DOI: 10.3842/umzh.v76i8.7858

UDC 519.1

Kevin O'Bryant[1] (City University of New York, The Graduate Center and the College of Staten Island)

ON THE SIZE OF FINITE SIDON SETS

ПРО РОЗМІР СКІНЧЕННИХ МНОЖИН СІДОНА

A Sidon set (also called a Golomb ruler) is a B_2 sequence and a 1-thin set is a set of integers containing no nontrivial solutions to the equation $a+b=c+d$. We improve the lower bound for the diameter of a Sidon set with k elements, namely, if k is sufficiently large and $\mathcal{A}$ is a Sidon set with k elements, then $\operatorname{diam}(\mathcal{A}) \geq k^2 - 1.99405k^{3/2}$. Alternatively, if n is sufficiently large, then the cardinality of the largest subset of $\{1,2,\dots,n\}$, which is a Sidon set, does not exceed $n^{1/2} + 0.99703n^{1/4}$.

Множина Сідона (що також називається лінійкою Голомба) — це послідовність B_2, а 1-тонка множина — це множина цілих чисел, що не містить нетривіальних розв'язків рівняння $a+b=c+d$. Ми покращуємо нижню межу для діаметра множини Сідона з k елементів, тобто якщо k є достатньо великим, а $\mathcal{A}$ є множиною Сідона з k елементами, то $\operatorname{diam}(\mathcal{A}) \geq k^2 - 1,99405k^{3/2}$. Навпаки, якщо n достатньо велике, то потужність найбільшої підмножини $\{1,2,\dots,n\}$, що є множиною Сідона, не перевищує $n^{1/2} + 0.99703n^{1/4}$.

1. Introduction. A Sidon set [10] is a set $\mathcal{A}$ of integers with no solutions to $a_1+a_2=a_3+a_4$, $a_i \in \mathcal{A}$, aside from the trivial $\{a_1,a_2\}=\{a_3,a_4\}$. Equivalently, $\mathcal{A}$ is a Sidon set if the coefficients of $\left(\sum_{a\in\mathcal{A}} z^a\right)^2$ are bounded by 2. More usefully, $\mathcal{A}$ is a Sidon set if and only if there are no solutions to $a_1-a_2=a_3-a_4$ with $a_1 \neq a_2$. We refer our readers to [8] for a survey of Sidon sets and an extensive bibliography. Sidon sets are also known as B_2 sets, Golomb rulers, and 1-thin sets.

Throughout this work, $\mathcal{A}=\{a_1<a_2<\ldots<a_k\}$ is a finite Sidon set of integers. We seek a lower bound on the diameter $\operatorname{diam}(\mathcal{A}) := a_k - a_1$ in terms of the cardinality $|\mathcal{A}|=k$. For a given k, the minimum possible value of $\operatorname{diam}(\mathcal{A})$ is denoted s_k. Let $R(n)$ be the maximum value of k with $s_k \leq n-1$, i.e., the maximum possible size of a Sidon set contained in $\{1,2,\dots,n\}$. Clearly, lower bounds on $\operatorname{diam}(\mathcal{A})$ are equivalent to upper bounds on $R(n)$.

In 1938, Singer [11] constructed a Sidon set with $q+1$ elements and diameter at most q^2+q+1, where q is any prime power, whence $s_k \leq k^2$ for infinitely many k. Alternatively, $R(n) > \sqrt{n}$ for infinitely many n. Using results on the distribution of primes (assuming RH), this construction gives $s_k \leq k^2 + k^{3/2+\epsilon}$, $R(n) \geq \sqrt{n} - n^{1/4+\epsilon}$ for any $\epsilon > 0$ and sufficiently large k, n.

In 1941, Erdős and Turán [6] (hereafter referred to as ET) used a "windowing" argument to derive the inequality (valid for any positive integers n, T)

$$n-1 \geq \frac{R(n)^2 T}{T+R(n)-1} - T, \tag{1}$$

and from this inequality find that $R(n) = n^{1/2} + O(n^{1/4})$, although a more careful analysis [3] gives $R(n) < n^{1/2} + n^{1/4} + \frac{1}{2}$. In 1969, Lindström [7] gave another proof, deriving a different inequality which gives the same bound on $R(n)$. In Section 2, we give an elementary form of the ET argument and a "proof-from-the-book" analysis of (1), giving the sharpest expicit bound on s_k in the literature, improving on [2]. This theorem implies, but is not implied by, $R(n) < n^{1/2} + n^{1/4} + \frac{1}{2}$.

