Equality fails for infinitely many groups of rank four [11, 8]. In rank three, it is conjectured that

$$\mathsf{D}(C_{n_1} \oplus C_{n_2} \oplus C_{n_3}) = n_1 + n_2 + n_3 - 2 \qquad (1 < n_1 \mid n_2 \mid n_3). \tag{1.1}$$

For background on the conjecture, see [7, 8, 19, 10]. In this paper, we develop a method for attacking particular cases of this conjecture. We write the group as $Q \oplus H$ with $H$ a $p$-group,

*Mathematical Institute, Master ALGANT, Université de Bordeaux, 351 cours de la Libération, 33405 Talence, France. E-mail: popclaudiu38@gmail.com

†Faculty of Mathematics and Computer Science, Babeş-Bolyai University, Cluj-Napoca, Romania. E-mails: george.ciprian.rad@stud.ubbcluj.ro, george.turcas@ubbcluj.ro

and read a sequence over it as a sequence over the *quotient* $Q$ whose terms carry labels in the *kernel* $H$. We first study identities among the zero-sum subsequences of sequences over a small quotient, and then use those identities for arbitrary labels in a $p$-group kernel.

Our method allows us to prove the conjecture (1.1) for infinitely many mixed-prime groups of rank three with a quotient $C_3^3$ or $C_4^3$, and the values it produces include the two smallest cases of (1.1) for $C_n^3$ that the classical theory leaves open, $n = 15$ and $n = 20$.

**The inductive method.** The standard way to bound $\mathsf{D}(G)$ from above when $G$ is not a $p$-group reduces the question to two smaller groups, a subgroup $H$ and the quotient $Q = G/H$. It goes back to the earliest work on the subject [17, 20], and is known in the zero-sum literature as the *inductive method* [19, Section 3], [3, 14]. A zero sum in a quotient need not be a zero sum in the original group. Project a sequence over $G$ to $Q$, and call a subsequence a *block* if its projection has sum zero. Each block has a sum in $H$; if we can find $\mathsf{D}(H)$ pairwise disjoint blocks, some nonempty collection of their sums adds to zero in $H$, and the union of those blocks is a zero sum in $G$ [5, Proposition 2.6].

Short blocks make this argument efficient. Write $\eta(Q)$ for the least length such that every sequence over $Q$ of that length contains a nonempty zero-sum subsequence of length at most $\exp(Q)$. Extracting short blocks successively gives, in particular,

$$\mathsf{D}(Q \oplus H) \le \eta(Q) + (\mathsf{D}(H) - 1)\exp(Q). \tag{1.2}$$

The same estimate holds for $G$ in the extension above.

The last block need not be short, and this improves the count. With $\mathsf{D}(H) \ge 2$, extract $\mathsf{D}(H) - 1$ short blocks and then one arbitrary zero-sum block. This requires at most

$$\max\{\eta(Q) + (\mathsf{D}(H) - 2)\exp(Q),\ \mathsf{D}(Q) + (\mathsf{D}(H) - 1)\exp(Q)\}$$

terms. The first expression ensures that the last short block can be extracted; the second ensures that a final zero sum remains. The maximum is the second expression precisely when

$$\eta(Q) \le \mathsf{D}(Q) + \exp(Q).$$

For $Q = C_p^2$, the values $\eta(Q) = 3p - 2$ and $\mathsf{D}(Q) = 2p - 1$ satisfy this inequality [17, 8]; this is the count that makes the inductive method exact in rank two. For $Q = C_3^3$ and $Q = C_4^3$, however, the comparison is $17 > 7 + 3$ and $22 > 10 + 4$, respectively [9, 15]. For the groups $C_m^3 \oplus H$ studied below, the second expression is the basis lower bound, so for $m = 3, 4$ the count overshoots it. Nor is the loss due to the insistence on short blocks: ten terms over $C_3^3$ need not contain two disjoint blocks of any size (Appendix A), although $\mathsf{D}(C_3^3 \oplus C_2) = 10$.

Once disjoint blocks have been chosen, this argument uses only their sums in $H$. It forgets the other zero sums of the projection and the ways in which they overlap. Our approach keeps that incidence information and combines the zero sums with signed weights.

**Incidence identities.** We regard sequences as indexed, so equal group elements at different positions are considered different terms, since the kernel labels attached to those positions may differ. For $U = (u_1, \dots, u_N)$ over $G$, write

$$\mathcal{Z}(U) = \{\, \varnothing \ne E \subseteq [N] : \textstyle\sum_{j \in E} u_j = 0 \,\}$$

for the family of its *zero sets*, and let $\mathbf{1}_E \in \{0,1\}^N$ be the incidence vector of $E$.

Let $t$ be a non-negative integer, and let $R$ be a commutative ring with identity. An *incidence identity of degree $t$ over $R$*, or *$\mathcal{I}_t$-identity*, is a family $(c_E)_{E \in \mathcal{Z}(U)}$ of elements of $R$ satisfying

$$\sum_E c_E = 1, \qquad \sum_{E \supseteq J} c_E = 0 \quad \text{for every } J \subseteq [N] \text{ with } 1 \le |J| \le t. \tag{1.3}$$

The sum indexed by $J$ is the *moment* at $J$. Thus the weights add to one, but the weights through any prescribed nonempty set of at most $t$ positions cancel. We say the identity is *integral* when $R = \mathbb{Z}$.

For example, if $B$ and $C$ are disjoint nonempty zero sets, give weights $1, 1, -1$ to $B, C, B \cup C$, respectively. The total weight is one, and the total through each individual position is zero. These are exactly the conditions for degree one.

The polynomial meaning is the reason for requiring all these cancellations. On Boolean inputs, the monomial $\prod_{j \in J} z_j$ records whether a set contains every position of $J$. Consequently (1.3) is equivalent to

$$\sum_E c_E P(\mathbf{1}_E) = P(0) \quad \text{for every polynomial } P \text{ of degree at most } t.$$

We prove this in Lemma 2.1. The empty subsequence receives no weight; nevertheless, these signed evaluations reproduce its value for every polynomial of the indicated degree.

For an abelian $p$-group $H$, the test for a selected set of kernel labels to have sum zero is such a polynomial over $\mathbb{F}_p$: its degree is at most $\mathsf{D}(H) - 1$, independently of the number of labels (Lemma 3.1). An identity of this degree for the sequence over the quotient can therefore be evaluated at the kernel's zero-sum test, and this gives the transfer principle.

**Theorem A** (Transfer principle)**.** Let $Q$ be a finite abelian group, let $p$ be a prime, and let $L(0), L(1), L(2), \ldots$ be integers such that every sequence of $L(t)$ terms over $Q$ has an $\mathcal{I}_t$-identity over $\mathbb{F}_p$. Then

$$\mathsf{D}(Q \oplus H) \;\le\; L\big(\mathsf{D}(H) - 1\big) \qquad \text{for every finite abelian } p\text{-group } H.$$

If the identities are integral, the conclusion holds for every prime $p$.

To see the mechanism, let $P$ be the zero-sum indicator for the kernel labels and evaluate the quotient identity at $P$. The result is

$$1 = P(0) = \sum_E c_E P(\mathbf{1}_E).$$

Some summand is nonzero, so some nonempty zero set in the quotient also has sum zero in the kernel. For a fixed degree, the weights depend only on the quotient sequence; the same identity works for every choice of kernel labels. Integer weights can be reduced modulo any prime, which makes a single certificate useful for many different kernels.

