GAP-SEQUENCE INVARIANTS OF SIDON SETS: AN ORDER-SENSITIVE ESCAPE FROM AUTOCORRELATION THAT CANNOT MATCH ERDŐS–TURÁN

LIGHTMAN CHANG

Abstract. For a Sidon set $S = \{s_1 < s_2 < \cdots < s_k\} \subset [0, N]$ with gap sequence $g_i := s_{i+1} - s_i$ we examine the *second gap moment* $M_2(S) := \sum_{i=1}^{k-1} g_i^2$ and the centered moments $m_{2r}(S) := \sum_i (s_i - \bar{s})^{2r}$. We first record a 49-year-old empirical fact made explicit only in 2026: the Bloom–Golomb 1977 homometric Sidon pair $(R(3, -2), \mathrm{refl}S(3, -2))$, equivalently $A = \{0, 1, 5, 7, 15, 18\}$ and $B = \{0, 1, 3, 8, 14, 18\}$, has identical autocorrelation r_{S-S} but differs in M_2 (94 versus 82) and in the centered higher moments m_6, m_8. Hence the gap-moment invariants M_p and m_{2r} for $r \geq 3$ genuinely escape the natural Fourier-kernel observation that "the most-studied shift-invariant Sidon invariants factor through r_{S-S}." Our main contribution is the negative result Theorem 4.7; Theorem 3.1 documents the empirical M_2-discrepancy on the Bloom–Golomb 1977 pair that motivates the impossibility analysis. The natural follow-up question is whether M_2, or a similar order-sensitive gap-moment, can give a non-trivial upper bound on $|S|$. Theorem 4.7 answers in the negative: the only Sidon-derivable lower bound on M_2 via the gap sequence, combined with the trivial $M_2 \leq N^2$, yields $k = O(N^{2/3})$, strictly weaker than the Erdős–Turán bound $\sqrt{2N} + O(1)$. We compute M_2 explicitly on Bose–Chowla constructions for primes $p \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$ and observe the saturation $M_2 = \Theta(N^{3/2})$. We propose this combined behaviour – an escape from the autocorrelation kernel paired with a structural weakness in the upper-bound direction – as a diagnostic label for the systematic exploration of additive-combinatorial invariants on Sidon sets.

1. Introduction

1.1. Sidon sets and the Erdős–Sidon question.

A finite set $S \subset \mathbb{Z}$ is a *Sidon set* (or B_2-set, in Sidon's original 1932 terminology [16]) if all its ordered pairwise nonzero differences are distinct. Equivalently, the autocorrelation

$$r_{S-S}(d) := \#\{(a, b) \in S^2 : a - b = d\}$$

Date: May 19, 2026.

2020 *Mathematics Subject Classification.* Primary 11B83, 11B30; Secondary 11B13.

Key words and phrases. Sidon set, B_2-set, gap sequence, second gap moment, homometric pair, Bloom–Golomb, Bose–Chowla, autocorrelation, Erdős–Turán bound, order-sensitive invariant.

satisfies $r_{S-S}(0) = |S|$ and $r_{S-S}(d) \in \{0,1\}$ for $d \neq 0$. Sidon sets in $[1,N]$ satisfy $|S| \leq \sqrt{2N} + O(1)$ (Erdős–Turán [8]), and the sharper $|S| \leq \sqrt{N} + N^{1/4} + 1$ (Lindström [10]); from below, the Singer [17] and Bose–Chowla [5] constructions give $|S| \geq \sqrt{N} - O(N^{1/2-c})$. Closing the remaining gap is the long-standing Erdős–Sidon problem; recent analytic improvements include Balogh–Füredi–Roy [2] and Carter–Hunter–O'Bryant [6], both of which sharpen Lindström's constant inside the same $\sqrt{N} + O(N^{1/4})$ scale and stay within the autocorrelation / Fourier kernel. The annotated bibliography of O'Bryant [12] surveys the area.

1.2. Folklore: most studied invariants factor through r_{S-S}.

Many shift-invariant Sidon invariants of interest are functions of the autocorrelation r_{S-S} alone, and the standard upper-bound techniques exploit this exclusively. Lindström's bound is derived from $\sum_d r_{S-S}(d)^2$ via Parseval; the Bloom–Sisask restriction-style refinements [3] use higher Fourier energies $\int |\widehat{\mathbf{1}_S}|^p$; the additive-combinatorial work of Tao–Vu [19] and Ortega–Prendiville [13] likewise operates on quantities expressible through r_{S-S}.

This phenomenon – "shift-invariant Sidon invariants factor through r_{S-S}" – is folklore in the sense that no published Sidon paper appears to have isolated invariants outside this class for the *purpose* of size bounds. It is not, however, a theorem: an order-sensitive invariant can be shift-invariant in the sense that $\mathcal{I}(S+t) = \mathcal{I}(S)$ for every t keeping S inside the ambient interval, yet depend on the linear ordering of S through gaps or partial sums.

1.3. Gap-sequence invariants.

For $S = \{s_1 < \cdots < s_k\} \subset [0,N]$, define the *gap sequence*

$$g_i := s_{i+1} - s_i, \qquad i = 1, \ldots, k-1,$$

the *p-th gap moment* $M_p(S) := \sum_{i=1}^{k-1} g_i^p$, the *centered* $2r$*-th moment* $m_{2r}(S) := \sum_{i=1}^{k} (s_i - \bar{s})^{2r}$ with $\bar{s} = \frac{1}{k}\sum_i s_i$, the *gap multiset* $G_k(S) := \{g_1, \ldots, g_{k-1}\}$, and the *span* $\sigma(S) := s_k - s_1$. Each is invariant under shifting S inside the integers; only G_k ignores the linear ordering, and even G_k does so only by symmetrising over a sequence that intrinsically arose from the ordering.

The first contribution of this note is the observation that these invariants are *not* functions of r_{S-S}. Section 3 proves

$$M_2(\{0,1,5,7,15,18\}) = 94 \neq 82 = M_2(\{0,1,3,8,14,18\}),$$

on a homometric pair whose autocorrelations coincide, and similarly records the discrepancies $m_6(A) \neq m_6(B)$, $m_8(A) \neq m_8(B)$, $G_k(A) \neq G_k(B)$. The pair (A,B) has been known since Bloom–Golomb 1977 [4]; what we add is the computation of the gap-moment discrepancy on the 49-year-old pair, which appears never to have been recorded.

1.4. The negative theorem.

The natural follow-up question is whether the escape from the r_{S-S}-kernel buys anything in the upper-bound direction.

The second and main contribution of this note (Section 4) is that it does not.

Theorem 1.1 (Main; cf. Theorem 4.7)**.** *Let $S \subset [0, N]$ be a Sidon set with $|S| = k$. Any size bound on k derivable from*

- (C1) *the gap-distinctness $g_i \neq g_j$ for $i \neq j$ (a direct consequence of the Sidon property), and*
- (U) *the trivial $M_2 \leq N^2$,*

yields at best $k \leq (3N^2)^{1/3} = O(N^{2/3})$, strictly weaker than the Erdős–Turán bound $\sqrt{2N} + O(1)$.

