ON A PROBLEM OF ERDŐS, BEREND, AND FREUD CONCERNING BOUNDED SUMS AND BOUNDED DIFFERENCES

BOON SUAN HO

ABSTRACT. Let $S_r(N)$ be the largest cardinality of a set $A \subseteq \{1, \dots, N\}$ for which every integer has at most r representations as $a + a'$ with $a, a' \in A$ and $a \le a'$. Let $D_r(N)$ be the corresponding maximum for sets $B \subseteq \{1, \dots, N\}$ for which every nonzero difference has at most r representations as $b - b'$ with $b, b' \in B$. We prove, for every fixed $r \ge 2$,

$$\limsup_{N\to\infty} \frac{D_r(N)}{\sqrt{N}} \le \sqrt{r} < \frac{r + \lfloor r/2 \rfloor}{\sqrt{r + 2\lfloor r/2 \rfloor}} \le \liminf_{N\to\infty} \frac{S_r(N)}{\sqrt{N}}.$$

Consequently, for fixed $r \ge 2$, if $S_r(N) \sim c_r\sqrt{N}$ and $D_r(N) \sim c_r'\sqrt{N}$, then $c_r' < c_r$. The upper bound for $D_r(N)$ is a local second-moment argument, and the lower bound for $S_r(N)$ is a Singer-set lifting construction, equivalent in this case to the $h = 2$ lower-bound construction of Cilleruelo–Ruzsa–Trujillo.

1. ORIGIN OF THE QUESTION, CONVENTIONS, AND THE EXISTENCE ISSUE

In his 1992 paper *Some of my forgotten problems in number theory*, Erdős attributes the comparison considered here to an observation made with D. Berend during a visit to Ben-Gurion University, and adds that he later independently reformulated it with R. Freud [1, pp. 39–40]. Erdős considers the maximum size $k^{(r)}(n)$ of a set

$$1 \le a_1 < \cdots < a_k \le n$$

for which the equation $m = a_i + a_j$ has at most r solutions, and the analogous maximum $\ell^{(r)}(n)$ for sets

$$b_1 < \cdots < b_\ell < n$$

for which the equation $m = b_i - b_j$ has at most r solutions. Erdős then writes these maxima in the asymptotic form

$$\max k^{(r)}(n) = (c_r + o(1))\sqrt{n}, \qquad \max \ell^{(r)}(n) = (c_r' + o(1))\sqrt{n},$$

and states the expectation that, for $r > 1$, the two constants should be unequal, in fact with $c_r' < c_r$ [1, pp. 39–40]. He noted that $c_1 = c_1' = 1$. In the surrounding discussion he also points to a one-exception variant for differences as evidence that the sum and difference conditions are genuinely different, saying that it "seems to give hope" for the inequality $c_r' < c_r$ [1, p. 40]. Bloom's website lists the same comparison as Erdős Problem #863 [2].

Erdős writes the constants through the displayed asymptotic formulae; the comparison question is therefore about the relative sizes of those constants *if* the two constants exist.

The result below proves the stronger limsup/liminf separation

$$\limsup_{N\to\infty} \frac{D_r(N)}{\sqrt{N}} < \liminf_{N\to\infty} \frac{S_r(N)}{\sqrt{N}}$$

for every $r \geq 2$. Thus it settles the comparison part of Erdős's formulation without proving or needing the existence of either individual limiting constant.

There are two standard conventions to make explicit. First, "solutions" of $m = a_i + a_j$ are counted in the Sidon sense, namely with $i \leq j$, or equivalently as unordered representations. This is the convention already forced by the preceding definition of a Sidon sequence in Erdős's paper: otherwise the equality $a_i + a_j = a_j + a_i$ would make the case $r = 1$ meaningless for sets of size greater than one. Second, in the difference problem the represented integer m is nonzero. If $m = 0$ were included, the $|B|$ identities $b_i - b_i = 0$ would already force $|B| \leq r$, so no $\sqrt{N}$-order maximum could occur. Also, we replace Erdős's upper bound $b_\ell < n$ with $b_\ell \leq N$; doing so does not change the constants c_r and c'_r.

