SETTLING THE OPTIMAL EXPONENT RELATING SUMSETS AND DIFFERENCE SETS

Haowei Lin
PKU & Tencent
linhaowei@pku.edu.cn

Shanda Li
Carnegie Mellon University
shandal@cs.cmu.edu

Abstract. For a finite nonempty subset A of an abelian group, let $\sigma(A) = |A + A|/|A|$, $\delta(A) = |A - A|/|A|$. The classical sum–difference inequalities state that

$$\sigma(A)^{1/2} \leqslant \delta(A) \leqslant \sigma(A)^2.$$

The exponent 2 in the second inequality is known to be optimal, whereas it has remained open whether the exponent $1/2$ in the first inequality can be improved. We settle this question by constructing an explicit family of finite sets $A_K \subset \mathbb{Z}$ such that

$$\frac{\log \sigma(A_K)}{\log \delta(A_K)} \longrightarrow 2,$$

hence the exponent $1/2$ in the first inequality is also optimal.

The construction and its proof were developed with the assistance of Hyra, an AI research agent based on the open-weights Hy3 model.

1. Introduction

Let A be a finite nonempty subset of an abelian group. Its doubling and difference constants are

$$\sigma(A) = \frac{|A + A|}{|A|}, \qquad \delta(A) = \frac{|A - A|}{|A|}.$$

The classical sum–difference inequalities state

$$\sigma(A)^{1/2} \leqslant \delta(A) \leqslant \sigma(A)^2. \tag{1}$$

For a finite set $A \subset \mathbb{Z}$ with $|A| \geqslant 2$, define

$$C(A) := \frac{\log \sigma(A)}{\log \delta(A)}.$$

The problem is to determine how large $C(A)$ can be, or equivalently to determine the least *universal* exponent c for which $\sigma(A) \leqslant \delta(A)^c$. Note that (1) immediately implies that, for every finite set $A \subset \mathbb{Z}$ with $|A| \geqslant 2$,

$$C(A) \leqslant 2. \tag{2}$$

Georgiev, Gómez-Serrano, Tao, and Wagner studied this question using AlphaEvolve [4]. In their study, they used the Freiman–Pigarev value

$$\frac{\log(59/17)}{\log(55/17)} = 1.059793\ldots$$

as a baseline, and their AI-assisted search found a construction with $C(A) \approx 1.1219$. Under the present normalization, however, Penman and Wells had previously constructed a sequence (Q_j) of finite integer sets for which

$$C(Q_j) \geqslant 1.125944$$

for all sufficiently large j; see [9, 2].

We prove that the classical upper bound (2) is optimal. More precisely, our main result is the following.

Theorem 1.1. *For every positive even integer K, there is an explicitly defined finite set $A_K \subset \mathbb{Z}$ such that*

$$C(A_K) > \frac{2K}{K+3}.$$

Consequently, the least universal exponent is 2.

The sets A_K are described in (12) and (13). The proof combines a base-12 digit gadget, a three-state carry automaton, a symmetric additive basis in a cyclic group, and a Chinese remainder construction. We include all details below. We also provide a lean-based formal proof at https://github.com/linhaowei1/sum-diff-proof.

2. Proof

2.1. **A base-12 digit gadget.** Let

$$W = \{0, 1, 2, 4, 5, 9\} \subset \mathbb{Z}.$$

Reducing the corresponding sumset and difference set modulo 12, a direct calculation gives

$$(W + W) \bmod 12 = \mathbb{Z}/12\mathbb{Z}, \qquad (W - W) \bmod 12 = (\mathbb{Z}/12\mathbb{Z})\backslash\{6\}. \tag{3}$$

As an integer difference set,

$$\Delta := W - W = \{-9, -8, -7, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 7, 8, 9\}.$$

Set $n_0 = 1, Y_0 = \{0\}$. For an integer $j \geqslant 1$, put

$$n_j = 12^j, \qquad Y_j = \left\{ \sum_{i=0}^{j-1} w_i 12^i : w_i \in W \right\} \subseteq \{0, 1, \ldots, n_j - 1\}.$$

Then

$$|Y_j| = 6^j. \tag{4}$$

Lemma 2.1. *For every $j \geqslant 1$,*

$$(Y_j + Y_j) \bmod n_j = \mathbb{Z}/n_j\mathbb{Z}.$$

Proof. Since $Y_j = W + 12Y_{j-1}$, the result follows by induction from

$$(W + W) \bmod 12 = \mathbb{Z}/12\mathbb{Z},$$

lifting one base-12 digit at a time. □

We next estimate the modular difference set. For $j \geqslant 0$, define

$$t_j := |(Y_j - Y_j) \bmod n_j|.$$

Lemma 2.2. *The sequence t_j satisfies*

$$t_0 = 1, \qquad t_1 = 11, \qquad t_{j+2} = 13t_{j+1} - 16t_j \quad (j \geqslant 0).$$