A few remarks. First, (C1) is one of three Sidon-derivable gap-sequence properties (the others, (C2) and (C3), are recorded in Section 4); these stronger properties refine (C1) but, as we show, all of them route through Erdős–Turán's $\binom{k}{2} \leq N$ counting and add no asymptotic improvement. Second, the bound $k = O(N^{2/3})$ is genuinely worse than Erdős–Turán, not merely worse than Lindström: the M_2-derived obstacle is therefore a structural weakness of gap-moment language, not a fixable constant. Third, the theorem applies just as forcefully to higher gap moments M_p for $p \geq 3$ and to centered higher moments m_{2r} for $r \geq 3$ (Section 6).

1.5. **Empirical anchor: Bose–Chowla numerics.** Section 5 computes $M_2(S_{\mathrm{BC}}(p))$ on the Bose–Chowla construction $S_{\mathrm{BC}}(p) \subset \mathbb{Z}/(p^2 - 1)$ for the primes $p \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$. The empirical saturation is

$$M_2(S_{\mathrm{BC}}(p)) = \Theta(N^{3/2}), \qquad N = p^2 - 1,$$

with the ratio fluctuating in $[0.68, 1.77]$ across the surveyed range, and the Cauchy–Schwarz saturation ratio $M_2(k-1)/\sigma^2$ in $[1.44, 1.88]$. The numerics confirm the heuristic regime of the negative theorem: Bose–Chowla saturates the Cauchy–Schwarz lower bound by a constant factor, no Sidon-specific upper bound on M_2 is implied by the construction, and the would-be implication "small $M_2 \Rightarrow$ large $|S|$" is unavailable.

1.6. **Position relative to prior work.** The pair (A, B) is from Bloom–Golomb [4], who used it to refute Piccard's 1939 uniqueness theorem for difference sets in the crystallographic context; they did not compute any gap-moment invariant on it. Cilleruelo [7] studied gap sequences for Sidon, but for the L^∞ statistic $\max_i g_i$, not for any L^p moment. The classical L^2 *autocorrelation moment* $\sum_d r_{S-S}(d)^2$ and its weighted variants $\sum_d r_{S-S}(d)\, d^{2r}$ appear in the additive-combinatorial literature via the Plancherel / L^4-energy identity for Sidon sets [19, Prop. 4.29 and §§6.1–6.2]; this is not the same quantity as the gap moment $\sum_i g_i^{2r}$, and we make this distinction explicit in Section 3. The post-2020 Sidon-bound work of Balogh–Füredi–Roy [2] and Carter–Hunter–O'Bryant [6] sharpens Lindström's Fourier argument within the r_{S-S}-kernel, and so does not address gap moments as $|S|$-controllers. The turnpike / partial-digest literature (Skiena–Smith–Lemke [18], and the crystallographic homometric-pair survey of Grimm–Baake [9]) is concerned with the *algorithmic* ambiguity inherent in r_{S-S}, not with positive distinguishing invariants of the order-sensitive type considered here.

A companion note [14] treats the same pair (A,B) from the Gowers-uniformity-norm angle: it records that the integer cube count $T_k(S)$ satisfies the rigid identity $T_k(S) = n + k\,n(n-1)$ for any integer Sidon set, and analyses the cyclic U^3 behaviour of (A,B) on $\mathbb{Z}/N\mathbb{Z}$. The two notes share the pair (A,B) but treat different invariants and reach different conclusions; we cite the companion at the appropriate point in Section 3.

1.7. **An order-sensitive failure mode.** In Section 7 we propose the combined behaviour – *escape from the autocorrelation kernel paired with a structural weakness in the upper-bound direction* – as a diagnostic label for the systematic exploration of additive-combinatorial invariants on Sidon sets. We refer to this label as *order-sensitive Sidon-weakness.* The naming is modest: we do *not* claim a Razborov–Rudich-style barrier in the sense of [15] or the relativisation surveys of Aaronson–Wigderson [1]. We claim only that the structure of Sidon's B_2 condition, when transferred into gap-sequence language, is too weak to give upper bounds matching even Erdős–Turán, let alone Lindström, and that recognising this as a pattern is prima facie useful for cataloguing future invariant-search efforts.

1.8. **Structure.** Section 2 fixes notation. Section 3 proves that gap-moment invariants escape the autocorrelation kernel via the Bloom–Golomb pair (A,B) and contrasts the gap moment $\sum g_i^{2r}$ with the autocorrelation moment $\sum_d r_{S-S}(d)d^{2r}$. Section 4 contains the main negative theorem and its proof. Section 5 records the Bose–Chowla numerical table. Section 6 extends the negative theorem to higher moments and gap-distribution statistics. Section 7 discusses the failure mode and its position relative to the structural-barrier literature. Section 8 lists open questions.

2. SETUP AND NOTATION

Throughout $S = \{s_1 < s_2 < \cdots < s_k\} \subset \{0,1,\ldots,N\}$ is a finite Sidon set in the integers, with cardinality $k = |S|$, span $\sigma = \sigma(S) := s_k - s_1$, and gap sequence $g_i := s_{i+1} - s_i$ for $i = 1,\ldots,k-1$.

Definition 2.1 (Gap and centered moments)**.** For $p \geq 1$ and $r \geq 1$ define

$$M_p(S) := \sum_{i=1}^{k-1} g_i^p, \qquad m_{2r}(S) := \sum_{i=1}^{k} (s_i - \bar{s})^{2r}, \qquad \bar{s} := \frac{1}{k}\sum_{i=1}^{k} s_i.$$

The *gap multiset* is $G_k(S) := \{\{g_1,\ldots,g_{k-1}\}\}$ (an unordered multiset).

Definition 2.2 (Homometric pair)**.** Two finite integer sets S, S' are *homometric* if $r_{S-S} = r_{S'-S'}$ as functions $\mathbb{Z} \to \mathbb{Z}_{\geq 0}$. We always consider homometric pairs up to translation and reflection.

All invariants in Definition 2.1 are shift-invariant on $\mathbb{Z}$: $M_p(S+t) = M_p(S)$, $m_{2r}(S+t) = m_{2r}(S)$, and $G_k(S+t) = G_k(S)$ for every $t \in \mathbb{Z}$ keeping S in the ambient interval, as is immediate from the definitions.