Over a field $K$, the alternative to an $\mathcal{I}_t$-identity is a *separator of degree at most* $t$: a polynomial $P$ of degree at most $t$ such that $P(0) = 1$ and $P(\mathbf{1}_E) = 0$ for every $E \in \mathcal{Z}(U)$. Lemma 2.1 shows that exactly one of these alternatives occurs. We write $\kappa_t(G; K)$ for the least $N$ such that no sequence of $N$ terms over $G$ has a separator of degree at most $t$. In degree zero the only possible separator is the constant polynomial 1, which works exactly when there is no nonempty zero sum. Thus $\kappa_0(G; K) = \mathsf{D}(G)$.

**The quotient hierarchy.** For $Q = C_m^3$ and $H = C_{p^a} \oplus C_{p^b} \oplus C_{p^c}$ with $p \nmid m$, Olson's theorem and the Chinese remainder theorem give

$$\mathsf{D}^*(C_m^3 \oplus H) = m(\mathsf{D}(H) - 1) + 3m - 2.$$

This singles out the target length $L_m(t) = mt + 3m - 2 = m(t + 3) - 2$: a quotient identity at this length has exactly the degree and length needed to reach the basis lower bound after transfer.

**Theorem B.** Let $m \in \{2, 3, 4\}$ and let $t \ge 0$ be an integer. Every indexed sequence of $m(t+3)-2$ terms over $C_m^3$ has an integral $\mathcal{I}_t$-identity. Consequently $\kappa_t(C_m^3; K) \le m(t + 3) - 2$ for every field $K$, with equality whenever the characteristic of $K$ is zero or does not divide $m$.

The $m = 2$ case gives a small geometric model of the argument: a signed identity on the Fano plane with one point removed. For $m = 3$ and $m = 4$, finite computations supply the base cases, and the three constructions of Lemma 2.2 propagate them to all degrees.

Combining Theorems A and B gives $\mathsf{D}(C_m^3 \oplus H) \le m(\mathsf{D}(H) - 1) + 3m - 2$ for every finite abelian $p$-group $H$. When $H$ has rank at most three and $p \nmid m$, the right-hand side is the basis lower bound, giving the following consequence.

**Corollary C.** Let $m \in \{2, 3, 4\}$, let $p$ be a prime with $p \nmid m$, and let $0 \le a \le b \le c$ be integers. Then

$$\mathsf{D}(C_{mp^a} \oplus C_{mp^b} \oplus C_{mp^c}) = m(p^a + p^b + p^c) - 2. \tag{1.4}$$

In particular $\mathsf{D}(C_{3p^a}^3) = 9p^a - 2$ for $p \ne 3$ and $\mathsf{D}(C_{4p^a}^3) = 12p^a - 2$ for odd $p$.

For example, $\mathsf{D}(C_{15}^3) = 43$. As $C_{15}^3 \simeq C_3^3 \oplus C_5^3$ and $\mathsf{D}(C_5^3) = 13$, the classical estimate (1.2) only gives the upper bound 53.

Trivial kernel factors are allowed, with $C_{p^0} = C_1$. When $p \mid m$, the rank-three groups displayed in (1.4) are themselves $p$-groups, and their Davenport constants are already given by Olson's theorem.

**Earlier work and our contribution.** Corollary C includes classical families: the doubled $p$-groups and tripled 2-groups of van Emde Boas and Kruyswijk [20, 21], as well as special cases covered by later rank-three results [4, 3, 19, 14]. For $C_n^3$ earlier work covers, besides the prime powers, the exponents $n = 2p^a$ and $n = 3 \cdot 2^a$ [19, 13], but not $n = 3p^a$ or $n = 4p^a$ with $p \ge 5$.[1]

The group-algebra input goes back to Olson, and polynomial methods have a substantial history in zero-sum theory [16, 1]. Finite computational input to the inductive method also occurs in the work of Bhowmik, Halupczok and Schlage-Puchta [3]. Related signed zero-block and moment methods occur in Volkmann's work on nonabelian groups of exponent three [22, 23, 24]. Here we establish complete incidence identities over the integers, throughout the degree hierarchy for three small quotients. The transfer principle explains how those identities control arbitrary labels in an abelian $p$-group kernel, while integrality supplies a common certificate in every characteristic.

**Scope.** The bounded-degree indicator in Theorem A uses a $p$-group kernel. Remark 3.3 explains why a degree bound independent of the number of labels fails for other kernels in characteristic $p$. If $n$ has at least three distinct prime divisors, separating off one primary component of $C_n^3$ leaves a quotient $C_m^3$ with at least two prime divisors. An incidence hierarchy at length $m(t+3)-2$ for such a quotient would already include the Davenport conjecture for that quotient in degree zero. Deleting short zero sets, as in Section 5, reduces a proposed hierarchy to finitely many base degrees for each fixed $m$; establishing those base cases is still a mathematical task.

**Organisation.** Section 2 develops the identities and their three constructions. Section 3 proves the transfer principle, and Section 4 gives the lower bound. Section 5 establishes the quotient hierarchies and Section 6 is dedicated to the proof of the announced Davenport values. Section 7 records the computational dependencies and the formal verification, with the coverage arguments and certificate specifications in Appendix A.

**AI disclosure.** Large language models (OpenAI's Codex and ChatGPT, Anthropic's Claude) were used in an essential way for this work: in the exploration that led to the incidence identities, which play a key role in the main results of this paper, in coding the enumeration programs, in writing and revising the exposition and the proofs, and in a substantial part of the Lean

[1] A remark preceding [12, Theorem 6.6] lists $n = 3p^a$ among the known cases, citing [19, Section 4]. The tripling result recalled there requires a group of even order and gives $n = 3 \cdot 2^a$; we know of no proof for $p \ge 5$.

formalisation. The authors made a significant effort to improve the exposition of the AI-produced mathematics and to give proper credit to prior work that uses similar ideas. Every argument was check independently by at least one author and the author take full responsibility for the paper.

## 2 Incidence identities and three constructions

For a sequence $U = (u_1, \dots, u_N)$ write $\sigma(U) = \sum_{j=1}^{N} u_j$; the notation $x^k$ denotes $k$ occurrences of $x$. A subsequence is specified by its set of positions.

**Lemma 2.1.** *Let $(c_E)$ be a family of elements of $R$ indexed by $\mathcal{Z}(U)$.*

1. *$(c_E)$ is an $\mathcal{I}_t$-identity over $R$ if and only if*

$$\sum_{E \in \mathcal{Z}(U)} c_E \, P(\mathbf{1}_E) = P(0) \tag{2.1}$$

   *for every polynomial $P \in R[z_1, \dots, z_N]$ of degree at most $t$.*

2. *An $\mathcal{I}_t$-identity over $\mathbb{Z}$ is an $\mathcal{I}_t$-identity over every commutative ring, by reduction of the coefficients.*

3. *If $R = K$ is a field, $U$ has an $\mathcal{I}_t$-identity over $K$ if and only if $U$ has no separator of degree at most $t$ over $K$.*

*Proof.* Both sides of (2.1) are linear in $P$. On Boolean inputs, every polynomial agrees with a multilinear polynomial of no greater degree, so it is enough to test the monomials $z_J = \prod_{j \in J} z_j$ with $|J| \le t$, including $z_\varnothing = 1$. For these monomials the equality is $\sum_{E \supseteq J} c_E = [J = \varnothing]$, exactly the moment conditions.

Part (2) is clear, because we always have a ring morphism $\mathbb{Z} \to R$.