We shall write N for the ambient interval length and reserve m, t for represented integers. For a finite set $A \subseteq \mathbb{Z}$, define the unordered sum representation function

$$R_A^+(m) \coloneqq \#\big\{(a, a') \in A^2 : a \leq a',\ a + a' = m\big\}.$$

Thus A is a finite $B_2[r]$ set, in the convention relevant here, if $R_A^+(m) \leq r$ for every integer m. Put

$$S_r(N) \coloneqq \max\big\{|A| : A \subseteq \{1, \dots, N\},\ R_A^+(m) \leq r \text{ for all } m \in \mathbb{Z}\big\}.$$

For $B \subseteq \mathbb{Z}$ and $d \geq 1$, write

$$\Delta_B(d) \coloneqq \#\big\{(b, b') \in B^2 : b - b' = d\big\},$$

and define

$$D_r(N) \coloneqq \max\big\{|B| : B \subseteq \{1, \dots, N\},\ \Delta_B(d) \leq r \text{ for all } 1 \leq d \leq N - 1\big\}.$$

Equivalently, every nonzero difference has at most r ordered representations as $b - b'$.

2. Statement of the separation

The main result is the following limsup/liminf separation.

Theorem 1. *For every fixed integer $r \geq 2$, putting $s = \lfloor r/2 \rfloor$, one has*

$$\limsup_{N\to\infty} \frac{D_r(N)}{\sqrt{N}} \leq \sqrt{r} < \frac{r+s}{\sqrt{r+2s}} \leq \liminf_{N\to\infty} \frac{S_r(N)}{\sqrt{N}}.$$

Corollary 1. *Assume that, for a fixed $r \geq 2$, the asymptotic formulae written in Erdős's formulation are valid; that is,*

$$S_r(N) \sim c_r\sqrt{N}, \qquad D_r(N) \sim c'_r\sqrt{N} \qquad (N \to \infty).$$

Then $c'_r < c_r$.

3. The bounded-difference upper bound

Lemma 1. *For every fixed $r \geq 1$,*

$$D_r(N) \leq (\sqrt{r} + o(1))\sqrt{N}.$$

Proof. Suppose $B \subseteq \{1, \dots, N\}$ satisfies $\Delta_B(d) \leq r$ for all $1 \leq d \leq N-1$, and put $M = |B|$. The global difference count gives

$$\binom{M}{2} = \sum_{d=1}^{N-1} \Delta_B(d) \leq r(N-1),$$

so $M = O_r(\sqrt{N})$.

Fix an integer H with $1 \leq H \leq N$. For

$$x = 1-H,\ 2-H, \dots, N-1,$$

let

$$I_x = \{x+1, x+2, \dots, x+H\}, \qquad w_x = |B \cap I_x|.$$

Each element of B lies in exactly H of these intervals, and there are $N+H-1$ intervals. Hence

$$\sum_x w_x = MH,$$

and Cauchy–Schwarz gives

$$\sum_x w_x(w_x - 1) = \sum_x w_x^2 - \sum_x w_x \geq \frac{M^2H^2}{N+H-1} - MH. \tag{1}$$

The same sum counts ordered pairs of distinct elements of B lying in a common interval. A pair at positive distance d lies in exactly $H-d$ of the intervals if $1 \leq d \leq H-1$, and in none if $d \geq H$. Therefore

$$\sum_x w_x(w_x-1) = 2\sum_{d=1}^{H-1}(H-d)\Delta_B(d) \leq 2r\sum_{d=1}^{H-1}(H-d) = rH(H-1). \tag{2}$$

Combining (1) and (2) yields

$$\frac{M^2H^2}{N+H-1} - MH \leq rH(H-1),$$

and hence

$$M^2 \leq r\left(1 - \frac{1}{H}\right)(N+H-1) + M\frac{N+H-1}{H} \leq r(N+H-1) + M\frac{N+H-1}{H}. \tag{3}$$

Take $H = \lfloor N^{2/3} \rfloor$. Since $M = O_r(\sqrt{N})$, the second term on the right of (3) is $o(N)$, while $H = o(N)$. Thus

$$M^2 \leq rN + o(N),$$

so $M \leq (\sqrt{r} + o(1))\sqrt{N}$. Taking the maximum over B proves the lemma. □