3. Gap-moment invariants escape the autocorrelation kernel

3.1. **The Bloom–Golomb homometric Sidon pair.** The Bloom–Golomb two-parameter family of homometric Sidon pairs [4, Theorem 3] is

$$\begin{aligned} R(u,v) &= \{0,\ u,\ u+v,\ 4u+2v,\ 6u+2v,\ 8u+3v\}, \\ S(u,v) &= \{0,\ u,\ 5u+v,\ 5u+2v,\ 7u+2v,\ 8u+3v\}, \end{aligned} \tag{1}$$

which produces a Sidon-homometric pair for generic $(u,v) \in \mathbb{Z}^2$. For $(u,v) = (3,-2)$ one computes

$$R(3,-2) = \{0,1,3,8,14,18\}, \qquad S(3,-2) = \{0,3,11,13,17,18\},$$

and the reflection $x \mapsto 18-x$ of $S(3,-2)$ is $\{0,1,5,7,15,18\}$. The following pair has been known for nearly half a century:

$$A := \{0,1,5,7,15,18\}, \qquad B := \{0,1,3,8,14,18\}. \tag{2}$$

Both are integer Sidon sets in $[0,18]$; both have the same multiset of 30 ordered nonzero pairwise differences

$$D_A = D_B \;=\; \pm\{1,2,3,4,5,6,7,8,10,11,13,14,15,17,18\}.$$

The two are not related by translation, reflection, or their composition: their gap sequences $(1,4,2,8,3)$ for A and $(1,2,5,6,4)$ for B are neither cyclic rotations nor reversals of each other. Both observations are immediate by direct enumeration; the homometric property is by [4].

3.2. The discrepancy in M_2, m_6, m_8, and G_k.

Theorem 3.1. *The pair* (A,B) *of* (2) *satisfies* $r^A_{S-S} = r^B_{S-S}$ *but*

$$\begin{aligned} &M_2(A) = 94, && M_2(B) = 82, \\ &m_6(A) = 404\,393\,894/243 \approx 1\,664\,172.40, && m_6(B) = 434\,331\,494/243 \approx 1\,787\,372.40, \\ &m_8(A) = 337\,231\,557\,910/2187 \approx 154\,198\,243.21, && m_8(B) = 399\,262\,265\,110/2187 \approx 182\,561\,620.99, \\ &G_k(A) = \{1,2,3,4,8\}, && G_k(B) = \{1,2,4,5,6\}. \end{aligned}$$

In particular, M_2*,* m_6*,* m_8*, and the gap multiset* G_k *are not functions of* r_{S-S} *for size-*6 *Sidon sets in* $[0,18]$.

Proof. The autocorrelation equality $r^A_{S-S} = r^B_{S-S}$ is immediate from $D_A = D_B$. For M_2: the gap sequences are $(1,4,2,8,3)$ for A and $(1,2,5,6,4)$ for B, hence $M_2(A) = 1+16+4+64+9 = 94$ and $M_2(B) = 1+4+25+36+16 = 82$. For m_6, m_8: the means differ, $\bar{s}_A = 46/6 = 23/3$ and $\bar{s}_B = 44/6 = 22/3$. Direct rational arithmetic in $\mathbb{Q}$ yields the centered moments

$$m_2(A) = m_2(B) = 814/3, \quad m_4(A) = m_4(B) = 177970/9,$$

and

$$m_6(A) = 404393894/243 \;\neq\; 434331494/243 = m_6(B),$$

$$m_8(A) = 337231557910/2187 \neq 399262265110/2187 = m_8(B).$$

The explicit rational forms are reproduced exactly by the supporting Python script (Remark 5.4). For G_k: read off from the gap sequences above. □

We remark that the equality $m_4(A) = m_4(B)$ in Theorem 3.1 is in fact *forced* by $r^A_{S-S} = r^B_{S-S}$ for any size-k Sidon set, by the algebraic identity recorded in the next subsection. The discrepancy in m_6 and m_8 is therefore the first centered moment for which order-sensitivity becomes visible.

3.3. **Centered moments: which factor through r_{S-S}?** For finite $S \subset \mathbb{Z}$ of size k, define power sums $p_j(S) := \sum_i s_i^j$ for $j \geq 0$. The identity

$$\sum_{a,b\in S} (a-b)^{2r} \;=\; \sum_{d\neq 0} r_{S-S}(d)\cdot d^{2r} \tag{3}$$

(where $r_{S-S}(d) = \#\{(a,b) \in S^2 : a-b = d\}$ already counts ordered pairs) expresses the symmetrised autocorrelation moment as an explicit polynomial in $p_0, p_1, \ldots, p_{2r}$. After translation to $p_1 = 0$ (translation invariance), the right-hand side becomes a polynomial in the centered power sums $p_2, \ldots, p_{2r}$.

Lemma 3.2. *For any finite $S \subset \mathbb{Z}$ with $|S| = k$, the centered fourth moment $m_4(S)$ is a polynomial function of $\{r_{S-S}(d)\}_{d\in\mathbb{Z}}$ and k alone; in particular, $m_4(S)$ depends only on the autocorrelation of S, modulo translation.*

Proof. After translating so that $\bar{s} = 0$ (equivalently $p_1 = 0$), the centered moment satisfies $m_4 = p_4$ where $p_j := \sum_i s_i^j$. Expanding by the binomial theorem and using antisymmetric cancellation,

$$\sum_{a,b\in S} (a-b)^4 \;=\; 2k\,p_4 - 8p_1p_3 + 6p_2^2 \;=\; 2k\,p_4 + 6p_2^2.$$

The left-hand side equals $\sum_d r_{S-S}(d)d^4$, so p_4 is expressible as $p_4 = \big(\sum_d r_{S-S}(d)d^4 - 6p_2^2\big)/(2k)$. Since $p_2 = (1/(2k))\sum_d r_{S-S}(d)d^2$ is itself a polynomial in r_{S-S} and k – this being the $r = 1$ case of (3) – the combined expression realises $m_4 = p_4$ as a polynomial in $\{r_{S-S}(d)\}_d$ and k. The explicit closed form, while straightforward to write down, is not load-bearing in the sequel and we suppress it. □

Lemma 3.3. *For $r \geq 3$, the centered moment m_{2r} is* not *a function of r_{S-S}, even modulo translation.*

Proof. The argument of Lemma 3.2 extends to m_{2r} as follows. Write m_{2r} (after centering, $p_1 = 0$) as a polynomial in the centered power sums $p_2, p_3, \ldots, p_{2r}$. The *odd* centered power sums $p_3, p_5, \ldots, p_{2r-1}$ are *not* recoverable from r_{S-S} alone: indeed, $\sum_{i,j}(s_i - s_j)^{2\ell+1} = 0$ identically by antisymmetry, so the autocorrelation moments of odd order vanish and cannot pin down the odd power sums of S. For $r = 3$, m_6 contains a non-zero p_3^2 coefficient in its expansion; for $r = 4$, m_8 contains p_3p_5 and $p_3^2p_2$ terms; in each case the unrecoverable p_3 enters non-trivially. Theorem 3.1 exhibits an explicit pair on which the resulting freedom is realised: with centered

$A' := A - 23/3$ and $B' := B - 22/3$ (the two means differ; see Theorem 3.1), one computes $p_3(A') = 6584/9 \neq 7024/9 = p_3(B')$, so the centered odd power-sum p_3 separates the pair and the p_3^2 contributions to m_6 differ accordingly. □

The same algebraic mechanism applies to M_p and to the gap multiset G_k. The gap sequence $(g_1, \dots, g_{k-1})$ depends on the *linear ordering* of S, and the autocorrelation r_{S-S} encodes only the symmetric multiset of differences with no record of which differences arise from consecutive pairs.