For (3), consider the vectors $m_E = (\mathbf{1}_E{}^J)_{|J| \le t} \in K^{\binom{N}{\le t}}$ of monomial values, for $E \in \mathcal{Z}(U)$, and the vector $m_\varnothing = (1, 0, \dots, 0)$ of the empty set. Observe that an identity is an expression of $m_\varnothing$ as a linear combination of the $m_E$, and a separator is a linear functional vanishing on all $m_E$ and equal to 1 on $m_\varnothing$. Over a field, either $m_\varnothing$ belongs to the span of the vectors $m_E$, or there is a linear functional vanishing on that span and taking the value 1 at $m_\varnothing$. The first alternative gives the identity; the second gives the separator. □

An identity on a subsequence extends to the full sequence by assigning zero weight to the other zero sets. Conversely, a separator for the full sequence restricts to one for a subsequence by setting the omitted coordinates to zero. Thus existence of an identity, and absence of a separator, are inherited by longer sequences. The invariant $\kappa_t$ is finite: $(t+1)\mathsf{D}(G)$ terms contain $t+1$ disjoint zero sets, and Lemma 2.2(1) supplies an identity.

The identities that Section 5 obtains by computer are stored with integer weights. Reducing their coefficients modulo $p$ gives the identities needed for Theorem A, so one exact certificate check serves every characteristic. Solvability over each field separately would give neither the integral assertion of Theorem B nor such a common certificate.

We use three ways to build identities. Disjoint zero sets give inclusion–exclusion. Adjoining a disjoint zero set turns a finite difference into an identity of one higher degree. Taking complements inside a zero set cancels the highest-degree terms in a different way.

**Lemma 2.2** (Three constructions)**.** *Let $U$ be an indexed sequence and $t \ge 0$. The following produce integral $\mathcal{I}_t$-identities for $U$ from integral identities of lower degree.*

1. *If $U$ has $t+1$ pairwise disjoint zero sets, then $U$ has an $\mathcal{I}_t$-identity.*

2. *Let $t \geq 1$. If $B \in \mathcal{Z}(U)$ and a subsequence of $U$ disjoint from $B$ has an $\mathcal{I}_{t-1}$-identity, then $U$ has an $\mathcal{I}_t$-identity.*

3. *Let $t \geq 1$. If $Z \in \mathcal{Z}(U)$ and a proper subsequence $T \subsetneq Z$ has an $\mathcal{I}_{t-1}$-identity, then $U$ has an $\mathcal{I}_t$-identity.*

*Proof.* For (1), let $B_1, \ldots, B_{t+1}$ be disjoint nonempty zero sets. Give the union of every nonempty collection of $k$ blocks the weight $(-1)^{k+1}$, and give every other zero set weight zero. Distinct collections have distinct unions. If a nonempty set $J$ of at most $t$ positions is contained in such a union, it misses some block $B_i$. The collections whose union contains $J$ are paired by adding or removing $B_i$, with opposite weights. Thus every required nonconstant moment vanishes. The total weight is $\sum_{k=1}^{t+1}(-1)^{k+1}\binom{t+1}{k} = 1$.

For (2), let $(c_E)$ be the identity of degree $t-1$ on a subsequence $U'$ disjoint from $B$. Define new weights by

$$d_E = c_E, \qquad d_{E \cup B} = -c_E \quad (E \in \mathcal{Z}(U')), \qquad d_B = 1,$$

and set the remaining weights to zero. These sets are nonempty zero sets and are pairwise distinct. Let $P$ be multilinear of degree at most $t$. Restricting to the coordinates outside $B$, the polynomial

$$P(z + \mathbf{1}_B) - P(z)$$

has degree at most $t-1$. Indeed, terms involving no coordinate of $B$ cancel, and each remaining term has spent at least one degree on a coordinate of $B$. Applying the old identity gives

$$\sum_{E \in \mathcal{Z}(U')} c_E\big(P(\mathbf{1}_{E \cup B}) - P(\mathbf{1}_E)\big) = P(\mathbf{1}_B) - P(0).$$

Rearranging yields $\sum_F d_F P(\mathbf{1}_F) = P(0)$.

For (3), let $(c_E)$ be the identity on $T \subsetneq Z$, and put $s = (-1)^t$. Give weight $c_E$ to $E$, weight $-sc_E$ to $Z \setminus E$, and weight $s$ to $Z$, with zero weights elsewhere. The complements are nonempty zero sets. The assigned sets are distinct: each complement contains $Z \setminus T$, whereas each $E$ lies in $T$; and $Z$ is neither an $E$ nor the complement of a nonempty $E$. Restrict a multilinear polynomial $P$ of degree at most $t$ to the coordinates of $Z$. Then

$$R_P(z) = P(z) - sP(\mathbf{1}_Z - z)$$

has degree at most $t-1$: complementation multiplies each degree-$t$ term by $(-1)^t$, so the degree-$t$ parts cancel. Applying the identity on $T$ to $R_P$ and rearranging gives

$$\sum_E c_E P(\mathbf{1}_E) - s\sum_E c_E P(\mathbf{1}_{Z \setminus E}) + sP(\mathbf{1}_Z) = P(0).$$

All three constructions use only addition and subtraction of coefficients, so they preserve integrality. □

## 3 The transfer principle

For a cyclic kernel $H = C_p$, identified with the additive group of $\mathbb{F}_p$, the required indicator is familiar. Fermat's theorem gives

$$P(z) = 1 - \Big(\sum_j v_j z_j\Big)^{p-1}.$$

At a Boolean vector $z = \mathbf{1}_E$, this is 1 precisely when $\sum_{j \in E} v_j = 0$, and it has degree at most $p-1$, however many labels there are. Multiplying one such factor for each coordinate gives the same phenomenon for $C_p^r$. The next lemma extends it to arbitrary abelian $p$-groups, including cyclic factors of order $p^a$.

**Lemma 3.1.** *Let $H = \bigoplus_{i=1}^{r} C_{p^{a_i}}$ and $M = \sum_i (p^{a_i} - 1)$. For arbitrary $v_1, \dots, v_N \in H$, the Boolean function*

$$f(z) = \mathbf{1}_{\{\sum_j z_j v_j = 0\}} \in \mathbb{F}_p, \qquad z \in \{0,1\}^N,$$

*is represented by a multilinear polynomial over $\mathbb{F}_p$ of degree at most $M$.*

*Proof.* Write $X^h$ for the basis element of $\mathbb{F}_p[H]$ indexed by $h \in H$, so that $X^a X^b = X^{a+b}$. Choose generators $e_i$ of the cyclic factors, with $e_i$ of order $p^{a_i}$, and put $Y_i = X^{e_i} - 1$. Then

$$\mathbb{F}_p[H] \simeq \mathbb{F}_p[Y_1, \dots, Y_r]/(Y_1^{p^{a_1}}, \dots, Y_r^{p^{a_r}}),$$

and the augmentation ideal $I = (Y_1, \dots, Y_r)$ satisfies $I^{M+1} = 0$, since a monomial of total degree $M+1$ in the $Y_i$ has some exponent at least $p^{a_i}$. Now we consider the multilinear polynomial

$$P(z) = [X^0] \prod_{j=1}^{N} (1 + z_j (X^{v_j} - 1)),$$

where $[X^0]$ extracts the identity coefficient in the group basis. Multiplication records the selected sum: setting $z_j = 0$ omits $v_j$, and setting $z_j = 1$ includes it. For a Boolean vector $\mathbf{1}_E$ the product collapses to $X^{\sum_{j \in E} v_j}$, so $P(\mathbf{1}_E) = f(\mathbf{1}_E)$. The coefficient of $z_J$ in $P$ is $[X^0] \prod_{j \in J} (X^{v_j} - 1)$. Before taking $[X^0]$, this is a product of $|J|$ elements of the augmentation ideal, and therefore lies in $I^{|J|}$. Once $|J| > M$, that product, and hence the corresponding scalar coefficient of $P$, is zero. This is why the degree is bounded by $M$ rather than by the number $N$ of labels. Thus the degree of our polynomial $P$ is at most $M$. □

**Olson's theorem.** The same nilpotence gives $\mathsf{D}(H) = M + 1$. If $M + 1$ terms were zero-sum free, the product $\prod_j (1 - X^{v_j})$ would have identity coefficient 1, contributed only by the empty selection. But this product lies in $I^{M+1} = 0$. Hence $\mathsf{D}(H) \le M + 1$. Conversely, $p^{a_i} - 1$ copies of each $e_i$ form a zero-sum free sequence of length $M$, giving equality. For this basis sequence, only the empty subset has sum zero. Its unique multilinear indicator is $\prod_{j=1}^{M} (1 - z_j)$, of degree $M$. Thus the indicator degree bound is best possible in general.

