

THE SMALL DAVENPORT CONSTANT OF THE EXTRASPECIAL GROUPS OF ORDER p^{1+2m}

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. For a finite group G the *small Davenport constant* $\mathbf{d}(G)$ is the greatest length of a sequence over G no non-empty subsequence of which admits an ordering whose product is the identity. Godara and Sarkar conjectured $\mathbf{d}(H_{p^3}) = 3p - 3$ for the Heisenberg group of order p^3 and odd p , and the case $p = 2$ is a genuine exception: $\mathbf{d}(H_8) = 4 \neq 3$. We study the continuation of that family, the extraspecial groups $H(p, m)$ of order p^{1+2m} , for which no value and no group-specific bound appears in the literature when $m \geq 2$. Our main theorem is that $\mathbf{d}(H(2, m)) \geq 2m + 2$ for every $m \geq 1$: the shape $n(p - 1)$, which is correct for elementary abelian p -groups by Olson's theorem and for H_{p^3} at odd p , fails at $p = 2$ for *every* m , not only at $m = 1$. The bound is attained at both values of m for which $\mathbf{d}$ is known, and combined with an upper bound that we derive here from published theorems of Dimitrov and Jennings — a two-line consequence, recorded as a remark and not formalised — it determines $\mathbf{d}(H(2, m)) = 2m + 2$ at every m . We prove alongside it that $\mathbf{d}(G) \geq n(p - 1)$ for every group of order p^n ; that $\mathbf{d}(H(p, m)) \leq 2mp(p - 1) + p - 1$, replacing the exponential bound $p^{1+2m} - 1$ by a polynomial one at every prime and every m , together with the sharp reduction $\mathbf{d}(H(p, m)) \leq \mathbf{d}_p(\mathbb{F}_p^{2m})$ to a higher-order Davenport constant; and that $\mathbf{d}(H_8) = 4$ with no search. All the theorems and propositions below are machine-checked in Lean 4.

1. INTRODUCTION

Let G be a finite group, written multiplicatively. A *sequence* over G is a finite unordered list of elements of G , repetition allowed. A non-empty subsequence $T = h_1 \cdots h_k$ of a sequence S is a *product-one* subsequence if some ordering of its terms multiplies to the identity, that is, if $h_{\sigma(1)} h_{\sigma(2)} \cdots h_{\sigma(k)} = 1$ for some permutation σ of $\{1, \dots, k\}$; and S is *product-one free* if it has no product-one subsequence. The *small Davenport constant* $\mathbf{d}(G)$ is the greatest length of a product-one free sequence over G . For abelian G this is the classical zero-sum invariant $\mathbf{D}(G) - 1$; for non-abelian G the existential quantifier over orderings is essential, and it separates $\mathbf{d}$ from the *ordered* Davenport constant $\mathbf{D}_{\text{ord}}(G)$, the least ℓ such that every sequence of ℓ terms has a non-empty subsequence whose product is 1 *read in the given order*. One always has $\mathbf{d}(G) + 1 \leq \mathbf{D}_{\text{ord}}(G)$ [11, Lem. 2.5], and already at the Heisenberg group of order 27 the gap is wide: $\mathbf{d} = 6$ while $\mathbf{D}_{\text{ord}} = 9$ [10, 22].

The object of this paper is the family of *extraspecial* groups

$$H(p, m) = \{(a, b, c) : a, b \in \mathbb{F}_p^m, c \in \mathbb{F}_p\}, \quad (a, b, c)(a', b', c') = (a + a', b + b', c + c' + \langle a, b' \rangle),$$

of order p^{1+2m} , where $\langle \cdot, \cdot \rangle$ is the standard bilinear form on $\mathbb{F}_p^m$. At $m = 1$ this is the Heisenberg group $H_{p^3} = \text{UT}_3(\mathbb{F}_p)$ of upper unitriangular 3×3 matrices, and the whole literature on $\mathbf{d}$ for these groups lives at $m = 1$. Godara and Sarkar [12] computed $\mathbf{d}(H_{27}) = 6$ — a value that a computer search of Csiszter, Domokos and Szöllősi [5] had already produced — and asked whether $\mathbf{d}(H_{p^3}) = 3p - 3$ for every odd prime. White [22] settled $p = 5$ and Volkmann [20] settled $p = 7$, both by large computations, and Volkmann [21] then proved the conjecture for every odd prime. Qu and Wang [19] have since used that value to settle the Gao–Zhuang conjecture for the same group, $\mathbf{E}(H_{p^3}) = p^3 + 3p - 3$. (A preprint of Maghradze [15], unrefereed and not on arXiv, claims the same theorem by a different route — through Property B for C_p^2 rather than through an order-value growth theorem — and carries a Zenodo deposit timestamped 30 July 2026, three weeks before [21] of 19 August 2026; we record it as a possible priority claim without endorsing it.) At $p = 2$ the formula is simply false: $H_8 \cong D_8$, the dihedral group of order 8, and $\mathbf{d}(H_8) = 4$, whereas $3p - 3 = 3$. The

odd-prime hypothesis of [12] is doing real work, and the reason is structural — $H(p, m)$ has exponent p exactly when p is odd.

For $m \geq 2$ nothing group-specific is known. A literature sweep over a full-text arXiv corpus found the words “extraspecial” and “product-one free”/“small Davenport constant” together in exactly two papers, and in each the co-occurrence is a single sentence about H_{p^3} ; the exhaustive computations in the literature stop at group order 42 [1, §8]. Two *general* upper bounds do apply, and we compare against them in Remark 6.3.

What is settled here. Our headline result (Theorem 5.3) is a lower bound at $p = 2$, uniform in m :

$$\mathbf{d}(H(2, m)) \geq 2m + 2 \quad \text{for every } m \geq 1.$$

Its interest is what it rules out. Olson’s theorem gives $\mathbf{d}(C_p^n) = n(p - 1)$, Volkmann’s theorem gives $\mathbf{d}(H_{p^3}) = 3(p - 1)$ for odd p , and we prove below (Theorem 5.1) that $\mathbf{d}(G) \geq n(p - 1)$ for *every* group of order p^n — so $n(p - 1)$ is a natural candidate for the truth on p -groups of exponent p . Theorem 5.3 says that at $p = 2$, where the exponent hypothesis fails, the candidate value $n(p - 1) = 2m + 1$ is beaten at every m , and not merely in the one small case H_8 that was already visible. The bound is sharp wherever a value is known: it gives exactly $4 = \mathbf{d}(H_8)$ at $m = 1$ and exactly 6 at $m = 2$, the published value for both extraspecial groups of order 32 [1, 16]. Remark 5.5 derives a matching upper bound at every m from published theorems of Dimitrov and Jennings, so the value is in fact $2m + 2$ throughout; that derivation is a remark and is not part of the formal development.