3.4. Comparison with autocorrelation moments.

The classical L^2-autocorrelation estimate for Sidon sets [19, Prop. 4.29 and §§6.1–6.2] is the additive-energy identity

$$\sum_d r_{S-S}(d)^2 \;=\; \underbrace{k^2}_{d=0} + \underbrace{k(k-1)}_{d\neq 0} \;=\; 2k^2 - k, \tag{4}$$

i.e. $E(S,S) = 2k^2 - k$ for the Sidon set S, via the Plancherel–Parseval expansion of $\|\mathbf{1}_S\|_{U^2}^4$; the more refined weighted moments $\sum_d r_{S-S}(d)\, d^{2r}$ enter the Bloom–Sisask restriction work [3], the Carter–Hunter–O'Bryant analysis [6], and earlier Fourier-uniformity analyses of Lindström [10]. *These are all moments of the autocorrelation function* r_{S-S}, not moments of the gap sequence g. We emphasise the distinction:

$$\underbrace{\sum_d r_{S-S}(d)\, d^{2r}}_{\text{autocorrelation moment}} \;\neq\; \underbrace{\sum_i g_i^{2r} = M_{2r}(S)}_{\text{gap moment}}. \tag{5}$$

The left-hand side of (5) is a function of r_{S-S} by construction. The right-hand side is, by Theorem 3.1 at $r = 1$, not a function of r_{S-S}. The classical fourth-moment Sidon literature is exclusively concerned with the left-hand side; the gap-moment side is the object of this note.

A separate companion observation in [14] records that the integer Gowers cube count $T_k(S) = n + k\, n(n-1)$ for a Sidon set of size n is rigidly determined by $|S|$ alone, hence in particular agrees on (A, B): $T_k(A) = T_k(B) = 6 + 30k$ for every $k \geq 1$. The cyclic U^3 norms of A, B on $\mathbb{Z}/N\mathbb{Z}$, by contrast, are shown in [14] to disagree at $N \in \{41, 43\}$. The two notes treat orthogonal invariants of the same pair, and neither implies the conclusions of the other.

4. Main theorem: M_2 cannot improve on Erdős–Turán

In this section we prove that any size bound on a Sidon set $S \subset [0, N]$ obtained from the gap sequence g via elementary analytic tools yields at best $|S| = O(N^{2/3})$. The argument proceeds in three steps. First (§4.1) we record the elementary lower bound on M_2 available from Cauchy–Schwarz. Second (§4.2) we enumerate the Sidon-derivable constraints (C1)–(C3) on the gap sequence. Third (§4.3) we combine these with the trivial upper bound $M_2 \leq N^2$ and observe that the optimal implication is the displayed weaker $k = O(N^{2/3})$.

We emphasise at the outset that the argument below is elementary – essentially Cauchy–Schwarz combined with the Sidon gap-distinctness Lemma 4.2. The point of Theorem 4.7 is not technical novelty but structural inevitability: any Sidon-derivable lower bound on M_2 phrased in gap-sequence language must route through gap distinctness ($g_i \geq i$ for some enumeration), which is itself a one-line consequence of the Sidon property. Combined with the sharp trivial upper bound $M_2 \leq N^2$, the resulting size bound is intrinsically $k = O(N^{2/3})$, weaker than Erdős–Turán. We take this explicit failure of the most natural gap-moment route to be the content of the theorem: the impossibility is structural, not technical.

4.1. **Cauchy–Schwarz baseline.**

Lemma 4.1 (Cauchy–Schwarz on gaps)**.** *For every $S \subset [0, N]$ with $|S| = k \geq 2$,*

$$M_2(S) \cdot (k-1) \;\geq\; \sigma(S)^2.$$

Proof. By Cauchy–Schwarz applied to the inner product $\langle g, \mathbf{1} \rangle = \sum_i g_i \cdot 1 = \sigma(S)$,

$$\sigma(S)^2 = \Big(\sum_{i=1}^{k-1} g_i \cdot 1\Big)^2 \leq \Big(\sum_i g_i^2\Big) \cdot \Big(\sum_i 1^2\Big) = M_2(S) \cdot (k-1).$$

Equality holds iff all g_i are equal. □

Lemma 4.1 is universal (does not use Sidon) and is tight when g is arithmetic. For applications below we need also a lower bound on σ, which the Sidon constraint provides.

4.2. **Sidon-derivable constraints on the gap sequence.**

For a Sidon set $S = \{s_1 < \cdots < s_k\} \subset [0, N]$ the gap sequence $g = (g_1, \ldots, g_{k-1})$ enjoys the following properties.

Lemma 4.2 (Sidon ⇒ gap distinctness)**.** *For every Sidon set S with $|S| = k$, the gaps $g_1, \ldots, g_{k-1}$ are pairwise distinct positive integers.*

Proof. If $g_i = g_j$ for some $i \neq j$ then $s_{i+1} - s_i = s_{j+1} - s_j$, hence $r_{S-S}(g_i) \geq |\{(i+1, i), (j+1, j)\}| = 2$, contradicting Sidon. □

Lemma 4.3 (Consecutive partial sums)**.** *For every Sidon set S with $|S| = k$, the consecutive partial sums $\{g_a + g_{a+1} + \cdots + g_b : 1 \leq a \leq b \leq k-1\}$, of which there are $\binom{k}{2}$, are pairwise distinct positive integers, all bounded above by $\sigma(S) \leq N$.*

Proof. A consecutive partial sum $g_a + \cdots + g_b$ equals $s_{b+1} - s_a$, which is one of the $\binom{k}{2}$ positive pairwise differences of S. By Sidon these are all distinct. □

We refer to Lemmas 4.2 and 4.3 as *constraints (C1) and (C3)*, respectively. A weaker intermediate constraint

(C2) consecutive pair-sums $g_i + g_{i+1}$ ($i = 1, \dots, k-2$) are distinct,

is a special case of (C3).

Lemma 4.4 (Erdős–Turán from (C3))**.** *For every Sidon set $S \subset [0, N]$ with $|S| = k$,*

$$\binom{k}{2} \le N, \qquad \textit{equivalently} \qquad k \le \sqrt{2N} + O(1).$$

Proof. By Lemma 4.3 there are $\binom{k}{2}$ distinct positive integers in $[1, N]$, so $\binom{k}{2} \le N$. ☐

Lemma 4.5 (Lower bound on M_2 from (C1))**.** *For every Sidon set S with $|S| = k$,*

$$M_2(S) \;\ge\; \sum_{i=1}^{k-1} i^2 \;=\; \frac{(k-1)k(2k-1)}{6}.$$

Equality holds only if g is a permutation of $\{1, 2, \dots, k-1\}$.

