AN EXPLICIT CUBE-COUNT FORMULA FOR INTEGER SIDON SETS AND A CYCLIC U^3 ANALYSIS OF A CLASSICAL BLOOM–GOLOMB PAIR

LIGHTMAN CHANG

Abstract. For every integer Sidon set S with $|S| = n$ and every $k \geq 1$, we record the explicit closed form $T_k(S) = n + k\,n(n-1)$ for the number of integer 2^k-cubes $(x; h_1, \ldots, h_k)$ contained in S. The $k = 2$ case is the classical Sidon additive-energy identity $E(S, S) = 2n^2 - n$ recorded in Tao–Vu (Prop. 4.29) and Kowalski (Prop. 2.3.7); the extension to $k \geq 3$ is a two-line corollary of the same parallelogram-exclusion lemma, which we have not found stated explicitly in the surveyed literature. As an application we revisit the homometric Sidon pair $(R(3, -2), S(3, -2))$ from the Bloom–Golomb two-parameter family (Bloom 1977; Bloom–Golomb 1977), which up to reflection coincides with the size-6 pair $A = \{0, 1, 5, 7, 15, 18\}$, $B = \{0, 1, 3, 8, 14, 18\}$. The cube-count formula forces $T_k(A) = T_k(B)$ for every k. We prove, however, that the centered cyclic U^3 norms of $\mathbf{1}_A$ and $\mathbf{1}_B$ on $\mathbb{Z}/N\mathbb{Z}$ differ at $N = 41$ and $N = 43$ while coinciding at $N = 37, 47, 53$. The discrepancy is explained by the modular zero count of a length-5 linear relation with a doubled coefficient, $2s_1 - s_2 - s_3 - s_4 + s_5 \equiv 0 \pmod{N}$, whose integer version is shared by Sidon-homometric pairs but whose modular version need not be.

1. Introduction

1.1. **Setting and result.** A finite set $S \subset \mathbb{Z}$ is a *Sidon set* (or B_2-set, following Sidon's original work [12]) if its ordered pairwise differences $s - s'$, $s \neq s' \in S$, are distinct. Equivalently, the autocorrelation

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

satisfies $r_{S-S}(0) = |S|$ and $r_{S-S}(d) \in \{0, 1\}$ for $d \neq 0$. Sidon sets in $[1, N]$ have cardinality at most $\sqrt{N} + O(N^{1/4})$ (Erdős–Turán [5], Lindström [8]); the Singer [13] and Bose–Chowla [3] constructions give $\sqrt{N} - O(N^{1/2-c})$ from below. The remaining Erdős–Sidon gap is the long-standing open problem behind the field; we do not address it.

Date: May 19, 2026.

2020 *Mathematics Subject Classification.* Primary 11B83, 11B30; Secondary 05B10.

Key words and phrases. Sidon set, Gowers uniformity norm, additive energy, homometric set, Bloom–Golomb pair.

This note is concerned instead with two clean and seemingly unrecorded calculations on integer Sidon sets, and with an honest reading of a 49-year-old counterexample.

For $k \geq 1$, an *integer* 2^k*-cube in* S is a tuple $(x; h_1, \ldots, h_k) \in \mathbb{Z}^{k+1}$ with $x + \omega \cdot h \in S$ for every $\omega \in \{0,1\}^k$, where $\omega \cdot h := \sum_{i=1}^{k} \omega_i h_i$. Write $T_k(S) := \#\{\text{integer } 2^k\text{-cubes in } S\}$. Such cubes are the basic configuration controlled by the Gowers uniformity norm U^k: when N is large enough that no cube wraps around (concretely $N > 2k(\max S - \min S)$ suffices), $\|\mathbf{1}_S\|_{U^k(\mathbb{Z}/N\mathbb{Z})}^{2^k} = T_k(S)/N^{k+1}$ in the convention of Tao–Vu [15, Eq. (11.2)].

Theorem 1.1. *For every Sidon set $S \subset \mathbb{Z}$ of cardinality n and every $k \geq 1$,*

$$T_k(S) \;=\; n + k\,n(n-1) \;=\; n\big(k(n-1)+1\big).$$

In particular $T_k(S)$ depends only on $n = |S|$, not on the autocorrelation r_{S-S} and not on any finer arithmetic structure of S. The $k = 1$ value $T_1(S) = n^2$ is trivially $|S \times S|$. The $k = 2$ value $T_2(S) = 2n^2 - n$ is the classical additive-energy identity $E(S,S)$ for a Sidon set, recorded in Tao–Vu [15, Prop. 4.29, p. 173 and Eq. (11.2), pp. 418–419] and in Kowalski [7, Prop. 2.3.7]. The extension to $k \geq 3$ in Theorem 1.1 reduces by an elementary parallelogram-exclusion argument to the same Sidon property; we have not found the closed form $T_k = n + k\,n(n-1)$ for $k \geq 3$ explicitly written down in the references we surveyed, including Tao–Vu §§4 and 11 [15], Kowalski [7], the Sidon bibliography of O'Bryant [9], the Sidon-uniformity work of Ortega–Prendiville [10], the higher-energy papers of Shkredov [11], and the k-fold Sidon work of Cilleruelo–Timmons [4]. We therefore present Theorem 1.1 as an explicit closed form generalising the classical $k = 2$ identity rather than as a deep result.