The remaining results are supporting, and are stated because the main theorem is assembled from them. Section 4 records two extension inequalities for $\mathbf{d}$ along a normal subgroup, one additive and one multiplicative, together with Olson’s theorem at every rank. Section 5 proves the p -group lower bound $n(p - 1)$ and reads it on $H(p, m)$. Section 6 replaces the trivial bound $\mathbf{d}(H(p, m)) \leq p^{1+2m} - 1$ by $\mathbf{d}(H(p, m)) \leq 2mp(p - 1) + p - 1$, polynomial in p and linear in m , and sharpens it at $p = 2$ to a reduction to the higher-order constant $\mathbf{d}_2(\mathbb{F}_2^{2m})$; one consequence is a proof of $\mathbf{d}(H_8) = 4$ that uses no search at all. Section 7 reproduces the $m = 1$ literature, including Volkmann’s theorem $\mathbf{d}(H_{p^3}) = 3p - 3$ and the three ingredients it rests on. Section 8 lists the negative controls, and Section 9 the verification.

Conventions. p is a prime unless stated otherwise; $m \geq 1$; $e_1, \dots, e_m$ is the standard basis of $\mathbb{F}_p^m$; $v = (0, 0, 1) \in H(p, m)$ and, at $m = 1$, $x = (1, 0, 0)$, $y = (0, 1, 0)$. For a sequence S we write $|S|$ for its length, and x^k for the sequence consisting of k copies of x . We use the higher-order Davenport constants $\mathbf{d}_k$ of [4]: $\mathbf{d}_k(G)$ is the greatest length of a sequence over G carrying no k pairwise disjoint non-empty product-one subsequences, so $\mathbf{d}_1 = \mathbf{d}$; for abelian G it equals $\mathbf{D}_k(G) - 1$ for the constant $\mathbf{D}_k$ of [7].

2. THE CONSTANT

The definition above is transcribed from the sources. White [22, §1] writes that a sequence S is product-one-free if no non-empty subsequence I admits an ordering whose product is the identity; [20] states the same, and we take it literally, quantifying over sub-multisets and orderings at once.

Proposition 2.1 (the definition, and a decision procedure). *Let G be a finite group and S a sequence over G .*

- (1) *Product-one freeness is inherited by sub-multisets and is invariant under permutation of the terms, so it is a property of the underlying multiset.*
- (2) *If S is product-one free then $1 \notin S$. Consequently the convention of [22], which excludes the identity from sequences, and that of [20], which does not, define the same constant.*
- (3) *There is at most one d with $\mathbf{d}(G) = d$, and the predicate “ S is product-one free” is decidable by two procedures — one enumerating all subsequences against all orderings, one enumerating blocks by increasing size — each proved equivalent to the definition by a rearrangement of quantifiers rather than by an algorithmic argument.*

Item (3) matters for the two exhaustive computations of this paper: the checker is the definition, not a faster surrogate, so no property of its speed is load-bearing for correctness.

Proposition 2.2 (existence, and the pigeonhole bound). *Let G be a finite group. Every product-one free sequence over G has fewer than $|G|$ terms; consequently $\mathbf{d}(G)$ exists and $\mathbf{d}(G) \leq |G| - 1$.*

Proof sketch. If $|S| \geq |G|$, list the terms in any order and form the $|S|+1$ prefix products $1, g_1, g_1g_2, \dots$; two of them coincide, and the block between them multiplies to 1 *in the order in which it already occurs*. No commutativity is used, so this bounds even the ordered constant, and the entire difficulty of $\mathbf{d}(G)$ lives below length $|G|$. Existence then follows because the set of lengths of product-one free sequences is non-empty (the empty sequence) and bounded. $\square$

3. THE GROUPS

Proposition 3.1 (the extraspecial group $H(p, m)$). *With the multiplication of Section 1, $H(p, m)$ is a group of order p^{1+2m} , with identity $(0, 0, 0)$ and inverse $(a, b, c)^{-1} = (-a, -b, -c + \langle a, b \rangle)$. Every commutator is central:*

$$[g, h] = (0, 0, \langle a_g, b_h \rangle - \langle a_h, b_g \rangle).$$

Consequently every subgroup of $H(p, m)$ containing the central subgroup $Z = \{(0, 0, c) : c \in \mathbb{F}_p\} \cong C_p$ is normal. Reduction modulo Z is the map $(a, b, c) \mapsto (a, b)$ onto $\mathbb{F}_p^{2m}$, a homomorphism because the first two coordinates are additive along a product while the third is not. At $m = 1$ the map $(a, b, c) \mapsto (a_1, b_1, c)$ is an isomorphism $H(p, 1) \xrightarrow{\sim} H_{p^3}$.

The normality criterion is what makes the proof of Theorem 5.3 short: one exhibits a subgroup containing Z and never computes a conjugate.

Proposition 3.2 (the case $m = 1$). $H_{p^3} = \text{UT}_3(\mathbb{F}_p)$, written on triples with $M(a, b, c)M(a', b', c') = M(a + a', b + b', c + c' + ab')$, has order p^3 , satisfies $[M(a, b, c), M(a', b', c')] = M(0, 0, ab' - a'b)$ — so two elements commute exactly when their images in $\mathbb{F}_p^2$ are collinear — and, once $p > 1$, has centre exactly $\langle v \rangle$, with $[x, y] = v$ and $v^k = M(0, 0, k)$. Along any product of elements of H_{p^3} the first two coordinates add:

$$\left(\prod_i g_i\right)_a = \sum_i (g_i)_a, \quad \left(\prod_i g_i\right)_b = \sum_i (g_i)_b.$$

The last display is the pivot of every lower-bound argument below: the images of a product in the quotient $\mathbb{F}_p^2$ are known *without knowing the ordering*, while the third coordinate is not. That asymmetry is the whole non-abelian content of the problem.

