A rounding morphism for additive structure: Sidon subsets and codes with separated pair-sums

Pranava Kumar Sushaan Kandukoori Shrikrishna Ramesh

August 16, 2026

Abstract

For finite A in a torsion-free abelian group let $\|A\|$ be the largest size of a Sidon subset of A, and $\ell(N) = \min\{\|A\| : |A| = N\}$. We prove $\ell(N) \geq (2/(3\sqrt{3}) - o(1))\sqrt{N}$, twice Bailleul and Riblet's constant. Rounding A into $\mathbb{Z}_m$ at random is additive on every additive quadruple up to a defect of at most one bucket, in every dimension and every draw; in one dimension, with random scale, the pairwise collision probability is exactly $1/m$. A code from a planar difference set absorbs the defect, avoiding the restriction to half of A that earlier arguments pay.

A code tolerating perturbations of magnitude t satisfies $(t+1)(k(k-1)+1) \leq m$, with equality exactly at translated $(t+1)$-fold dilates of planar difference sets. This also bounds the method: using only $|A|$ and the collision law, no such argument passes $2/(3\sqrt{3})$, even with a measurable Sidon system in place of the code. Plain reduction modulo m has no defect; we weaken its diameter hypothesis to a condition on the image of A modulo m, and bound what a second point per fiber gains.

1 Introduction

1.1 The main theorem

A finite set S in an abelian group is a *Sidon set* if every solution of

$$s_1 + s_2 = s_3 + s_4, \qquad s_1, s_2, s_3, s_4 \in S,$$

is trivial, meaning $\{s_1, s_2\} = \{s_3, s_4\}$ as unordered pairs. We follow the convention that this includes the degenerate instances with $s_1 = s_2$; equivalently, the pairwise sums $s_i + s_j$ with $i \leq j$ are all distinct, so a Sidon set contains no nontrivial three-term arithmetic progression. Definition 1.4 builds the degenerate case into the definition, and Proposition 2.1 records the different defect distribution it produces.

For a finite set A write $\|A\|$ for the largest cardinality of a Sidon subset of A, and put

$$\ell(N) = \min\big\{\|A\| : |A| = N\big\}.$$

Riddell [26] asked for the order of $\ell(N)$. That $\ell(N) \gg \sqrt{N}$ follows from a theorem of Komlós, Sulyok and Szemerédi [25], whose argument gives the explicit constant 2^{-15}. Abbott [1] obtained every $c < 2/25$ (his proof in fact yields 0.0805, as quoted in [3]), and Bailleul and Riblet [3] every $c < 1/(3\sqrt{3}) = 0.1924\ldots$, also for finite subsets of $\mathbb{R}^d$ uniformly in d.

Theorem 1.1. *Every N-point subset A of a torsion-free abelian group satisfies*

$$\|A\| \;\geq\; \left(\frac{2}{3\sqrt{3}} - o(1)\right)\sqrt{N},$$

the $o(1)$ depending on N alone: neither on A nor on the group. In particular $\ell(N) \geq (2/(3\sqrt{3}) - o(1))\sqrt{N}$ with $2/(3\sqrt{3}) = 2\sqrt{3}/9 = 0.3849\ldots$, and the bound holds in $\mathbb{R}^d$ uniformly in d.

This doubles the constant of [3], in a setting that contains theirs. In the other direction an interval with the Erdős–Turán estimate [24] gives $\ell(N) \leq (1+o(1))\sqrt{N}$; for the interval extremal function itself Hou and Zhao [5] proved $F(n) \leq \sqrt{n} + 0.9435\, n^{1/4} + O(1)$, improving the best published coefficient of Carter, Hunter and O'Bryant [4], and also a smaller value announced subsequently by Tao and coauthors (reported in the introduction of [5]). Alon and Erdős [2] raised the possibility that $\ell(N) = (1 + o(1))\sqrt{N}$ and called the question difficult; it remains open, as does their stronger conjecture on partitioning an N-point set into $(1 + o(1))\sqrt{N}$ Sidon sets. Theorem 1.1 concerns a constant and leaves the gap between $0.3849\ldots$ and 1 untouched.

Remark 1.2. $\|A\|$ is an independence number: the largest independent set in the hypergraph on A whose edges are the nontrivial additive quadruples together with the three-term progressions, edges of size 4 and 3, the latter because our convention forbids $2a = b + c$. Both parts appear in [2]: the four-uniform one in the proof of their Theorem 1, and the three-uniform one, with edges $a_i + a_j = 2a_l$, in the proof of their Theorem 3. A different invariant, the least size of an inclusion-maximal Sidon subset, is studied by Ruzsa [7] in the interval and by Redman, Rose and Walker [6] in $\mathbb{Z}_2^n$.

1.2 The mechanism: rounding as a morphism with bounded defect

Every quantitative approach to $\ell(N)$ transports A into a cyclic group and intersects with a large Sidon set there. The obstruction is that the transport is a rounding, and rounding is not additive. Fix an integer $m \geq 2$ and a width $w > 0$; for a direction $g \in \mathbb{R}^d$ and an offset o uniform on $[0, w)$, set

$$\psi(x) = \frac{\langle g, x\rangle + o}{w}, \qquad \varphi(x) = \lfloor \psi(x) \rfloor \bmod m. \tag{1}$$

The defect bound and the collision law, which together form Theorem 1.3 below, require different amounts of randomness. The bound on the defect is deterministic, holding for every fixed g, w and o. The collision law needs the scale to be random as well, and is stated in the one-dimensional model

$$d = 1, \quad g = 1, \quad w = \tfrac{1}{m\theta}, \quad o = \beta w, \qquad \text{so that} \qquad \psi(a) = ma\theta + \beta, \tag{2}$$

with θ, β independent and uniform on $[0, 1)$. Every statement below about collisions or bucket occupancy refers to (2); every defect statement holds for arbitrary (g, w, o). We call a draw of (θ, β) a *dither*. Call a map $\pi\colon A \to H$ into an abelian group H a *Freiman 2-homomorphism* if $x + y = x' + y'$ in A implies $\pi(x) + \pi(y) = \pi(x') + \pi(y')$; neither injectivity nor the converse implication is required. Existing arguments restrict to the subset of A on which φ is an exact Freiman 2-homomorphism, a subset of density $1/2$. Bounding the defect instead lets us keep all of A.

Theorem 1.3 (Mechanism)**.** *Let $x, y, x', y' \in \mathbb{R}^d$ satisfy $x + y = x' + y'$. Then for* every *g, w and o,*

$$\varphi(x) + \varphi(y) - \varphi(x') - \varphi(y') \equiv \delta \pmod m, \qquad \delta \in \{-1, 0, 1\}.$$

Moreover, in the model (2), $\mathbb{P}[\varphi(a) = \varphi(b)] = 1/m$ exactly for all integers $a \neq b$.

The defect bound is deterministic, holding for every draw, so no conditioning and no union bound are needed. It is also independent of the dimension, equal to 1 for every d, because $\langle g, \cdot \rangle$ is linear and the rounding is applied only after projection to one dimension. The uniform offset is what makes the collision probability exact. To prove Theorem 1.1, we intersect the rounded image with a code that tolerates a defect of size one.

1.3 The size bound for codes, and the limit of the method

The codes that cancel the defect satisfy an extremal condition, and that condition admits a complete classification.

Definition 1.4. For $t \geq 0$, a set $S \subset \mathbb{Z}_m$ is *t-separated* if the only solutions of $s_1+s_2-s_3-s_4 \equiv \delta \pmod m$ with $s_i \in S$ and $|\delta|_m \leq t$ are those with $\delta = 0$ and $\{s_1, s_2\} = \{s_3, s_4\}$. Equivalently, distinct pair-sums of S lie more than t apart in $\mathbb{Z}_m$. Here $|x|_m = \min(x \bmod m,\, m-(x \bmod m))$ is the distance from x to 0 in $\mathbb{Z}_m$.

In the terminology of Nathanson [12] a t-separated set is precisely a $B_{2,\Delta}$-set with $\Delta = t+1$, that is, a Sidon set whose sumset is Δ-separated. Two of the three ingredients below are his, transported to $\mathbb{Z}_m$: the equivalence with a Δ-separated *unique* difference set is his Lemma 4, and the dilation $D \mapsto (t+1)D$ underlying $S = a+(t+1)D$ is his Lemma 2. At $t = 0$ a separated set is simply a Sidon set, the bound is the classical modular Golomb ruler bound $k(k-1)+1 \leq m$, and equality holds precisely at the planar difference sets of Singer [27]; Remark 4.1 gives the design-theoretic dictionary and its literature.

For $t \geq 1$, Theorem 1.5 below supplies two statements absent from [12]: the inequality $(t+1)(k(k-1)+1) \leq m$ for every m, with no error term, and the converse forcing every extremal set to be a translated dilate $a+(t+1)D$ of a planar difference set. The general case is thus the classical one with the modulus replaced by $m/(t+1)$. In the cyclic model this settles the $h = 2$ analogues of Problems 4 and 5 of [12], which are posed for $B_{h,\Delta}$-sets of maximum size in the interval $\{1, \ldots, n\}$ and for every $h \geq 2$; the interval questions themselves remain open. For intervals the sharp leading constant is already known, by an argument of O'Bryant adapting Lindström [10] and reported in [12, §4]; the classification is what is added.

Theorem 1.5 (Size bound and equality case)**.** *Let $S \subset \mathbb{Z}_m$ be t-separated with $|S| = k \geq 3$. Then*

$$(t+1)\big(k(k-1)+1\big) \;\leq\; m,$$

with equality if and only if $S = a+(t+1)D$ for some a and some planar difference set $D \subset \mathbb{Z}_{m/(t+1)}$, in particular equality forces $(t+1) \mid m$. Consequently an extremal t-separated code of size k exists in $\mathbb{Z}_m$ if and only if $m = (t+1)(q^2+q+1)$, $k = q+1$, and a cyclic *projective plane of order q exists.*

The inequality may be written $k(k-1)+1 \leq \lfloor m/(t+1) \rfloor$, but the equality clause must be read in the displayed form: equality in the rounded-down version is strictly weaker and does not force the structure. For instance $S = \{0, 2, 6\} \subset \mathbb{Z}_{15}$ is 1-separated with $k(k-1)+1 = 7 = \lfloor 15/2 \rfloor$, yet $2 \nmid 15$ and S is not such a dilate; here $2 \cdot 7 = 14 < 15$, so the displayed inequality is strict, as it must be.