1.2. **An application to a classical Bloom–Golomb pair.** A homometric pair of integer Sidon sets is a pair $S, S' \subset \mathbb{Z}$ with $r_{S-S} = r_{S'-S'}$ as functions on $\mathbb{Z}$. The first explicit example is due to Bloom [1], who showed $\{0,1,4,10,12,17\}$ and $\{0,1,8,11,13,17\}$ are Sidon-homometric, refuting an earlier claim of Piccard. Bloom and Golomb extended this single example to a two-parameter family [2]:

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

whose members are Sidon-homometric for generic (u,v). The work of Gilbert–Postpischil [6] confirmed by exhaustive search that for $|S| \leq 12$ all known homometric Sidon pairs come from (1), and that no new 7– to 12-mark pairs exist.

For the parameters $(u,v) = (3,-2)$ one computes

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

The set $A := \{0,1,5,7,15,18\}$ is the reflection of $S(3,-2)$ under $x \mapsto 18-x$, and $B := R(3,-2)$. The pair (A,B) is therefore a 49-year-old classical

Bloom–Golomb instance; this fact appears not to have been recorded in the Gowers-norm or Sidon-uniformity literature, where the pair (or its reflection-equivalent) reappears repeatedly in numerical experiments without attribution.

By Theorem 1.1, $T_k(A) = T_k(B) = 6 + 30k$ for every $k \geq 1$. The natural question is whether their indicator functions distinguish on the cyclic Gowers norm $U^3(\mathbb{Z}/N\mathbb{Z})$ for some moderate N. We show that they do.

Theorem 1.2. *Let* $A = \{0, 1, 5, 7, 15, 18\}$ *and* $B = \{0, 1, 3, 8, 14, 18\}$ *as above. Set* $f_S := \mathbf{1}_S - 6/N$*. Then for every* $N \geq 37$ *both* A *and* B *are Sidon in* $\mathbb{Z}/N\mathbb{Z}$*. The centered cyclic* U^3 *norms satisfy*

$$\|f_A\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})} = \|f_B\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})} \quad \text{for } N \in \{37, 47, 53\},$$

while

$$\|f_A\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})} \neq \|f_B\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})} \quad \text{for } N \in \{41, 43\}.$$

The discrepancy at $N \in \{41, 43\}$ *is detected by the modular zero count*

$$M_5^{(N)}(S) := \#\{(s_1, \ldots, s_5) \in S^5 : 2s_1 - s_2 - s_3 - s_4 + s_5 \equiv 0 \pmod N\},$$

which has $M_5^{(N)}(A) - M_5^{(N)}(B) = +4$ *at* $N = 41$*,* -4 *at* $N = 43$*, and* 0 *at* $N \in \{37, 47, 53\}$*.*

Our proof of Theorem 1.2 verifies the mechanism numerically (in exact rational arithmetic) and provides an algebraic skeleton (Lemma 4.1); a closed-form polynomial identity for $M_5^{(\infty)}$ as a function of r_{S-S} alone remains open.

Theorem 1.2 should be read as a cyclic-U^3 analysis of the Bloom–Golomb pair $(R(3, -2), S(3, -2))$, not as a new construction. The pair itself has been known for nearly half a century; what we add is (a) the cube-count rigidity in Theorem 1.1 that forces $T_k(A) = T_k(B)$ on the integer side, and (b) the identification of a specific *doubling relation* with a coefficient ±2 as the modular mechanism by which the cyclic U^3 norm distinguishes them. Both items appear to be new; neither is deep.

1.3. Notational disambiguation.

The symbol $T_k(A)$ is used in the additive-combinatorics literature for the higher-energy invariant $T_k^{\mathrm{Shk}}(A) := \#\{(a_1, \ldots, a_k, a'_1, \ldots, a'_k) \in A^{2k} : a_1 + \cdots + a_k = a'_1 + \cdots + a'_k\}$ (Shkredov [11], and earlier Schoen–Shkredov). This is the ℓ^{2k}-moment of the convolution and *differs* from our cube count $T_k(S)$ for $k \geq 3$; the two coincide at $k = 2$, both equalling $E(S, S) = 2n^2 - n$ on a Sidon set. Separately, Cilleruelo–Timmons [4] use the term "k-fold Sidon set" for a different invariant defined by integer relations $\sum c_i x_i = 0$ with $|c_i| \leq k$, $\sum c_i = 0$. Neither of these notational neighbours subsumes our $T_k(S) = n + k\,n(n-1)$. We use the symbol T_k throughout for the Gowers-cube count, following Tao–Vu §11.

