Power-Saving Lower Bounds for Additive Bases of Polynomial Sequences

Alper Ferudun*

August 29, 2026

Abstract

Let $h \geq 2$ be fixed, let f be a natural-valued polynomial of degree $d \geq 2$, and suppose that $A \subseteq \mathbb{N}$ satisfies $f(\mathbb{N}) \subseteq hA$. We prove

$$|A \cap [0, X]| \geq \begin{cases} X^{4/(3hd)-o(1)}, & h \text{ even}, \\ X^{4/((3h+1)d)-o(1)}, & h \text{ odd}. \end{cases}$$

Both exponents are strictly larger than the elementary exponent $1/(hd)$. This gives an affirmative qualitative answer, for every fixed $h \geq 2$, to Problem 2.8 from the 2004 AIM problem list on recent trends in additive combinatorics. The argument combines a self-contained graph-path form of an Erdős–Newman two-basis estimate with a divisor bound for repeated differences of polynomial values. For odd h, one summand is first frozen on a large fibre and the remaining summands are then split into two equal blocks. No optimality of the displayed exponents is asserted.

1 Introduction

For a set A of nonnegative integers and an integer $h \geq 1$, write

$$hA = \{a_1 + \cdots + a_h : a_1, \ldots, a_h \in A\}, \qquad A(X) = |A \cap [0, X]|.$$

We call A an additive basis of order h for the polynomial sequence $f(1), f(2), \ldots$ if $f(n) \in hA$ for every positive integer n. The choice between the conventions $\mathbb{N} = \{0, 1, \ldots\}$ and $\mathbb{N} = \{1, 2, \ldots\}$ has no effect on the asymptotic conclusions below.

Problem 2.8, attributed to Wooley in the AIM workshop list [3], asks whether the elementary lower bound

$$A(X) \geq X^{1/(hd)-o(1)} \tag{1.1}$$

can be substantially sharpened when $d = \deg f \geq 2$. The bound (1.1) comes simply from counting h-tuples: the first N distinct values of f are contained in $h(A \cap [0, O_f(N^d)])$.

The main result gives a strict power improvement for every fixed order and every natural-valued polynomial.

*Mercury Software GmbH. Email: alper@mercurycodelab.com. GitHub: `https://github.com/AlperTheKing`.

Theorem 1.1. *Fix integers $h \geq 2$ and $d \geq 2$, and let $f \in \mathbb{R}[x]$ have degree d and satisfy $f(n) \in \mathbb{N}$ for every positive integer n. If $A \subseteq \mathbb{N}$ and*

$$f(n) \in hA \qquad (n = 1, 2, \ldots),$$

then, as $X \to \infty$,

$$A(X) \geq \begin{cases} X^{\frac{4}{3hd} - o(1)}, & h \text{ even}, \\ X^{\frac{4}{(3h+1)d} - o(1)}, & h \text{ odd}. \end{cases} \tag{1.2}$$

Equivalently, for every $\varepsilon > 0$, the corresponding power in (1.2) with its exponent decreased by ε is a lower bound for all sufficiently large X, up to a positive constant depending on f, h, ε.

For even h the gain over (1.1) is

$$\frac{4}{3hd} - \frac{1}{hd} = \frac{1}{3hd} > 0,$$

whereas for odd $h \geq 3$ it is

$$\frac{4}{(3h+1)d} - \frac{1}{hd} = \frac{h-1}{hd(3h+1)} > 0.$$

Thus Theorem 1.1 answers the literal qualitative AIM question. It does not determine the optimal exponent. Indeed, even for two-bases of powers, a much stronger lower bound of order $N^{1-o(1)}$ in the polynomial index variable is expected and remains open; see [1, 2].

The proof has two inputs. First, a finite set $S \subseteq C + C$ forces C to be large unless S has many repeated nonzero differences. This is the graph-counting mechanism of Erdős and Newman [4, Theorem 3]; we include the short proof. Second, a fixed polynomial sequence has only $N^{o(1)}$ representations of any nonzero difference among its first N values. For even h, an h-term representation is split into two equal blocks. For odd h, one summand is first fixed on a pigeonhole fibre, after which the remaining $h - 1$ terms can be split equally.

2 A finite two-basis estimate

For a finite set S of integers define its nonzero difference multiplicity by

$$\Delta(S) = \max_{t \neq 0} |\{(u, v) \in S^2 : u - v = t\}|.$$

Lemma 2.1 (Two-basis bound)**.** *There is an absolute constant $c > 0$ with the following property. If C is a finite set of nonnegative integers and $S \subseteq C + C$, then*

$$|C| \geq c\,|S|^{2/3}\big(\Delta(S) + 1\big)^{-1/3}. \tag{2.1}$$

One may take $c = 1/4$.