Allowing perturbations of magnitude t multiplies the required modulus by $t+1$, or equivalently reduces the code size by a factor $\sqrt{t+1}$ at leading order. Theorem 4.3 interprets this as decoding pairs, where errors of size at most e correspond to $t = 2e$. The equality classification

also shows that a different fixed code cannot improve the constant in the argument that keeps one point per fiber.

Theorem 1.6 (Optimality of the method, informal; Corollary 5.3)**.** *Any argument that takes $m = (c + o(1))N$, deletes points to make φ injective using only the collision law, and intersects with a translate of a fixed 1-separated code, yields at most $2/(3\sqrt{3}) + o(1)$, uniformly in A.*

The limiting condition is 1-separation, which is required only because rounding introduces a defect. Plain reduction modulo m has no defect, so a planar difference set of density $m^{-1/2}$ can be used directly. Proposition 5.12 records the classical argument of [1] under a diameter $O(N)$ hypothesis. Remark 5.14 weakens this to a condition on $\nu_A(m) = |\{a \bmod m : a \in A\}|$, the number of residues modulo m that A occupies, and then to any Freiman 2-homomorphism with a sufficiently large image. Theorem 1.6 therefore limits only the route that tolerates a defect; an improvement along the route with no defect must instead find a transport whose image does not collapse.

1.4 Further consequences

Retaining two points per fiber would raise the coefficient to $2/3$, but the construction must discard fibers that repeat a gap. Theorem 6.2 bounds the resulting gain by the number of distinct positive differences of A, so for an interval it is $O(1)$ points and the constant is unchanged. Separately, Proposition 5.12 gives coefficient $1/\sqrt{K}$ for a set with an integer model of diameter KN, using an embedding with no defect.

1.5 Relation to prior work

Before the final reduction modulo m, the map (1) is the p-stable locality-sensitive hash $h_{a,b}(v) = \lfloor(\langle a, v\rangle + b)/r\rfloor$ of Datar, Immorlica, Indyk and Mirrokni [23], offset included: their b is likewise uniform on $[0, r)$, and in both settings it is the uniform offset that makes the collision law exact; Theorem 1.3 therefore states a property of that family, namely that p-stable LSH is a Freiman 2-homomorphism up to one bucket, for every draw and in every dimension. Neither is the morphism property itself, which is a named standard property in fine-grained complexity: the requirement that $h(x) + h(y) - h(x + y)$ take one of a bounded number of values is the *almost linearity* of [13], attributed there to Kopelowitz, Pettie and Porat. For the integer linear hash $h(x) = ((\sigma x + \tau) \bmod p) \bmod m$ its sharp form is the *almost-affinity* of Bringmann, Fischer and Nakos [8, Lemma 4.1], who prove that $h(x) + h(y) = h(0) + h(x + y) + \epsilon$ for one of three shifts $\epsilon \in \{-p, 0, p\}$ and use the resulting three-way bucket split throughout their sparse-convolution algorithm. Chaining two copies of that triple form to compare $x + y$ with $x' + y'$ yields five shifts, and Jin and Xu [9, Eq. (17)] sharpen the pair-sum itself to two by hashing the query separately. Theorem 1.3 gives three for the quadruple directly. Its contribution is the setting more than the count: the bound is deterministic, holds in every dimension, and applies to the scalar rounding (1) over $\mathbb{R}^d$ in place of a modular linear hash. We obtain in addition an exact one-dimensional collision law, and classify the codes that cancel the defect. We do not improve any locality-sensitive hashing guarantee.

Notation. For real u, $\lfloor u\rfloor$ is the integer part and $\{u\} = u - \lfloor u\rfloor \in [0, 1)$ the fractional part.

2 The rounding morphism

Proof of Theorem 1.3, defect bound. Because $\langle g, \cdot \rangle$ is linear and $x + y = x' + y'$, and because each side of the relation carries exactly two offsets,

$$\psi(x) + \psi(y) - \psi(x') - \psi(y') = \frac{\langle g, x + y - x' - y' \rangle}{w} + \frac{2o - 2o}{w} = 0.$$

Hence

$$\delta = \lfloor \psi(x) \rfloor + \lfloor \psi(y) \rfloor - \lfloor \psi(x') \rfloor - \lfloor \psi(y') \rfloor = -\big(\{\psi(x)\} + \{\psi(y)\} - \{\psi(x')\} - \{\psi(y')\}\big),$$

an integer lying in $(-2, 2)$. □

Proof of Theorem 1.3, collision identity. Take $d = 1$, $g = 1$, and rescale so that $\psi(a) = ma\theta + \beta$ with θ, β independent and uniform on $[0, 1)$. Put $n = a - b \neq 0$ and $\Delta = \psi(a) - \psi(b) = mn\theta$. For all reals u, Δ,

$$\lfloor u + \Delta \rfloor - \lfloor u \rfloor = \lfloor \Delta \rfloor + \mathbf{1}\big[\{u\} + \{\Delta\} \geq 1\big].$$

Let $v = \Delta \bmod m \in [0, m)$; then $\lfloor \Delta \rfloor \equiv \lfloor v \rfloor \pmod m$ and $\{\Delta\} = \{v\}$, so

$$\varphi(a) - \varphi(b) \equiv \lfloor v \rfloor + \mathbf{1}[\{\psi(b)\} + \{v\} \geq 1] \pmod m.$$

The right-hand side lies in $\{0, \dots, m\}$ and so vanishes modulo m exactly when it is 0 or m: either $v \in [0, 1)$ and $\{\psi(b)\} < 1 - v$, or $v \in [m - 1, m)$ and $\{\psi(b)\} \geq 1 - (v - (m - 1))$. Now v is uniform on $[0, m)$ because n is a nonzero integer, and v depends only on θ, while conditionally on θ the value $\{\psi(b)\}$ is uniform on $[0, 1)$ because β is. Writing $v = (m - 1) + u$ in the second case,

$$\mathbb{P}[\varphi(a) = \varphi(b)] = \frac{1}{m}\left(\int_0^1 (1 - v)\, dv + \int_0^1 u\, du\right) = \frac{1}{m}.$$ □

The defect takes all three values, and in the model (2) its law can be computed in closed form. Write $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and let $\|u\|_{\mathbb{Z}}$ denote the distance from a real number u to the nearest integer.

Proposition 2.1 (Law of the defect)**.** *Work in the model* (2) *and let $x, y, x', y' \in \mathbb{Z}$ satisfy $x + y = x' + y'$. Write $a_1 = \psi(x)$, $a_2 = \psi(y)$, $a_3 = \psi(x')$ and $a_4 = \psi(y')$, so that $a_1 + a_2 = a_3 + a_4$ identically. Then*

$$\delta = -\big\lfloor \{a_1\} + \{a_2\} - \{a_3\} \big\rfloor \in \{-1, 0, 1\},$$

and, conditionally on the scale θ,

$$\mathbb{P}[\delta = 1 \mid \theta] = \mathbb{P}[\delta = -1 \mid \theta] = \min\big(\|m(x - x')\theta\|_{\mathbb{Z}},\ \|m(y - x')\theta\|_{\mathbb{Z}}\big). \tag{3}$$

Consequently:

(i) if x, y, x', y' are pairwise distinct, then $\mathbb{P}[\delta = -1] = \mathbb{P}[\delta = 1] = \frac{1}{6}$ and $\mathbb{P}[\delta = 0] = \frac{2}{3}$;

(ii) if the relation is a three-term progression, that is $x = y$ or $x' = y'$ while $\{x, y\} \neq \{x', y'\}$, then $\mathbb{P}[\delta = -1] = \mathbb{P}[\delta = 1] = \frac{1}{4}$ and $\mathbb{P}[\delta = 0] = \frac{1}{2}$;

(iii) if $\{x, y\} = \{x', y'\}$ then $\delta = 0$ surely.

Proof. Since $a_4 = a_1 + a_2 - a_3$ we have $\{a_4\} = \{\{a_1\} + \{a_2\} - \{a_3\}\}$, so $\{a_1\} + \{a_2\} - \{a_3\} - \{a_4\} = \lfloor \{a_1\} + \{a_2\} - \{a_3\} \rfloor$, which is the displayed formula for δ; it lies in $\{-1, 0, 1\}$ because $\{a_1\} + \{a_2\} - \{a_3\} \in (-1, 2)$. Case (iii) is immediate, since equal multisets give $\{a_1\} + \{a_2\} = \{a_3\} + \{a_4\}$.

For (3) put $\zeta = \{a_3\}$, $\xi = \{m(x - x')\theta\}$ and $\eta = \{m(y - x')\theta\}$. Since $a_1 - a_3 = m(x - x')\theta$ and $a_2 - a_3 = m(y - x')\theta$, the two quantities ξ, η are functions of θ alone, while $\{a_1\} = \{\zeta + \xi\}$ and $\{a_2\} = \{\zeta + \eta\}$; and conditionally on θ the variable ζ is uniform on $[0, 1)$, because β is and enters a_3 additively. From $\{\zeta + \xi\} = \zeta + \xi - \mathbf{1}[\zeta \geq 1 - \xi]$,

$$\{a_1\} + \{a_2\} - \{a_3\} = \zeta + \xi + \eta - \mathbf{1}[\zeta \geq 1 - \xi] - \mathbf{1}[\zeta \geq 1 - \eta].$$

Assume $\xi \leq \eta$; the right-hand side is symmetric in ξ, η. Cutting $[0, 1)$ at $1 - \eta$ and $1 - \xi$, the right-hand side equals $\zeta + \xi + \eta$ on $[0, 1 - \eta)$, equals $\zeta + \xi + \eta - 1 \in [\xi, \eta) \subset [0, 1)$ on $[1 - \eta, 1 - \xi)$, and equals $\zeta + \xi + \eta - 2$ on $[1 - \xi, 1)$.

If $\xi + \eta < 1$ the first piece lies in $[1, 2)$ exactly for $\zeta \geq 1 - \xi - \eta$, a set of measure ξ, and the third piece lies in $[-1, 0)$ throughout, a set of measure ξ. If $\xi + \eta \geq 1$ the first piece lies in $[1, 2)$ throughout, a set of measure $1 - \eta$, and the third lies in $[-1, 0)$ exactly for $\zeta < 2 - \xi - \eta$, a set of measure $1 - \eta$. In both cases the common measure is $\min(\xi, 1 - \eta) = \min(\xi, \eta, 1 - \xi, 1 - \eta) = \min(\|\xi\|_{\mathbb{Z}}, \|\eta\|_{\mathbb{Z}})$, and a value in $[1, 2)$ means $\delta = -1$, a value in $[-1, 0)$ means $\delta = 1$. This is (3).