1.4. **Structure.** Section 2 fixes notation and recalls the relevant Gowers-norm formalism. Section 3 proves Theorem 1.1. Section 4 proves Theorem 1.2: §4.1 identifies (A, B) inside the Bloom–Golomb family (1), §4.2 verifies the Sidon conditions, §4.3 reports the numerical U^3 table, and §4.4 derives the doubling-relation mechanism. Section 5 discusses the boundary between integer and cyclic invariants and Section 6 lists open questions.

2. Background and notation

2.1. **Sidon sets and homometry.** Throughout $S \subset \mathbb{Z}$ is a finite Sidon set, $n := |S|$. The autocorrelation $r_{S-S} : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ is the shift-invariant invariant of S at first order. Two Sidon sets S, S' are *homometric* (in the integers) if $r_{S-S} = r_{S'-S'}$, i.e. they have the same multiset of ordered differences. The first explicit Sidon-homometric pair is due to Bloom [1]; the two-parameter family in which it sits is (1) [2]; the turnpike / partial-digest reconstruction problem [14] and crystallographic Patterson-function problem are alternative names for asking for an integer set with given r_{S-S}.

2.2. **Integer 2^k-cubes.** For $k \geq 1$, define

$$\mathcal{C}_k(S) \ := \ \{(x; h_1, \ldots, h_k) \in \mathbb{Z}^{k+1} : x + \omega \cdot h \in S \text{ for every } \omega \in \{0,1\}^k\},$$

and $T_k(S) := |\mathcal{C}_k(S)|$. A cube is *degenerate* if some $h_i = 0$ and *non-degenerate* otherwise.

2.3. **Gowers U^k norm on $\mathbb{Z}/N\mathbb{Z}$.** For $f \colon \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and $k \geq 1$, Tao–Vu [15, Eq. (11.1)] define the Gowers uniformity norm of order k by

$$\|f\|_{U^k(\mathbb{Z}/N\mathbb{Z})}^{2^k} \ = \ \mathbb{E}_{x,h_1,\ldots,h_k \in \mathbb{Z}/N\mathbb{Z}} \prod_{\omega \in \{0,1\}^k} \mathcal{C}^{|\omega|} f(x + \omega \cdot h),$$

where $\mathcal{C}$ denotes complex conjugation (so for f real-valued the conjugation drops). Substituting $f = \mathbf{1}_S$ gives $\|\mathbf{1}_S\|_{U^k(\mathbb{Z}/N\mathbb{Z})}^{2^k} = \mathbb{E}_{x,h_1,\ldots,h_k} \prod_\omega \mathbf{1}_S(x + \omega \cdot h) = T_k^{(N)}(S)/N^{k+1}$, where $T_k^{(N)}(S)$ counts cubes in $\mathbb{Z}/N\mathbb{Z}$ [15, Eq. (11.2)]. When no cube wraps around $\bmod N$ – which holds whenever $N > 2k(\max S - \min S)$ – every modular cube lifts uniquely to an integer cube and $T_k^{(N)}(S) = T_k(S)$.

2.4. **Centered version.** For applications of U^3 to homometric pairs, the centered indicator $f_S := \mathbf{1}_S - n/N$ is more informative because the constant function has trivial U^k for $k \geq 2$. Expanding $f_S = \mathbf{1}_S - \alpha$ with $\alpha = n/N$,

$$\|f_S\|_{U^3(\mathbb{Z}/N\mathbb{Z})}^8 = \sum_{T \subseteq \{0,1\}^3} (-\alpha)^{8-|T|} \, \mathbb{E}_{x,h_1,h_2,h_3} \prod_{\omega \in T} \mathbf{1}_S(x + \omega \cdot h). \tag{2}$$

The leading term ($T = \{0,1\}^3$) is the normalised cube count $T_3^{(N)}(S)/N^4$. The subleading terms count constrained sub-cubes; each is a probability in $[0, 1]$.

3. Proof of Theorem 1.1

Fix a Sidon set $S \subset \mathbb{Z}$, $n = |S|$, and $k \geq 1$.

Lemma 3.1 (Sidon parallelogram exclusion)**.** *If $s_0, s_1, s_2, s_3 \in S$ satisfy $s_0 + s_3 = s_1 + s_2$, then $\{s_0, s_3\} = \{s_1, s_2\}$ as multisets.*

Proof. The equation rearranges to $s_0 - s_1 = s_2 - s_3$. If $s_0 \neq s_1$ the common value is a nonzero difference of S; by the Sidon property it has a unique ordered representation, forcing $(s_0, s_1) = (s_2, s_3)$ and hence $s_3 = s_1$, giving $\{s_0, s_3\} = \{s_1, s_2\}$ as multisets. If $s_0 = s_1$ then $s_2 = s_3$ from the rearrangement, and the multiset equality holds trivially. □