In particular, if

$$\lambda = \frac{13 + \sqrt{105}}{2}, \qquad \mu = \frac{13 - \sqrt{105}}{2},$$

then

$$t_j = \frac{\sqrt{105}+9}{2\sqrt{105}}\lambda^j + \frac{\sqrt{105}-9}{2\sqrt{105}}\mu^j < \lambda^j \qquad (j \geqslant 1). \tag{5}$$

Proof. Every residue modulo 12^j has a unique balanced expansion

$$\sum_{i=0}^{j-1} \varepsilon_i 12^i, \qquad \varepsilon_i \in E := \{-6,-5,\dots,5\}.$$

The residue represented by such a balanced digit string belongs to $(Y_j - Y_j) \bmod 12^j$ if and only if there are carries

$$c_0 = 0, \qquad c_i \in \{-1,0,1\},$$

such that

$$\delta_i = \varepsilon_i + c_i - 12c_{i+1} \in \Delta \qquad (0 \leqslant i < j). \tag{6}$$

Indeed, summing (6) after multiplication by 12^i shows that the two digit strings differ by $-c_j 12^j$.

After any balanced prefix, the only possible nonempty sets of current carries are

$$X_1 = \{0\}, \qquad X_2 = \{-1,0\}, \qquad X_3 = \{0,1\}.$$

For a current carry-set X and a balanced digit ε, define

$$\Phi_\varepsilon(X) = \left\{c' \in \{-1,0,1\} : \varepsilon + c - 12c' \in \Delta \text{ for some } c \in X\right\}.$$

A check of the twelve possible values of ε gives the transition counts

	X_1	X_2	X_3
X_1	5	3	3
X_2	4	5	3
X_3	4	4	4

(7)

where rows are current states and columns are next states. Thus, with

$$M = \begin{pmatrix} 5 & 3 & 3 \\ 4 & 5 & 3 \\ 4 & 4 & 4 \end{pmatrix}, \qquad e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad \mathbf{1} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

we have

$$t_j = e_1^{\mathsf{T}} M^j \mathbf{1}.$$

A direct multiplication gives

$$M^2 - 13M + 16I_3 = \begin{pmatrix} 0 & 3 & -3 \\ 0 & 0 & 0 \\ 0 & -4 & 4 \end{pmatrix}, \qquad (M^2 - 13M + 16I_3)\mathbf{1} = 0.$$

Therefore

$$t_{j+2} - 13t_{j+1} + 16t_j = 0.$$

The initial values are $t_0 = 1$ and $t_1 = 11$. Solving the recurrence gives (5). Both coefficients in (5) are positive and sum to 1, while $0 < \mu < \lambda$, so $t_j < \lambda^j$ for $j \geqslant 1$. □

The following elementary numerical estimate will be useful.

Lemma 2.3. *We have*

$$\frac{\lambda}{12} < \frac{31}{32}, \qquad \left(\frac{31}{32}\right)^{22} < \frac{1}{2}.$$

Proof. Straightforward calculation. □

2.2. **A symmetric additive basis in a cyclic group.** Fix a positive even integer K and set

$$s = 2^K + 1, \qquad Q = s^2, \qquad m = \frac{s-1}{2}. \tag{8}$$

Inside $\mathbb{Z}/Q\mathbb{Z}$, define

$$H = \{-m, -m+1, \dots, m\}, \qquad V = \{0, s, 2s, \dots, (s-1)s\},$$

and put

$$I = H \cup V, \qquad B = I \backslash \{0\}.$$

Since $H \cap V = \{0\}$,

$$\rho := |I| = 2s - 1, \qquad |B| = 2s - 2. \tag{9}$$

Both H and V are symmetric, so $I = -I$ in $\mathbb{Z}/Q\mathbb{Z}$.

Lemma 2.4. *The set I is an additive basis of $\mathbb{Z}/Q\mathbb{Z}$:*

$$I + I = \mathbb{Z}/Q\mathbb{Z}.$$

Moreover, every $x \notin I$ lies in both $B + B$ and $B - B$.

Proof. Given $x \in \mathbb{Z}/Q\mathbb{Z}$, let $h \in H$ be the unique balanced representative of x modulo s. Then $v = x - h$ is divisible by s, so $v \in V$, and $x = h + v$. Hence $I + I = \mathbb{Z}/Q\mathbb{Z}$.