*Proof of Theorem A.* Put $M = \mathsf{D}(H) - 1$ and take $L(M)$ terms $(u_j, v_j)$ in $Q \oplus H$. The quotient sequence $(u_j)$ has an $\mathcal{I}_M$-identity $(c_E)$ over $\mathbb{F}_p$. Let $P$ be the indicator polynomial for the kernel labels $(v_j)$ supplied by Lemma 3.1. Since $\deg P \le M$,

$$1 = P(0) = \sum_{E \in \mathcal{Z}((u_j))} c_E P(\mathbf{1}_E).$$

Some summand is nonzero. For its nonempty set $E$, $\sum_{j \in E} u_j = 0$ by definition, while $P(\mathbf{1}_E) = 1$ gives $\sum_{j \in E} v_j = 0$. Thus the original sequence has a nonempty zero sum, and $\mathsf{D}(Q \oplus H) \le L(M)$. If the identities are integral, reducing their coefficients modulo $p$ makes the same argument available for every prime. □

**Remark 3.2** (The elementary block bound)**.** A sequence of length $\eta(Q) + t \exp(Q)$ contains $t + 1$ disjoint short zero sets, obtained by repeated extraction. Their unions, with inclusion–exclusion weights, give an $\mathcal{I}_t$-identity by Lemma 2.2(1). For a $p$-group kernel, Theorem A therefore recovers (1.2), and in the same way every bound obtained from $\mathsf{D}(H)$ disjoint blocks, whatever their sizes. Incidence identities allow further cancellations among zero sets that do not arise from a disjoint block decomposition. The six-term Fano example below already requires such overlap.

**Remark 3.3** (The kernel hypothesis)**.** The degree bound in Lemma 3.1 cannot hold uniformly in the number of labels when $H$ is not a $p$-group. Choose an element $g$ of prime order $q \neq p$ and take all $N = p^s$ labels equal to $g$. The coefficient of $z_1 \cdots z_N$ in their zero-sum indicator is

$$[X^0](X^g - 1)^N = [X^0](X^{Ng} - 1) = -1 \neq 0,$$

where the middle equality is Frobenius and $Ng \neq 0$ because $q \nmid N$. A function on $\{0,1\}^N$ has a unique multilinear representative over $\mathbb{F}_p$, so the indicator has degree exactly $N$. Since $s$ is arbitrary, there is no bound depending only on $H$.

For example, when $g$ has order two and $p$ is odd, the indicator is

$$\frac{1}{2}\left(1 + \prod_{j=1}^{N}(1 - 2z_j)\right),$$

the test that the number of selected labels is even. Thus the bounded-degree indicator argument cannot be applied unchanged to such kernels.

# 4 Sharpness

**Proposition 4.1.** *Let $m \geq 2$ and $t \geq 0$, and let $K$ be a field of characteristic zero or of characteristic not dividing $m$. Then*

$$\kappa_t(C_m^3; K) \geq m(t+3) - 2.$$

*Proof.* We choose a sequence whose zero sets are especially simple:

$$U = e_1^{m-1} e_2^{m-1} e_3^{m(t+1)-1},$$

of length $m(t+3) - 3$. A zero set contains no first- or second-axis term, because there are fewer than $m$ of each. It therefore consists of third-axis positions, and its size is $mk$ for some $1 \leq k \leq t$.

We look for a separator among the linear combinations of the elementary symmetric polynomials $s_0, \ldots, s_t$ in those third-axis coordinates. On a set of size $l$, their values are $s_j(\mathbf{1}_E) = \binom{l}{j}$. It suffices to show that the integer matrix

$$B = \left(\binom{mk}{j}\right)_{0 \leq k,j \leq t}$$

is invertible over $K$.

To compute its determinant, let $a_{j,i}$ count the $j$-element subsets of a fixed union of $i$ disjoint $m$-element blocks that meet every block. Put $a_{0,0} = 1$ and $a_{j,0} = 0$ for $j > 0$. A $j$-element subset of a union of $k$ blocks first chooses the $i$ blocks it meets, giving

$$\binom{mk}{j} = \sum_{i=0}^{k} \binom{k}{i} a_{j,i}.$$

Thus $B = ST$, where $S = (\binom{k}{i})_{0 \leq k,i \leq t}$ is lower triangular with diagonal entries one, and $T = (a_{j,i})_{0 \leq i,j \leq t}$ is upper triangular. Moreover, $a_{j,j} = m^j$: a $j$-element subset meeting $j$ blocks chooses one element from each. Consequently

$$\det B = \prod_{j=0}^{t} m^j = m^{t(t+1)/2}.$$

This identity was obtained over the integers without division. The determinant has nonzero image in $K$ under the stated characteristic hypothesis. We can therefore choose a linear combination of $s_0, \ldots, s_t$ taking the values $1, 0, \ldots, 0$ at subset sizes $0, m, \ldots, tm$. It is a separator for $U$ of degree at most $t$. Hence $\kappa_t(C_m^3; K) \geq m(t+3) - 2$. □

**Remark 4.2.** The restriction on the characteristic cannot be dropped, and the smallest case shows the threshold moving: $\kappa_1(C_2^3;\mathbb{F}_2) = 5$, one less than the value 6 that Theorem B gives over every field of characteristic different from two. Indeed, for five terms $u_1, \dots, u_5$ over $C_2^3 = \mathbb{F}_2^3$ the linear map $\mathbb{F}_2^5 \to \mathbb{F}_2^3$, $z \mapsto \sum_j z_j u_j$, has a null space of dimension at least two, and its nonzero elements are the incidence vectors of the zero sets. If $x$ and $y$ are two independent vectors of this null space, an affine separator $1+\ell$ with $\ell$ linear would have to satisfy $\ell(x) = \ell(y) = \ell(x+y) = 1$, which is impossible; so no five-term sequence has an affine separator over $\mathbb{F}_2$. On the other hand $e_1e_2e_3^2$ has the affine separator $1 + z_3$, its only zero set being $\{3, 4\}$. Thus $\kappa_1(C_2^3;\mathbb{F}_2) = 5$. The integral six-term identity supplied by Theorem B remains valid in characteristic two; the least length is simply smaller there.

# 5 The quotients $C_2^3$, $C_3^3$ and $C_4^3$

We now prove that every sequence of $L_m(t) = m(t + 3) - 2$ terms over $C_m^3$ has an integral $\mathcal{I}_t$-identity. Call a sequence *short-zero-free* if it has no nonempty zero set of size at most the exponent. For $t \geq 1$, if a sequence of length $L_m(t)$ has a zero set $B$ with $|B| \leq m$, deleting it leaves at least

$$L_m(t) - m = L_m(t - 1)$$

terms. An identity of degree $t - 1$ on the remainder therefore gives one of degree $t$ by Lemma 2.2(2). We call this step the *short-zero recurrence*. Once $L_m(t) \geq \eta(C_m^3)$, it is automatic. The work is concentrated in the degrees before that point.