It remains to average (3) over θ. Put $n = m(x - x')$ and $k = m(y - x')$; these are nonzero integers unless the relation is trivial, which is case (iii). Set $F(\xi, \eta) = \min(\|\xi\|_{\mathbb{Z}}, \|\eta\|_{\mathbb{Z}})$ on $\mathbb{T}^2$, so that

$$F(\xi, \eta) = \int_0^{1/2} \mathbf{1}\big[\|\xi\|_{\mathbb{Z}} > u\big]\, \mathbf{1}\big[\|\eta\|_{\mathbb{Z}} > u\big]\, du.$$

The indicator $\mathbf{1}[\|\cdot\|_{\mathbb{Z}} > u]$ on $\mathbb{T}$ has Fourier coefficients $A_0(u) = 1 - 2u$ and $A_p(u) = -\sin(2\pi p u)/(\pi p)$ for $p \neq 0$, so $\widehat{F}(p, q) = \int_0^{1/2} A_p(u) A_q(u)\, du$. Since $\theta \mapsto (n\theta, k\theta)$ is a homomorphism $\mathbb{T} \to \mathbb{T}^2$, only the characters annihilating its image survive:

$$\mathbb{E}_\theta\big[F(n\theta, k\theta)\big] = \sum_{pn + qk = 0} \widehat{F}(p, q).$$

Let $g = \gcd(|n|, |k|)$, so that the solutions of $pn + qk = 0$ are $(p, q) = (tk/g, -tn/g)$ with $t \in \mathbb{Z}$. For $t \neq 0$ both coordinates are nonzero, and, using $2\sin(2\pi p u)\sin(2\pi q u) = \cos(2\pi(p - q)u) - \cos(2\pi(p + q)u)$ with $p - q = t(k + n)/g$ and $p + q = t(k - n)/g$,

$$\widehat{F}\Big(\frac{tk}{g}, -\frac{tn}{g}\Big) = \frac{-g^2}{2\pi^2 t^2 nk} \int_0^{1/2} \left[\cos\frac{2\pi t(k + n)u}{g} - \cos\frac{2\pi t(k - n)u}{g}\right] du.$$

Both $t(k \pm n)/g$ are integers, and $\int_0^{1/2} \cos(2\pi M u)\, du$ equals 0 for every nonzero integer M and $\frac{1}{2}$ for $M = 0$. They vanish exactly when $k = \mp n$. Hence if $|n| \neq |k|$ every term with $t \neq 0$ vanishes and

$$\mathbb{E}_\theta\big[F(n\theta, k\theta)\big] = \widehat{F}(0, 0) = \int_0^{1/2} (1 - 2u)^2\, du = \tfrac{1}{6},$$

which is (i), because $|n| = |k|$ says precisely that $x = y$ or $x' = y'$. If $k = n \neq 0$ then $g = |n|$ and the surviving terms are $\widehat{F}(t, -t) = 1/(4\pi^2 t^2)$, whence $\frac{1}{6} + 2\sum_{t \geq 1} (4\pi^2 t^2)^{-1} = \frac{1}{6} + \frac{1}{12} = \frac{1}{4}$; the case $k = -n$ gives the same value because $\|\cdot\|_{\mathbb{Z}}$ is even. That is (ii). $\square$

Remark 2.2. The value $\frac{1}{6}$ in (i) is what independent uniform fractional parts would give, since $\mathbb{P}[U_1 + U_2 < U_3] = \int_0^1 \frac{1}{2}U^2\,dU = \frac{1}{6}$. The fractional parts are not independent: the triple $(\{a_1\}, \{a_2\}, \{a_3\})$ lies in the image of a homomorphism $\mathbb{T}^2 \to \mathbb{T}^3$, a closed subgroup of dimension at most 2 and therefore Haar-null. Statement (i) consequently does not follow from that heuristic, which in case (ii) gives the wrong value.

3 Sidon subsets of arbitrary sets

3.1 Reduction to the integers, and the code

Lemma 3.1. *For every finite A in a torsion-free abelian group there is a bijection ρ onto a finite $A' \subset \mathbb{Z}$ with $a + b = c + d \iff \rho(a) + \rho(b) = \rho(c) + \rho(d)$.*

Proof. The subgroup generated by A is finitely generated and torsion free, hence isomorphic to $\mathbb{Z}^r$; a group isomorphism preserves and reflects all additive relations. Translating, assume $A \subset \mathbb{Z}^r_{\geq 0}$, let $B > 4 \max_{x \in A} \max_i x_i + 1$ and $\pi(x) = \sum_i x_i B^{i-1}$. All coordinates of a sum of two elements lie in $[0, B)$, so π preserves and reflects such sums. □

The three lemmas that follow build the code that cancels the defect; it is 1-separated in the sense of Definition 1.4.

Lemma 3.2 (Singer [27])**.** *For every prime power q there is a planar difference set $D \subset \mathbb{Z}_v$ of order q, where $v = q^2 + q + 1$: a set of $q + 1$ residues in which every nonzero residue has exactly one representation as a difference of two elements.*

Lemma 3.3. *A planar difference set $D \subset \mathbb{Z}_v$ is a Sidon set in $\mathbb{Z}_v$, and $D - D = \mathbb{Z}_v$.*

Proof. If $d_1 + d_2 = d_3 + d_4$ then $d_1 - d_3 = d_4 - d_2$. If $d_1 \neq d_3$ this exhibits a nonzero residue with two representations as a difference of elements of D, so by definition the two coincide as ordered pairs, giving $d_1 = d_4$ and $d_3 = d_2$; if $d_1 = d_3$ then $d_2 = d_4$. Either way $\{d_1, d_2\} = \{d_3, d_4\}$, including when $d_1 = d_2$. The $|D|(|D| - 1) = v - 1$ differences of distinct elements are distinct and nonzero, so with 0 they exhaust $\mathbb{Z}_v$. □

Lemma 3.4 (Dilation by two)**.** *Let $D \subset \mathbb{Z}_v$ be a planar difference set of order q, let $m = 2v$, and let $S_\alpha = \alpha + 2D$. Then $|S_\alpha| = q + 1$ and S_α is 1-separated.*

Proof. Distinctness is clear since $2d \equiv 2d' \pmod{2v}$ forces $d \equiv d' \pmod{v}$. For $s_i = t + 2d_i$ the translations cancel and $s_1 + s_2 - s_3 - s_4 = 2(d_1 + d_2 - d_3 - d_4)$ is even; as m is even, any δ it realizes is even, and the only even δ with $|\delta|_m \leq 1$ is 0. Dividing by 2 gives $d_1 + d_2 \equiv d_3 + d_4 \pmod{v}$, and Lemma 3.3 gives $\{d_1, d_2\} = \{d_3, d_4\}$. □

Lemma 3.5 (Pullback and translates)**.** *Let φ be injective on $C \subset A$ and let $S \subset \mathbb{Z}_m$ be 1-separated. Then $\varphi^{-1}(S) \cap C$ is Sidon. Moreover, with $m = 2v$ and $S_\alpha = \alpha + 2D$: every residue lies in exactly $q + 1$ of the S_α, and two distinct residues lie in a common S_α for at most one α.*

Proof. If $a + b = c + d$ in $\varphi^{-1}(S) \cap C$, Theorem 1.3 gives a relation among four elements of S with defect in $\{-1, 0, 1\}$; 1-separation forces the defect to vanish and the multisets of images to agree, and injectivity transfers this to $\{a, b\} = \{c, d\}$. For the second claim, $r \in S_\alpha$ iff $\alpha \in r - 2D$, a set of $q + 1$ residues; and if $r, r' \in S_\alpha$ then $r \equiv r' \equiv \alpha \pmod 2$, while for equal parities $d - d' = (r - r')/2 \neq 0$ determines the ordered pair (d, d'), hence $\alpha = r - 2d$. □

Lemma 3.6 (Deletion)**.** *There are θ, β and a set $C \subset A$ with $|C| \geq N - \binom{N}{2}/m$ on which φ is injective.*

Proof. Let P count the pairs $\{a, b\} \subset A$ with $\varphi(a) = \varphi(b)$. By the collision identity of Theorem 1.3 and linearity, $\mathbb{E}P = \binom{N}{2}/m$, so fix a dither with $P \leq \binom{N}{2}/m$. If the fibers have sizes $r_1, r_2, \ldots$ then $\sum_i \binom{r_i}{2} = P$, and deleting all but one point of each fiber removes $\sum_i (r_i - 1) \leq \sum_i \binom{r_i}{2} = P$ points, using $r - 1 \leq \binom{r}{2}$ for $r \geq 1$. □

3.2 Proof of Theorem 1.1

Proof. By Lemma 3.1 assume $A \subset \mathbb{Z}$, $|A| = N$. Let q be a prime power, $v = q^2 + q + 1$, $m = 2v$, D a Singer set.

By Lemma 3.6 there are a dither and a set $C \subset A$ with $|C| \geq N - \binom{N}{2}/m$ on which φ is injective. By Lemma 3.5 some translate satisfies $|\varphi(C) \cap S_\alpha| \geq (q+1)|C|/m$, and its preimage is a Sidon subset of A of that size. Hence

$$\|A\| \;\geq\; \frac{q+1}{m}\left(N - \frac{1}{m}\binom{N}{2}\right), \tag{4}$$

for every prime power q; it is a finite inequality holding simultaneously for all A of size N, so the $o(1)$ of Theorem 1.1 is uniform in A.

Fix $c > 1/2$ and pick a prime $q = (1 + o(1))\sqrt{cN/2}$, so $m = (c + o(1))N$. Then (4) gives $\|A\| \geq (1 + o(1))\big(1 - \frac{1}{2c}\big)(2c)^{-1/2}\sqrt{N}$. Writing $u = 2c$, the coefficient is $f(u) = u^{-1/2} - u^{-3/2}$ with $f'(u) = \frac{1}{2}u^{-5/2}(3 - u)$, so the maximum is at $u = 3$, i.e. $c = 3/2$, where $f(3) = 2/(3\sqrt{3})$. All error terms come from the prime number theorem and depend on N alone. □

Remark 3.7. The argument of [3] also attains collision probability $1/m$; it then restricts to the half of A on which rounding is an exact morphism, which costs a factor 2 but permits a Singer set in $\mathbb{Z}_m$ itself, of density $\approx m^{-1/2}$, and a deletion term $1 - 1/c$, giving $(c-1)/(2c\sqrt{c})$ maximized at $c = 3$ with value $1/(3\sqrt{3})$. Here the dilate $a + 2D$ removes the restriction at the cost of density $\approx (m/2)^{1/2}/m$ and with deletion term $1 - 1/(2c)$. The ratio of the maxima is exactly 2.