[1] E-mail: kevin.obryant@csi.cuny.edu.

Theorem 1. *For* $k \geq 1,\ s_k \geq k^2 - 2k^{3/2} + k + \sqrt{k} - 1.$

In light of the results cited above, the main term in $\mathrm{diam}(\mathcal{A})$ is k^2, and the secondary term is between $k^{3/2+\epsilon}$ and $-2k^{3/2}$. Recently, Balogh, Füredi, and Roy [1] (hereafter referred to as BFR) gave the first improvement to the lower bound on s_k since 1941, improving $-2k^{3/2}$ to $-1.996k^{3/2}$. A bird's eye view of their argument is this: the ET argument uses two inequalities, and the Lindström argument uses two inequalities. By playing one of the inequalities from the ET argument against one of the inequalities from the Lindström argument, they were able to do better. A striking aspect of their work was the necessity of running both arguments simultaneously.

In this paper, we further improve the secondary term to $-1.99405k^{3/2}$. The numerical improvement is slight, but the value of the current paper is in demonstrating that it is possible to improve the secondary term $-2k^{3/2}$ by playing the two inequalities of the ET argument against each other and not using the Lindström argument at all. Thus, our method is logically simpler than the BFR method, but to get a numerical improvement, we have to make it computationally more involved.

Theorem 2. *Suppose that* $\mathcal{A}$ *is a finite Sidon set of integers. If* k *is sufficiently large, then* $\mathrm{diam}(\mathcal{A}) \geq k^2 - 1.99405k^{3/2}$. *Also, if* n *is sufficiently large, then* $R(n) < n^{1/2} + 0.99703n^{1/4}$.

The "sufficiently large" phrase is not fundamentally needed. We expect further numerical improvements will appear in the next few years and it is premature to overly optimize at this stage.

We define b_k by $s_k = k^2 - b_k k^{3/2}$, and $b_\infty = \limsup_{k\to\infty} b_k$. The Erdős – Turán work proves that $b_k < 2$, and the Balogh – Füredi – Roy work proves that $b_\infty \leq 1.996$. In this paper, we prove that $b_\infty \leq 1.99405$. Explicit values of b_k are known for $1 \leq k \leq 28$ thanks to the Distributed.net "Optimal Golomb Ruler" project [4]. Lower bounds on b_k have been constructed by Dogon – Rokicki [5], and are shown in Fig. 1.

2. The Erdős – Turán Sidon set equation. We first give an account of the inequality (1) that Erdős – Turán derived and used to prove $R(n) < n^{1/2} + O(n^{1/4})$ with a sharper derivation of the resulting bound. In fact, the bound given here is sharper than any explicit bound explicitly given in the literature of which this author is aware.

Theorem 3. *For* $k \geq 1$, *we have* $s_k \geq k^2 - 2k^{3/2} + k + \sqrt{k} - 1$. *For* $n \geq 1$, *we get* $R(n) < n^{1/2} + n^{1/4} + \dfrac{1}{2}$.

Proof. Let $\mathcal{A} = \{0 = a_1 < a_2 < \ldots < a_k\}$ be a k-element Sidon set with minimum possible diameter. Let A_j be the size of the intersection of $\mathcal{A}$ with $[j - T, j)$.

First, each of the k elements of $\mathcal{A}$ contributes to exactly T of the A_j, so that

$$\sum_{j=1}^{a_k+T} A_j = kT. \tag{2}$$

By expanding $\left(A_j - \dfrac{kT}{a_k + T}\right)^2$ and using (2), straightforward algebra now confirms that

$$\sum_{j=1}^{a_k+T} A_j^2 = \frac{k^2T^2}{a_k+T} + \sum_{j=1}^{a_k+T}\left(A_j - \frac{kT}{a_k+T}\right)^2 \geq \frac{k^2T^2}{a_k+T}. \tag{3}$$