Identities of degree one and two are tested on affine and on quadratic polynomials, and we call them *affine* and *quadratic* identities. The following table summarises where the finite work lies; the computations behind the finite certificates are described in Appendix A, and sharpness is Proposition 4.1.

| Quotient | Target length | Before the automatic recurrence | Automatic recurrence |
|---|---|---|---|
| $C_2^3$ | $2t + 4$ | $t = 0$: $\mathsf{D}(C_2^3) = 4$; $t = 1$: the Fano configuration | $t \geq 2$, using $\eta(C_2^3) \leq 8$ |
| $C_3^3$ | $3t + 7$ | $t = 0$: $\mathsf{D}(C_3^3) = 7$; $t = 1$: finite affine certificates; $t = 2, 3$: the support facts and the constructions | $t \geq 4$, using $\eta(C_3^3) \leq 17$ |
| $C_4^3$ | $4t + 10$ | $t = 0$: $\mathsf{D}(C_4^3) = 10$; $t = 1, 2$: finite certificates | $t \geq 3$, using $\eta(C_4^3) \leq 22$ |

## 5.1 The case $C_2^3$

The Fano configuration shows the mechanism in miniature. Degree zero is $\mathsf{D}(C_2^3) = 4$. For degree one, consider six terms. If a term is zero or repeated, there is a zero set of at most two positions; deleting it leaves at least four terms and hence a second, disjoint zero set. Lemma 2.2(1) applies.

Otherwise the six terms are distinct nonzero vectors of $\mathbb{F}_2^3$: the Fano plane with one point $x$ removed. Its lines are the triples $\{u, v, u + v\}$, each of which has sum zero. Give weight 1 to the four lines not through $x$, and weight $-1$ to the complements, in the seven-point plane, of the three lines through $x$. The latter are zero quadruples and do not contain $x$. Each remaining point lies on two of the selected lines and in two of the selected quadruples. Its total weight is therefore $2 - 2 = 0$, whereas the total weight of the seven sets is $4 - 3 = 1$.

This identity uses overlap in an essential way. Every zero set among six distinct nonzero vectors has at least three terms. Two disjoint zero sets would therefore exhaust the six points, but their total is the omitted nonzero point $x$, since all seven Fano points sum to zero.

Finally, any eight terms contain zero or a repetition, so $\eta(C_2^3) \leq 8$. The short-zero recurrence gives all degrees $t \geq 2$ at length $2t+4$. These are integral identities, valid after reduction in every characteristic; Proposition 4.1 gives equality in characteristic zero and in odd characteristic.

## 5.2 The case $C_3^3$

We need the ten-term incidence identity and two elementary facts about supports.

**Lemma 5.1** (Ternary base facts)**.** *The following assertions hold.*

1. *Every ten-term sequence over $C_3^3$ has an integral $\mathcal{I}_1$-identity.*
2. *The support of a short-zero-free sequence over $C_3^3$ has at most eight points. Every such support with seven points has nonzero sum, and every such support with eight points has sum zero.*

We start by proving the second assertion.

*Proof of Lemma 5.1(2).* Let $A$ be the support of a short-zero-free sequence and put $C = A \cup \{0\}$. Then $C$ is a *cap*, that is, it contains no three distinct collinear points (this is the connection with affine caps studied in [6]). Indeed, over $\mathbb{F}_3$, three distinct points are collinear exactly when their sum is zero. A line through 0 would give an opposite pair in $A$, and any other line would give a zero triple in $A$.

An affine plane contains at most four cap points. Otherwise choose five. In each of the four directions, the three parallel lines would contain $2, 2, 1$ of these points, accounting for two pairs in that direction. This accounts for at most eight pairs, rather than $\binom{5}{2} = 10$.

Put $N = |C|$ and let $n_i$ be the number of affine planes meeting $C$ in exactly $i$ points, for $0 \le i \le 4$. There are $(3^3 - 1)/2 = 13$ parallel classes of planes, each with three members, hence 39 planes. A point belongs to 13 planes, a pair to $(3^2 - 1)/2 = 4$, and a noncollinear triple to one. Counting these incidences gives

$$\sum_{i=0}^{4} n_i = 39, \qquad \sum_{i=0}^{4} i n_i = 13N,$$
$$\sum_{i=0}^{4} \binom{i}{2} n_i = 4\binom{N}{2}, \quad \sum_{i=0}^{4} \binom{i}{3} n_i = \binom{N}{3}.$$

For $N = 10$, these equations give $n_3 + 4n_0 = -4$, a contradiction. A larger cap would contain a ten-point cap, so $N \le 9$ and $|A| \le 8$.

Suppose $|A| = 7$, so $N = 8$. The same equations give $n_2 = 6n_0 - 2$, hence some affine plane is disjoint from $C$. Write it as $\ell = c$, where $\ell$ is a nonzero linear functional. Since $0 \in C$, one has $c \neq 0$. The other two parallel planes contain four points each, and therefore

$$\ell\left(\sum_{x \in C} x\right) = 4 \sum_{a \in \mathbb{F}_3 \setminus \{c\}} a = -c \neq 0.$$

Thus $\sigma(A) = \sigma(C) \neq 0$.

Finally suppose $|A| = 8$, so $N = 9$. No affine plane is empty, because the other two parallel planes could hold at most eight cap points. Thus $n_0 = 0$, and the incidence equations give $n_2 = 6n_0 = 0$. For every nonzero linear functional $\ell$, the three parallel slices have sizes $3, 3, 3$ or a permutation of $1, 4, 4$. In either case their sizes are congruent modulo three, so $\ell(\sigma(C)) = 0$. This holds for every $\ell$, hence $\sigma(A) = \sigma(C) = 0$. □

*Proof of Lemma 5.1(1), computer-assisted.* If a ten-term sequence has a zero set of at most three positions, its deletion leaves at least seven terms and hence a disjoint zero set, since $\mathsf{D}(C_3^3) = 7$. Lemma 2.2(1) then gives the required affine identity.

It remains to consider the short-zero-free sequences. Their multiplicities are at most two, and their supports satisfy the cap conditions used above. The complete enumeration and its symmetry reductions are given in Appendix A. Each case is supplied either with two disjoint

zero sets or with an explicit integral affine identity. The certificate check verifies the zero sums, total weight one, and zero total weight through each individual position. The transports between normalised representatives and the indexed sequences they represent are checked together with the certificates. □

Call a set $A \subseteq C_3^3$ *allowed* if it contains neither zero nor a pair of opposite points, and no three distinct points of $A$ sum to zero. Write $2A$ for the sequence containing two copies of each point of $A$.

**Lemma 5.2.** *Every short-zero-free sequence of thirteen terms over $C_3^3$ has a zero set of size at least eleven.*

*Proof.* The plan is to write $\sigma(U)$ as a sum of at most two terms of $U$: deleting them leaves a zero set of size at least eleven. The representation will come from the maximality of an allowed support, and the only point to watch is whether it uses a term more often than $U$ contains it.

We first observe that if $A$ is an inclusion-maximal allowed support, then every $x \in C_3^3$ is a sum of at most two terms of $2A$. For $x = 0$ take no terms, for $x \in A$ one term, and if $-x \in A$ take two copies of $-x$. Otherwise $-x$ is a nonzero point outside $A$ whose opposite $x$ is also outside $A$, so adjoining $-x$ to $A$ can only violate the third condition: there is a zero triple $-x + a + b = 0$ with distinct $a, b \in A$, which represents $x = a + b$.