4. TWO EXTENSION INEQUALITIES, AND OLSON'S THEOREM

Both inequalities of this section are known — they are items of [4, Prop. 3.9] — and are included because the results of Sections 5 and 6 are built from them, and because the ordering quantifier makes their proofs less immediate than in the abelian case.

Theorem 4.1 (concatenation; $\mathbf{d}(G) \geq \mathbf{d}(N) + \mathbf{d}(G/N)$). *Let $f : G \rightarrow K$ be a homomorphism of finite groups and let S, T be sequences over G . If every term of S lies in $\ker f$, S is product-one free, and the image sequence $f(T)$ is product-one free over K , then the concatenation $S \cup T$ is product-one free over G . Consequently, if $N \trianglelefteq G$ then $\mathbf{d}(G) \geq \mathbf{d}(N) + \mathbf{d}(G/N)$. Moreover x^k is product-one free whenever $k < \text{ord}(x)$.*

Proof sketch. A candidate product-one subsequence U of $S \cup T$ interleaves the two parts arbitrarily, and its product is taken in that interleaved order. Push it through f : the image of the product is the product of the images, the S -part contributes only identity terms, and deleting identity terms from a list does not change its product. What survives is an ordering of a subsequence of $f(T)$, non-empty precisely because product-one freeness of $f(T)$ forces $1 \notin f(T)$. This is [4, Prop. 3.9(1)] at $k = \ell = 1$, with the same proof; see also [16, Lem. 3.1(2)] and [3, Lem. 2.1(a)]. $\square$

Theorem 4.2 (the multiplicative bound and its sharp form). *Let $f : G \rightarrow K$ be a homomorphism of finite groups, $a, b \geq 0$.*

- (1) *If every product-one free sequence with terms in $\ker f$ has at most a terms, and every product-one free sequence over K has at most b terms, then every product-one free sequence over G has fewer than $(a + 1)(b + 1)$ terms. In particular, for $N \trianglelefteq G$,*

$$d(G) + 1 \leq (d(N) + 1)(d(G/N) + 1).$$

- (2) (Sharp form.) *If moreover every sequence over K of more than b terms carries $a + 1$ pairwise disjoint non-empty product-one subsequences, then every product-one free sequence over G has at most b terms; that is, $d(G) \leq d_{d(N)+1}(G/N)$.*

Proof sketch. For (1) one extracts blocks: if R has $b + 1$ terms then some non-empty subsequence of those $b + 1$ terms has product in $\ker f$ (otherwise the image of R would be a product-one free sequence of length $b + 1$), and the extraction must be run on a *prefix* of controlled length, or the resulting block is uncontrolled and the count fails. Iterating gives j disjoint blocks in any sequence of length $j(b + 1)$; if $|S| \geq (a + 1)(b + 1)$ we obtain $a + 1$ disjoint blocks with products in $\ker f$, and their products form a sequence of length $a + 1$ inside $\ker f$, which therefore has a product-one subsequence — lifting it back contradicts freeness. The extraction argument is that of [4, Prop. 3.9(4)], which we follow; part (1) is the composite of items (2) and (4) of that proposition at $k = 1$, and part (2) is item (2) itself. Two lifting lemmas do the work the ordering quantifier demands: a permutation of an image is the image of a permutation, and a sub-multiset of an image is the image of a sub-multiset. Without them one proves the bound only for the ordered constant. $\square$

Theorem 4.3 (Olson, at every rank). *Let p be a prime and ι a finite index set. Then $d(C_p^\iota) = |\iota|(p - 1)$. Equivalently, any sequence of more than $|\iota|(p - 1)$ elements of $\mathbb{F}_p^\iota$ has a non-empty zero-sum subsequence, while some sequence of exactly $|\iota|(p - 1)$ elements has none.*

Proof sketch. The upper half is a Chevalley–Warning argument (for the additive group theory in the background see [9, Ch. 5]): read the terms through $|\iota|$ coordinate functions and apply Chevalley–Warning to the system $f_j = \sum_i u_{j,i} X_i^{p-1}$, whose common zero locus is larger than the single trivial solution as soon as the number of variables exceeds $|\iota|(p - 1)$. The lower half is Theorem 5.1 below at $n = |\iota|$, which needs no witness of its own. The result is Olson’s [17]; only its formalization is new. $\square$

5. LOWER BOUNDS

Theorem 5.1 (p -groups). *Let p be a prime and let G be a group of order p^n . Then G carries a product-one free sequence of length $n(p - 1)$; hence*

$$n(p - 1) \leq d(G) \leq p^n - 1,$$

both ends by argument and neither by search.

Proof sketch. Induction on n . A non-trivial finite p -group has non-trivial centre, and Cauchy’s theorem inside the centre supplies a central element x of order exactly p ; $\langle x \rangle$ is normal because it is central, $|G/\langle x \rangle| = p^{n-1}$, and x^{p-1} is product-one free inside $\langle x \rangle$. Theorem 4.1 concatenates it with the sequence supplied by the induction hypothesis downstairs. No commutativity is used and no structure of G beyond its order. The right-hand end is Proposition 2.2. $\square$

This is where the length $3(p - 1)$ of the classical witness $x^{p-1}y^{p-1}v^{p-1}$ over H_{p^3} comes from: three chief factors, $p - 1$ apiece. We were unable to find the statement in the literature — a corpus-wide search for “chief series” or “composition series” against “Davenport” or “product-one” returned nothing, and a sweep for the expression $n(p - 1)$ over a 45-paper Davenport slice found nothing — but it is a one-line corollary of Theorem 4.1 together with $d(C_p) = p - 1$, and we claim no novelty for it.

Corollary 5.2 (the extraspecial family, lower half). *For every prime p and every m ,*

$$(2m+1)(p-1) \leq d(H(p, m)) \leq p^{1+2m} - 1.$$

In particular $d(H(3, 2)) \geq 10$, $d(H(5, 2)) \geq 20$ and $d(H(3, 3)) \geq 14$.