We can combine (2) and (3) to get

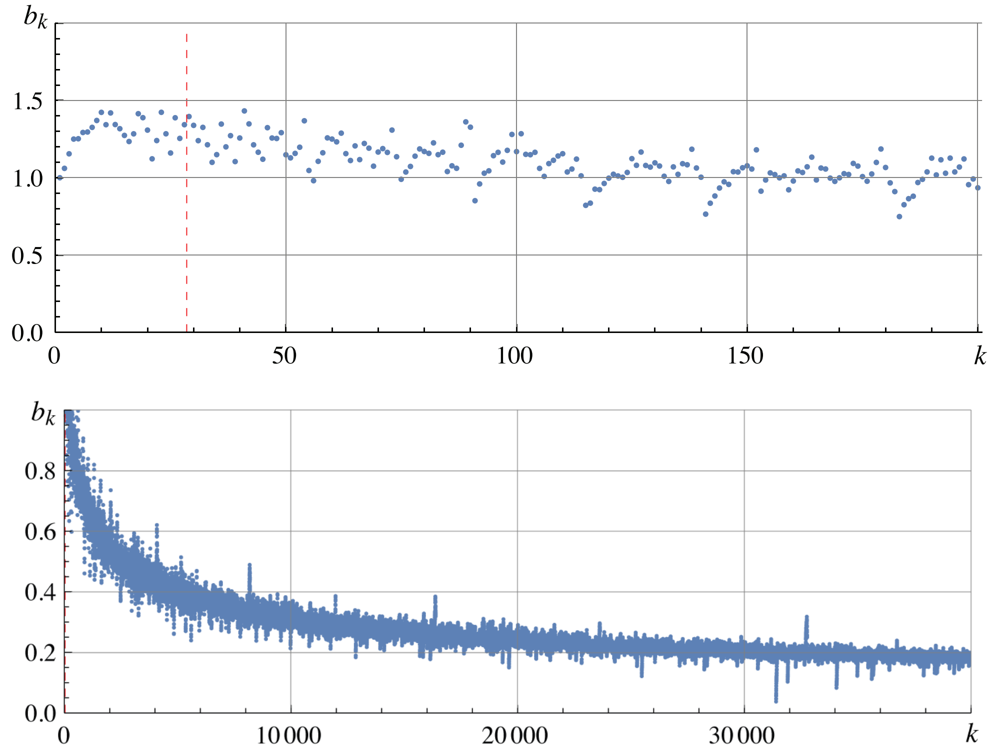


Fig. 1. Lower bound on b_k for $1 \leq k \leq 40\,000$, as computed by Shearer [9] and Dogon–Rokicki [5]. The vertical red line separates the known exact values [4] from the mere lower bounds. There are unexplained spikes up at powers of 2, and spikes down at long stretches of composites, such as $[31398, 31468]$.

$$\sum_{j=1}^{a_k+T} \binom{A_j}{2} \geq \frac{1}{2} \frac{k^2T^2}{a_k+T} - \frac{1}{2}kT,$$

and this raises a combinatorial interpretation. The binomial coefficient $\binom{A_j}{2}$ is counting the number of pairs of elements of $\mathcal{A}$ in the interval $[j-T, j)$. Each pair (a_y, a_x) of elements of $\mathcal{A}$ with $a_x > a_y$ contributes 1 to $\binom{A_j}{2}$ for $j \in [a_x+1, a_y+T]$ if $r = a_x - a_y \leq T-1$, and contributes nothing to any $\binom{A_j}{2}$ if $r \geq T$. By the Sidon property, if $r \in \mathcal{A} - \mathcal{A}$, then there is a unique pair (a_y, a_x) with $r = a_x - a_y$. Ergo, as $\big|[a_x+1, a_y+T]\big| = T - r$, we have

$$\sum_{j=1}^{a_k+T} \binom{A_j}{2} = \sum_{\substack{r=1 \\ r \in \mathcal{A}-\mathcal{A}}}^{T-1} (T-r) = \frac{T(T-1)}{2} - \sum_{\substack{r=1 \\ r \notin \mathcal{A}-\mathcal{A}}}^{T-1} (T-r) \leq \frac{T(T-1)}{2}. \tag{4}$$