If $x \notin I$, then neither h nor v is zero. Thus $h, v \in B$ and $x = h + v \in B + B$. Since $-v \in B$, we also have $x = h - (-v) \in B - B$. □

2.3. **The CRT construction.** For a fixed positive even integer K, set

$$d = 22(K+2), \qquad n = 12^d, \qquad q = Qn, \qquad Y = Y_d, \qquad t = t_d. \tag{10}$$

Because K is even, $2^K \equiv 1 \pmod 3$; $s = 2^K + 1 \equiv 2 \pmod 3$. Also s is odd. Therefore $\gcd(Q, n) = 1$, and the Chinese remainder theorem gives

$$\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

In this product group define

$$\mathcal{R} = \big(\{0\} \times \mathbb{Z}/n\mathbb{Z}\big) \cup \big(B \times Y\big). \tag{11}$$

Let $R \subseteq \{0, 1, \dots, q-1\}$ be the set of least nonnegative representatives of the inverse image of $\mathcal{R}$. Equivalently,

$$\begin{aligned} R = \{&x \in \mathbb{Z} : 0 \leqslant x < q,\ x \equiv 0 \pmod Q\} \\ &\cup \{x \in \mathbb{Z} : 0 \leqslant x < q,\ x \bmod Q \in B,\ x \bmod n \in Y\}. \end{aligned} \tag{12}$$

Finally define the finite integer set A_K (abbreviated to A when K is fixed) by

$$\boxed{A_K = R \cup (R + q) = R + q\{0, 1\}.} \tag{13}$$

The two copies are disjoint, and hence

$$|A| = 2|R| = 2\big(n + (\rho - 1)6^d\big). \tag{14}$$

2.4. **Exact modular counts.**

Lemma 2.5. *Modulo q, the sumset of R is the whole group:*

$$|(R+R) \bmod q| = q = Qn.$$

Proof. Work in $\mathbb{Z}/Q\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. For outer coordinate 0, the sum of the full zero row with itself is full. For an outer coordinate $b \in B$, the sum of the full zero row and the row $\{b\} \times Y$ is full in the inner coordinate. Finally, if $x \notin I$, Lemma 2.4 gives $x = b_1 + b_2$ with $b_1, b_2 \in B$, and Lemma 2.1 gives $(Y+Y) \bmod n = \mathbb{Z}/n\mathbb{Z}$. Thus every outer coordinate has a full inner fiber. □

Lemma 2.6. *Modulo q, the difference set of R has cardinality*

$$|(R-R) \bmod q| = \rho n + (Q-\rho)t.$$

Proof. Again work in the CRT product. The outer coordinates in I have full inner fibers. For outer coordinate 0, use the full zero row minus itself. For $b \in B$, use the row $\{b\} \times Y$ minus the full zero row; symmetry gives the same conclusion for all of $I = -I$.

Now let $x \notin I$. Any difference with outer coordinate x must use two nonzero rows, because using the zero row would give an outer coordinate in I. Hence its inner fiber is contained in $Y - Y$. Conversely, Lemma 2.4 gives $x = b_1 - b_2$ with $b_1, b_2 \in B$, so every element of $Y - Y$ occurs. Thus each of the $Q - \rho$ outer coordinates outside I has an inner fiber of size exactly t. □

2.5. **Lifting the modular counts to integers.**

Lemma 2.7. *Let $R \subseteq \{0, 1, \ldots, q-1\}$ and let $A = R + q\{0,1\}$. Then*

$$|A + A| \geqslant 3|(R+R) \bmod q|, \qquad |A - A| \leqslant 4|(R-R) \bmod q|.$$

Proof. Fix a residue $c \pmod q$ occurring in $R + R$. Its ordinary representatives in $R + R$ have the form $c + kq$ with k in a nonempty subset of $\{0,1\}$. The block sums from $q\{0,1\} + q\{0,1\}$ have indices $\{0,1,2\}$. Therefore the integers in $A + A$ above the residue c have at least three distinct quotient indices. Summing over residues proves the first inequality.

For differences, the ordinary representatives in $R - R$ above a fixed residue have quotient indices in a nonempty subset of $\{-1, 0\}$, while the block differences have indices $\{-1, 0, 1\}$. The sum of these two index sets has at most four elements. Summing over the modular difference residues proves the second inequality. □

2.6. **The final estimate.** Define the two small parameters

$$\alpha = \frac{(\rho - 1)6^d}{n}, \qquad \beta = \frac{t}{n}.$$

Using (9), (8), and (10), we obtain

$$\alpha = (2s-2)2^{-d} = 2^{K+1-d} = 2^{-21K-43} < \frac{1}{2}. \tag{15}$$

By Lemmas 2.2 and 2.3,

$$\beta < \left(\frac{\lambda}{12}\right)^d < \left(\frac{31}{32}\right)^{22(K+2)} < 2^{-(K+2)}. \tag{16}$$

Proof of Theorem 1.1. By Lemma 2.5, Lemma 2.7, and (14),

$$\sigma(A) = \frac{|A+A|}{|A|} \geqslant \frac{3Qn}{2n(1+\alpha)} = \frac{3Q}{2(1+\alpha)} > Q = s^2,$$

where the last inequality uses $\alpha < 1/2$.