The proof is Theorem 5.1 at $n = 2m+1$; it uses only the order of the group and no Heisenberg input whatever. At $m = 1$ and odd p the left end is $3p - 3$, which by Volkmann's theorem (Theorem 7.7 below) is exactly $d(H_{p^3})$ — so the bound is attained and cannot be raised in general. The next theorem says that it is nevertheless not attained at $p = 2$.

Theorem 5.3 (main). *Let $m \geq 1$. In $H(2, m)$ the element $w = (e_1, e_1, 0)$ has order 4 and $\langle w \rangle \cong C_4$ is a normal subgroup containing the centre. Consequently*

$$d(H(2, m)) \geq 2m + 2 > 2m + 1 = (2m + 1)(2 - 1),$$

so the value $n(p-1)$ of Theorem 5.1 is attained by no member of the family $H(2, m)$. In particular $d(H(2, 2)) \geq 6$ and $d(H(2, 3)) \geq 8$.

Proof sketch. At $p = 2$ the group is not of exponent p . Indeed $w^2 = (0, 0, \langle e_1, e_1 \rangle) = (0, 0, 1) = v \neq 1$ and $w^4 = v^2 = 1$, so $\text{ord}(w) = 4$. Since $v \in \langle w \rangle$ and the centre of $H(2, m)$ is $\{1, v\}$, the subgroup $\langle w \rangle$ contains the centre and is therefore normal by Proposition 3.1; and $|H(2, m)/\langle w \rangle| = 2^{1+2m}/4 = 2^{2m-1}$ (the quotient is in fact elementary abelian, though only its order is used). Now w^3 is product-one free because $3 < \text{ord}(w)$, every term of it lies in $\langle w \rangle$, and Theorem 5.1 applied to the quotient produces a product-one free sequence there of length $(2m-1)(2-1) = 2m-1$. Theorem 4.1 concatenates the two:

$$d(H(2, m)) \geq d(C_4) + d(C_2^{2m-1}) \geq 3 + (2m-1) = 2m+2.$$

Nothing here is a computation. $\square$

At $m = 1$ Theorem 5.3 recovers $d(H_8) \geq 4$, i.e. the classical failure of the Godara–Sarkar formula at $p = 2$; its content is that the failure persists, by a fixed margin of one, at every m .

Remark 5.4 (the bound is attained wherever a value is known). Only two members of the family have a known constant. At $m = 1$, $H(2, 1) \cong H_8 \cong D_8$ and $d = 4 = 2m + 2$ (Theorem 7.2 below, and Theorem 6.2). At $m = 2$ the group has order 32 and $d = 6 = 2m + 2$: the exhaustive computation of [1], tabulated in [16, Lem. 3.2], gives $d = 6$ for *both* extraspecial groups of order 32, so the value is settled whichever of the two $H(2, 2)$ is. It is in fact the plus type: at $p = 2$ the squaring map of $H(p, m)$ is $g \mapsto g^2 = (0, 0, \langle a, b \rangle)$, so the quadratic form it induces on $\mathbb{F}_2^{2m}$ is $\sum_i a_i b_i$, a sum of m hyperbolic planes, of Arf invariant 0; hence $H(2, m) \cong 2_+^{1+2m}$, the central product of m copies of D_8 , and $H(2, 1) \cong D_8$ as above. That identification is a remark, not part of the formal development, and nothing below uses it: the preceding sentence is what carries the weight. Independently of the published tables, we reproduced $d(H(2, 2)) = 6$ by an exhaustive search in C (Section 9); the generic bound of Theorem 5.1 gives only 5 there, so Theorem 5.3 is the correct bound at the one cell beyond $m = 1$ where a value exists. For $m \geq 3$, that is from order 128 upward, we know of no computed value: the exhaustive computations in the literature stop at order 42 by their authors' own statement [1, §8].

Remark 5.5 (the matching upper bound, and what it costs). Two published theorems combine to bound d from above on this family. Dimitrov [6] proved $D_{\text{ord}}(G) \leq L(G)$ for a finite p -group G , where $L(G)$, the *Loewy length* of $\mathbb{F}_p[G]$, is the nilpotency index of its Jacobson radical; and Jennings [14] computed $L(G) = 1 + (p-1) \sum_{i \geq 1} i e_i$ from the Brauer–Jennings–Zassenhaus series $M_1 = G$, $M_i = [M_{i-1}, G] M_{[i/p]}^p$, with $p^{e_i} = |M_i/M_{i+1}|$. (Both are restated, in the form used here, as [11, Lem. 2.2] and [11, Lem. 2.1].) For $H(p, m)$ the series is

$$M_1 = H(p, m), \quad M_2 = [H, H] H^p = Z, \quad M_3 = 1,$$

so $e_1 = 2m$, $e_2 = 1$ and

$$L(H(p, m)) = 1 + (p-1)(2m+2), \quad \text{hence} \quad d(H(p, m)) \leq (p-1)(2m+2),$$

using the inequality $d(G) + 1 \leq D_{\text{ord}}(G)$, valid for every finite group [11, Lem. 2.5]. The series is immediate at both parities. Always $[H, H] = Z$, while $H^p = 1$ for odd p and $H^2 = Z$ at $p = 2$ (Remark 5.4); either way $M_2 = Z \cong C_p$, so $e_1 = \dim_{\mathbb{F}_p} H/Z = 2m$ and $e_2 = 1$. Then $M_3 = [Z, H] M_{[3/p]}^p = 1$, because $[Z, H] = 1$ and the second factor is $H^p = 1$ when $p \geq 3$ and $M_2^2 = Z^2 = 1$ when $p = 2$. At $p = 2$ the bound is exactly $2m + 2$, so with Theorem 5.3 it *determines*

$$d(H(2, m)) = 2m + 2 \quad \text{for every } m \geq 1,$$

and it explains Remark 5.4. Three published values check the computation. At $m = 1$ the formula gives $L = 4p - 3$, which is the value $D_{\text{ord}}(H_{p^3}) = 4p - 3$ computed in [10] (their group $G_1(1, 1, 1)$) and quoted in [22, §5]. At $p = 2, m = 1$ it gives $L = 5$, which is $L(D_{2^r}) = 2^{r-1} + 1$ at $r = 3$, the value recorded after Koshitani in [10]; the resulting bound $d(H_8) \leq 4$ is attained (Theorem 7.2). At $p = 2, m = 2$ the bound is 6, again attained (Remark 5.4). We emphasise what this remark is and is not. It is a two-line consequence of two published theorems, so we claim nothing new for it; it is *not* part of the formal development, because the modular group algebra, its Jacobson radical and Jennings' theorem are not available in the library we verify against; and we did not find the consequence stated anywhere. Theorem 5.3 does not depend on any of it: it is a lower bound, and its proof uses none of this machinery.