Proof. Put $K = |S|$ and $L = |C|$. For every $s \in S$, choose one unordered representation $s = c_s + c'_s$. These representations give a simple graph on vertex set C, with loops allowed. Different elements of S give different edges, since an unordered edge determines its sum. There are at most L loops.

If $K < 4L$, then

$$L > K/4 \geq \tfrac{1}{4}K^{2/3}(\Delta(S)+1)^{-1/3},$$

and there is nothing to prove. Suppose henceforth that $K \geq 4L$. Delete the loops, and let E be the number of remaining edges. Then $E \geq K - L \geq 3K/4$. If $d(v)$ denotes degree in this loopless graph, the number P of ordered paths $u - v - w$ with $u \neq w$ is

$$P = \sum_v d(v)(d(v)-1) \geq \frac{(2E)^2}{L} - 2E \geq \frac{K^2}{L}. \tag{2.2}$$

The first inequality is Cauchy–Schwarz. For the second, use $E \geq 3K/4$, $E \leq K$, and $K \geq 4L$.

For fixed ordered endpoints $u \neq w$, a path $u - v - w$ determines

$$s_1 = u + v, \qquad s_2 = v + w, \qquad s_1 - s_2 = u - w \neq 0.$$

There are at most $\Delta(S)$ possible ordered pairs (s_1, s_2). Once u and s_1 are fixed, the middle vertex is forced by $v = s_1 - u$. Consequently

$$P \leq L^2\Delta(S).$$

Together with (2.2), this gives $L^3\Delta(S) \geq K^2$, which proves (2.1) in the remaining case. □

The exponent $2/3$ in Lemma 2.1 is the relevant content of the Erdős–Newman estimate. We have stated the lemma only in the form needed here.

3 Repeated differences of polynomial values

Lemma 3.1. *Let $f \in \mathbb{R}[x]$ have degree $d \geq 2$ and take natural-number values at all positive integers. There is an integer $n_0 = n_0(f)$ such that, for*

$$F_N = \{f(n) : n_0 \leq n \leq N\},$$

one has

$$\Delta(F_N) = N^{o(1)}. \tag{3.1}$$

More explicitly, for every $\rho > 0$ there is a constant $C_{f,\rho}$ such that $\Delta(F_N) \leq C_{f,\rho}N^{\rho}$.

Proof. The leading coefficient of f is positive. We may therefore choose n_0 so that f and f' are strictly increasing and $f'' > 0$ on $[n_0, \infty)$.

The coefficients of f are rational: its values at any $d+1$ distinct integers are integers, and Lagrange interpolation expresses its coefficients as rational combinations of those values. Hence there is a fixed positive integer Q such that $g = Qf \in \mathbb{Z}[x]$.

Fix $t > 0$ and suppose that

$$f(i) - f(j) = t, \qquad n_0 \leq j < i \leq N.$$

Writing $q = i - j$, the polynomial divisibility $i - j \mid g(i) - g(j)$ gives

$$q \mid Qt. \tag{3.2}$$

For a fixed positive q, the function

$$y \longmapsto f(y+q) - f(y)$$

is strictly increasing on $[n_0, \infty)$, since its derivative is $f'(y+q) - f'(y) > 0$. Thus each positive divisor q of Qt contributes at most one pair (i, j), and the number of pairs is at most the divisor function $\tau(Qt)$.

For completeness, $\tau(m) \ll_\eta m^\eta$ for every $\eta > 0$. To see this, write $m = \prod p^a$. For all sufficiently large primes p one has $a + 1 \le 2^a \le p^{\eta a}$, while for each of the finitely many remaining primes the ratio $(a+1)/p^{\eta a}$ is uniformly bounded in a. Multiplication over prime factors proves the estimate. Finally, $t \le f(N) - f(n_0) = O_f(N^d)$, so the divisor estimate, with η arbitrarily small, proves (3.1). Negative differences have the same multiplicities after reversing the ordered pairs. □

4 Proof of the main theorem

Let X be large. Since $f(n) \sim an^d$ for some $a > 0$, choose $N \asymp_f X^{1/d}$ such that

$$f(n) \le X \qquad (n_0 \le n \le N), \tag{4.1}$$

where n_0 is as in Lemma 3.1. Put

$$B = A \cap [0, X], \qquad M = |B|.$$

For each $n_0 \le n \le N$, choose one ordered representation of $f(n)$ as a sum of h elements of A. Every summand lies in B, because the summands are nonnegative and their sum is at most X. The targets are distinct on this tail, and there are $N - O_f(1)$ of them.