4 Codes with separated pair-sums

Proof of Theorem 1.5. Put $\Delta = S - S$. A t-separated set is Sidon, so the $k(k-1)$ differences of distinct elements are distinct and $|\Delta| = k(k-1) + 1$; also $\Delta = -\Delta$.

Fix $1 \leq j \leq t$. If $x \in \Delta \cap (j - \Delta)$ then $x = s_1 - s_3$ and $j - x = s_2 - s_4$, so $s_1 + s_2 - s_3 - s_4 \equiv j$ with $|j|_m \leq t$, contradicting separation. Hence $\Delta \cap (j + \Delta) = \varnothing$ for $1 \leq j \leq t$, so the $t + 1$ translates $\Delta, \Delta + 1, \ldots, \Delta + t$ are pairwise disjoint and $(t+1)|\Delta| \leq m$.

If equality holds these translates partition $\mathbb{Z}_m$, i.e. $\Delta \oplus \{0, 1, \ldots, t\} = \mathbb{Z}_m$: the arcs $\{x, \ldots, x + t\}$, $x \in \Delta$, tile the cycle $\mathbb{Z}_m$. Such a tiling forces consecutive arc starts to be spaced by $t+1$. Going once around the cycle therefore gives $(t+1) \mid m$, and the arc starts form a coset $a_0 + (t+1)\mathbb{Z}_m = \Delta$; since $0 \in \Delta$, we obtain $\Delta = (t+1)\mathbb{Z}_m$. Hence every difference of S is divisible by $t + 1$, so $S = a + (t+1)D$ with $D \subset \mathbb{Z}_v$, $v = m/(t+1)$. Then $(t+1)(D - D) = (t+1)\mathbb{Z}_m$ forces $D - D = \mathbb{Z}_v$; as $|D - D| \leq k(k-1) + 1 = v$ with equality, every nonzero residue has exactly one representation as a difference from D, i.e. D is planar.

Conversely for $S = a + (t+1)D$ with D planar and $m = (t+1)v$, the quantity $s_1 + s_2 - s_3 - s_4 = (t+1)(d_1 + d_2 - d_3 - d_4)$ is divisible by $t + 1$, as is m; so any δ it realizes with $|\delta|_m \leq t$ is 0, and

dividing by $t+1$ and applying Lemma 3.3 finishes the argument. Here $k(k-1)+1 = v = m/(t+1)$. A planar difference set of order q is equivalent to a cyclic projective plane of order q [27, 18]. □

Remark 4.1 (Theorem 1.5 in design-theoretic terms). In the language of cyclic designs, a t-separated k-subset $S \subset \mathbb{Z}_m$ is an (m, k)-modular Golomb ruler. Equivalently, it is the base block of an $(m, k; 1)$-difference packing or a single-codeword $(m, k, 1)$-optical orthogonal code [14], [15, §VI.19.3], [21, Thms. 1.5, 1.7]. Its difference set is $(t+1)$-separated in the cycle, and Theorem 1.5 says that the resulting arc packing is perfect exactly when S is a $(t+1)$-fold dilate of a base block of a cyclic $(q^2+q+1, q+1, 1)$-difference set [15, §VI.18]. So the bound is attained if and only if a cyclic projective plane of order $k-1$ exists, and the question for which k it is attained is the prime power conjecture, verified for $k-1 < 2\,000\,000$ by Gordon [17] and constrained by Bruck and Ryser [20].

Because the extremal codes are classified, they can also be counted.

Corollary 4.2 (Enumeration of the extremal codes)**.** *Let q be a prime power, $v = q^2+q+1$, $k = q+1$, $t \geq 0$ and $m = (t+1)v$. Let $\iota\colon \mathbb{Z}_v \to \mathbb{Z}_m$, $\iota(d) = (t+1)d$, be the isomorphism onto the subgroup of order v, and let $P(q)$ denote the number of planar difference sets of order q in $\mathbb{Z}_v$. Then*

(i) $S \mapsto \iota^{-1}(S)$ is a bijection from the extremal t-separated codes of size k in $\mathbb{Z}_m$ containing 0 onto the planar difference sets of order q containing 0; their common number is $kP(q)/v$, independent of t;

(ii) the extremal t-separated codes in $\mathbb{Z}_m$ number $(t+1)P(q)$, which does depend on t;

(iii) up to translation in $\mathbb{Z}_m$ they number $P(q)/v$, and up to translation and multiplication by units they fall into as many classes as the planar difference sets of order q do; both counts are independent of t.

Direct enumeration gives $P(q) = 14, 52, 42, 310$ for $q = 2, 3, 4, 5$, so the counts in (i) are $6, 16, 10, 60$ and those in (iii) are $2, 4, 2, 10$ translation classes, falling in each of these four cases into a single class under translation and units.

Proof. Throughout, translation acts freely on planar difference sets and on extremal codes alike: a nonzero b with $b + S = S$ would be a difference of S in $k \geq 3$ ways, whereas both objects are Sidon and represent each nonzero difference at most once.

(i) By Theorem 1.5 the extremal codes are exactly the sets $a + \iota(D)$ with $D \subset \mathbb{Z}_v$ planar. If $0 \in S = a + \iota(D)$ then $a \in -\iota(D) \subset \iota(\mathbb{Z}_v)$, so $S \subset \iota(\mathbb{Z}_v)$ and $\iota^{-1}(S)$ is a translate of D, hence planar and containing 0; the assignment $D' \mapsto \iota(D')$ is its inverse. The $P(q)$ planar difference sets fall into $P(q)/v$ translation classes of v sets each, of which exactly k contain 0, since $D + c \ni 0$ precisely for $-c \in D$; so the common number is $kP(q)/v$, with no t in it.

(ii) Every fibre of $\Phi(a, D) = a + \iota(D)$, a map onto the extremal codes, has exactly v elements: a occurs in a preimage of S precisely when $S - a \subset \iota(\mathbb{Z}_v)$, and all differences of S are divisible by $t+1$, so the admissible a form a single coset of $\iota(\mathbb{Z}_v)$, each value of which determines $D = \iota^{-1}(S - a)$ uniquely. Hence the codes number $mP(q)/v = (t+1)P(q)$.

(iii) Translation being free, the number of orbits is $(t+1)P(q)/m = P(q)/v$. For the unit action, reduction $\mathbb{Z}_m^\times \to \mathbb{Z}_v^\times$ is surjective and $\iota(uD) = \tilde{u}\,\iota(D)$ for any unit $\tilde{u}$ of $\mathbb{Z}_m$ reducing to u; conversely $\iota(D') = \tilde{u}\,\iota(D) + c$ forces $c \in \iota(\mathbb{Z}_v)$, because both sides lie in $\iota(\mathbb{Z}_v)$. So the two actions correspond and the orbit counts agree. □

The factor $t+1$ in (ii) is the number of cosets of $\iota(\mathbb{Z}_v)$ in $\mathbb{Z}_m$. Dilating by $t+1$ removes defects of size at most t and produces $t+1$ parallel copies of each code. For Theorem 1.1 the relevant count is (iii), since the proof already sweeps all m translates of one code. Finally, when translations and units act transitively on the planar difference sets of order q, as they do for $q \le 5$, one has $P(q) = v\,\#\mathbb{Z}_v^\times/|\mathcal{M}|$, with $\mathcal{M}$ the group of numerical multipliers of a fixed such set, constrained by Hall's multiplier theorem [18]; here $|\mathcal{M}| = 3, 3, 6, 3$ for $q = 2, 3, 4, 5$.

Theorem 4.3 (Decoding)**.** *Fix $e \ge 0$ and $S \subset \mathbb{Z}_m$. Suppose each unordered pair $\{s, s'\} \subset S$ is observed as $s + s' + \varepsilon$ with $|\varepsilon|_m \le e$ unknown and chosen adversarially per pair. Every pair is uniquely identifiable from its observation if and only if S is $2e$-separated; by Theorem 1.5 this costs exactly a factor $2e+1$ in the modulus.*

Proof. If S is $2e$-separated and $s_1 + s_2 + \varepsilon = s_3 + s_4 + \varepsilon'$ then $s_1 + s_2 - s_3 - s_4 = \varepsilon' - \varepsilon$ has modulus at most $2e$, hence vanishes with $\{s_1, s_2\} = \{s_3, s_4\}$. Conversely if S is not $2e$-separated, either two distinct pairs already share a sum, or $s_1 + s_2 - s_3 - s_4 \equiv \delta$ with $0 < |\delta|_m \le 2e$; in the latter case write $\delta = \varepsilon' - \varepsilon$ with $|\varepsilon|_m, |\varepsilon'|_m \le e$, which is possible, and the two distinct pairs share an observation. □

5 The limit of the rounding argument

Together with Section 3, Theorem 1.5 shows that changing the finite code cannot improve the constant of Theorem 1.1. The same upper bound holds for arbitrary measurable systems.

Write $\mathbb{T}_m = \mathbb{R}/m\mathbb{Z}$ with arclength $|\cdot|$.

Definition 5.1. Borel sets $C_1, \dots, C_s \subset \mathbb{T}_m$ with $\mu_i = |C_i| \le 1$ form a *Sidon system* if for all $x \in C_i$, $y \in C_l$, $u \in C_k$, $z \in C_j$,

$$x + y = u + z \ \text{ in } \mathbb{T}_m \quad \Longrightarrow \quad \{i, l\} = \{k, j\} \ \text{ as multisets.}$$

Put $W = \sum_i \mu_i$, the *capacity* of the system.

Accepting a point when its hash lands in C_i, and keeping one point per accepted cell, is exactly the operation performed in the proof of Theorem 1.1; a 1-separated code $S \subset \mathbb{Z}_m$ is the special case $C_i = \{s_i\} + [0, 1)$, for which $s = |S| = W$.

Proposition 5.2 (Fractional capacity)**.** *Let $m > 2$ and let $C_1, \dots, C_s$ be a Sidon system of capacity W. Then*

$$W^2 - W + 1 \ \le \ \frac{m}{2}, \qquad \textit{so} \qquad W \ \le \ \frac{1 + \sqrt{2m-3}}{2} = \sqrt{\tfrac{m}{2}} + O(1).$$

For unit cells this reads $k(k-1) + 1 \le m/2$, which is Theorem 1.5 at $t = 1$.

Proof. Discard null cells; this changes neither W nor the Sidon condition. If $x \in C_i \cap C_j$ then $x + x = x + x$ has label multisets $\{i, i\}$ and $\{j, j\}$, so $i = j$: the cells are disjoint.