Lemma 3.2 (Cubes are axial)**.** *For every $(x; h_1, \ldots, h_k) \in \mathcal{C}_k(S)$, at most one of $h_1, \ldots, h_k$ is non-zero.*

Proof. Suppose for contradiction that $h_i \neq 0$ and $h_j \neq 0$ for some $i \neq j$. The four vertices of the cube corresponding to $\omega \in \{0,1\}^k$ that are constant outside coordinates $\{i, j\}$ form a 2-face inside S:

$$\{x,\ x + h_i,\ x + h_j,\ x + h_i + h_j\} \subset S.$$

These satisfy $x + (x + h_i + h_j) = (x + h_i) + (x + h_j)$. By Lemma 3.1, the multiset $\{x, x + h_i + h_j\}$ equals $\{x + h_i, x + h_j\}$. Subtracting x from every element of both sides reduces the equality to $\{0, h_i + h_j\} = \{h_i, h_j\}$.

Either $0 = h_i$ and $h_i + h_j = h_j$ (which would give $h_i = 0$, contradicting our hypothesis), or $0 = h_j$ and $h_i + h_j = h_i$ (which would give $h_j = 0$, again a contradiction). No third case is possible. The contradiction completes the proof. □

Proof of Theorem 1.1. By Lemma 3.2 every cube in $\mathcal{C}_k(S)$ is *axial*: at most one height h_{i_0} is non-zero.

Type 0 (all-zero heights). Every vertex equals x, so the cube condition reduces to $x \in S$, contributing n cubes.

Type i_0 for $i_0 \in \{1, \ldots, k\}$ (exactly the i_0-th height non-zero). Each vertex of the cube equals either x or $x + h_{i_0}$ according to $\omega_{i_0} \in \{0, 1\}$, with all other coordinates of ω irrelevant. The cube condition becomes $\{x, x + h_{i_0}\} \subset S$ with $h_{i_0} \neq 0$. The number of ordered pairs $(s, s') \in S^2$ with $s \neq s'$ is $n(n-1)$, and each such pair determines a unique cube of this type with $x = s$, $h_{i_0} = s' - s$. Summing over the k choices of i_0 gives $k \cdot n(n-1)$ cubes.

Summing the two contributions,

$$T_k(S) = n + k\,n(n-1).$$

□

Remark 3.3 (Sanity checks)**.** For $k = 1$, $T_1(S) = n + n(n-1) = n^2 = |S \times S|$, as expected: each $(s, s') \in S^2$ gives a unique 2-cube $(s; s' - s)$. For $k = 2$, $T_2(S) = n + 2n(n-1) = 2n^2 - n$, the classical Sidon additive energy $E(S, S)$ [15, Prop. 4.29], [7, Prop. 2.3.7]. For $k = 3$ and the size-6 Sidon set $A = \{0, 1, 5, 7, 15, 18\}$ in Theorem 1.2, the formula gives $T_3(A) = 6 + 90 = 96$; direct enumeration confirms this value, and the same enumeration on B also yields 96, in agreement with Theorem 1.1.

4. Proof of Theorem 1.2

4.1. Identifying (A, B) inside the Bloom–Golomb family. The Bloom–Golomb two-parameter family (1) [2] is

$$R(u,v) = \{0,\ u,\ u+v,\ 4u+2v,\ 6u+2v,\ 8u+3v\},$$
$$S(u,v) = \{0,\ u,\ 5u+v,\ 5u+2v,\ 7u+2v,\ 8u+3v\}.$$

For $(u, v) = (3, -2)$,

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

The reflection $\mathrm{refl}_d : x \mapsto d - x$ with $d = 18$ sends $S(3, -2)$ to $\{18, 15, 7, 5, 1, 0\} = \{0, 1, 5, 7, 15, 18\}$. Thus $B = R(3, -2)$ and $A = \mathrm{refl}_{18}(S(3, -2))$. Reflection preserves the autocorrelation and the Sidon property, so the pair $(A, B) = (\mathrm{refl}_{18}(S(3, -2)),\ R(3, -2))$ is Sidon-homometric with identical r_{S-S} from the underlying Bloom–Golomb construction.

4.2. Verification of the Sidon and homometric conditions. Direct enumeration of the 30 ordered nonzero differences of A gives the positive-difference set

$$D_A^+ = \{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 15, 17, 18\} \subset \{1, \ldots, 18\},$$

each value occurring exactly once (the missing positive differences are $9, 12, 16$). The same enumeration on B produces $D_B^+ = D_A^+$. Hence both A and B are integer Sidon and $r_{A-A}(d) = r_{B-B}(d)$ for every $d \in \mathbb{Z}$. By Theorem 1.1, $T_k(A) = T_k(B) = 6 + 30k$ for every $k \geq 1$.

The consecutive-gap sequences of A and B are $(1, 4, 2, 8, 3)$ and $(1, 2, 5, 6, 4)$ respectively; these are not cyclic rotations or reversals of each other, so (A, B) is not related by a translation or reflection.