Proof. By Lemma 4.2 the values $g_1, \dots, g_{k-1}$ are distinct positive integers, so their multiset majorises $\{1, 2, \dots, k-1\}$ in the sense of distinct positive integers. The minimum of $\sum g_i^2$ over $k-1$ distinct positive integers is achieved by the smallest such multiset, which is $\{1, 2, \dots, k-1\}$, with value $\sum_{i=1}^{k-1} i^2 = (k-1)k(2k-1)/6$. ☐

Lemma 4.6 (No Sidon-derivable upper bound on M_2 better than N^2)**.** *For every $k \ge 2$ and every $N \ge \binom{k}{2}$ there exists a Sidon set $S \subset [0, N]$ with $|S| = k$ and*

$$M_2(S) \;\ge\; (1 - o(1))N^2 \qquad (N \to \infty),$$

where the $o(1)$ is uniform for $k = o(N^{1/3})$. Consequently, no Sidon-derivable inequality of the form $M_2(S) \le \alpha N^2$ for $\alpha < 1$ is available.

Proof. Take a Mian–Chowla-style greedy Sidon set [11] $T_{k-1} = \{0 = t_1 < t_2 < \cdots < t_{k-1}\} \subset [0, c(k-1)^3]$ with all pairwise differences distinct and $t_{k-1} \le ck^3$ for an absolute constant c; for $k = o(N^{1/3})$ the value ck^3 is $o(N)$. Define $S := T_{k-1} \cup \{N\}$. Since the only new pairwise differences introduced by N are $N - t_i$, all of which lie in $[N - ck^3, N]$ and so are pairwise distinct and disjoint from the differences of T_{k-1} (which are all bounded above by ck^3), the union S is Sidon. The last gap of S is $g_{k-1} = N - t_{k-1} \ge N - ck^3 = (1 - o(1))N$, hence $M_2(S) \ge g_{k-1}^2 \ge (1 - o(1))N^2$. (The range $k = o(N^{1/3})$ is sharp for the Mian–Chowla construction's $O(k^3)$ span; using a Bose–Chowla truncation in place of Mian–Chowla extends the lemma to the full $k = o(\sqrt{N})$ range, but this is unnecessary for the present argument, since Theorem 4.7 applies for any k at all.) ☐

Lemma 4.6 is the structural heart of the impossibility. A clustered Sidon set with one outlier saturates M_2 at the trivial upper bound; this Sidon-compatible configuration prevents any non-trivial $M_2 \leq \alpha N^2$ inequality from being established purely from the Sidon constraint.

4.3. **Main theorem and proof.**

Theorem 4.7. *Let* $S \subset [0, N]$ *be a Sidon set,* $|S| = k$*. The best size bound obtainable from the constraints*

(L) $M_2(S) \geq \sum_{i=1}^{k-1} i^2 = (k-1)k(2k-1)/6$ (Lemma 4.5)*, and*

(U) $M_2(S) \leq N^2$ (trivial, sharp by Lemma 4.6)*,*

is

$$k \;\leq\; (3N^2)^{1/3} \;+\; O(1) \;=\; O(N^{2/3}),$$

strictly weaker than the Erdős–Turán bound $k \leq \sqrt{2N} + O(1)$*.*

Proof. Combining (L) and (U) gives

$$\frac{(k-1)k(2k-1)}{6} \;\leq\; M_2(S) \;\leq\; N^2.$$

The left-hand side is $(k^3/3)(1 + O(1/k))$, so the implied bound on k is

$$k^3 \;\leq\; 3N^2(1 + O(1/k)), \qquad k \;\leq\; (3N^2)^{1/3} + O(1).$$

For all $N \geq 1$, $(3N^2)^{1/3} > \sqrt{2N}$ (a one-line check: $(3N^2)^{1/3} > \sqrt{2N}$ iff $(3N^2)^2 > (2N)^3$ iff $9N^4 > 8N^3$ iff $9N > 8$, which holds for $N \geq 1$), so the implied upper bound on k is strictly larger – i.e. *weaker as an upper bound* – than the Erdős–Turán upper bound. By Lemma 4.6, (U) cannot be sharpened to $M_2 \leq \alpha N^2$ for any constant $\alpha < 1$ using only the Sidon constraint, and by Lemma 4.5, (L) cannot be sharpened using only the gap-distinctness constraint (C1). Hence no combination of (L) and (U) yields a bound better than $O(N^{2/3})$, and the theorem follows. □

Remark 4.8 (On (C2) and (C3))**.** One might hope that the stronger constraints (C2) (distinctness of consecutive pair-sums $g_i + g_{i+1}$) or (C3) (distinctness of all consecutive partial sums) improve the lower bound on M_2 in Theorem 4.7. The picture is mixed: constraint (C3) already implies Erdős–Turán's $\binom{k}{2} \leq N$ (Lemma 4.4). The intermediate constraint (C3) applied with a Cauchy–Schwarz-style count on the $2k-3$ distinct values $\{g_i\} \cup \{g_i + g_{i+1}\}$ – distinct as positive integers in $[1, 2\sigma] \subseteq [1, 2N]$ summing to at most $3\sigma \leq 3N$ – gives $\binom{2k-2}{2} \leq 3N$, hence $k \leq \sqrt{3N/2} + O(1)$. Since $\sqrt{3N/2} < \sqrt{2N}$, this (C3)-derived bound is in fact *stronger* (i.e. a smaller upper bound on k) than Erdős–Turán by a constant factor $\sqrt{3/4} \approx 0.866$, though still weaker than Lindström's $\sqrt{N} + O(N^{1/4})$ asymptotically. Crucially, however, this constant-factor improvement does *not* help the gap-moment route of Theorem 4.7: even granting the strongest (C3)-derived information on σ, the M_2-via-trivial-N^2-upper-bound combination still gives only $k = O(N^{2/3})$. The structural reason is that gap-language constraints are local, while Sidon is a global constraint on all $\binom{k}{2}$ pair-differences; localising into $k-1$ consecutive differences loses the bulk of the available counting power.

Remark 4.9 (Conditional on additional structure)**.** Theorem 4.7 concerns the *unconditional* Sidon-derivable bound on M_2. For specific Sidon constructions (e.g. Bose–Chowla, Singer) one has tighter – but construction-dependent – knowledge of M_2; the numerics in Section 5 record $M_2 = \Theta(N^{3/2})$ on Bose–Chowla. Such conditional information cannot be used in a size bound that is to hold for all Sidon sets, since the would-be size bound must respect the Mian–Chowla-style construction of Lemma 4.6, which has $M_2 = \Theta(N^2)$.