Likewise, Lemmas 2.6 and 2.7 give

$$\begin{aligned}\delta(A) &\leqslant \frac{4\big(\rho n + (Q-\rho)t\big)}{2n(1+\alpha)} \\ &= \frac{2\big(\rho + (Q-\rho)\beta\big)}{1+\alpha} < 2\rho + 2Q\beta.\end{aligned}$$

Since $s = 2^K + 1 < 2^{K+1}$, (16) implies

$$Q\beta < \frac{s^2}{2^{K+2}} < \frac{s}{2}.$$

As $\rho = 2s - 1$, it follows that

$$\delta(A) < 2(2s-1) + s = 5s - 2 < 5s < 8s.$$

Therefore

$$C(A) = \frac{\log \sigma(A)}{\log \delta(A)} > \frac{2\log s}{\log(8s)} = \frac{2\log s}{\log s + 3\log 2}.$$

The function

$$x \longmapsto \frac{2x}{x + 3\log 2}$$

is strictly increasing for $x > 0$, and $\log s > K \log 2$. Hence

$$C(A) > \frac{2K\log 2}{K\log 2 + 3\log 2} = \frac{2K}{K+3}.$$

Letting the positive even integer K tend to infinity shows that no universal exponent smaller than 2 can work, while the classical upper bound in (1) shows that the exponent 2 does work. □

Corollary 2.1. *Among finite subsets $A \subset \mathbb{Z}$ with $|A| \geqslant 2$,*

$$\sup_A C(A) = 2.$$

Proof. The equality characterization of Staps [10] gives $C(A) < 2$ for every admissible A. On the other hand, Theorem 1.1 gives a family with

$$C(A_K) > \frac{2K}{K+3} \longrightarrow 2$$

as the positive even integer K tends to infinity. □

3. Use of AI Tools

AI tools supported the exploratory and optimization stages of this work; the mathematical claims rest on the explicit construction and self-contained proofs above. Following the SimpleTES framework [12], we used Hyra [6], powered by the Hy3 model, to optimize finite-set constructions from scratch, raising the best value in its autonomous finite-search trajectory from approximately 1.14 to 1.21.

SimpleTES evaluates $C(A)$ from an explicitly enumerated Python list, so memory and enumeration costs limit the size of searchable sets. We therefore allowed agents to

TABLE 1. Published and manuscript-internal result comparison.

Date	Method, reference, and system	Value / bound
Published mathematical constructions		
Unknown	Conway eight-point MSTD set [8, 5]	1.0344
1969	Marica [7]	1.0290
1973	Freiman–Pigarev [3]	1.0598
2013	Penman–Wells family [9, 2]	1.1259
Published agent-search results		
2025-11	AlphaEvolve (Gemini 2.0 Pro + Flash) [4]	1.1219
2025-12	LoongFlow (DeepSeek-R1-250528) [11, 1]	1.1035
2026-04	SimpleTES (gpt-oss-120b) [12]	1.1440
2026-04	SimpleTES with post-training (gpt-oss-120b) [12]	1.1449
2026-07	OpenHands (GPT-5.4 medium) [13]	1.0786
2026-07	OpenClaw (GPT-5.4 medium) [13]	1.1099
2026-07	Codex (GPT-5.4 medium) [13]	1.1121
2026-07	EvoMaster (GPT-5.4 medium) [13]	1.1207
Exploratory runs reported only in this manuscript		
2026-07	Claude Fable 5	1.1133
2026-07	Codex (GPT-5.5) with human guidance	1.2851
Theorem proved in this work		
2026-07	Explicit family A_K (this work; Hyra with Hy3)	$\sup C(A) = 2$

propose constructions and supporting arguments in natural language. Using GPT-5.6 Sol as the judge, we ran Hyra for approximately 24 hours, producing the construction underlying the paper. The LLM-based judgment was used only to guide exploration, not to certify mathematical correctness. We then independently checked the construction and proof, corrected the exposition, and prepared the argument presented here manually.