4.1 Even order

Let $h = 2s$ and set $C = sB$. Each selected target lies in $C + C$, while

$$|C| \le M^s.$$

Apply Lemmas 2.1 and 3.1 to the set of selected targets. They give

$$M^s \ge N^{2/3 - o(1)}.$$

It follows that

$$M \ge N^{2/(3s) - o(1)} = N^{4/(3h) - o(1)} = X^{4/(3hd) - o(1)}.$$

4.2 Odd order

Let $h = 2s + 1$. If $M \ge N/2$, the claimed estimate is immediate because $4/(3h+1) < 1$. We may therefore suppose that $M < N/2$. For all sufficiently large N, at least $N/2$ targets have been selected.

Consider the first coordinate in each chosen ordered representation. It takes at most M values, so some $a \in B$ occurs on a set I of indices with

$$|I| \ge \frac{N}{2M}. \tag{4.2}$$

Define

$$S = \{f(n) - a : n \in I\}, \qquad C = sB.$$

The elements of S are distinct and nonnegative, $S \subseteq C + C$, and $|C| \le M^s$. Translation and restriction cannot increase difference multiplicity, so

$$\Delta(S) \le \Delta(F_N) = N^{o(1)}.$$

Lemmas 2.1 and 3.1, together with (4.2), yield

$$M^s \ge (N/M)^{2/3} N^{-o(1)}.$$

Equivalently,

$$M^{s+2/3} \ge N^{2/3-o(1)},$$

and hence

$$M \ge N^{2/(3s+2)-o(1)} = N^{4/(3h+1)-o(1)} = X^{4/((3h+1)d)-o(1)}.$$

This completes the proof of Theorem 1.1.

5 Context and scope

Erdős and Newman applied their two-basis method to squares and obtained the exponent $2/3 - o(1)$ in the polynomial index variable [4]. The divisor-injection argument in Lemma 3.1 shows that the same baseline applies to every fixed natural-valued polynomial. For two-bases of dth powers, Alon, Bukh, and Sudakov proved the stronger exponent

$$\frac{3}{4} - \frac{1}{2\sqrt{d}} - \frac{1}{2(d-1)} - o(1),$$

which exceeds $2/3$ beginning at $d = 48$ [1, Theorem 1.6]. Their incidence estimate is not used here.

Passing from a higher-order basis to a two-basis by grouping summands is a standard idea; it appears explicitly, in a different setting, in [2]. The odd-order fibre argument above is the additional step needed to retain a strict power gain for every odd $h \ge 3$, including $h = 3$. A search of the direct and adjacent literature located no statement of the pair of all-polynomial, all-order exponents in (1.2). Because the ingredients are elementary, the result should be described cautiously as apparently unrecorded rather than as an absolute novelty claim.

Related work on additive bases for sets with small multiplicative doubling gives different hypotheses and exponents [6]. Conversely, Ruzsa and Zhelezov constructed arbitrarily large convex sets having essentially square-root-size two-bases [5]. Thus convexity alone cannot produce the gain used here; the arithmetic divisor restriction for differences of one fixed polynomial sequence is essential.

Two boundaries are worth recording. First, when $h = 1$, the elementary exponent $1/d$ is sharp, since A must contain the polynomial sequence. Second, no universal exponent larger than $1/d$ can hold. Under the nonnegative-integer convention, $\{0\} \cup f(\mathbb{N})$ is an order-h basis for the sequence and has counting order $O(X^{1/d})$. Under the positive-integer convention, use 1 together with $f(n) - (h-1)$ for all sufficiently large n, and add finitely many elements to handle the initial values.

Theorem 1.1 therefore resolves the qualitative improvement asked for in the AIM problem, while leaving the optimal-exponent problem open.

Acknowledgements

The author thanks the American Institute of Mathematics for maintaining the problem list that motivated this note.

AI-assisted tools were used for research and manuscript preparation.

References

[1] Noga Alon, Boris Bukh, and Benny Sudakov. Discrete Kakeya-type problems and small bases. *Israel Journal of Mathematics*, 174:285–301, 2009.

[2] Boris Bukh, Peter van Hintum, and Peter Keevash. Additive bases: Change of domain. *Acta Arithmetica*, 221:239–252, 2025.

[3] Ernie Croot and Vsevolod F. Lev. Problems presented at the workshop on recent trends in additive combinatorics. American Institute of Mathematics workshop problem list, 2004. Problem 2.8, attributed to T. Wooley.

[4] Paul Erdős and Donald J. Newman. Bases for sets of integers. *Journal of Number Theory*, 9(4):420–425, 1977.

[5] Imre Z. Ruzsa and Dmitrii Zhelezov. Convex sequences may have thin additive bases, 2017.

[6] Ilya D. Shkredov and Dmitrii Zhelezov. On additive bases of sets with small product set, 2016.