Comparing the upper and lower bounds on $\sum \binom{A_j}{2}$, we obtain

$$\frac{1}{2} \frac{k^2T^2}{a_k+T} - \frac{kT}{2} \geq \frac{T(T-1)}{2}.$$

Solving for a_k gives the Erdős – Turán Sidon set inequality: for positive integers T,

$$a_k \geq \frac{k^2 T}{T+k-1} - T.$$

Set $T = k^{3/2} - k + \epsilon$, with $\epsilon \in (0,1]$ chosen to make T a positive integer. We have the factorization

$$\left(\frac{k^2 T}{T+k-1} - T\right) - \left(k^2 - 2k^{3/2} + k + \sqrt{k} - 1\right) = \frac{(1-\epsilon)\left(\sqrt{k}+\epsilon-1\right)}{T+k-1},$$

which is clearly nonnegative for $k \geq 1$. Therefore, $s_k = a_k \geq k^2 - 2k^{3/2} + k + \sqrt{k} - 1$, as claimed.

The theorem is proved.

We can convert this to a bound on $k = R(n)$. The expression $k^2 - 2k^{3/2} + k + \sqrt{k} - 1$ is a polynomial in $\sqrt{k}$, and one easily sees that its derivative (with respect to $\sqrt{k}$) is positive for $k \geq 0$. Thus, the inequality $n - 1 \geq k^2 - 2k^{3/2} + k + \sqrt{k} - 1$ implies an upper bound on k. To prove that $R(n) < n^{1/2} + n^{1/4} + \frac{1}{2}$, for example, one only needs to derive a contradiction from

$$\begin{aligned} n - 1 \geq {} & \left(n^{1/2} + n^{1/4} + \frac{1}{2}\right)^2 - 2\left(n^{1/2} + n^{1/4} + \frac{1}{2}\right)^{3/2} \\ & + \left(n^{1/2} + n^{1/4} + \frac{1}{2}\right) + \sqrt{n^{1/2} + n^{1/4} + \frac{1}{2}} - 1. \end{aligned}$$

While tedious, this purported inequality simplifies algebraically and can be proved impossible by hand.

This proof contains two innovations and a useful consequence. The first innovation is on (3), where we used algebra instead of Cauchy's inequality. The algebra of course constitutes a proof of Cauchy's inequality, but the crux of this article rests on this nontrivial change. The second innovation is the discovery that this bound on s_k produces a pleasantly useful factorization, allowing us to also replace asymptotic analysis entirely with simple algebra.

The "useful consequence" is made possible by the first innovation. We can use the equalities in (3) and (4) instead of the inequalities, and we arrive at the following theorem, which drives the rest of this work.

Theorem 4 (The Erdős – Turán Sidon set equality)**.** *Let $\mathcal{A}$ be a finite Sidon set of integers and T be a positive integer. Then*

$$\operatorname{diam}(\mathcal{A}) = \frac{|\mathcal{A}|^2 T^2}{T(T + |\mathcal{A}| - 1) - (2S(\mathcal{A},T) + V(\mathcal{A},T))} - T,$$

where $A_i := |\mathcal{A} \cap [i-T, i)|$,

$$S(\mathcal{A},T) := \sum_{\substack{r=1 \\ r \notin \mathcal{A}-\mathcal{A}}}^{T-1} (T - r) \qquad \textit{and} \qquad V(\mathcal{A},T) := \sum_{i=\min\mathcal{A}+1}^{T+\max\mathcal{A}} \left(A_i - \frac{kT}{T+\max\mathcal{A}}\right)^2.$$

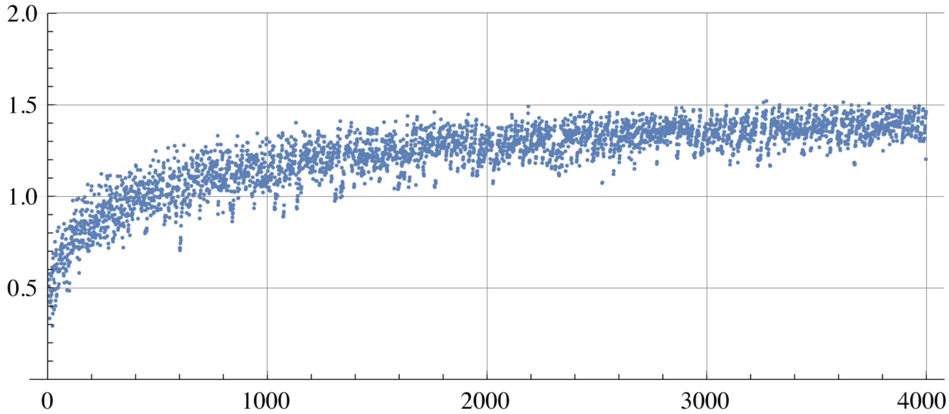


Fig. 2. $V(\mathcal{A}, k^{3/2})/k^{5/2}$ for the Sidon sets $\mathcal{A}$ in the Dogon – Rokicki dataset $(28 \le k < 4000)$.