For $i \ne j$ put $E_{ij} = C_i - C_j$, and put $F = \bigcup_i (C_i - C_i)$. These are pairwise disjoint. Indeed, if $d \in E_{ij} \cap E_{kl}$ then $d = x - y = u - v$ with $x \in C_i$, $y \in C_j$, $u \in C_k$, $v \in C_l$, so $x + v = u + y$ and label safety gives $\{i, l\} = \{k, j\}$, whence $(i, j) = (k, l)$ because $i \ne j$. And if $d \in E_{kl} \cap (C_i - C_i)$ with $k \ne l$, writing $d = x - y = u - v$ with $x, y \in C_i$ gives $x + v = u + y$ and $\{i, l\} = \{k, i\}$, forcing $k = l$, which is excluded.

By the sum theorem for the torus [11], and because $\mathbb{T}_m$ is connected so that the stabiliser of a sumset is null or everything, inner measure satisfies $|E+F|_* \geq \min(m, |E|+|F|)$. Since $\mu_i + \mu_j \leq 2 < m$ we get $|E_{ij}|_* \geq \mu_i + \mu_j$, and taking a largest cell C_{i_0}, $|F|_* \geq 2\mu_{i_0} \geq 2W/s$. Inner measure is superadditive on disjoint sets, so

$$\sum_{i \neq j} (\mu_i + \mu_j) + \frac{2W}{s} \;=\; 2(s-1)W + \frac{2W}{s} \;\leq\; m.$$

Also $W \leq s$ because $\mu_i \leq 1$. Hence $W \leq \min\bigl(s,\ m/(2(s-1+1/s))\bigr)$. The first argument increases in s and the second decreases, so the minimum is largest at the crossing point σ with $2\sigma(\sigma - 1 + 1/\sigma) = m$, that is $\sigma^2 - \sigma + 1 = m/2$. Therefore $W \leq \sigma$, and since $\tau \mapsto \tau^2 - \tau + 1$ increases for $\tau \geq \frac{1}{2}$ the displayed bound follows. □

The diagonal term F contributes the $+1$ that makes the fractional bound coincide with the discrete one.

Corollary 5.3 (Optimality for Sidon systems)**.** *Consider any argument of the following form: choose m, a Sidon system, and a dither; accept the points of A whose hash lands in the system; delete points to leave one per cell; and average over translates, using no property of A beyond $|A| = N$, so that the deletion loss is estimated by the collision law of Theorem 1.3. The quantity such an argument certifies is at most $\bigl(2/(3\sqrt{3}) + o(1)\bigr)\sqrt{N}$.*

Proof. Averaging over translates of the system certifies $(W/m)\bigl(N - \binom{N}{2}/m\bigr)$, and Proposition 5.2 gives $W \leq \sqrt{m/2} + O(1)$. With $m = (c + o(1))N$ the certified quantity is at most $(1+o(1))(1 - 1/(2c))\sqrt{N}/\sqrt{2c}$, whose maximum over $c > 1/2$ is $2/(3\sqrt{3})$, by the computation in the proof of Theorem 1.1. The bound caps what the argument proves, not $\|A\|$ itself. □

Proposition 5.8 below shows that the collision law is all such an argument can say about how many residues the rounded image occupies.

Remark 5.4 (Dependence on the input set). For a fixed A, the dither may be chosen using information about that set, so the uniform bound need not apply. Take $A = \{1, \dots, N\}$, $m \geq N$ and $\theta = 1/m$ in the model (2): then $\psi(a) = a + \beta$ and $\varphi(a) = a \bmod m$, which is injective on A, so no deletion occurs at all. The same 1-separated code and the same averaging over translates give $\|A\| \geq (1+o(1))N(q+1)/m = (1+o(1))N/\sqrt{2m}$, which at $m = (1+o(1))N$ is $(1/\sqrt{2} + o(1))\sqrt{N}$, above the uniform bound. Corollary 5.3 limits the constant certified simultaneously for every A; it does not limit a dither selected for a particular set. Remark 5.14 uses the same distinction.

When the continuous bound is attained, the continuous and discrete extremal problems have the same value and the same optimizers. Martin and O'Bryant [19, Prop. 5.3] prove a related exact identity between a measure problem on $[0, 1)$ and a discrete $B^*[g]$ extremal function, and their extremal continuous sets are likewise equal-length intervals placed at a discrete Sidon-type set. Their identity is an infimum over discrete parameters whose extremal function remains unknown; here the coincidence holds at each such m, with the optimizers classified.

Corollary 5.5 (Equality in the fractional bound)**.** *Let $m > 2$ and suppose the bound of Proposition 5.2 is attained, that is, some Sidon system in $\mathbb{T}_m$ has capacity $W = \sigma$, where $\sigma^2 - \sigma + 1 = m/2$. Then the systems attaining it are, among all measurable systems, exactly the systems of σ unit cells placed at a 1-separated code, and hence, by Theorem 1.5, exactly the systems*

$$C_i = \{a + 2d_i\} + [0, 1), \qquad d_i \in D,$$

for a planar difference set $D \subset \mathbb{Z}_{m/2}$. In particular the continuous relaxation of the discrete packing problem has at such m no fractional optimizer and no integrality gap; and this occurs precisely when $m = 2(q^2 + q + 1)$ and a cyclic projective plane of order q exists, in which case $\sigma = q + 1$.

Proof. Equality in Proposition 5.2 forces equality in $W \leq s$, hence $\mu_i = 1$ for every i, so the cells are unit intervals $C_i = \{s_i\} + [0, 1)$. For such cells, $C_i + C_l$ and $C_k + C_j$ are intervals of length 2 based at $s_i + s_l$ and $s_k + s_j$; they are disjoint precisely when those base points differ by at least 2 in $\mathbb{T}_m$. Label safety is therefore exactly the condition that distinct pair-sums of $\{s_i\}$ are 2-separated, that is, that $\{s_i\}$ is a 1-separated code in the sense of Definition 1.4. The classification of equality is then Theorem 1.5 with $t = 1$. The converse is the computation $k(k-1) + 1 = q^2 + q + 1 = m/2$. □

Corollary 5.5 also gives a measure-theoretic statement on the circle. Maximizing the total length of a family of arcs with disjoint pairwise sumsets reduces, at every modulus where equality holds, to lifted cyclic projective planes. The moduli admitting equality are therefore governed by the prime power conjecture [17, 20]. We prove exact equality only; the stability question is open, and even for Sidon sets of size $\approx \sqrt{|G|}$ in an abelian group G the analogous analogous classification remains a conjecture of Eberhard and Manners [16].

Proposition 5.2 assumes no relation between m and N, so this bound is uniform in the aspect ratio.

5.1 Sources of the constant

The factor $\sqrt{2}$ comes from a clique number, by an argument independent of Theorem 1.5, and it applies to every abelian target.

For a finite abelian group G and a symmetric set $\mathcal{D} \subset G$ with $0 \in \mathcal{D}$, call $S \subset G$ *$\mathcal{D}$-separated* if the only solutions of $s_1 + s_2 - s_3 - s_4 \in \mathcal{D}$ with $s_i \in S$ are the trivial ones, and put

$$\omega(\mathcal{D}) = \max\big\{|\mathcal{D}'| : \mathcal{D}' \subset G,\ \mathcal{D}' - \mathcal{D}' \subset \mathcal{D}\big\},$$

the clique number of the Cayley graph of $\mathcal{D}$.

Lemma 5.6 (Clique bound for defect sets)**.** *Let $S \subset G$ be $\mathcal{D}$-separated with $|S| = k \geq 3$. Then*

$$\omega(\mathcal{D}) \cdot \big(k(k-1) + 1\big) \ \leq \ |G|.$$

Moreover $\omega(\mathcal{D}) \geq 2$ whenever $\mathcal{D} \neq \{0\}$, in every abelian group; and for $G = \mathbb{Z}_m^d$ with $\mathcal{D} = \{-1, 0, 1\}^d$ and $m \geq 4$ one has $\omega(\mathcal{D}) = 2^d$.

Proof. Write $\Delta = S - S$. The separation condition says exactly that Δ is a Sidon difference set and that $(\Delta - \Delta) \cap (\mathcal{D} \setminus \{0\}) = \emptyset$; hence for $\mathcal{D}'$ with $\mathcal{D}' - \mathcal{D}' \subset \mathcal{D}$ the translates $\Delta + d'$, $d' \in \mathcal{D}'$, are pairwise disjoint, and $|\Delta| = k(k-1) + 1$ gives the bound. For the second claim, $\mathcal{D}$ is symmetric, swapping the two sides of $x + y = x' + y'$ negates the defect, so any $\delta \in \mathcal{D} \setminus \{0\}$ yields $\mathcal{D}' = \{0, \delta\}$ with $\mathcal{D}' - \mathcal{D}' = \{0, \pm\delta\} \subset \mathcal{D}$. For the third, a subset of $\mathbb{Z}_m^d$ with all differences in $\{-1, 0, 1\}^d$ has at most two distinct values in each coordinate. □

Since every defect set here is symmetric, Lemma 5.6 implies a density loss of at least $\sqrt{2}$ whenever the defect set contains a nonzero element, for every abelian target. The $\sqrt{2}$ of Theorem 1.5 is therefore not a feature of cyclic groups, and Proposition 5.11 is the case $\omega = 2^d$.

The constant can be decomposed into the collision and code factors. Let a be the constant in the collision loss aN^2/m, and let x be the fraction of A deleted, so that $x = a/c$ for $m = cN$. The certificate is

$$\frac{(1-x)\sqrt{x}}{\sqrt{a(t+1)}}\,\sqrt{N},$$

and $\max_x (1-x)\sqrt{x} = 2/(3\sqrt{3})$ at $x = 1/3$.

Remark 5.7. The maximizing deletion fraction is $x = 1/3$ for every a and t, because the deletion factor is linear in $1-x$ while the code density is proportional to $\sqrt{x}$. The optimal aspect ratio is $c^* = 3a$, giving $c = 3/2$ in Theorem 1.1. For defect radius t, the corresponding upper bound is $\rho^*/\sqrt{t+1}$ with $\rho^* = 2\sqrt{6}/9 = 0.5443\ldots$, decreasing in t. At $t = 1$ the collision constant $a = \frac{1}{2}$ and the code factor $t+1 = 2$ satisfy $a(t+1) = 1$, which is why $2/(3\sqrt{3})$ appears with no prefactor.

For a dither and a modulus m, let n_r be the number of residues having exactly r preimages in A, let $\nu = \sum_{r\geq 1} n_r$ be the number of occupied residues, and for $j \geq 1$ let

$$M_j = \sum_{r\geq j} \binom{r}{j} n_r$$

be the number of j-element subsets of A lying in a common fibre, so that $M_1 = N$ and M_2 is the pair count of Lemma 3.6.