6. UPPER BOUNDS

Corollary 5.2 leaves an exponential right-hand end. Theorem 4.2 applied to the central extension $Z \rightarrow H(p, m) \rightarrow \mathbb{F}_p^{2m}$ replaces it by a polynomial one.

Theorem 6.1 (the polynomial bracket). *Let p be a prime and $m \geq 0$. Every product-one free sequence over $H(p, m)$ has fewer than $p(2m(p-1) + 1)$ terms, so that*

$$(2m + 1)(p - 1) \leq d(H(p, m)) \leq 2mp(p - 1) + p - 1.$$

More sharply, $d(H(p, m)) \leq d_p(\mathbb{F}_p^{2m})$: any bound on the higher-order Davenport constant of the elementary abelian quotient transfers verbatim.

Proof sketch. Apply Theorem 4.2 to reduction modulo the centre. A product-one free sequence with all terms central has at most $p - 1$ terms, because a central product has third coordinate the sum of the third coordinates and $d(C_p) = p - 1$; a product-one free sequence over $\mathbb{F}_p^{2m}$ has at most $2m(p - 1)$ terms by Theorem 4.3. Part (1) of Theorem 4.2 then gives $|S| < p(2m(p - 1) + 1)$ and part (2) gives the sharp form with $a + 1 = p$. $\square$

Numerically, at the smallest cells beyond $m = 1$:

group	order	bracket of Theorem 6.1	previous right end
$H(3, 2)$	243	$10 \leq d \leq 26$	242
$H(5, 2)$	3125	$20 \leq d \leq 84$	3124
$H(3, 3)$	2187	$14 \leq d \leq 38$	2186
$H(2, 2)$	32	$6 \leq d \leq 9$	31
$H(2, 3)$	128	$8 \leq d \leq 13$	127

Theorem 6.2 ($p = 2$: two blocks suffice). *Let $m \geq 0$. A product-one free sequence over $H(2, m)$ projects to a sequence over $\mathbb{F}_2^{2m}$ with no two disjoint non-empty zero-sum subsequences; that is,*

$$d(H(2, m)) \leq d_2(C_2^{2m}).$$

Moreover $d(H(2, m)) \leq \max(2m + 2, 2^{2m} - 1)$, with no search. At $m = 1$ the second bound is $\max(4, 3) = 4$, which together with Theorem 5.3 gives $d(H_8) = 4$ by argument alone.

Proof sketch. At $p = 2$ the centre is $\{1, v\}$, so a non-empty subsequence whose product is central has product exactly v — the product cannot be 1, or the sequence would not be free. Two disjoint such blocks would have products v and v , whose concatenation multiplies to $v^2 = 1$: contradiction. That is the first display. For the second, split on whether the projected sequence repeats a value or meets

the identity. If it does, a block of at most two terms is central, and the remaining terms project to a sequence with no zero-sum subsequence at all, hence number at most $2m$ by Theorem 4.3; if it does not, the projections are distinct and non-trivial, and there are only $2^{2m} - 1$ such values. $\square$

The bound $d(H_8) = 4$ so obtained is the value already recorded in Theorem 7.2; what is new is the route, which is free of the exhaustive search that the earlier proof runs, and which therefore removes the only compiled-evaluation step on which that value depended.

Remark 6.3 (where these bounds stand against the literature). Theorem 6.1 is not the best bound in print, and we state the comparison as numerals rather than as prose. Gryniewicz [13, Lem. 4.2], restated as [4, Thm. 3.11(4)], proves $d(G) \leq (d(H) + 2)p - 2 \leq |G|/p + p - 2$ whenever $H \trianglelefteq G$ with $G/H \cong C_p^2$; this applies to $H(p, m)$ with H the preimage of a codimension-2 symplectic subspace. Its weak half gives $p^{2m} + p - 2$, which Theorem 6.1 beats from $m = 2$ on ($26 < 82$, $9 < 16$, $13 < 64$) but not at $m = 1$ ($14 > 10$); its recursive half, started from $d = 3p - 3$ at $m = 1$, is geometric in m and gives $22 < 26$ at $p = 3, m = 2$ but loses from $m = 3$ on ($38 < 70$ at $p = 3$, $13 < 22$ at $p = 2$). The bound $d(G) \leq |G|/p + p - 2$ for non-cyclic G , with p the least prime divisor of $|G|$, was conjectured by Gao, Li and Peng [8] and proved by Qu, Li and Teeuwen [18]. Dominating both is the Loewy-length route of Remark 5.5, which gives $(p - 1)(2m + 2) = 12$ at $p = 3, m = 2$. Finally, through the sharp form of Theorem 6.1 the published values $D_2(C_2^4) = 8$ and $D_2(C_2^6) = 11$ of Freeze and Schmid [7] give $d(H(2, 2)) \leq 7$ and $d(H(2, 3)) \leq 10$ as citations, better than the 9 and 13 proved here; we do not include them among the theorems because their inputs are not verified here. What the present bounds contribute is that they are polynomial in p and linear in m , that they are proved rather than cited, and that at $p = 2$ they are exact at $m = 1$.

7. THE CASE $m = 1$

This section records the $m = 1$ literature. Nothing in it is new; it is reproduced because the family's own claims about $H(p, m)$ are calibrated against it and because Remarks 5.4 and 5.5 use its values.