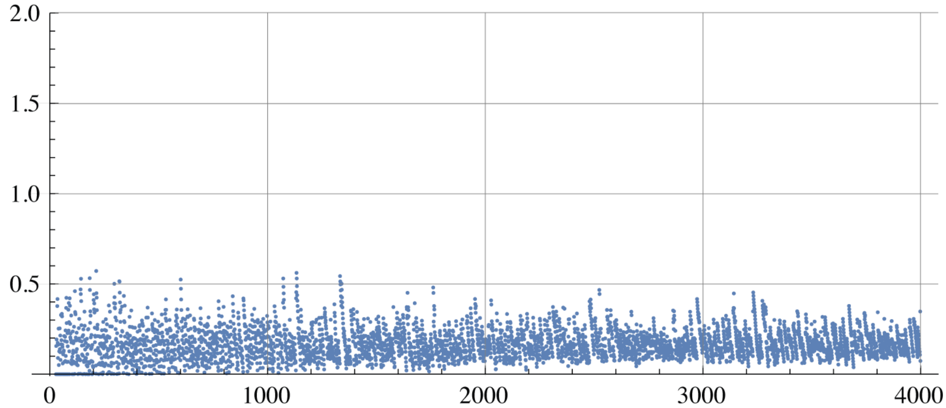


Fig. 3. $2S(\mathcal{A}, k^{3/2})/k^{5/2}$ for the Sidon sets $\mathcal{A}$ in the Dogon – Rokicki dataset $(28 \le k < 4000)$.

We find it philosophically interesting that Theorem 4 gives an *equality*. Given $|\mathcal{A}|$, any lower bound on $\operatorname{diam}(\mathcal{A})$ is equivalent to a lower bound on $2S(\mathcal{A}, T) + V(\mathcal{A}, T)$, and vice versa. Know any three of $|\mathcal{A}|, \operatorname{diam}(\mathcal{A}), V(\mathcal{A}, T), S(\mathcal{A}, T)$ for a Sidon set, and the fourth is uniquely determined.

For $i \le T$, one has $A_i \le R(i)$, and this gives a "trivial" lower bound on $V(\mathcal{A}, T)$. This allows Theorem 4 to improve the inequality $R(n) < n^{1/2} + n^{1/4} + \dfrac{1}{2}$ explicitly by $O(1)$. We mention this only because the number $1/2$ has previously been called the limit of what can be accomplished with the ET style argument.

2.1. Exploring the Erdős – Turán Sidon set equation. This subsection contains no rigorous logic, but explores the dataset of Dogon – Rokicki [5] to motivate the rest of this paper, and perhaps also suggest avenues for further progress.

Asymptotic analysis gives that if $2S(\mathcal{A}, T) + V(\mathcal{A}, T) \ge \nu k T$ (where $\nu \in (0, 1)$ is fixed and $T = \tau k^{3/2}$ is allowed to vary), then Theorem 4 yields

$$\operatorname{diam}(\mathcal{A}) \ge k^2 - 2\sqrt{1-\nu}\, k^{3/2} + O(k).$$

In particular, we need to find a bound on $2S + V$ that is $\Omega(kT)$ to impact the $k^{3/2}$ coefficient. In Fig. 2, we show $V(\mathcal{A}, k^{3/2})/k^{5/2}$ for $k < 4000$.