Since $\nu \leq \min(m, N)$ for any transport, the certificate displayed above is bounded by $\max_m \min(m,N)/\sqrt{(t+1)m} = \sqrt{N/(t+1)}$, attained only at $m = N$. At $t = 1$ this is $0.7071\ldots\sqrt{N}$, which is exactly the value certified by the adapted dither of Remark 5.4. At $t = 0$ the cap is $\sqrt{N}$, consistent with Erdős–Turán. The largest value that $\nu \leq \min(m,N)$ allows is $1/\sqrt{2}$, which exceeds the uniform certificate $2/(3\sqrt{3})$ by a factor $3\sqrt{6}/4 = 1.8371\ldots$. Any improvement within this argument therefore needs a uniform lower bound on the occupancy ν. Proposition 5.8 shows that the first two occupancy moments give only the existing bound from the pair count.

Proposition 5.8 (Which occupancy moments are universal)**.** *Work in the model* (2) *with* $A \subset \mathbb{Z}$, $|A| = N$, *and fix* $m \geq 3$.

(i) If $y_1, \ldots, y_J$ *satisfy* $\sum_{j\leq J} y_j \binom{r}{j} \leq 1$ *for every integer* $r \geq 1$, *then* $\nu \geq \sum_{j\leq J} y_j M_j$, *for every* A *and every dither. The alternating choice* $y_j = (-1)^{j+1}$ *is admissible exactly for* J *even, since* $\sum_{j=1}^{J} (-1)^{j+1}\binom{r}{j} = 1 - (-1)^J\binom{r-1}{J}$.

(ii) $M_1 = N$ *surely, and* $\mathbb{E}M_2 = \binom{N}{2}/m$ *for every* A.

(iii) $\mathbb{E}M_3$ *is not determined by* N *and* m. *For* $A = \{0,1,2\}$ *it equals* $1/(2m)$; *for* $A = \{0,11,29\}$ *and* $m = 40$ *it equals* $1/1160$, *against* $1/80$ *for* $\{0,1,2\}$ *at the same modulus.*

(iv) Consequently, for $m \geq N$ *the best bound of the form* (i) *using only* M_1 *and* M_2 *(the two whose expectations are determined by* N *and* m*) is the case* $J = 2$, *namely* $\mathbb{E}\nu \geq N - \binom{N}{2}/m$, *which is the estimate of Lemma 3.6; optimizing the resulting certificate over* $m = cN$ *returns* $2/(3\sqrt{3})$ *at* $c = 3/2$.

Proof. (i) A residue with $r \geq 1$ preimages contributes 1 to ν and $\sum_j y_j \binom{r}{j}$ to the right-hand side; sum over residues. The displayed identity is $\sum_{j=0}^{J} (-1)^j \binom{r}{j} = (-1)^J \binom{r-1}{J}$, and for J even it gives $1 - \binom{r-1}{J} \leq 1$ for every $r \geq 1$, while for J odd it gives $1 + \binom{r-1}{J} > 1$ as soon as $r \geq J+1$.

(ii) M_2 counts the pairs of A in a common fibre, so $\mathbb{E}M_2 = \binom{N}{2}/m$ by the collision identity of Theorem 1.3.

(iii) Let $s = m\theta$, uniform on $[0, m)$. Writing $zs = u + km$ with $u = zs \bmod m$ gives $\varphi(z) \equiv \lfloor u + \beta \rfloor \pmod m$, which vanishes exactly when $u + \beta < 1$ or $u + \beta \geq m$. Since $\varphi(0) = 0$, the three points $0, a, b$ therefore share a fibre precisely when as and bs both lie, modulo m, in the arc $[0, 1-\beta) \cup [m-\beta, m)$.

Take $(a, b) = (1, 2)$ and $m \geq 3$, and recall $s \in [0, m)$. If $s \in [0, 1-\beta)$ then $2s < 2 - 2\beta \leq m - \beta$, so $2s$ cannot lie in the upper piece and must lie in $[0, 1-\beta)$, which happens exactly for $s < (1-\beta)/2$. If $s = m - \sigma$ with $\sigma \in (0, \beta]$ then $2s \equiv m - 2\sigma \pmod m$ with $0 < 2\sigma \leq 2\beta < 2$, so $m - 2\sigma > m - 2 \geq 1 > 1 - \beta$; again the lower piece is excluded, and $m - 2\sigma \geq m - \beta$ happens exactly for $\sigma \leq \beta/2$. The s-measure is $(1-\beta)/2 + \beta/2 = 1/2$ for every β, so the probability is $1/(2m)$.

For $\{0, 11, 29\}$ at $m = 40$ the same integral, a definite integral of a piecewise linear function of s with breakpoints in $\frac{1}{11}\mathbb{Z} \cup \frac{1}{29}\mathbb{Z}$, evaluates to $1/1160$. Independent placement would give $1/m^2$ in both cases; the two values are $m/2$ and $m/29$ times that.

(iv) For y supported on $\{1, 2\}$ one maximizes $y_1 N + y_2 \binom{N}{2}/m$. Feasibility for large r forces $y_2 \leq 0$, and the objective increases in y_2, so y_2 is as large as the constraints allow. If $y_1 < \frac{1}{2}$ this means $y_2 = 0$, and then $y_1 r \leq 1$ for all r forces $y_1 \leq 0$ and a nonpositive objective. Otherwise $y_2 = 1 - 2y_1$, the value making the constraint at $r = 2$ tight; the constraint at $r = 3$ then reads $3 - 3y_1 \leq 1$, forcing $y_1 \geq \frac{2}{3}$, while $r = 1$ gives $y_1 \leq 1$. Writing $\lambda = (N-1)/m \leq 1$, the objective is $N\big(y_1(1-\lambda) + \lambda/2\big)$, nondecreasing in y_1, so $y = (1, -1)$. The optimization over c is then the one in the proof of Theorem 1.1. □

Remark 5.9 (A conditional occupancy bound). We do not assert or conjecture the following estimate. If $\mathbb{E}\nu \geq (1 - o(1))\, m(1 - e^{-N/m})$ held uniformly in A, then the proof of Theorem 1.1, with no other change, would give $\|A\| \geq (0.45125\ldots - o(1))\sqrt{N}$, the maximum of $(1 - e^{-1/c})\sqrt{c/2}$, attained at $c = 0.7959\ldots$. This remains below $1/\sqrt{2}$. Two obstacles to proving such a bound are already visible in Proposition 5.8. By (i) and (iv) any proof must use moments of order at least three, and by (iii) those are not determined by N and m; and knowing merely that every M_j exceeds its value under independent placement yields nothing about ν, since the coefficients in (i) alternate in sign. These higher occupancy moments are the information not controlled by Corollary 5.3.

Within this class of bounds, part (iv) explains why the estimate from the pair count is the strongest universal estimate available from the first two occupancy moments: M_1 and M_2 have expectations determined by N and m, whereas M_3 does not. Part (iii) shows that structured inputs can have probabilities of triple collisions far above the value under independent placement. Because the coefficients in (i) alternate in sign, that increase alone does not yield a lower bound on ν.

5.2 Boxes and higher-dimensional targets

The next two results identify limitations of rounding that tolerates a defect, and of higher-dimensional targets.

Proposition 5.10 (Box examples)**.** *Let $A = \{0, 1, \dots, n-1\}^d$, identified with a subset of $\mathbb{Z}$ by the base-$(2n-1)$ model, and let $N = n^d$. Then, as $n \to \infty$ with d fixed:*

(i) writing $Q(A)$ for the number of four-point subsets of A that support a nontrivial equal-sum relation, $Q(A)/N^{5/2} \to \infty$, so any bound of the form $\gamma \mapsto c(\gamma)\sqrt{N}$ for $Q(A) = \gamma N^{5/2}$ with $c(\gamma) \to 0$, including the hypergraph bound of [22], is vacuous;

(ii) the number $\Delta^+(A)$ of distinct positive differences of A equals $\big((2n-1)^d - 1\big)/2 = O_d(N)$, so by Theorem 6.2 keeping two points per fiber gains $O_d(1)$ points;

(iii) every *integer model of A has diameter at least $\big((2n-1)^d - 1\big)/2 \sim 2^{d-1}N$, with equality for the base-$(2n-1)$ model, so Proposition 5.12 certifies at most $(1 + o(1))2^{-(d-1)/2}\sqrt{N}$, which is below $2/(3\sqrt{3})$ once $d \geq 4$, and no change of model repairs this;*

(iv) the base-n map $\pi(x) = \sum_i x_i n^{i-1}$ is a group homomorphism $\mathbb{Z}^d \to \mathbb{Z}$, injective on A with image the interval $\{0, \dots, N-1\}$. It is a Freiman 2-homomorphism but not a model, and pushing forward through it (Remark 5.14) gives $\|A\| \geq (1 - o(1))\sqrt{N}$ for every n and every d.

So $\|A\| \geq (1 - o(1))\sqrt{N}$, by (iv). For n an odd prime and d even the same bound follows directly, the graph $\{(x, x^2) : x \in \mathbb{F}_{n^{d/2}}\}$ being a Sidon set of size $n^{d/2} = \sqrt{N}$ in $\mathbb{Z}_n^d$ that lifts to the box, since a relation in $\mathbb{Z}^d$ reduces modulo n; part (iv) needs neither hypothesis.

Proof. For (i), let $E(A)$ count the ordered quadruples of A with $x + y = x' + y'$. Then $E(A) = E(\{0, \dots, n-1\})^d \sim (\frac{2}{3}n^3)^d$ and $Q(A) \asymp E(A)$, so $Q(A)/N^{5/2} \asymp (\frac{2}{3})^d n^{d/2} \to \infty$.

Part (ii) is the count $|A - A| = (2n-1)^d$.

For (iii), the largest element of the base-$(2n-1)$ model is $(n-1)\sum_{i<d}(2n-1)^i = \big((2n-1)^d - 1\big)/2$, which is therefore its diameter and coincides with $\Delta^+(A)$; no model is shorter, because $|A - A|$ is a Freiman 2-invariant: $x - y = x' - y'$ is equivalent to the relation $x + y' = x' + y$. A subset of $\mathbb{Z}$ with $|A - A| = W$ has diameter at least $(W-1)/2$. Finally $2^{-(d-1)/2} < 2/(3\sqrt{3}) \iff 2^{d-1} > 27/4 \iff d \geq 4$.