Now let $U$ be short-zero-free of length thirteen. Its multiplicities are at most two, so its support has seven or eight points, and there are three cases.

*Case 1: the support is an eight-set $B$.* Then $U = 2B - b - c - d$ for three distinct points $b, c, d$ of multiplicity one. By Lemma 5.1, $\sigma(B) = 0$, so $\sigma(U) = -b - c - d$, and $B$ is maximal by the support bound. A representation of $\sigma(U)$ by at most two terms of $2B$ is unavailable in $U$, that is, it uses a term more often than $U$ contains it, only if it uses one of $b, c, d$ twice, say $2b = -b - c - d$; this gives $c + d = 0$, impossible in an allowed support.

*Case 2: the support is a seven-set $A$ which is maximal.* Then $U = 2A - a_0$ for one point $a_0$ of multiplicity one, and the only unavailable representation is $2a_0 = \sigma(U) = 2\sigma(A) - a_0$, which forces $\sigma(A) = 0$, contradicting Lemma 5.1.

*Case 3: the support is a seven-set $A$ which is not maximal.* Again $U = 2A - a_0$, and $A$ extends to an allowed eight-set $B = A \cup \{b\}$, which is maximal, with $\sigma(B) = 0$ and hence $\sigma(U) = b - a_0$. A representation of $b - a_0$ by at most two terms of $2B$ is unavailable in $U$ only if it uses $b$, which $U$ does not contain, or $a_0$ twice, so it is one of

$$b, \qquad 2b, \qquad b + c \ \text{ with } c \in A, \qquad 2a_0,$$

and these force $a_0 = 0$, $a_0 = -b$, $c = -a_0$ and $b = 0$ respectively. Each contradicts the support conditions. □

*Proof of Theorem B for $m = 3$.* The target lengths are $3t + 7$. Degree zero is $\mathsf{D}(C_3^3) = 7$; degree one is Lemma 5.1(1).

For degree two, consider thirteen terms. A zero set of at most three positions leaves at least ten terms, so Lemma 2.2(2) applies to the affine identity on the remainder. Otherwise Lemma 5.2 gives a zero set of at least eleven positions. It properly contains a ten-term subsequence, and Lemma 2.2(3) raises that subsequence's affine identity to degree two.

For degree three, a short zero set among sixteen terms again reduces to the preceding degree. If there is none, the support bound and the multiplicity bound force eight support points, each appearing twice. Their sum is zero by Lemma 5.1(2), so the whole sequence is a zero set. A thirteen-term subsequence properly inside it has a degree-two identity, which Lemma 2.2(3) raises to degree three.

The support and multiplicity bounds also show that every seventeen terms contain a short zero set: $\eta(C_3^3) \le 17$ (in fact $\eta(C_3^3) = 17$, see [9]). For $t \ge 4$, the target length is at least nineteen, so the short-zero recurrence proves all further degrees. Proposition 4.1 gives sharpness under its characteristic hypothesis. □

### 5.3 The case $C_4^3$

**Lemma 5.3** (Quaternary finite input)**.** *Every fourteen-term sequence over $C_4^3$ has an integral $\mathcal{I}_1$-identity, and every eighteen-term sequence over $C_4^3$ has an integral $\mathcal{I}_2$-identity.*

The proof is computer-assisted; its reductions are as follows. Since $\mathsf{D}(C_4^3) = 10$, a zero set of at most four positions among fourteen terms leaves a disjoint zero set. The two sets give an affine identity by Lemma 2.2(1). Each remaining fourteen-term case receives either a disjoint-pair witness or an explicit integral affine identity.

For eighteen terms, a short zero set reduces to the fourteen-term claim by Lemma 2.2(2). Three disjoint zero sets also suffice, by part (1). A zero set of at least fifteen positions gives a third route: it properly contains fourteen positions, whose affine identity lifts by part (3). The remaining cases are supplied with explicit integral quadratic identities.

Appendix A gives the complete finite domains, the coverage arguments for two normalisations, and the counts of the positive witnesses. The checks verify the group sums and every required incidence moment over the integers. The enumeration includes multiplicities and accounts for sequences in proper subgroups; all transports preserve indexed occurrences.

The following example shows what the finite search can find beyond these length-based reductions. Take

$$U = (100)^3(010)^3(110)^3(001)^3(101)^3(131)^3$$

in $(\mathbb{Z}/4\mathbb{Z})^3$, with positions numbered $1, \dots, 18$ in this order.

Inspecting the first, third and second coordinates shows that a nonempty zero set of at most four terms would require four equal terms, which are unavailable. Also $\sigma(U) = (0, 3, 1)$. A zero set of at least fifteen terms would leave at most three terms with this sum. Their first coordinates force them to be 010 or 001, requiring three copies of 010 and one of 001, a contradiction. Three disjoint zero sets would have a zero union of at least fifteen terms, so they are impossible too.

There is nevertheless a useful five-term zero set

$$B = \{9, 11, 13, 14, 16\}.$$

Deleting it leaves only thirteen terms, one fewer than the length at which an affine identity is guaranteed for every sequence. For this particular remainder, such an identity can be written down. The following five sets are zero sets disjoint from $B$:

$$\begin{aligned} A &= \{1, 2, 4, 5, 7, 8\}, \\ C &= \{3, 8, 10, 12, 15, 18\}, \\ D &= \{6, 7, 12, 15, 17, 18\}, \\ C' &= \{4, 5, 6, 7, 8, 10, 12, 15, 18\}, \\ D' &= \{1, 2, 3, 7, 8, 12, 15, 17, 18\}. \end{aligned}$$

Position by position, they satisfy the integer identity

$$\mathbf{1}_A + \mathbf{1}_C + \mathbf{1}_D = \mathbf{1}_{C'} + \mathbf{1}_{D'}.$$

The coefficients $1, 1, 1, -1, -1$ add to one and cancel through every position, so they give an integral $\mathcal{I}_1$-identity on the remainder. Lemma 2.2(2) now produces an $\mathcal{I}_2$-identity on $U$: keep these five weights, give their negatives to the unions of the five sets with $B$, and give weight 1 to $B$.

Thus the eleven-set quadratic certificate is a lower-degree identity lifted by one of the elementary constructions. The useful extra information is the affine identity on this particular thirteen-term remainder; its existence does not follow from the universal fourteen-term threshold. The certificate itself, in the form in which it is stored and checked, is reproduced in the supplement.

*Proof of Theorem B for $m = 4$.* The target lengths are $4t + 10$. Degree zero is $\mathsf{D}(C_4^3) = 10$, and degrees one and two are Lemma 5.3. The bound $\eta(C_4^3) \le 22$ follows from the classical result $\eta(C_4^3) = 22$ of Harborth [15], see [9, Theorem 2.2(2)]. For $t \ge 3$, the target length is at least 22; deleting a short zero set leaves at least $4(t-1)+10$ terms. Lemma 2.2(2) therefore proves every further degree. Proposition 4.1 gives sharpness under its characteristic hypothesis. □

## 6 Davenport constants

*Proof of Corollary C.* Theorems A and B give

$$\mathsf{D}(C_m^3 \oplus H) \le m(\mathsf{D}(H) - 1) + 3m - 2 \tag{6.1}$$

for every finite abelian $p$-group $H$. Take $H = C_{p^a} \oplus C_{p^b} \oplus C_{p^c}$, allowing trivial factors. Olson's theorem gives

$$\mathsf{D}(H) - 1 = p^a + p^b + p^c - 3.$$

Since $p \nmid m$, the Chinese remainder theorem identifies $C_m^3 \oplus H$ with $G = C_{mp^a} \oplus C_{mp^b} \oplus C_{mp^c}$. Its invariant factors are in divisibility order, so substitution yields

$$\mathsf{D}(G) \le m(p^a + p^b + p^c) - 2 = \mathsf{D}^*(G).$$

The basis lower bound gives the reverse inequality. □

The general bound (6.1) holds for kernels of every rank and for every prime. Coprimality and the rank bound are used in the comparison with $\mathsf{D}^*$ above.