4. The bounded-sum lower bound

We next give a self-contained construction of large $B_2[r]$ sets. The construction uses Singer's cyclic difference sets. Namely, for every prime power q, putting

$$Q = q^2 + q + 1,$$

there is a set

$$C \subseteq \mathbb{Z}/Q\mathbb{Z}, \qquad |C| = q + 1,$$

such that every nonzero residue modulo Q has exactly one ordered representation as $c - c'$ with $c, c' \in C$ [4]. Such a set is also a cyclic Sidon set for sums: every residue modulo Q has at most one unordered representation as $c + c'$ with $c, c' \in C$. Indeed, if

$$c_1 + c_2 \equiv c_3 + c_4 \pmod{Q},$$

and $c_1 \neq c_3$, then

$$c_1 - c_3 \equiv c_4 - c_2 \pmod{Q};$$

uniqueness of the nonzero difference representation forces $(c_1, c_3) = (c_4, c_2)$, so the two unordered pairs are the same. If $c_1 = c_3$, then also $c_2 = c_4$.

We first isolate the finite pattern used in the lifting. The superscript "ord" emphasizes that the pattern is controlled by ordered layer-pair counts, in contrast with the unordered sum representation function R_A^+ above.

Lemma 2. *Let $r \geq 2$ and $s = \lfloor r/2 \rfloor$. Put*

$$P = P_r \coloneqq \{0, 1, \ldots, r-1\} \cup \{r+s, r+s+1, \ldots, r+2s-1\}.$$

Then $|P| = r + s$, $P \subseteq \{0, 1, \ldots, r+2s-1\}$, and

$$R_P^{\mathrm{ord}}(t) \coloneqq \#\{(u, v) \in P^2 : u + v = t\} \leq r$$

for every integer t.

Proof. Write

$$I = \{0, 1, \ldots, r-1\}, \qquad J = \{r+s, r+s+1, \ldots, r+2s-1\},$$

so $P = I \cup J$. The supports of $I + I$, of the cross-sums $I + J$ and $J + I$, and of $J + J$ are respectively

$$[0, 2r-2], \qquad [r+s, 2r+2s-2], \qquad [2r+2s, 2r+4s-2].$$

Thus $J + J$ is disjoint from the other two regions. Away from the possible overlap of $I + I$ with the cross-sums, the multiplicity is at most r from $I + I$, at most $s \leq r$ from $J + J$, and at most $2s \leq r$ from the two cross-sum directions together.

It remains only to check the overlap of $I + I$ with the cross-sums. If this overlap is nonempty, any relevant sum has the form

$$t = r + s + u, \qquad 0 \leq u \leq r - s - 2.$$

For this t, the contribution from $I + I$ is $r - s - 1 - u$. The contribution from $I + J$ and $J + I$ together is

$$2\min(u + 1, s),$$

since a pair in $I+J$ is the same as a solution of $x+j=u$ with $0\le x\le r-1$ and $0\le j\le s-1$. Therefore

$$R_P^{\mathrm{ord}}(t)=r-s-1-u+2\min(u+1,s)\le r-s-1-u+(u+1+s)=r.$$

This proves $R_P^{\mathrm{ord}}(t)\le r$ for all t. □

Lemma 3. *Let $r\ge 2$, $s=\lfloor r/2\rfloor$, and $K=r+2s$. If q is a prime power and $Q=q^2+q+1$, then*

$$S_r(KQ)\ge (r+s)(q+1).$$

Proof. Let $C\subseteq \mathbb{Z}/Q\mathbb{Z}$ be a Singer cyclic Sidon set of size $q+1$, and choose representatives $C\subseteq\{0,1,\dots,Q-1\}$. With $P=P_r$ as in Lemma 2, define

$$A=\{uQ+c+1 : u\in P,\ c\in C\}.$$

Since $P\subseteq\{0,1,\dots,K-1\}$, we have $A\subseteq\{1,\dots,KQ\}$, and

$$|A|=|P||C|=(r+s)(q+1).$$

It remains to show that A is a $B_2[r]$ set.