5. Bose–Chowla numerics: $M_2 = \Theta(N^{3/2})$

This section computes M_2 on the Bose–Chowla construction $S_{\mathrm{BC}}(p)$ for small primes p and observes the empirical regime $M_2 = \Theta(N^{3/2})$.

5.1. Construction recap.

Definition 5.1 (Bose–Chowla 1962 [5])**.** Let p be a prime, realise $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2-r)$ for r the least quadratic non-residue modulo p, and let $\theta \in \mathbb{F}_{p^2}^*$ be a fixed primitive root. The *Bose–Chowla set* is

$$S_{\mathrm{BC}}(p) \ := \ \{\, \log_\theta(x+a) \bmod (p^2-1) : a \in \mathbb{F}_p \,\} \ \subseteq \ \mathbb{Z}/(p^2-1)\mathbb{Z},$$

where $x \in \mathbb{F}_{p^2}$ is the image of the formal indeterminate in $\mathbb{F}_p[x]/(x^2-r)$.

By the Bose–Chowla theorem, $|S_{\mathrm{BC}}(p)| = p$ and $S_{\mathrm{BC}}(p)$ is Sidon modulo p^2-1. Lifting to $[0, p^2-2]$ via the canonical representative gives an integer Sidon set with ambient $N = p^2-1$ and size $k = p \approx \sqrt{N}$.

5.2. **Computation.** The set $S_{\mathrm{BC}}(p)$ depends on a choice of primitive root $\theta \in \mathbb{F}_{p^2}^*$; different choices give translation- and permutation-equivalent sets in $\mathbb{Z}/(p^2-1)\mathbb{Z}$, but the lift to $[0, p^2-2]$ can differ. We fix the canonical choice: represent $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2-r)$ where r is the least quadratic non-residue modulo p, enumerate elements of $\mathbb{F}_{p^2}$ in the lexicographic order $a + b\,x \mapsto (a,b)$ with a-coordinate first, take the primitive root θ of smallest such order, and read off the discrete logs of $x+a$ for $a = 0, 1, \ldots, p-1$ as integers in $[0, p^2-2]$. The resulting Sidon sets and their second gap moments are recorded in Table 1; the verification of the Sidon property and the M_2 computation are exact.

5.3. **Discussion of the numerics.** The empirical ratio $M_2/N^{3/2}$ fluctuates in the range $[0.68, 1.77]$ over the surveyed primes, with no monotone trend. The fluctuation reflects the dependence of the canonical lift on the primitive root: the discrete logarithms $\log_\theta(x+a)$ scatter across $[0, p^2-2]$ in a manner sensitive to the lift, and the resulting gap pattern is correspondingly variable.

Table 1. Second gap moment on the canonical Bose–Chowla Sidon set $S_{\mathrm{BC}}(p) \subset [0, p^2 - 2]$. The columns are: prime p; cardinality $k = p$; ambient $N = p^2 - 1$; exact integer $M_2 = \sum_i g_i^2$; the empirical ratio $M_2/N^{3/2}$; and the Cauchy–Schwarz saturation ratio $M_2(k-1)/\sigma^2$ from Lemma 4.1 (with $\sigma = s_k - s_1$).

p	k	N	M_2	$M_2/N^{3/2}$	$M_2(k-1)/\sigma^2$
3	3	8	26	1.149	1.444
5	5	24	102	0.867	1.594
7	7	48	226	0.680	1.507
11	11	120	2 242	1.705	1.666
13	13	168	1 633	0.750	1.591
17	17	288	8 664	1.773	1.874
19	19	360	11 592	1.697	1.703
23	23	528	15 505	1.278	1.786
29	29	840	39 501	1.622	1.768
31	31	960	48 677	1.637	1.722

The mean of the ten observed ratios is approximately 1.32, with a rough "working value" of 1.6 for the primes $p \geq 11$.

The saturation ratio $M_2(k-1)/\sigma^2$, which equals 1 if and only if all gaps are equal, sits in the range $[1.44, 1.88]$. The Bose–Chowla gap sequence is therefore not equi-spaced; the deviations from equispacing account for the factor of order 1.6.

Proposition 5.2. *For Bose–Chowla $S_{\mathrm{BC}}(p)$ with $|S_{\mathrm{BC}}| = p$ and ambient $N = p^2 - 1$, the empirical regime of Table 1 is consistent with the heuristic $M_2(S_{\mathrm{BC}}(p)) = \Theta(N^{3/2})$ with constant in $[1, 2]$. Specifically, the Cauchy–Schwarz lower bound of Lemma 4.1 reads*

$$M_2(S_{\mathrm{BC}}(p)) \;\geq\; \frac{\sigma^2}{k-1} \;\geq\; \frac{(N-1)^2}{p-1} \;\sim\; N^{3/2},$$

and the empirical ratio of M_2 to this lower bound is 1.44 to 1.88 across the surveyed range.

Proof. The first inequality is Lemma 4.1; the second uses $\sigma = s_k - s_1 \leq N - 1$ in either direction together with the observation that for the canonical Bose–Chowla lift, the maximum element exceeds $N/2$ and the minimum is bounded above by N/p^2, so $\sigma \geq N - O(N/p^2)$. The asymptotic is then immediate from $k - 1 = p - 1 \sim \sqrt{N}$, and the empirical confirmation is the rightmost column of Table 1. $\square$

Remark 5.3 (On non-existence of a sharper construction-free bound)**.** We emphasise that Proposition 5.2 is specific to Bose–Chowla. A clustered Sidon set as in Lemma 4.6 has $M_2 = \Theta(N^2)$, far above the Bose–Chowla value, so the Bose–Chowla regime $M_2 = \Theta(N^{3/2})$ is *not* a Sidon-universal upper bound and cannot be used as the (U)-input in Theorem 4.7.

Remark 5.4 (Reproducibility)**.** The Sidon-property verification and the M_2 values in Table 1 were computed in exact integer arithmetic in Python: $\mathbb{F}_{p^2}$ is implemented as $\mathbb{F}_p[x]/(x^2 - r)$ for the least non-residue r, the primitive root is selected by direct order computation, and the discrete logarithm table is built by repeated multiplication. A self-contained script reproducing Table 1 is available from the author. The same script verifies Theorem 3.1 on the pair (A, B) at the rational level (i.e. produces exact $\mathbb{Q}$-valued m_4, m_6, m_8).

6. HIGHER MOMENTS AND GAP-DISTRIBUTION STATISTICS

The negative theorem of Section 4 extends to the higher gap moments M_p and to the centered moments m_{2r} with the obvious modifications. We record the salient extensions briefly, since the underlying mechanism is the same: a Sidon-derivable lower bound from distinctness, combined with a trivial Sidon-compatible upper bound, that fails to match Erdős–Turán.