Theorem 7.1 (the classical witness). *Let $p > 1$, not necessarily prime. The sequence $x^{p-1}y^{p-1}v^{p-1}$ over H_{p^3} is product-one free, so $d(H_{p^3}) \geq 3p - 3$; in particular $d(H_{27}) \geq 6$, $d(H_{125}) \geq 12$, $d(H_{343}) \geq 18$ and $d(H_{1331}) \geq 30$.*

Proof sketch. The argument is that of [20, Prop. 3.1], stated there for odd primes; it uses only $p > 1$. A product-one subsequence uses α copies of x and β of y with $\alpha, \beta \leq p - 1$; by Proposition 3.2 the first two coordinates of its product are α and β read in $\mathbb{F}_p$, whatever the ordering, so both vanish only if $\alpha = \beta = 0$. What remains is v^γ with $1 \leq \gamma \leq p - 1$, which is not the identity. Primality is what makes $3p - 3$ the conjectured truth, not what makes the bound valid. $\square$

Theorem 7.2 ($p = 2$, by exhaustion). $d(H_8) = 4$. Hence $3p - 3$ is false at $p = 2$, where it would give 3, and the witness of Theorem 7.1 is product-one free but not extremal there.

Proof sketch. The lower half is the explicit sequence $(0, 1, 0), (1, 1, 0), (1, 1, 0), (1, 1, 0)$, checked free by evaluating the decision procedure of Proposition 2.1 on all of its non-empty sub-multisets and all their orderings. The upper half is an exhaustive search: for a fixed total order on H_8 let F_L be the list of all sorted product-one free sequences of length L , built by prepending an element to a member of F_{L-1} . A covering lemma — proved by induction on the list, using that freeness is inherited by sub-multisets — shows that every sorted product-one free sequence of length L occurs in F_L , and since freeness is invariant under permutation, sorting an arbitrary free sequence loses nothing. Hence $F_5 = \emptyset$ implies that no product-one free sequence of length 5 exists. The evaluation $F_5 = \emptyset$ over the 8-element group, and the check on the four-term witness, are the only two exhaustive computations in the paper; see Section 9. Theorem 6.2 re-proves the same value without them. The value itself is classical — $H_8 \cong D_8$ and $d(D_{2n}) = n$ — and is tabulated in [16, Lem. 3.2]. $\square$

The upper half at odd p is a different matter, and is Volkmann's. Its three ingredients are the following; none of them is available ready-made in the library we verify against, so each is proved here.

Theorem 7.3 (Olson at rank 2, and the line bound). *For p prime, $D(\mathbb{F}_p^2) = 2p - 1$: any $2p - 1$ vectors of $\mathbb{F}_p^2$ have a non-empty zero-sum subsequence, and the sequence made of $p - 1$ copies of $(1, 0)$ and $p - 1$ copies of $(0, 1)$ has none. Consequently, in a product-one free sequence S over H_{p^3} with p odd, any sub-multiset whose terms pairwise commute has at most $2p - 2$ terms; and, at every prime p , any sub-multiset of central terms has at most $p - 1$ terms.*

Theorem 7.4 (relative subsums). *Let p be a prime, l a list, u, v two $\mathbb{F}_p$ -valued functions on its terms, and $R \subseteq \mathbb{F}_p$ a finite set with $0 \notin R$. If every non-empty sublist t of l with $\sum_t u = 0$ satisfies $\sum_t v \in R$, then $|l| \leq p - 1 + |R|$. Moreover the set of subsums of a list of n non-zero elements of $\mathbb{F}_p$ has at least $\min(p, n + 1)$ elements, and at least $\min(p - 1, n)$ of them are non-zero.*

The first assertion is [21, Thm. 4.1] and is proved by Alon's Combinatorial Nullstellensatz [2]; the second is an iteration of the Cauchy–Davenport inequality.

Theorem 7.5 (order-value growth). *For a sequence l over H_{p^3} let $\Gamma(l) \subseteq \mathbb{F}_p$ be the set of third coordinates of the products of l over all orderings. Write $\omega(g, h) = a_g b_h - a_h b_g$, so that g and h commute exactly when $\omega(g, h) = 0$; call l mixed if ω is non-zero on some pair of its terms, balanced if its first two coordinate sums vanish, and non-central if no term is central. If l is mixed, balanced and non-central then*

$$\min(p, |l| - 1) \leq |\Gamma(l)|.$$

Consequently, if S is product-one free over H_{p^3} and T is a non-empty balanced sub-multiset of S that is mixed and non-central, then $|T| \leq p$.

Proof sketch. Transposing two adjacent terms g, h of a product multiplies it by $(0, 0, -\omega(g, h))$, so a mixed list already reaches two values; a contraction step then replaces a non-commuting pair s, y by the single term sy while keeping the list mixed, and $\Gamma(sy \cdot R) + \{0, -\omega(s, y)\} \subseteq \Gamma(syR)$ makes the set grow by one at each step until it saturates at p . The consequence follows because $0 \notin \Gamma(T)$ for a balanced sub-multiset of a free sequence. This is [21, Thm. 3.2], read inside the group rather than through the quotient; the argument needs no hypothesis that p is odd. $\square$

Theorem 7.6 (the block theorem). *Let p be a prime, $k \geq 1$ and let Q be a sequence of non-central elements of H_{p^3} with $|Q| \geq 2p + k - 2$. If for every non-central w at most $p + k - 2$ terms of Q commute with w , then Q has a sub-multiset that is mixed and balanced.*

This is the first half of [21, Thm. 5.1], which is stated there for odd p and $1 \leq k \leq p$; the half proved here needs neither restriction. Formalised alongside it, because the second half of that theorem uses them, are the equality case of the cyclic bound [21, Lem. 4.3] and the rigidity statement for the representation of a sequence on a line [21, Lem. 4.4].

Theorem 7.7 (Volkmann). *For every odd prime p , $d(H_{p^3}) = 3p - 3$. In particular $d(H_{27}) = 6$, $d(H_{125}) = 12$, $d(H_{343}) = 18$ and $d(H_{1331}) = 30$.*

Proof sketch. The lower half is Theorem 7.1. For the upper half one peels a maximal union of balanced blocks off a product-one free sequence S , writing S as $U \cup A$ with U balanced and A carrying no non-empty balanced sub-multiset; Theorem 7.3 bounds A , and Theorems 7.5 and 7.6 bound the blocks inside U . Carried out crudely this gives $d \leq 4p - 3$; refined by treating central terms separately it gives $d \leq 3p - 2$; and the boundary case of Theorem 7.6 closes the last unit to $3p - 3$. The theorem is [21]; [22] and [20] had settled $p = 5$ and $p = 7$ by computation, and [12] the case $p = 3$. See also [15] and the priority remark in Section 1. $\square$

8. NEGATIVE CONTROLS

A formal development can be internally consistent and still be about the wrong object. We therefore state, and verify, the following refutations; each is chosen so that a plausible mis-reading of a definition or a plausible over-statement of a theorem would make it fail.