For context, we also tested Claude Fable 5 and Codex (GPT-5.5) with human guidance. Table 1 places the manuscript-internal runs alongside published constructions and agent-search results. We also used GPT-5.6 Sol to convert natural-language proofs into verifiable Lean 4 formal proofs (`https://github.com/linhaowei1/sum-diff-proof`).

4. CONCLUSION

We determine the optimal universal exponent relating sumsets and difference sets. For every positive even integer K, our explicit construction satisfies

$$C(A_K) > \frac{2K}{K+3},$$

and hence $C(A_K) \to 2$ as $K \to \infty$. Together with the classical inequality $\sigma(A)^{1/2} \leqslant \delta(A)$, this proves that the least exponent c for which $\sigma(A) \leqslant \delta(A)^c$ holds for every finite nonempty set $A \subset \mathbb{Z}$ is exactly 2.

The supremum is approached but, by Staps' characterization of the equality cases, is not attained by any integer set with at least two elements [10].

Acknowledgments

We thank Letian Huang and Shuo Zhou from Peking University, Baihe Huang from UC Berkeley, and Honghao Lin from Carnegie Mellon University for helpful discussions. We also thank the Hyra team at Tencent Hunyuan for their work on Hyra.

References

1. Baidu Baige, *LoongFlow source repository and sum–difference example*, https://github.com/baidu-baige/LoongFlow, 2026, Accessed 2026-07-29.
2. Jonathan Cutler, Luke Pebody, and Amites Sarkar, *Sums, differences and dilates*, 2024.
3. G. A. Freiman and V. P. Pigarev, *The relation between the invariants r and t*, Number-Theoretic Studies in the Markov Spectrum and in the Structural Theory of Set Addition, Kalinin State University, Moscow, 1973, The surname is also transliterated as Pigaev in some sources, pp. 172–174 (Russian).
4. Bogdan Georgiev, Javier Gómez-Serrano, Terence Tao, and Adam Zsolt Wagner, *Mathematical exploration and discovery at scale*, 2025.
5. Peter V. Hegarty, *Some explicit constructions of sets with more sums than differences*, Acta Arithmetica **130** (2007), no. 1, 61–77.
6. Hyra Team, *Hyra: Hunyuan research agent*, https://hy.tencent.com/research/hyra, 2026, Accessed 2026-07-29.
7. Joseph Marica, *On a conjecture of conway*, Canadian Mathematical Bulletin **12** (1969), no. 2, 233–234.
8. Melvyn B. Nathanson, *Problems in additive number theory, V: Affinely inequivalent MSTD sets*, North-Western European Journal of Mathematics **3** (2017), 123–141.
9. David Penman and Matthew Wells, *On sets with more restricted sums than differences*, Integers **13** (2013), A57, 24 pages.
10. Merlijn Staps, *The relative sizes of sumsets and difference sets*, Integers **15** (2015), A42.
11. Chunhui Wan, Xunan Dai, Zhuo Wang, Minglei Li, Yanpeng Wang, Yinan Mao, Yu Lan, and Zhiwen Xiao, *LoongFlow: Directed evolutionary search via a cognitive plan–execute–summarize paradigm*, 2025.
12. Haotian Ye, Haowei Lin, Jingyi Tang, Yizhen Luo, Rahul Thapa, Caiyin Yang, Chang Su, Rui Yang, Ruihua Liu, Rundao Li, Zeyu Li, Pengwei Sun, Chong Gao, Dachao Ding, Guangrong He, Miaolei Zhang, Lina Sun, Wenyang Wang, Yuchen Zhong, Zhuohao Shen, Puheng Li, Pan Lu, Bianxiao Cui, Di He, Jianzhu Ma, Junfeng Li, Hexi Baoyin, Yejin Choi, Stefano Ermon, Xiaowen Chu, Tongyang Li, Yuzhi Xu, and James Zou, *Structured scaling of AI discovery across diverse scientific domains*, 2026, Version 2, revised 27 July 2026; version 1 was titled "Evaluation-driven Scaling for Scientific Discovery".
13. Xinyu Zhu, Yuzhu Cai, Zexi Liu, Cheng Wang, Fengyang Li, Wenkai Jin, Wanxu Liu, Zehao Bing, Bingyang Zheng, Jingyi Chai, Shuo Tang, Rui Ye, Yuwen Du, Xianghe Pang, Yaxin Du, Tingjia Miao, Yuzhi Zhang, Ruoxue Liao, Zhaohan Ding, Linfeng Zhang, Yanfeng Wang, Weinan E, and Siheng Chen, *EvoMaster: A foundational evolving agent framework for agentic science at scale*, 2026, Version 4, revised 1 July 2026.