For (iv), the map π is linear, hence preserves every additive relation, and it is injective on A with $\pi(A) = \{0, \dots, N-1\}$; it is not a model, since already at $n = 3$, $d = 2$ the distinct sums $(0,0) + (0,1)$ and $(1,0) + (2,0)$ both go to 3. Apply (5) and then (6) with m the least Singer modulus $\geq N$, so that $m = (1 + o(1))N$ and $\nu_{\pi(A)}(m) = N$. □

The factor $2^{(d-1)/2}$ in (iii) comes from requiring a bounded- diameter Freiman 2-*isomorphism*. The relevant quantity for the argument of §5.3 is the image size (§5.3): part (iv) uses the same cyclic group $\mathbb{Z}_m$ with $m = (1 + o(1))N$ and certifies $(1 - o(1))\sqrt{N}$, in every dimension.

A model whose image modulo some $m \asymp N$ does not collapse does nevertheless exist, so the obstruction in (iii) is one of diameter alone: with m the least Singer modulus $\geq N$, the linear map

$$L(x) = \sum_{i=1}^{d} \big(n^{i-1} + m(4n)^i\big)x_i$$

is a Freiman 2-isomorphism on A with $\nu_{L(A)}(m) = N$. Indeed L is linear, so only its injectivity on $A + A = \{0, \dots, 2n-2\}^d$ has to be checked: if $L(s) = L(s')$ there, then $\sum_i (s_i - s_i')n^{i-1} = -m\sum_i (s_i - s_i')(4n)^i$, whose left side has modulus less than $2N \leq 2m$ while its right side is a multiple of $4nm$; so both vanish, and the vanishing of the second forces $s = s'$ because the

digits $|s_i - s'_i| \le 2n-2$ are smaller than $2n$. Finally $L(x) \equiv \sum_i x_i n^{i-1} \pmod m$, and that runs injectively over $\{0,\dots,N-1\}$. Thus the box example separates diameter from the number of occupied residues.

One alternative rounds into $\mathbb{Z}_m^d$. The resulting bound is weaker than the bound for a scalar target.

Proposition 5.11 (Higher-dimensional targets)**.** *Let $\varphi(x) = \big(\lfloor(\langle g_i, x\rangle + o_i)/w\rfloor \bmod m\big)_{i=1}^{d}$ with independent offsets. Then for $x+y = x'+y'$ the defect lies in $\{-1,0,1\}^d$ and every value is attained. A code $S \subset \mathbb{Z}_m^d$ cancelling it must have $\Delta = S - S$ disjoint from $\Delta + e$ for every $e \in \{0,1\}^d \setminus \{0\}$, whence $2^d|\Delta| \le m^d$ and $|S| \le (m/2)^{d/2} + O(1)$. The resulting coefficient is*

$$\max_{c>1/2} \; 2^{-d/2}\,\frac{1-\frac{1}{2c}}{\sqrt{c}} \;=\; 2^{-(d-1)/2}\cdot\frac{2}{3\sqrt{3}},$$

attained at $c = 3/2$, which is strictly decreasing in d.

Proof. The defect is coordinatewise, so Theorem 1.3 applies in each coordinate independently and the offsets do not interact. The packing bound is Lemma 5.6 with $\mathcal{D} = \{-1,0,1\}^d$, for which $\{0,1\}^d$ is a clique and hence $\omega(\mathcal{D}) \ge 2^d$; the optimization is that of Theorem 1.1 with the extra factor $2^{-d/2}$. □

The defect set grows like 3^d and the packing cost like 2^d, which outweighs the increase in Sidon density from the larger target. Thus enlarging the target alone cannot improve $2/(3\sqrt{3})$; an improvement of this type would need a transport with no defect.

5.3 Occupied residues and embeddings with no defect

The defect is not intrinsic to modular embedding. If the integer model is short, rounding can be replaced by an exact morphism: reduction is a homomorphism, so no separation is required and a planar difference set of full density may be used.

Proposition 5.12. *Let A be finite, $|A| = N$, in a torsion-free abelian group, admitting an integer model (Lemma 3.1) of diameter at most KN. Then*

$$\|A\| \;\ge\; \left(\frac{1}{\sqrt{K}} - o(1)\right)\sqrt{N},$$

by an embedding with no defect and no deletion. This exceeds $2/(3\sqrt{3})$ whenever $K < 27/4$.

The statement is classical: it is the closing step of Abbott's proof [1, p. 340], where the set already lies inside $\{1,\dots,q^2+q+1\}$ and Singer's covering of that interval is applied directly, so that no reduction is performed and the modulus need only exceed the diameter; no factor of two is required. The variant we use, averaging over translates, is Lemma 6 of [25].

Proof. Translate so $A \subset [0,D]$ with $D \le KN$. Choose a prime power q with $v = q^2+q+1 = (1+o(1))D$ and $v > D$, and a Singer set $D_S \subset \mathbb{Z}_v$. Reduction π_v modulo v is injective on A because $D < v$. If $a+b = c+d$ holds in $\mathbb{Z}$ for $a,b,c,d \in A$, then $\pi_v(a)+\pi_v(b) = \pi_v(c)+\pi_v(d)$ in $\mathbb{Z}_v$, so if the four images lie in a Sidon set the pair is trivial, and injectivity lifts this back to $\{a,b\} = \{c,d\}$; the converse implication is not needed, which is why $v > D$ suffices and not $v > 2D$. Averaging over translates, some t has $|\pi_v(A) \cap (\alpha + D_S)| \ge (q+1)N/v$, and its preimage is Sidon. Finally $(q+1)N/v = (1+o(1))N/\sqrt{v} = (1+o(1))N/\sqrt{KN}$. □

The proof only requires that the image of A modulo m remain large; m need not exceed the diameter.

Definition 5.13. For a finite $A \subset \mathbb{Z}$ and $m \geq 1$, write $\nu_A(m) = \big|\{a \bmod m : a \in A\}\big|$ for the number of residues modulo m that A occupies.

Remark 5.14 (Bound in terms of $\nu_A(m)$). Two hypotheses of Proposition 5.12 can be weakened, and only one of them concerns m. Injectivity is used only to lift a trivial pair back to A, and may be replaced by passing to a transversal of the fibres; the transport is then asked only to be a Freiman 2-homomorphism, that is, only to push relations forward. In that generality,

$$\|A\| \;\geq\; \|\pi(A)\| \qquad \text{for every Freiman 2-homomorphism } \pi\colon A \to H. \tag{5}$$

Indeed, let $S \subset \pi(A)$ be Sidon in H and choose one $a_s \in A$ with $\pi(a_s) = s$ for each $s \in S$. If $a_{s_1} + a_{s_2} = a_{s_3} + a_{s_4}$, then $s_1 + s_2 = s_3 + s_4$, so $\{s_1, s_2\} = \{s_3, s_4\}$ as multisets, and π separates the chosen lifts, whence $\{a_{s_1}, a_{s_2}\} = \{a_{s_3}, a_{s_4}\}$. The degenerate quadruples need no separate treatment: $s_1 = s_2$ forces $s_3 = s_4 = s_1$ and hence $a_{s_3} = a_{s_4} = a_{s_1}$, so the lifted set contains no three-term progression either.

Taking π to be reduction modulo m and covering $\mathbb{Z}_m$ by translates of a Singer set gives the bound in terms of $\nu_A(m)$: for $A \subset \mathbb{Z}$ finite with $|A| = N$, and every prime power q with $m = q^2 + q + 1$,

$$\|A\| \;\geq\; \nu_A(m)\,\frac{q+1}{m} \;\geq\; \frac{\nu_A(m)}{\sqrt{m}}. \tag{6}$$

Indeed, fix a Singer set $D_S \subset \mathbb{Z}_m$, $|D_S| = q + 1$ (Lemma 3.2), and let $T \subset A$ meet each residue class modulo m exactly once, so $|T| = \nu_A(m)$ and reduction π_m modulo m is injective on T. Some translate has $|\pi_m(T) \cap (\alpha + D_S)| \geq |T|(q+1)/m$, and that intersection is Sidon, so (5) gives $\|A\| \geq \|T\| \geq \|\pi_m(T)\| \geq |T|(q+1)/m$. For an arbitrary modulus $m \geq 1$ one gets $\|A\| \geq (1 - o(1))\,\nu_A(m)/\sqrt{2m}$: take the largest Singer modulus v with $2v \leq m$ and represent D_S by integers in $[0, v)$, so that pairwise sums lie in $[0, 2v) \subset [0, m)$, congruence modulo m is equality, and D_S remains Sidon in $\mathbb{Z}_m$, of size $(1-o(1))\sqrt{m/2}$. Inequality (6) is finite: it carries no error term, and no relation between m, N and the diameter is involved. Since $\nu_A(m) = N$ as soon as $m > \operatorname{diam} A$, taking m to be the least Singer modulus above the diameter recovers Proposition 5.12 model by model.

Inequality (5) covers both families of transports, which are incomparable. Applying (6) to an integer model ρ and taking the supremum over models restricts (5) to the transports $\pi_m \circ \rho$, which are injective and reflect relations; a homomorphism of $\langle A \rangle$ does neither in general, while a model need not even be affine, since any bijection between two Sidon sets of equal size is a Freiman 2-isomorphism. The model family sits strictly inside: for the box of Proposition 5.10 the base-n map is a Freiman 2-homomorphism, not a model, through which (5) certifies $(1 - o(1))\sqrt{N}$ in every dimension. The box example does not separate the corresponding suprema: the model L of §5.2 attains the same value there.

Inequality (6) is not new. It is the degenerate case $\theta = 1/m$ of the construction in the proof of Lemma 2.3 of [3], where the rounding φ_θ becomes plain reduction modulo m and the passage to a transversal of the fibres is already theirs; carried through their proof of Theorem 2.2 it returns (6). Both halves are older still: the lifting step is Fact 1 of [1, p. 336], attributed there in turn to [25], and the averaging step is Lemma 6 of [25]. The argument reduces to (5): a transversal of the fibres of π needs only the forward implication. The useful conclusion is the hypothesis exposed by the inequality: a Freiman 2-homomorphism into a cyclic target whose

image does not collapse. Short diameter and injectivity are sufficient conditions, not necessary ones.

The number of occupied residues can remain large even when every model has large diameter. Recall from the proof of Proposition 5.10 that $|A-A|$ is a Freiman 2-invariant, so that every integer model of A has diameter at least $(|A-A|-1)/2$. Let $m = q^2+q+1$ be the least Singer modulus with $m \geq 2N$, so that $m = (2+o(1))N$, and put

$$A = \{\, i + mi^2 \;:\; 0 \leq i < N \,\}.$$

Then A is Sidon: $a_i + a_j = (i+j) + m(i^2+j^2)$ with $0 \leq i+j < 2N \leq m$, so $i+j$ and i^2+j^2 are read off from the sum, and together they determine $\{i,j\}$. Hence $|A-A| = N(N-1)+1$, every model of A has diameter at least $N(N-1)/2$, and Proposition 5.12 applies only with $K \geq (N-1)/2$, certifying $O(1)$ points. But $a_i \equiv i \pmod m$, so $\nu_A(m) = N$ and (6) certifies $(1-o(1))N/\sqrt{m} = (1/\sqrt{2}-o(1))\sqrt{N}$. Here A itself is Sidon, so $\|A\| = N$; the example is used only to separate the two certificates. A short model is thus sufficient for the argument with no defect, and far from necessary.