Proposition 8.1 (the ordering quantifier, and the product law). *Over H_{27} the sequence*

$$(0, 0, 1), (0, 1, 0), (0, 1, 0), (1, 0, 0), (0, 2, 1), (1, 0, 0), (1, 0, 1)$$

has no subsequence that multiplies to 1 in its given order, yet its sub-multiset

$$(0, 1, 0), (1, 0, 0), (1, 0, 0), (0, 2, 1), (1, 0, 1)$$

has a product equal to 1 — so the ordered and unordered readings of “product-one” are inequivalent predicates, and a development that read the definition the weaker way would prove a different theorem. The cross term of the product law uses the first factor’s a against the second factor’s b : $(xy)_c = 1$ while $(yx)_c = 0$, so reading it backwards gives the opposite group. Further: the identity is never a term of a free sequence; x^3 is not free at $p = 3$, so x occurs at most twice, and the witness of Theorem 7.1 is exactly at that ceiling, one more x breaking it; and $d(H_8) \neq 3$, $d(H_8) \neq 5$, $d(H_{27}) \neq 5$.

Proposition 8.2 (the hypotheses of Section 7). *The non-centrality hypothesis of Theorem 7.5 cannot be dropped: over H_{27} the mixed, balanced sequence $(1, 0, 0), (0, 1, 0), (2, 2, 0), (0, 0, 1)$ of length 4 has $|\Gamma| < \min(3, 3)$. The balancedness hypothesis cannot be dropped either: $x^{p-1}y^{p-1}$ is mixed, non-central, free and longer than p . The line bound of Theorem 7.3 is false at $p = 2$: three copies of $(1, 1, 0)$ over H_8 are pairwise commuting, product-one free, and longer than $2p - 2 = 2$. The growth bound is attained — over H_{125} the sequence $(1, 0, 0)^3, (0, 1, 0), (2, 4, 0)$ is mixed, balanced, non-central with $|\Gamma| = \min(5, 4)$ — so $\min(p, |l| - 1)$ cannot be raised. No upper bound below $3p - 3$ can hold, since the witness attains it; and the intermediate bound $4p - 3$ is strictly weaker than the truth at every odd p .*

Proposition 8.3 (the hypotheses of Theorem 4.1, and sharpness). *d is an isomorphism invariant, and transporting along the isomorphism of Proposition 3.1 shows that the lower bound of Corollary 5.2 is attained at $m = 1$ for odd p (value $3p - 3$) and that of Theorem 5.3 at $m = 1$ for $p = 2$ (value 4). Both hypotheses of Theorem 4.1 are necessary, inside H_8 : dropping “ $S \subseteq \ker f$ ” fails on $S = T = [x]$ with $x^2 = 1$, and dropping product-one freeness of the image fails on $T = [v, v]$, whose image is $[1, 1]$. The condition $k < \text{ord}(x)$ in x^k is sharp at $k = \text{ord}(x)$. Theorem 5.1 is neither always nor never an equality: $n(p - 1) = 3 < 4 = d(H_8)$, while $n(p - 1) = 6 = d(H_{27})$. Finally $d(H(2, 2)) \notin \{5, 32\}$ and $d(H(3, 2)) \notin \{9, 243\}$, and the constant of $H(2, 2)$ exists, so the bounds are about something.*

Proposition 8.4 (the shape of the upper bounds). *The product $(a + 1)(b + 1)$ of Theorem 4.2 cannot be shaved: with trivial kernel it is an equality. An additive analogue is false as an upper bound — over H_8 the kernel bound is 1, the image bound 2, and $d = 4 > 3$ — so Theorem 4.1 cannot be reversed. Lowering either the kernel bound or the image bound by one breaks Theorem 4.2 at H_8 . The polynomial bound of Theorem 6.1 is not tight (5 against 4 at H_8) while the $p = 2$ bound of Theorem 6.2 is exact there. Theorem 4.3 at rank 2 gives $d(C_3^2) = 4$, with 5 and 3 both refuted. The new bracket is strict at the first odd cell, $26 < 3^5 - 1$; and $d(H(3, 2)) \neq 27$, $d(H(2, 3)) \neq 14$, $d(H(2, 3)) \neq 7$. The comparison with the literature of Remark 6.3 is itself verified as a statement about numerals. Reduction modulo the centre kills the centre, ignores the third coordinate, and is not injective.*

9. VERIFICATION

Every theorem and proposition of this paper has been formally verified in Lean 4 against *Mathlib*; the development contains no `sorry` and no added axiom (repository reference to be added at submission). The remarks are not part of it, and say so: the Loewy-length bound of Remark 5.5 is a derivation from published theorems that we did not formalise, and the published values quoted in Remarks 5.4 and 6.3 are citations. All of Sections 2–6 — in particular Theorems 4.1, 4.2, 4.3, 5.1, Corollary 5.2, the main Theorem 5.3, Theorems 6.1 and 6.2, and Propositions 2.1–3.2 — depends on

no axioms beyond `propext`, `Classical.choice` and `Quot.sound`, and several statements on strictly fewer. The same holds throughout Section 7 apart from Theorem 7.2, and throughout Section 8 apart from Propositions 8.1, 8.2 and 8.3. What is delegated to compiled evaluation, through Lean’s `native_decide`, is exactly the following finite searches, all over groups of order 8, 27 or 125: the emptiness of the level-5 enumeration of sorted product-one free sequences over H_8 and the freeness of the four-term witness there (Theorem 7.2); the freeness of the six-term witness over H_{27} and the ordered-freeness of the seven-term separating sequence of Proposition 8.1 — whose companion, the product-one block inside it, is checked in the kernel; and the cardinality $|\Gamma| = 4$ of the five-term sharpness example over H_{125} in Proposition 8.2. Two statements of Proposition 8.3 inherit the two evaluations of Theorem 7.2 by quoting the value $d(H_8) = 4$; Theorem 6.2 re-proves that value with none. No theorem of Sections 4–6 depends on any compiled evaluation.