For Sidon to transfer to $\mathbb{Z}/N\mathbb{Z}$, every nonzero integer difference in $[-18, 18]$ must remain nonzero and distinct $\pmod N$, which holds whenever $N \geq 37$. Hence both A and B are Sidon in $\mathbb{Z}/N\mathbb{Z}$ for all $N \geq 37$.

4.3. Numerical U^3 table. For $f_S := \mathbf{1}_S - 6/N$ and $S \in \{A, B\}$, exact rational computation of $\|f_S\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})}$ gives the table

(3)

N	$\|f_A\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})}$	$\|f_B\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})}$	differ?
37	2.41658×10^{-5}	2.41658×10^{-5}	no
41	1.64460×10^{-5}	1.64815×10^{-5}	yes
43	1.37970×10^{-5}	1.37715×10^{-5}	yes
47	9.92868×10^{-6}	9.92868×10^{-6}	no
53	6.39310×10^{-6}	6.39310×10^{-6}	no

(The displayed entries are six-significant-figure roundings of exact rationals; the underlying script reproduces the rational values bit-for-bit. See Remark 4.3.)

The cube count $T_3^{(N)}(S)$, which is N^4 times the leading $T = \{0,1\}^3$ term in (2), equals $T_3(S) = 96$ for both $S \in \{A, B\}$ at every $N \geq 37$. Although the general no-wraparound criterion of §2 requires $N > 2k(\max S - \min S) = 6 \cdot 18 = 108$ for $k = 3$, the $T_3^{(N)}(S) = T_3(S)$ identity in fact holds for all $N \geq 37$ here: by Lemma 3.2 every integer 2^3-cube in S is axial, so it spans at most one nonzero height $h \in [-18, 18]$ and fits inside a single residue class once $N > 36$. The discrepancy in (3) is therefore confined to the sub-cube terms with $|T| < 8$.

4.4. **The mechanism: a doubling-relation count.** We now identify the source of the $N \in \{41, 43\}$ discrepancy.

4.4.1. *Sub-cube probabilities and* r_{S-S}. For each $T \subseteq \{0,1\}^3$ define

$$P_T^{(N)}(S) := \mathbb{E}_{x,h_1,h_2,h_3 \in \mathbb{Z}/N\mathbb{Z}} \prod_{\omega \in T} \mathbf{1}_S(x + \omega \cdot h).$$

A sub-cube probability $P_T^{(N)}(S)$ counts (up to normalisation N^{-4}) the tuples $(x, h_1, h_2, h_3) \in (\mathbb{Z}/N\mathbb{Z})^4$ such that the prescribed vertices of the 2^3-cube lie in S. Each constraint $x + \omega \cdot h \in S$ is a linear condition on (x, h_1, h_2, h_3) with integer coefficient vector $(1, \omega_1, \omega_2, \omega_3) \in \{0,1\}^4$.

Lemma 4.1. *For every $T \subseteq \{0,1\}^3$, $P_T^{(N)}(S)$ equals N^{-4} times the count of solutions to a homogeneous integer linear system in $(x, h_1, h_2, h_3, \{s_\omega\}_{\omega \in T})$ in $(\mathbb{Z}/N\mathbb{Z})^4 \times S^T$. The contribution of any solution with all linear forms $x + \omega \cdot h - s_\omega$ vanishing in $\mathbb{Z}$ (rather than only* mod N*) depends only on r_{S-S}.*

Proof. The constraint $x + \omega \cdot h \in S$ is the union over $s_\omega \in S$ of the affine condition $x + \omega \cdot h = s_\omega$. Hence

$$P_T^{(N)}(S) = N^{-4} \sum_{\{s_\omega\}_{\omega \in T} \in S^T} \#\big\{(x, h_1, h_2, h_3) \in (\mathbb{Z}/N\mathbb{Z})^4 : x + \omega \cdot h \equiv s_\omega \pmod{N}\ \forall \omega \in T\big\}.$$

For a solution in which the integer linear forms $x + \omega \cdot h - s_\omega$ all *vanish in* $\mathbb{Z}$ (rather than only modulo N), each pair of indices $\omega, \omega' \in T$ contributes the affine constraint $s_\omega - s_{\omega'} = (\omega - \omega') \cdot h$, which pins the integer value $s_\omega - s_{\omega'}$. The number of $(x, h_1, h_2, h_3) \in \mathbb{Z}^4$ that satisfy a prescribed compatible collection of such affine constraints depends only on the linear algebra of the coefficient matrix $(\omega - \omega')_{\omega, \omega' \in T}$ and not on S at all; the number of choices of $\{s_\omega\}_{\omega \in T} \in S^T$ realising a prescribed difference vector $(s_\omega - s_{\omega'})_{\omega, \omega'}$ is the multiplicity in the multiset of $|T|$-tuples of S with that difference profile, which is a polynomial in the autocorrelation values $\{r_{S-S}(d)\}_d$ – here the absence of repeated nonzero differences (Sidon's defining condition, invoked via Lemma 3.1) ensures that the sub-cube count factors as a polynomial in r_{S-S} rather than requiring higher-order correlations. Hence the non-wraparound contribution to $P_T^{(N)}(S)$ is a function of r_{S-S} only. ☐

By Lemma 4.1, two Sidon-homometric sets A, B can produce different $P_T^{(N)}(A) \neq P_T^{(N)}(B)$ only through solutions for which at least one linear form $x + \omega \cdot h - s_\omega$ is non-zero in $\mathbb{Z}$ but vanishes $\bmod N$. These are precisely the *wraparound* solutions.