Proposition 6.1 (Higher gap moments)**.** *Let $S \subset [0, N]$ be a Sidon set with $|S| = k$ and gap sequence g, and let $p \geq 2$.*

1. *Lower bound: $M_p(S) \geq \sum_{i=1}^{k-1} i^p \sim k^{p+1}/(p+1)$ by the distinctness of gaps (Lemma 4.2).*
2. *Upper bound: $M_p(S) \leq N^p$ is the best Sidon-compatible upper bound; specifically, the Mian–Chowla-plus-outlier construction of Lemma 4.6 attains $M_p(S) \geq (1 - o(1))N^p$ for $k = o(N^{1/3})$.*
3. *Implied size bound: $k^{p+1}/(p+1) \leq N^p$ gives $k \leq ((p+1)N^p)^{1/(p+1)} = O(N^{p/(p+1)})$.*

The implied size bound is strictly weaker than Erdős–Turán's $\sqrt{2N}$ for every $p \geq 2$, since $p/(p+1) \geq 2/3 > 1/2$.

Proof. Items (1) and (3) are the obvious analogues of Lemma 4.5 and Theorem 4.7. Item (2) follows from the construction of Lemma 4.6: the clustered Sidon set has its last gap $g_{k-1} = N - o(N)$, hence $M_p \geq g_{k-1}^p = (1 - o(1))N^p$. $\square$

Proposition 6.2 (Higher centered moments)**.** *Let $S \subset [0, N]$ be a Sidon set with $|S| = k$ and $r \geq 3$.*

1. *m_{2r} does not factor through r_{S-S} (Lemma 3.3).*
2. *No non-trivial Sidon-derivable upper bound $m_{2r} \leq f(N, k)$ with $f(N, k) = o(kN^{2r})$ is available: the clustered Sidon set of Lemma 4.6 achieves $m_{2r}(S) \geq (1 - o(1))(k - 1)N^{2r}/k$ for $k = o(N^{1/3})$.*
3. *Consequently m_{2r} does not yield a size bound matching Erdős–Turán.*

Proof. Item (1) is Lemma 3.3. For (2) we note that the Mian–Chowla-plus-outlier set has $k - 1$ points near 0 and one point near N; the mean is $\bar{s} \approx N/k$, and the contribution of the outlier to m_{2r} is $(N - \bar{s})^{2r} \geq (1 -$

$o(1))N^{2r}$, while the other $k-1$ points contribute at most $k\,\bar{s}^{2r} = k\,(N/k)^{2r} \leq N^{2r}/k^{2r-1}$, smaller by a factor of k^{2r-1}. Hence $m_{2r}(S) \geq (1-o(1))N^{2r}$, and a Sidon-derivable upper bound of order $o(N^{2r})$ is impossible. Item (3) is then immediate: any size bound derived from m_{2r} via power-mean-style lower bound and trivial N^{2r} upper bound is asymptotically weaker than Erdős–Turán by the same arithmetic as in Theorem 4.7. $\square$

Proposition 6.3 (Gap distribution variance)**.** *Let* $S \subset [0, N]$ *be a Sidon set with* $|S| = k$ *and gap variance* $\mathrm{Var}(g) := M_2/(k-1) - (\sigma/(k-1))^2$*. Then the constraint* $\mathrm{Var}(g) \geq \frac{1}{12}k^2 - O(k)$ *from* (C1) *– the minimum variance of* $k-1$ *distinct positive integers – is satisfied with strict inequality on Bose–Chowla, where empirically* $\mathrm{Var}(g) \approx 0.6\,(N/k)^2 \approx 0.6\,N$ *for* $k \approx \sqrt{N}$*. Consequently, the variance does not yield a Sidon-derivable upper bound on* k *matching Erdős–Turán.*

Proof. The lower bound on $\mathrm{Var}(g)$ is by Lemma 4.2 and direct computation of the variance of $\{1, 2, \ldots, k-1\}$. The Bose–Chowla empirical estimate follows from Table 1: $\mathrm{Var}(g) = M_2/(k-1) - \bar{g}^2$ with $\bar{g} = \sigma/(k-1) \approx N/k$ and $M_2/(k-1) \approx 1.6N$ in the saturation regime of Proposition 5.2, giving $\mathrm{Var}(g) \approx 1.6N - N = 0.6N$. The implication for size bounds is then the same as in Theorem 4.7, since $\mathrm{Var}(g) \leq M_2/(k-1)$. $\square$

The conclusion across M_p, m_{2r}, and $\mathrm{Var}(g)$ is uniform: gap-language constraints from the Sidon property are necessary (lower bounds via distinctness) but not sufficient (no matching upper bounds), and combining them with trivial N^p- or N^{2r}-scale upper bounds produces size bounds weaker than Erdős–Turán.

7. Discussion: an order-sensitive failure mode

7.1. **What the negative theorem says, and what it does not.** Theorem 4.7 establishes that the gap-moment M_2, considered as an upper-bound proof tool for Sidon size, is strictly weaker than the classical Erdős–Turán bound. The extensions in Section 6 show the same for higher gap moments, centered higher moments, and the gap-distribution variance.

The theorem is unconditional but *narrow*: it constrains only the family of would-be size bounds derived from gap-language inequalities of the type "$M_2 \geq f(k)$ from (C1)/(C3) plus $M_2 \leq g(N)$". It does not preclude:

- joint use of M_2 and r_{S-S}: a bound combining the autocorrelation with order-sensitive data might in principle beat Erdős–Turán, although no concrete such argument is known;
- construction-dependent bounds: for explicit Sidon families one can use the specific structure (e.g. multiplicative origins for Bose–Chowla) to sharpen M_2, but the resulting bound will not transfer to general Sidon sets;

- refined Fourier methods that go beyond r_{S-S} via higher Gowers norms or restriction estimates, as in Bloom–Sisask [3] and Ortega–Prendiville [13]: these live in the autocorrelation kernel or its higher-order generalisations and are orthogonal to the gap-language route considered here.

What the theorem rules out is the most natural variant of the gap-moment programme as a stand-alone attack vector.

7.2. **An order-sensitive failure mode.** The combined behaviour exhibited by M_2 – escape from the autocorrelation kernel (Theorem 3.1) paired with structural weakness in the upper-bound direction (Theorem 4.7) – suggests a meta-theoretic pattern that we propose to name as a stand-alone failure mode:

> *Order-sensitive Sidon-weakness.*
> A shift-invariant Sidon invariant $\mathcal{I}$ that depends on the gap sequence beyond the autocorrelation r_{S-S} may genuinely escape the autocorrelation kernel (so its values can distinguish homometric sets), yet the only Sidon-derivable inequalities expressible in the language of $\mathcal{I}$ may be too weak to recover even Erdős–Turán. The escape and the weakness arise from the same source: $\mathcal{I}$ sees the linear ordering of S, but the Sidon constraint does not constrain the linear ordering except through local relations among consecutive partial sums, and those local relations are dominated by the global Erdős–Turán $\binom{k}{2} \leq N$ counting.