Every numerical value quoted was produced first by an independent implementation in C and the formal proof was written against it. Exhaustive search over $H(p, m)$, organised as a depth-first enumeration of sorted product-one free multisets in which the set of products over *all* orderings of each sub-multiset is carried explicitly — so that the ordering quantifier is nowhere approximated — reproduces $d(H_8) = 4$ in 68 nodes, $d(H_{27}) = 6$ in 69 053 nodes and 0.24s, and $d(H(2, 2)) = 6$ in 134 327 nodes and 0.39s, the last two agreeing with the published values of [12, 5] and [1, 16]. A second program computes the higher-order constants $d_2(C_2^n) = 3, 4, 6, 7, 9$ for $n = 1, \dots, 5$, reproducing the values $D_2 = d_2 + 1$ of [7]. Beyond that the search does not go, and we record the price rather than working around it: at order 243 the node count grows by a factor of about 58.9 per level and the needed level extrapolates to some $3 \cdot 10^{21}$ nodes; at order 128 to some 10^{11} nodes, about 83 CPU-hours. The exact value of $d(H(3, 2))$ — the first odd cell beyond H_{p^3} — is therefore out of reach of enumeration, and Theorem 6.1 leaves it bracketed in [10, 26].

REFERENCES

- [1] R. András, K. Csiszter, M. Domokos and I. Szöllősi, *The directed Cayley diameter and the Davenport constant*, in: Recent Progress in Ring and Factorization Theory, Springer Proc. Math. Stat. **477**, Springer, Cham, 2025, 1–17; doi:10.1007/978-3-031-75326-8_1; arXiv:2401.04607. Section numbers are those of arXiv:2401.04607v2.
- [2] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1–2, 7–29.
- [3] F. E. Brochero Martínez, A. Lemos, B. K. Moriya and S. Ribas, *The main zero-sum constants over $D_{2n} \times C_2$* , SIAM J. Discrete Math. **37** (2023), no. 3, 1496–1508; arXiv:2108.00823. Lemma numbers are those of arXiv:2108.00823v1.
- [4] K. Csiszter, M. Domokos and A. Geroldinger, *The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics*, in: Multiplicative Ideal Theory and Factorization Theory, Springer Proc. Math. Stat. **170**, Springer, Cham, 2016, 43–95; arXiv:1505.06059. Numbering is that of arXiv:1505.06059v3, in which Proposition 3.9 is the list of d_k -inequalities and Theorem 3.11 the list of general upper bounds.
- [5] K. Csiszter, M. Domokos and I. Szöllősi, *The Noether numbers and the Davenport constants of the groups of order less than 32*, J. Algebra **510** (2018), 513–541; doi:10.1016/j.jalgebra.2018.02.040; arXiv:1702.02997.
- [6] V. Dimitrov, *On the strong Davenport constant of nonabelian finite p -groups*, Math. Balkanica (N.S.) **18** (2004), no. 1–2, 129–140.
- [7] M. Freeze and W. A. Schmid, *Remarks on a generalization of the Davenport constant*, Discrete Math. **310** (2010), no. 23, 3373–3389; arXiv:0905.4248.
- [8] W. Gao, Y. Li and J. Peng, *An upper bound for the Davenport constant of finite groups*, J. Pure Appl. Algebra **218** (2014), no. 10, 1838–1844; doi:10.1016/j.jpaa.2014.02.009; arXiv:1308.2364. The conjecture $d(G) \leq |G|/p + p - 2$ is in the published version, not in the arXiv preprint.
- [9] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics (Boca Raton) **278**, Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [10] N. K. Godara, R. Joshi and E. Mazumdar, *An algebraic approach towards a conjecture on the Davenport constant*, preprint, arXiv:2407.01148.
- [11] N. K. Godara, R. Joshi and E. Mazumdar, *Combinatorial invariants for certain classes of non-abelian groups*, J. Number Theory **283** (2026), 44–63; doi:10.1016/j.jnt.2025.11.011; arXiv:2408.13558. Lemma numbers are those of arXiv:2408.13558v2.
- [12] N. K. Godara and S. Sarkar, *A note on a conjecture of Gao and Zhuang for groups of order 27*, J. Algebra Appl. **24** (2025), no. 11, Paper 2550268; doi:10.1142/S0219498825502688; arXiv:2311.02387.
- [13] D. J. Grynkiewicz, *The large Davenport constant II: general upper bounds*, J. Pure Appl. Algebra **217** (2013), no. 12, 2221–2246; doi:10.1016/j.jpaa.2013.03.002; arXiv:1211.2614. Lemma numbers are those of arXiv:1211.2614v1.
- [14] S. A. Jennings, *The structure of the group ring of a p -group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), no. 1, 175–185.

- [15] T. Maghradze, *The small Davenport constant of odd-prime Heisenberg groups*, Zenodo, 30 July 2026; doi:10.5281/zenodo.21708260. A preprint, not peer-reviewed and not posted on arXiv, claiming $d(H_{p^3}) = 3p - 3$ for every odd prime.
- [16] J. S. Oh, *A classification of finite groups with small Davenport constant*, Comm. Algebra **54** (2026), no. 3, 871–908; doi:10.1080/00927872.2025.2536568; arXiv:2409.00363. Lemma numbers are those of arXiv:2409.00363v2.
- [17] J. E. Olson, *A combinatorial problem on finite Abelian groups, I*, J. Number Theory **1** (1969), no. 1, 8–10; *A combinatorial problem on finite Abelian groups, II*, ibid., no. 2, 195–199.
- [18] Y. Qu, Y. Li and D. Teeuwsen, *On a conjecture of the small Davenport constant for finite groups*, J. Combin. Theory Ser. A **189** (2022), Paper 105617, 14 pp.; doi:10.1016/j.jcta.2022.105617.
- [19] Y. Qu and G. Wang, *The Gao–Zhuang conjecture for the Heisenberg group*, preprint, arXiv:2608.23319 (2026).
- [20] A. Volkmann, *The small Davenport constant of the Heisenberg group of order $3^4 3$* , preprint, arXiv:2608.13747 (2026).
- [21] A. Volkmann, *A uniform proof for the small Davenport constant of the exponent- p Heisenberg group*, preprint, arXiv:2608.18651 (19 August 2026).
- [22] P. White, *The small Davenport constant of the Heisenberg group of order 125*, preprint, arXiv:2607.14379 (2026).