4.4.2. *The doubling relation as the simplest wraparound generator.* We now argue informally that the simplest non-trivial wraparound contribution to the difference $\|f_A\|_{U^3}^8 - \|f_B\|_{U^3}^8$ is captured by the *doubling relation*

$$L(s) := 2s_1 - s_2 - s_3 - s_4 + s_5, \qquad (s_1, \ldots, s_5) \in S^5. \tag{4}$$

The coefficient vector $(2, -1, -1, -1, 1)$ of L has zero sum and contains a coefficient with absolute value $\neq 1$; consequently $L(s) = 0$ in $\mathbb{Z}$ cannot be reduced to two paired equalities $s_i = s_j$, $s_k = s_l$. The integer relation is therefore invisible to the Sidon (r_{S-S}) constraint.

Define the modular and integer zero counts

$$M_5^{(N)}(S) := \#\{s \in S^5 : L(s) \equiv 0 \pmod N\}, \qquad M_5^{(\infty)}(S) := \#\{s \in S^5 : L(s) = 0\}.$$

Direct rational computation on A and B yields:

(5)

N	$M_5^{(N)}(A)$	$M_5^{(N)}(B)$	$M_5^{(N)}(A) - M_5^{(N)}(B)$
∞	158	158	0
37	210	210	0
41	192	188	+4
43	182	186	−4
47	172	172	0
53	162	162	0

We note the following.

The integer value is the same. Direct enumeration gives $M_5^{(\infty)}(A) = M_5^{(\infty)}(B) = 158$ for the two Sidon-homometric sets. Rewriting $L(s) = 0$ in $\mathbb{Z}$ as $(s_1 - s_2) + (s_1 - s_3) = s_4 - s_5$ exhibits $M_5^{(\infty)}$ as a shift-invariant statistic of S, but the variable s_1 is shared between the two left-hand differences, so the value is not a convolution of r_{S-S} alone (see Remark 4.2). The numerical equality in (5) is consistent with the general expectation that two Sidon-homometric sets share all integer shift-invariant statistics, but we do not give a closed-form proof here.

Modular zero counts can differ. The total modular count $M_5^{(N)}(S)$ admits the decomposition

$$M_5^{(N)}(S) = M_5^{(\infty)}(S) + \sum_{v \neq 0,\ N \mid v} \nu_S(v), \qquad \nu_S(v) := \#\{s \in S^5 : L(s) = v\}. \tag{6}$$

The values $L(s)$ for $s \in S^5$ lie in the interval $[-3D, 3D]$ where $D = \max S - \min S = 18$; thus $L(s) \in [-54, 54]$, and the only nonzero multiples of N that can occur in the sum of (6) are $v = \pm N$ for $N \in (27, 54]$ (and additionally

$v = \pm 2N$ for $N \leq 27$). For $N = 41$, 43, 47, 53 only the $v = \pm N$ contributions appear. Direct computation on A and B gives the level-set differences in Table 1.

Table 1. Signed level-set differences $\nu_A(v) - \nu_B(v)$ at $v = \pm N$ for $N \in \{37, 41, 43, 47, 53\}$.

N	$\nu_A(+N) - \nu_B(+N)$	$\nu_A(-N) - \nu_B(-N)$	$M_5^{(N)}(A) - M_5^{(N)}(B)$
37	0	0	0
41	+2	+2	+4
43	0	−4	−4
47	+2	−2	0
53	0	0	0

The pattern $\nu_A(\pm 41) - \nu_B(\pm 41) = (+2, +2)$ adds constructively and explains $M_5^{(41)}(A) - M_5^{(41)}(B) = +4$; at $N = 43$ the entire $\pm N$ imbalance is concentrated on the $v = -43$ side, $(0, -4)$, again summing to -4; at $N = 47$ the differences $(+2, -2)$ cancel and contribute 0. This signed level-set behaviour at $|v| = N$ is the modular mechanism that distinguishes A and B.

The cyclic U^3 table is consistent with this mechanism. At every N in (3) for which $M_5^{(N)}(A) = M_5^{(N)}(B)$ the centered U^3 values agree, and at every N for which they differ the U^3 values also differ. The ± 4 deviation at $N \in \{41, 43\}$ in (5) is consistent with the U^3 gap visible in (3) at the same moduli to within the numerical precision shown.