We propose this naming modestly. The failure mode is *not* a Razborov–Rudich-style structural barrier [15] in the complexity-theoretic sense: it does not assert that all techniques in some natural class must fail, only that a specific and natural family of inequalities does. Compared with the relativisation surveys of Aaronson–Wigderson [1], the analogy is at most that both record a class of proof techniques whose limitations are intrinsic to the language they use, rather than to the underlying conjecture's difficulty.

The contribution of giving the failure mode a name is in the catalogue: when surveying possible invariants for Sidon size bounds, one can now diagnose "does this invariant exhibit order-sensitive Sidon-weakness?" as a screening question, and if so, avoid pursuing the obvious stand-alone variant.

7.3. **Generalisation beyond M_2.** The same pattern is expected – but not proved here – for the other order-sensitive Sidon invariants surveyed in our companion exploration: the interval discrepancy $D(S) := \sup_{[a,b]\subseteq[0,N]} \big| |S \cap [a,b]| - \frac{b-a}{N+1}\, k \big|$, the gap distribution G_k itself, and the order-rank $R(S) := \sum_i i\, s_i$. We have not analysed these systematically. Each is shift-invariant and order-sensitive, hence outside the r_{S-S}-kernel by structural analogy with M_2; in each case the question of whether the Sidon-derivable bounds (analogous to (C1) and (C3) above) yield Erdős–Turán-matching or sub-Erdős–Turán implications is open.

A natural conjecture, which we leave open, is:

Conjecture 7.1. Every shift-invariant Sidon invariant $\mathcal{I} : 2^{[0,N]} \to \mathbb{R}$ that is polynomial in the gap sequence $g = (g_1, \ldots, g_{k-1})$ with coefficients independent of the enumeration of S, and used as a stand-alone constraint (without joint use of r_{S-S}), gives a size bound at most $|S| = O(\sqrt{2N})$. That is, no such invariant can match Lindström's $\sqrt{N} + O(N^{1/4})$.

The motivation for Conjecture 7.1 is that Lindström's $\sqrt{N} + N^{1/4} + 1$ bound is proved via a Fourier estimate on the autocorrelation, and the gap-sequence route appears to lose the Fourier information by construction. The conjecture is not a theorem: a polynomial-in-gaps invariant could in principle combine the constraints (C1), (C2), (C3) with subtler arithmetic of the partial sums to recover the Erdős–Turán constant. We are not aware of such a construction.

8. Open questions

Question 8.1 (Joint M_2 + autocorrelation bound)**.** Can a combined size bound using both M_2 and r_{S-S} – i.e. a proof technique that exploits the order-sensitive information in M_2 together with the standard Fourier information in r_{S-S} – yield $|S| \leq \sqrt{N} + o(N^{1/4})$? The numerics in Section 5 are consistent with the Cauchy–Schwarz lower bound $M_2 \geq \sigma^2/(k-1)$ being tight up to a constant on Bose–Chowla, suggesting that any joint bound would have to use a strictly different inequality.

Question 8.2 (Other Bloom–Golomb pairs)**.** The Bloom–Golomb family (1) contains a two-parameter family of Sidon-homometric pairs. We have computed M_2 on one parameter pair, $(u, v) = (3, -2)$. For other choices of (u, v) giving Sidon pairs, how does the M_2 discrepancy $|M_2(R(u, v)) - M_2(S(u, v))|$ scale, and does it ever vanish?

Question 8.3 (Bose–Chowla constant)**.** Does $M_2(S_{\mathrm{BC}}(p))/N^{3/2}$ converge to a specific constant as $p \to \infty$, or remain in a non-degenerate range? The numerics in Table 1 suggest a working value of ≈ 1.6 but show fluctuation in $[0.68, 1.77]$, and the extrapolation to $p \to \infty$ is conditional on the canonical-lift heuristic.

Question 8.4 (Conjecture 7.1)**.** Conjecture 7.1 is an empirical generalisation of Theorem 4.7; a sharper statement would identify a precise notion of "polynomial-in-gap-sequence Sidon invariant used without joint r_{S-S}" within which the negative implication can be tested. We do not pursue such a formalisation here and record the question only as a direction for further investigation.

ACKNOWLEDGMENTS

This note arose during an LLM-assisted exploration of order-sensitive invariants on integer Sidon sets, in the course of which the gap-moment discrepancy on the Bloom–Golomb pair (A, B) was made explicit. The author thanks the adversarial review process for surfacing the Bloom–Golomb attribution of the pair and for clarifying the distinction between gap moments and autocorrelation moments. The author has no competing interests. All numerical computations of Sections 3 and 5 are exactly reproducible in standard Python with exact rational arithmetic; the verification script is available from the author.

REFERENCES

[1] S. Aaronson and A. Wigderson, *Algebrization: a new barrier in complexity theory*, ACM Trans. Comput. Theory **1** (2009), no. 1, Article 2, 54 pp.

[2] J. Balogh, Z. Füredi, and S. Roy, *An upper bound on the size of Sidon sets*, preprint, arXiv:2103.15850 (2021).

[3] T. F. Bloom and O. Sisask, *Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions*, preprint, arXiv:2007.03528 (2020); subsequent restriction-style refinements in the same kernel.

[4] G. S. Bloom and S. W. Golomb, *Applications of numbered undirected graphs*, Proc. IEEE **65** (1977), 562–570.

[5] R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962), 141–147.

[6] D. Carter, Z. Hunter, and K. O'Bryant, *On the diameter of finite Sidon sets*, preprint, arXiv:2310.20032 (2023).

[7] J. Cilleruelo, *Gaps in dense Sidon sets*, Integers **0** (2000), A11, 6 pp.

[8] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215.

[9] M. Baake and U. Grimm, *Homometric model sets and window covariograms*, Z. Kristallogr. **222** (2007), 54–58.

[10] B. Lindström, *An inequality for B_2-sequences*, J. Combin. Theory **6** (1969), 211–212.

[11] A. M. Mian and S. Chowla, *On the B_2-sequences of Sidon*, Proc. Nat. Acad. Sci. India **14** (1944), 3–4.

[12] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electron. J. Combin., Dynamic Survey DS11 (2004); arXiv:math/0407117.

[13] M. Ortega and S. Prendiville, *Extremal Sidon sets are Fourier uniform, with applications to partition regularity*, preprint, arXiv:2110.13447 (2021).

[14] L. Chang, *An explicit cube-count formula for integer Sidon sets and the first cyclic U^3 analysis of a classical Bloom–Golomb pair*, companion note (2026); manuscript in preparation.

[15] A. Razborov and S. Rudich, *Natural proofs*, J. Comput. System Sci. **55** (1997), no. 1, part 1, 24–35.

[16] S. Sidon, *Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen*, Math. Ann. **106** (1932), 536–539.

[17] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.

[18] S. S. Skiena, W. D. Smith, and P. Lemke, *Reconstructing sets from interpoint distances*, Proc. 6th Annual Sympos. Comput. Geom. (1990), 332–339.

[19] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006.

Independent Researcher
Email address: `lightman.chang@gmail.com`