Fix an integer m. If m has a representation

$$m=(uQ+c+1)+(vQ+d+1),\qquad u,v\in P,\quad c,d\in C,$$

then reducing modulo Q gives

$$c+d\equiv m-2 \pmod{Q}.$$

Since C is cyclic Sidon, this congruence fixes the unordered residue pair $\{c,d\}$ whenever a representation exists. Once $\{c,d\}$ is fixed, the ordinary integer $c+d$ is also fixed, and hence every representation has the same layer sum

$$u+v=T:=\frac{m-2-c-d}{Q}.$$

If $c\ne d$, choose one ordering of the fixed pair and record the layer of the summand with residue c first and the layer of the summand with residue d second. This injects the unordered representations of m by elements of A into the ordered pairs $(u,v)\in P^2$ with $u+v=T$. If $c=d$, the unordered layer pairs are again no more numerous than the ordered layer pairs with sum T. Therefore

$$R_A^{+}(m)\le R_P^{\mathrm{ord}}(T)\le r$$

by Lemma 2. Thus A is a $B_2[r]$ set, and the claimed lower bound follows. □

Lemma 4. *For every fixed $r\ge 2$, with $s=\lfloor r/2\rfloor$,*

$$\liminf_{N\to\infty}\frac{S_r(N)}{\sqrt{N}}\ge\frac{r+s}{\sqrt{r+2s}}.$$

Proof. Let $K=r+2s$ and $L=r+s$. By Lemma 3, for every prime q,

$$S_r\big(K(q^2+q+1)\big)\ge L(q+1).$$

Now let

$$X=\sqrt{N/K}.$$

By the prime number theorem, for all sufficiently large N there is a prime $q \le X-1$ with $q = (1-o(1))X$. Then $q^2+q+1 \le X^2$, so

$$K(q^2+q+1) \le KX^2 = N.$$

By monotonicity of $S_r(N)$,

$$S_r(N) \ge S_r\big(K(q^2+q+1)\big) \ge L(q+1) = \left(\frac{L}{\sqrt{K}} + o(1)\right)\sqrt{N}.$$

This proves the lemma. □

5. Proof of the theorem

Lemma 1 gives

$$\limsup_{N\to\infty} \frac{D_r(N)}{\sqrt{N}} \le \sqrt{r}.$$

Lemma 4 gives

$$\liminf_{N\to\infty} \frac{S_r(N)}{\sqrt{N}} \ge \frac{r+s}{\sqrt{r+2s}}, \qquad s = \lfloor r/2 \rfloor .$$

Finally, since $r \ge 2$ implies $s \ge 1$,

$$\left(\frac{r+s}{\sqrt{r+2s}}\right)^2 - r = \frac{(r+s)^2 - r(r+2s)}{r+2s} = \frac{s^2}{r+2s} > 0.$$

Therefore

$$\sqrt{r} < \frac{r+s}{\sqrt{r+2s}},$$

and Theorem 1 follows. Corollary 1 follows immediately from Theorem 1 if the two asymptotic constants exist.

Remark 1. *The proof gives the separation needed for the comparison in Erdős's original question, as stated through the constants c_r and c_r' on pages 39–40 of [1]; it does not assert the existence of either limiting constant. The lower bound for $S_r(N)$ is a special case of the finite $B_h[g]$ lower-bound construction of Cilleruelo, Ruzsa, and Trujillo [3], while the elementary argument above is included to make the comparison self-contained.*

References

[1] P. Erdős, *Some of my forgotten problems in number theory*, Hardy-Ramanujan Journal **15** (1992), 34–50, doi:10.46298/hrj.1992.125.

[2] T. F. Bloom, *Erdős Problem #863*, https://www.erdosproblems.com/863, accessed April 22, 2026.

[3] J. Cilleruelo, I. Z. Ruzsa, and C. Trujillo, *Upper and lower bounds for finite $B_h[g]$ sequences*, Journal of Number Theory **97** (2002), no. 1, 26–34, doi:10.1006/jnth.2001.2767.

[4] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society **43** (1938), no. 3, 377–385.