Remark 4.2 (On the integer identity for $M_5^{(\infty)}$)**.** Rewriting $L(s) = 0$ as $(s_1 - s_2) + (s_1 - s_3) = s_4 - s_5$ shows that $M_5^{(\infty)}(S)$ is a shift-invariant statistic of S in which the variable s_1 is shared between the two left-hand differences. A naive convolution of three pair-difference counts treats these summands as independent and *overcounts*; a closed form for $M_5^{(\infty)}(S)$ purely as a polynomial in $\{r_{S-S}(d)\}_d$ therefore does not arise from this rearrangement alone. Direct enumeration of S^5 gives $M_5^{(\infty)}(A) = M_5^{(\infty)}(B) = 158$ for the two $|S| = 6$ Sidon-homometric sets of (5); we record the integer-side equality numerically and leave a closed-form derivation in terms of r_{S-S} together with the higher-order shared-variable corrections to follow-up work.

Remark 4.3 (Reproducibility)**.** The numerical tables (3), (5) and Table 1 were produced by exact rational arithmetic in Python (`fractions.Fraction`); a self-contained verification script is available from the author. The script enumerates all 30 ordered nonzero pair-differences of each of A, B to verify the Sidon and homometric conditions, computes $\|f_S\|^8_{U^3(\mathbb{Z}/N\mathbb{Z})}$ by direct evaluation of (2), and computes $M_5^{(N)}(S)$ by enumeration of S^5.

Remark 4.4 (Scope of §4.4.1)**.** We have shown in Lemma 4.1 that all non-wraparound contributions to $P_T^{(N)}(S)$ factor through r_{S-S}, and we have numerically verified that the residual wraparound contributions are accurately captured by the level-set differences $\nu_S(\pm N)$ of the doubling relation L. A complete algebraic enumeration of every $T \subseteq \{0,1\}^3$ contribution in (2) and a closed-form expression of $\|f_A\|_{U^3}^8 - \|f_B\|_{U^3}^8$ as an explicit linear combination of $\nu_A(\pm N) - \nu_B(\pm N)$ is left to follow-up work; the script in Remark 4.3 certifies the numerical identities of this section.

Theorem 1.2 now follows by combining §§4.1–4.4: (3) establishes the agreement at $N \in \{37, 47, 53\}$ and the inequality at $N \in \{41, 43\}$; (5) identifies the doubling-relation count $M_5^{(N)}$ as the discrepancy source; Lemma 4.1 explains why the r_{S-S}-determined sub-cubes cannot account for the gap, leaving the wraparound contributions through the integer level set of L as the only available mechanism.

5. Discussion

5.1. **Integer rigidity versus cyclic flexibility.** Theorem 1.1 records that the integer 2^k-cube count of a Sidon set is rigid in the strongest possible sense: $T_k(S) = n(k(n-1)+1)$ depends only on the cardinality. The Sidon parallelogram property (Lemma 3.1) forces every integer cube to be axial, and axial cubes are completely counted by n and $n(n-1)$. No higher-order information about S enters.

Theorem 1.2 records that this rigidity does *not* extend to $\mathbb{Z}/N\mathbb{Z}$ at moderate N. The mechanism is concrete: modular wraparound allows additional cube configurations to lie in S via linear relations whose integer counterpart is non-zero. The simplest such relation on $|S| = 6$ Sidon sets in $[0, 18]$ is the doubling relation L of (4), and the homometric pair in the Bloom–Golomb family $(R(3,-2), S(3,-2))$ realises a non-zero integer level-set imbalance $\nu_A(\pm N) - \nu_B(\pm N)$ at exactly $N \in \{41, 43\}$ within the surveyed range $37 \le N \le 53$.

We do not claim this delineates a sharp class of moduli at which homometric Sidon pairs are distinguished. The single Bloom–Golomb parameter pair $(u, v) = (3, -2)$ produces *at least* the two moduli $N = 41, 43$; whether other Bloom–Golomb parameter pairs (u, v) produce other modular discriminators, and whether the collection of such moduli admits a structural description, is §6.

5.2. **Relationship to homometric / turnpike literature.** The pair (A, B) analysed in Theorem 1.2 sits in a mature literature on homometric integer sets that includes Bloom [1], Bloom–Golomb [2], Gilbert–Postpischil [6], and the algorithmic turnpike framework of Skiena–Smith–Lemke [14]. None of these works asks for the cyclic U^k behaviour of the Bloom–Golomb pairs, but they collectively establish (and Gilbert–Postpischil proves) that (1) captures all 6-mark homometric Sidon pairs up to translation, reflection, and parameter choice. Our Theorem 1.2 is therefore a Gowers-norm reading of an example whose existence in the Sidon-homometric world has been known for nearly half a century.

The notation k-fold Sidon set used in Cilleruelo–Timmons [4] refers to a different (and unrelated) invariant; our notational convention follows Tao–Vu [15, §11.1] and is independent of the Cilleruelo–Timmons definition.