For example, take $m = 3$ and $H = C_1 \oplus C_5 \oplus C_{25}$. Here $\mathsf{D}(H) - 1 = 28$, so the quotient identity is used in degree 28, at length $3(28 + 3) - 2 = 91$. Transfer gives

$$\mathsf{D}(C_3 \oplus C_{15} \oplus C_{75}) = 91.$$

No enumeration at length 91 is needed: the constructions have already extended the finite base cases to degree 28. The basis sequence of length $2 + 14 + 74 = 90$ shows why the resulting value is sharp.

## 7 Verification, reproducibility and dependencies

The proofs of Lemma 5.1(1) and Lemma 5.3 are computer assisted. The support statement in Lemma 5.1(2) follows from affine-plane counting, and the proof of Lemma 5.2 uses it. The later incidence degrees are deductions from the finite base identities by the three constructions. Table 1 records these dependencies. Olson's small $p$-group values for the Davenport constant $\mathsf{D}(C_2^3) = 4$, $\mathsf{D}(C_3^3) = 7$ and $\mathsf{D}(C_4^3) = 10$ also supply degree zero and the short-zero reductions in the relevant rows.

For each computed case, the verification checks a positive witness: disjoint zero sets, a suitable long zero set, or an integer incidence identity. An incorrect negative classification, such as failing to detect a disjoint pair, cannot by itself certify a case; a valid positive witness must still pass the check. Appendix A specifies the full finite domains and justifies the reductions used to enumerate them. The certificate verification uses exact arithmetic and does not rely on the optimisation software used to discover the weights. All certificates and the instructions for reproducing their results are collected in a separate Supplement available on our Github repository [18].

The definitions, the lemmas, Proposition 4.1, Theorems A and B and Corollary C have also been formalised in Lean 4 with Mathlib [18], with proofs that follow the ones given here. In developing the formalisation, we made use of Scott Armstrong's *LeanAutoformalizationSkills*

collection [2]. For Lemma 5.1(1) and Lemma 5.3, the formalisation performs its own enumerations; their completeness is proved in Lean, together with the soundness of the certificate checks (see the supplement).

Table 1: Dependency map. "Ordinary" refers to the proof and its stated inputs; "computer-assisted" means an exhaustive enumeration with positive witnesses checked by an independent program; "deduction" means an ordinary argument some of whose inputs are computer-assisted statements.

| Statement | Nature | Essential inputs |
|---|---|---|
| Lemma 2.1 (duality) | ordinary | Boolean multilinearisation; linear algebra over a field |
| Lemma 2.2 (three constructions) | ordinary | Lemma 2.1(1); inclusion–exclusion; two degree-cancellation arguments |
| Lemma 3.1 (indicator) | ordinary | truncated group algebra; nilpotence of the augmentation ideal |
| Theorem A | ordinary | evaluation identity; Lemma 3.1; Olson's value of $\mathsf{D}(H)$ |
| Proposition 4.1 (sharpness) | ordinary | integer triangular factorisation of the binomial-value matrix |
| Theorem B, $m = 2$ | ordinary | Fano identity; $\eta(C_2^3) \le 8$; Lemma 2.2; Proposition 4.1 |
| Lemma 5.1(1) | computer-assisted | complete ten-term coverage (Appendix A); positive affine or disjoint-pair certificates and their transports |
| Lemma 5.1(2) | ordinary | cap–plane incidence counts; linear functionals |
| Lemma 5.2 | ordinary | maximal allowed supports; Lemma 5.1(2); multiplicity checks |
| Theorem B, $m = 3$ | deduction using finite input | Lemmas 5.1, 5.2, 2.2; $\mathsf{D}(C_3^3) = 7$; $\eta(C_3^3) \le 17$; Proposition 4.1 |
| Lemma 5.3 | computer-assisted | two quaternary enumerations (Table 3); exact certificates; the proper-subgroup bound used by the support-basis enumeration |
| Theorem B, $m = 4$ | deduction using finite input | Lemmas 5.3, 2.2; $\mathsf{D}(C_4^3) = 10$; $\eta(C_4^3) \le 22$; Proposition 4.1 |
| Corollary C | deduction using finite input | Theorems A and B; Olson's theorem; Chinese remainder theorem; basis lower bound |

# A Computational coverage and certificates

This appendix collects the parts of the proofs of Lemma 5.1(1) and Lemma 5.3 that justify the finite computations: the exact domains that were enumerated and the arguments showing that these domains cover every required sequence. Nothing is inferred from samples: each enumeration establishes a universal statement about all sequences of the stated length. The positive witnesses themselves, their statistics, the stored form of the eighteen-term example of Section 5 and the instructions for an independent replay are collected in the supplement.

## A.1 Ternary coverage

A short-zero-free sequence over $C_3^3$ has all multiplicities at most two, and its support $A$ contains no zero, no pair of opposite points and no three distinct points with sum zero; equivalently, $A \cup \{0\}$ is an affine cap in $\mathbb{F}_3^3$, a connection developed in [6]. A support with at least five points spans $\mathbb{F}_3^3$, since a plane contains only four pairs of opposite nonzero points. Mapping three independent support points to the standard basis leaves ten pairs of opposite points, each contributing none or exactly one of its two points, and the complete enumeration of these $3^{10} = 59\,049$ choices produces the support counts of Table 2; no support of size nine or more occurs. All 296 seven-point supports have nonzero sum and all 18 eight-point supports have

sum zero. A separate enumeration by direct basis completion confirms these two facts. These are the three facts of Lemma 5.1(2); they are proved in Section 5 by counting affine planes, and the enumeration is a redundant check of them.

For Lemma 5.1(1), a zero set of size at most three leaves seven terms and hence a disjoint zero set, since $\mathsf{D}(C_3^3) = 7$. It remains to treat the short-zero-free multiplicity vectors of total ten; their exact counts are given in Table 2. Most of them contain two disjoint zero sets. The remaining 5 006 cases form 43 orbits under the linear group, and each orbit representative receives an explicit integral identity with 5, 7 or 9 zero sets and coefficients $\pm 1$. An independent checker regenerates the complete case space and verifies every zero set and every moment of every identity, and a second one checks all transport matrices and index permutations between representatives and cases. No affine translations are used anywhere.

Table 2: The ternary ten-term computation, after normalising a support basis. Support counts are not orbit counts.

| Support size | Supports | Cases | Disjoint pair | Other identities |
|---:|---:|---:|---:|---:|
| 5 | 108 | 108 | 81 | 27 |
| 6 | 296 | 4,440 | 2,769 | 1,671 |
| 7 | 296 | 10,360 | 7,052 | 3,308 |
| 8 | 18 | 504 | 504 | 0 |
| Total | | 15,412 | 10,406 | 5,006 |

### A.2 Quaternary coverage by reduction modulo two

Represent $C_4^3$ as $(\mathbb{Z}/4\mathbb{Z})^3$ and reduce modulo two. In a short-zero-free sequence, the fibre over $0 \in \mathbb{F}_2^3$ contains at most three terms, which must be distinct and independent in $C_2^3$. A nonzero fibre contains at most four distinct elements, since its eight elements form four pairs of opposite elements, and at most one of these elements can repeat, because two distinct repeated elements $g, h$ in the same fibre satisfy $2g + 2h = 0$. Each multiplicity is at most three, so a fibre carries at most six terms.