This does not resolve the general case. The bound (6) fails only for models whose image is small at every relevant modulus, namely those with $\nu_A(m) \leq \frac{2}{3\sqrt{3}}\sqrt{mN}$ for every admissible m, a condition on the chosen model, not on A. Because $\nu_A(m) \leq \min(m,N)$, it is automatic outside the window $\frac{4}{27}N < m < \frac{27}{4}N$, which contains finitely many Singer moduli; dilating a model by an integer divisible by all of them is again a model, and drives ν to 1 at each, so every A has such models. Profile collapse is therefore controlled by the arithmetic of the separations, and in particular by divisibility by the moduli in this window. Large diameter alone does not force it.

6 Limits of keeping two points per fiber

Retaining two points per fiber raises the coefficient, before the deficit term is subtracted, from $2/(3\sqrt{3})$ to $2/3$. The construction below also shows why the extra term cannot improve the constant for intervals.

Let the fibers of φ on A be $\varphi^{-1}(r) \cap A$, let U be their number and L the number of size at least two. In each fiber of size ≥ 2 designate a pair $x_F < y_F$ with label $\lambda(F) = y_F - x_F$, call x_F its base point, and in a singleton fiber call its point the base; let L_e count the fibers of label e.

Proposition 6.1 (Two points per fiber)**.** *For every dither,*

$$\|A\| \;\geq\; \frac{q+1}{m}\,(U+L) \;-\; \frac{1}{m}\sum_{e>0}\binom{L_e}{2}.$$

Proof. Fix α. Call a fiber accepted if its residue lies in S_α. Retain the base point of every accepted fiber, and for each label e realized by an accepted fiber retain the second point of exactly one such fiber. We claim the resulting T_α is Sidon. Let $a+b = c+d$ in T_α. By Theorem 1.3 and Lemma 3.4 the defect vanishes and the image multisets agree. If $\varphi(a) = \varphi(b)$ all four points lie in one fiber, which contributed at most two points $x < y$, and $2x < x+y < 2y$ forces $\{a,b\} = \{c,d\}$. Otherwise assume $\varphi(a) = \varphi(c)$, $\varphi(b) = \varphi(d)$; if $a \neq c$ then $b \neq d$, the pairs $\{a,c\}$ and $\{b,d\}$ are the designated pairs of two distinct fibers, and $a-c = d-b$ makes their labels equal, contradicting the selection rule.

Now count. With $n_{\alpha,e}$ the number of accepted fibers of label e, $|T_\alpha| = \#\{\text{accepted}\} + \#\{e : n_{\alpha,e} \geq 1\}$. By Lemma 3.5, $\sum_\alpha \#\{\text{accepted}\} = (q+1)U$ and $\sum_\alpha n_{\alpha,e} = (q+1)L_e$, while each pair of distinct fibers of a common label is jointly accepted for at most one α, so $\sum_\alpha \binom{n_{\alpha,e}}{2} \leq \binom{L_e}{2}$. Since $\mathbf{1}[n \geq 1] \geq n - \binom{n}{2}$,

$$\max_\alpha |T_\alpha| \;\geq\; \frac{q+1}{m}(U+L) - \frac{1}{m}\sum_e \binom{L_e}{2},$$

which is the claim since $\|A\| \geq \max_\alpha |T_\alpha|$. □

Theorem 6.2 (The gain from two points per fiber is capped by the difference set)**.** *With $\Delta^+(A) = \#\{d > 0 : d \in A - A\}$ as in Proposition 5.10, let λ_φ be the largest number of fibers to which pairwise distinct labels can be assigned, so that Proposition 6.1 holds with L replaced by λ_φ and no deficit. Then, in the model* (2)*,*

$$\mathbb{E}\,\lambda_\varphi \;\leq\; \frac{2\,\Delta^+(A)}{m}.$$

In particular for the interval $A = \{1, \dots, N\}$, where $\Delta^+ = N - 1$, and $m = (c + o(1))N$, one has $\mathbb{E}\,\lambda_\varphi \leq 2/c + o(1)$: keeping two points per fiber improves on the bound from one point by $O(1)$ points, and the constant $2/(3\sqrt{3})$ is not improved.

Proof. Lemma 2.3 of [3] shows that the in-fibre collision event depends only on the difference, not on the base point. We use that fact by grouping pairs according to their difference. A designated pair lies inside a fiber, so it is a collision: $\varphi(a) = \varphi(a + d)$ where $d = \lambda(F) > 0$. By the computation in the proof of Theorem 1.3, with $u = m\{d\theta\}$, such a collision forces $u \in [0, 1) \cup [m - 1, m)$; and u is uniform on $[0, m)$ because d is a nonzero integer, so this event has probability exactly $2/m$ and depends only on d, not on a. Call d *active* when it occurs. Every label is an active element of $A - A$, and distinct fibers in a matching carry distinct labels, so λ_φ is at most the number of active positive differences, whose expectation is $\sum_{d>0,\, d\in A-A} 2/m = 2\Delta^+(A)/m$. □

Theorem 6.2 explains why every bound obtained this way carries a hypothesis. The gain is proportional to $\min\{L,\, 2\Delta^+/m\}$, and since $L \asymp N^2/m$ the two agree only when $\Delta^+ \asymp N^2$, that is when A is already almost Sidon. At the other extreme, a set with $\Delta^+ = O(N)$ gains only $O(1)$ points. Intervals have this property and also realize the Erdős–Turán upper bound.

The deficit term does yield a bound conditional on $Q(A)$. But the hypergraph independence bound of Caro and Tuza [22], applied to the hypergraph whose edges are the additive quadruples and three-term progressions of A, exceeds that bound whenever $Q(A) \ll N^{5/2}$, and uses none of the results proved here.

References

[1] H. L. Abbott, *Sidon sets*, Canadian Mathematical Bulletin **33** (1990), 335–341.

[2] N. Alon and P. Erdős, *An application of graph theory to additive number theory*, European Journal of Combinatorics **6** (1985), 201–203.

[3] A. Bailleul and R. Riblet, *On the largest Sidon subset in a finite subset of* $\mathbb{R}^N$, arXiv:2605.03181 (2026).

[4] D. Carter, Z. Hunter, and K. O'Bryant, *On the diameter of finite Sidon sets*, Acta Mathematica Hungarica **175** (2025), 108–126.

[5] J. Hou and H. Zhao, *Vector-valued smoothing for finite Sidon sets*, arXiv:2607.01169 (2026).

[6] M. Redman, L. Rose, and R. Walker, *A small maximal Sidon set in* $\mathbb{Z}_2^n$, SIAM Journal on Discrete Mathematics **36** (2022), no. 3, 1861–1867; arXiv:2109.00292.

[7] I. Z. Ruzsa, *A small maximal Sidon set*, The Ramanujan Journal **2** (1998), 55–58.

[8] K. Bringmann, N. Fischer, and V. Nakos, *Sparse nonnegative convolution is equivalent to dense nonnegative convolution*, Proceedings of the 53rd Annual ACM Symposium on Theory of Computing (STOC 2021), 1711–1724; arXiv:2105.05984.

[9] C. Jin and Y. Xu, *Shaving logs via large sieve inequality: faster algorithms for sparse convolution and more*, Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC 2024); arXiv:2403.20326.

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

[11] A. M. Macbeath, *On measure of sum sets. II. The sum-theorem for the torus*, Proceedings of the Cambridge Philosophical Society **49** (1953), 40–43.

[12] M. B. Nathanson, *Sidon sets with* Δ*-separated sumsets in additive number theory*, arXiv:2608.07416 (2026).

[13] T. M. Chan and Q. He, *Reducing 3SUM to Convolution-3SUM*, Proceedings of the 3rd Symposium on Simplicity in Algorithms (SOSA 2020), SIAM, 1–7.

[14] F. R. K. Chung, J. A. Salehi, and V. K. Wei, *Optical orthogonal codes: design, analysis, and applications*, IEEE Transactions on Information Theory **35** (1989), no. 3, 595–604.

[15] C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, 2nd ed., Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2007. Chapter VI.18, *Difference Sets*, by D. Jungnickel, A. Pott and K. W. Smith; §VI.19.3, *Modular Golomb rulers*, in Chapter VI.19, *Difference Triangle Sets*, by J. B. Shearer.

[16] S. Eberhard and F. Manners, *The apparent structure of dense Sidon sets*, Electronic Journal of Combinatorics **30** (2023), no. 1, Paper No. P1.33; arXiv:2107.05744.

[17] D. M. Gordon, *The prime power conjecture is true for* $n < 2{,}000{,}000$, Electronic Journal of Combinatorics **1** (1994), Research Paper R6.

[18] M. Hall, Jr., *Cyclic projective planes*, Duke Mathematical Journal **14** (1947), 1079–1090.

[19] G. Martin and K. O'Bryant, *The symmetric subset problem in continuous Ramsey theory*, Experimental Mathematics **16** (2007), no. 2, 145–165; arXiv:math/0210041.

[20] R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canadian Journal of Mathematics **1** (1949), 88–93.

[21] M. Buratti and D. R. Stinson, *New results on modular Golomb rulers, optical orthogonal codes and related structures*, Ars Mathematica Contemporanea **20** (2021), 1–27; arXiv:2007.01908.

[22] Y. Caro and Z. Tuza, *Improved lower bounds on k-independence*, Journal of Graph Theory **15** (1991), 99–107.

[23] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, *Locality-sensitive hashing scheme based on p-stable distributions*, Proceedings of the 20th Annual Symposium on Computational Geometry (2004), 253–262.

[24] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory and some related problems*, Journal of the London Mathematical Society **16** (1941), 212–215.

[25] J. Komlós, M. Sulyok, and E. Szemerédi, *Linear problems in combinatorial number theory*, Acta Mathematica Academiae Scientiarum Hungaricae **26** (1975), 113–121.

[26] J. Riddell, *On sets of numbers containing no l terms in arithmetic progression*, Nieuw Archief voor Wiskunde (3) **17** (1969), 204–209.

[27] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society **43** (1938), 377–385.