6. Open questions

Question 6.1 (Other Bloom–Golomb pairs)**.** The Bloom–Golomb family (1) contains a two-parameter family of Sidon-homometric pairs. We have analysed only the parameter pair $(u, v) = (3, -2)$. For which other $(u, v) \in \mathbb{Z}^2$ giving Sidon $R(u, v), S(u, v)$ does the cyclic U^3 on $\mathbb{Z}/N\mathbb{Z}$ distinguish them at some N? Is there a uniform mechanism (e.g., a single doubling-style relation valid for all parameters), or does the modular discriminator depend on (u, v)?

Question 6.2 (Characterisation of exceptional moduli)**.** Given a Sidon-homometric pair $A, B \subset [0, D]$, can the set $\{N : \|f_A\|_{U^3(\mathbb{Z}/N\mathbb{Z})} \neq \|f_B\|_{U^3(\mathbb{Z}/N\mathbb{Z})}\}$ be characterised in terms of explicit invariants of (A, B)? The analysis of §4.4 identifies a sufficient mechanism based on the level-set frequencies $\nu_S(\pm N)$ of the doubling relation L; we do not know whether it is also necessary, nor how to predict the cancellation phenomenon observed at $N = 47$ in Table 1.

Question 6.3 ($\pm N$-symmetry of ν_S)**.** A refinement of the previous question: characterise when the signed level-set difference $(\nu_A(+N)-\nu_B(+N),\ \nu_A(-N)-\nu_B(-N))$ is *symmetric* (e.g., $N = 41$ gives $(+2, +2)$, the two halves adding constructively) versus *antisymmetric* (e.g., $N = 43$ gives $(0, -4)$ with all weight on the negative side, or $N = 47$ gives $(+2, -2)$ where the two halves cancel). The cyclic U^3 discrepancy at modulus N depends on the sum $(\nu_A(+N)-\nu_B(+N))+(\nu_A(-N)-\nu_B(-N))$, so the symmetric/antisymmetric dichotomy of Table 1 directly governs which exceptional moduli are visible to U^3 and which are hidden by cancellation. We have no structural prediction for which moduli fall into which class.

Question 6.4 (Higher uniformity)**.** For each fixed $k \geq 4$, is there a B_2-set pair (necessarily Sidon-homometric and with identical T_j for all j) whose cyclic U^k norms differ at some moderate modulus? An analogue of the doubling relation L for U^k would be a length-$(2k-1)$ integer relation with a doubled coefficient; one expects such relations to exist and to support modular discriminators, but no explicit example is recorded.

Question 6.5 (B_h-extension of Theorem 1.1)**.** For B_h-sets $S \subset \mathbb{Z}$ (those with all h-fold sums distinct), the analogue of Lemma 3.2 should state that at most $h-1$ heights $h_1, \ldots, h_k$ of any cube in S are non-zero. The resulting formula for $T_k(S)$ would be a polynomial in $n = |S|$ of degree h with k-dependent coefficients. We have not worked out the case $h \geq 3$.

ACKNOWLEDGMENTS

This note arose during an extended LLM-assisted exploration of the literature on Sidon sets and their additive-combinatorial invariants; the identification of (A, B) as a Bloom–Golomb pair surfaced during adversarial review of an earlier draft, and the author thanks the review process for producing both Theorem 1.1 and its honest framing. The author has no competing interests. All numerical computations of §4 are exactly reproducible in standard Python with rational arithmetic.

REFERENCES

[1] G. S. Bloom, *A counterexample to a theorem of S. Piccard*, J. Combin. Theory Ser. A **22** (1977), 378–379.

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

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

[4] J. Cilleruelo and C. Timmons, *k-fold Sidon sets*, Electron. J. Combin. **21** (2014), no. 4, Paper 4.12, 9 pp.

[5] 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.

[6] P. Gilbert and E. Postpischil, *There are no new homometric Golomb ruler pairs with 12 marks or less*, Experimental Mathematics **3** (1994), no. 2, 147–152.

[7] E. Kowalski, *Introduction to additive combinatorics*, ETH Zürich lecture notes (2025), Proposition 2.3.7 (Sidon L^4 identity) and §4.4 (Gowers uniformity norms).

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

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

[10] M. Ortega and S. Prendiville, *Extremal Sidon sets are Fourier uniform, with applications to partition regularity*, J. Théor. Nombres Bordeaux **35** (2023), 115–134; preprint arXiv:2110.13447 (2021).

[11] I. D. Shkredov, *Energies and structure of additive sets*, Electron. J. Combin. **21** (2014), no. 3, Paper 3.44; preprint arXiv:1405.3132.

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

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

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

[15] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006. Proposition 4.29 (p. 173) and Equation (11.2) (pp. 418–419).

INDEPENDENT RESEARCHER
Email address: `lightman.chang@gmail.com`