We enumerate every projected multiplicity vector $(\mu_v)_{v \in \mathbb{F}_2^3}$ of the prescribed total with $\mu_0 \le 3$ and $\mu_v \le 6$ otherwise, up to the 168 elements of $\mathrm{GL}_3(\mathbb{F}_2)$. Every such linear map lifts to an automorphism of $(\mathbb{Z}/4\mathbb{Z})^3$, because a binary lift has odd determinant. Write a lifted element as $\widetilde{v} + 2w$ with $v, w \in \mathbb{F}_2^3$, where $\widetilde{v}$ is the binary representative. The automorphisms that reduce to the identity modulo two, and their action on high parts, are

$$\{\, I + 2N : N \in M_3(\mathbb{F}_2) \,\}, \qquad w \longmapsto w + Nv,$$

so choosing one term in each of the first independent occupied nonzero fibres, a suitable $N$ makes each chosen high part $w$ zero. Since zero is the least high part, requiring the first high part in each of these fibres to vanish, after sorting high parts within fibres, retains a representative of every orbit. This enumerator does not assume that the projection spans, so it covers sequences contained in proper subgroups as well.

Backtracking then generates all lifts in nondecreasing order within each fibre. It maintains the sets $R_1, R_2, R_3$ of sums of one, two and three previously placed terms with distinct indices. Appending $x$ is legal exactly when $x \neq 0$ and $-x \notin R_1 \cup R_2 \cup R_3$, and the update is

$$R_1' = R_1 \cup \{x\}, \quad R_2' = R_2 \cup (R_1 + x), \quad R_3' = R_3 \cup (R_2 + x),$$

with the old sets on the right. This is an exact test for short-zero-freeness that keeps track of repetitions.

### A.3 Independent support-basis enumeration

A second enumeration normalises a support basis instead. An exhaustive computation in the subgroup $C_4^2 \oplus C_2$ shows that short-zero-free sequences there have length at most thirteen. Every proper subgroup of $C_4^3$ lies in an index-two subgroup, all index-two subgroups are linearly equivalent, and therefore every short-zero-free sequence of length at least fourteen spans modulo two; three of its support vectors then have odd determinant and form a basis of $(\mathbb{Z}/4\mathbb{Z})^3$. We generate all short-zero-free multisets containing the standard basis and canonicalise each by the least sorted image under the maps that send an ordered support basis to the standard basis; this is a complete invariant for linear equivalence. The two enumerations produce identical canonical orbit lists.

Table 3: Quaternary finite coverage. Generated cases may repeat orbits; orbit counts refer to the full linear group.

| Quantity | Length 14 | Length 18 |
|---|---|---|
| Generated by projection and lifts | 308,051 | 18,224 |
| Generated with a fixed support basis | 24,445,377 | 1,267,272 |
| Distinct linear orbits | 106,655 | 4,941 |
| Disjoint-zero witnesses | 284,994 | 13,549 |
| Long-zero witnesses (after disjoint cases) | — | 4,171 |
| Direct integer certificates | 23,057 | 504 |
| Orbits receiving direct certificates | 6,963 | 64 |

## References


[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), 7–29. doi:10.1017/S0963548398003411.

[2] S. Armstrong, *LeanAutoformalizationSkills: Portable Lean 4 autoformalization skills for Codex and Claude Code*, GitHub repository (2026). github.com/scottnarmstrong/LeanAutoformalizationSkills.

[3] G. Bhowmik, I. Halupczok, and J.-C. Schlage-Puchta, *Inductive methods and zero-sum free sequences*, Integers **9** (2009), A40, 515–536. doi:10.1515/INTEG.2009.042; arXiv:0711.1262.

[4] G. Bhowmik and J.-C. Schlage-Puchta, *Davenport's constant for groups of the form* $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, in: Additive Combinatorics, CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007, pp. 307–326. arXiv:math/0610416.

[5] C. Delorme, O. Ordaz, and D. Quiroz, *Some remarks on Davenport constant*, Discrete Math. **237** (2001), 119–128.

[6] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham, *Zero-sum problems in finite abelian groups and affine caps*, Q. J. Math. **58** (2007), 159–186. doi:10.1093/qmath/ham003.

[7] W. Gao, *On Davenport's constant of finite abelian groups with rank three*, Discrete Math. **222** (2000), 111–124. doi:10.1016/S0012-365X(00)00010-8.

[8] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337–369. doi:10.1016/j.exmath.2006.07.002.

[9] W. D. Gao, Q. H. Hou, W. A. Schmid, and R. Thangadurai, *On short zero-sum subsequences. II*, Integers **7** (2007), Paper A21. doi:10.5281/zenodo.8281159.

[10] A. Geroldinger, D. J. Grynkiewicz, and Q. Zhong, *Combinatorial Factorization Theory. Factorization Theory of Krull Monoids via Additive Combinatorics*, Math. Surveys Monogr. **296**, Amer. Math. Soc., Providence, RI, 2026. doi:10.1090/surv/296.

[11] A. Geroldinger and R. Schneider, *On Davenport's constant*, J. Combin. Theory Ser. A **61** (1992), 147–152. doi:10.1016/0097-3165(92)90061-X.

[12] A. Geroldinger and W. Yang, *On a classical zero-sum invariant*, preprint (2026). arXiv:2608.19090v1.

[13] B. Girard, *An asymptotically tight bound for the Davenport constant*, J. Éc. polytech. Math. **5** (2018), 605–611. doi:10.5802/jep.79.

[14] B. Girard and W. A. Schmid, *Direct zero-sum problems for certain groups of rank three*, J. Number Theory **197** (2019), 297–316. doi:10.1016/j.jnt.2018.08.016.

[15] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. **262/263** (1973), 356–360. doi:10.1515/crll.1973.262-263.356.

[16] 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.

[17] J. E. Olson, *A combinatorial problem on finite Abelian groups. II*, J. Number Theory **1** (1969), 195–199. doi:10.1016/0022-314X(69)90037-7.

[18] C. G. Pop, G. C. Rad, and G. C. Ţurcaş, *Davenport_Project: a Lean 4 formalization of "Integral zero-sum incidence identities and Davenport constants in rank three"*, 2026. `https://github.com/CiprianRad/Davenport_Project`.

[19] W. A. Schmid, *The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups*, Electron. J. Combin. **18**(1) (2011), Paper P33. doi:10.37236/520.

[20] P. van Emde Boas, *A combinatorial problem on finite abelian groups. II*, Report ZW 7/69, Mathematisch Centrum, Amsterdam, 1969. CWI institutional repository.

[21] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups. III*, Report ZW 8/69, Mathematisch Centrum, Amsterdam, 1969. CWI institutional repository.

[22] A. Volkmann, *The small Davenport constant of $H_{27} \times C_3^r$*, preprint (2026). arXiv:2609.19810.

[23] A. Volkmann, *A twelve-term exclusion for the small Davenport constant of $E_2 \times C_3^r$*, preprint (2026). arXiv:2609.22972.

[24] A. Volkmann, *The small Davenport constant of $E_2 \times C_3^r$ for $0 \le r \le 3$*, preprint (2026). arXiv:2609.37262.