In contrast to $V(\mathcal{A}, T)$, which seems to be consistently more than kT in the Dogon – Rokicki dataset, the contribution from $S(\mathcal{A}, T)$ is small and irregular (see Fig. 3). The nearly vertical patterns

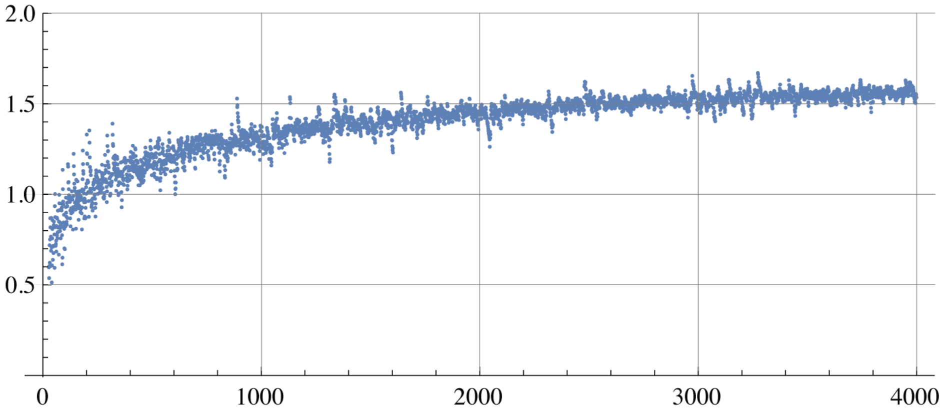


Fig. 4. $(V(\mathcal{A}, k^{3/2}) + 2S(\mathcal{A}, k^{3/2})/k^{5/2}$ for the Sidon sets $\mathcal{A}$ in the Dogon – Rokicki dataset ($28 \leq k < 4000$). Notice that this graph appears smoother than those in Figs. 2 and 3, showing the negative correlation.

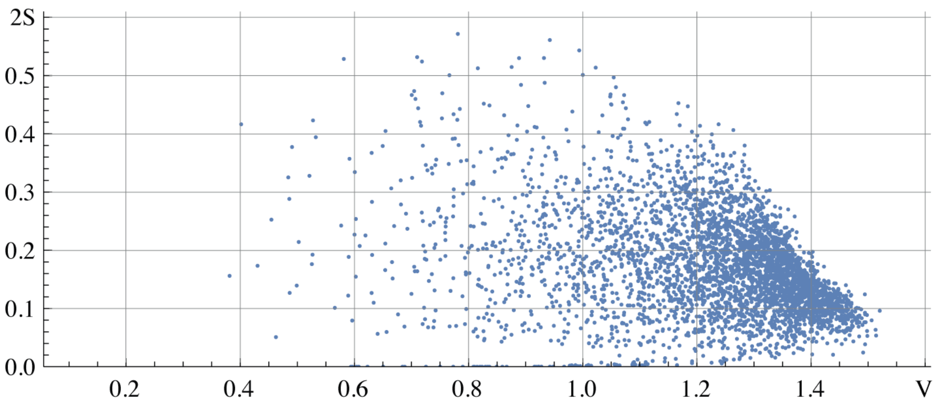


Fig. 5. The points $(V(\mathcal{A}, k^{3/2}), 2S(\mathcal{A}, k^{3/2})/k^{5/2}$ for the Sidon sets $\mathcal{A}$ in the Dogon – Rokicki dataset ($28 \leq k < 4000$). Notice that when V is particularly large, $2S$ is particularly small.

in the data points in Figs. 2 and 3 are not visual artifacts, but possibly arise from many of the sets with close k having small symmetric difference, and so similar values of V, S.

There is a negative correlation between $V(\mathcal{A}, T)$ and $S(\mathcal{A}, T)$, as can be seen in Figs. 4 and 5.

From these images, it seems apparent that one should focus more on V than S. In Fig. 6 we show four plots of $A_i := |\mathcal{A} \cap [i - k^{3/2}, i)|$, with the average value as a red dashed horizontal line, and $i = T, i = a_k$ as vertical black lines. The four, which appear to be typical, show that A_i is fairly smooth between T and a_k. In fact, about half of $V(\mathcal{A}, T)$ arises from $i \leq T$ and $i \geq a_k$. Figure 7 shows the proportion of V that arises from the edge values of i.

3. The BFR gambit. In [1], a small variance (which arose by way of an inequality from coding theory, and a rephrasing of the ET argument in terms of degree sequences of hypergraphs) was used to imply a lumpiness in the difference set. This lumpiness was then used to supercharge Lindström's proof, yielding

$$R(n) < n^{1/2} + 0.998 n^{1/4} \quad \text{for sufficiently large } n.$$

It is, as the proven value was rounded up to 0.998, equivalent to

$$s_k \geq k^2 - 1.996 k^{3/2} \quad \text{for sufficiently large } k.$$

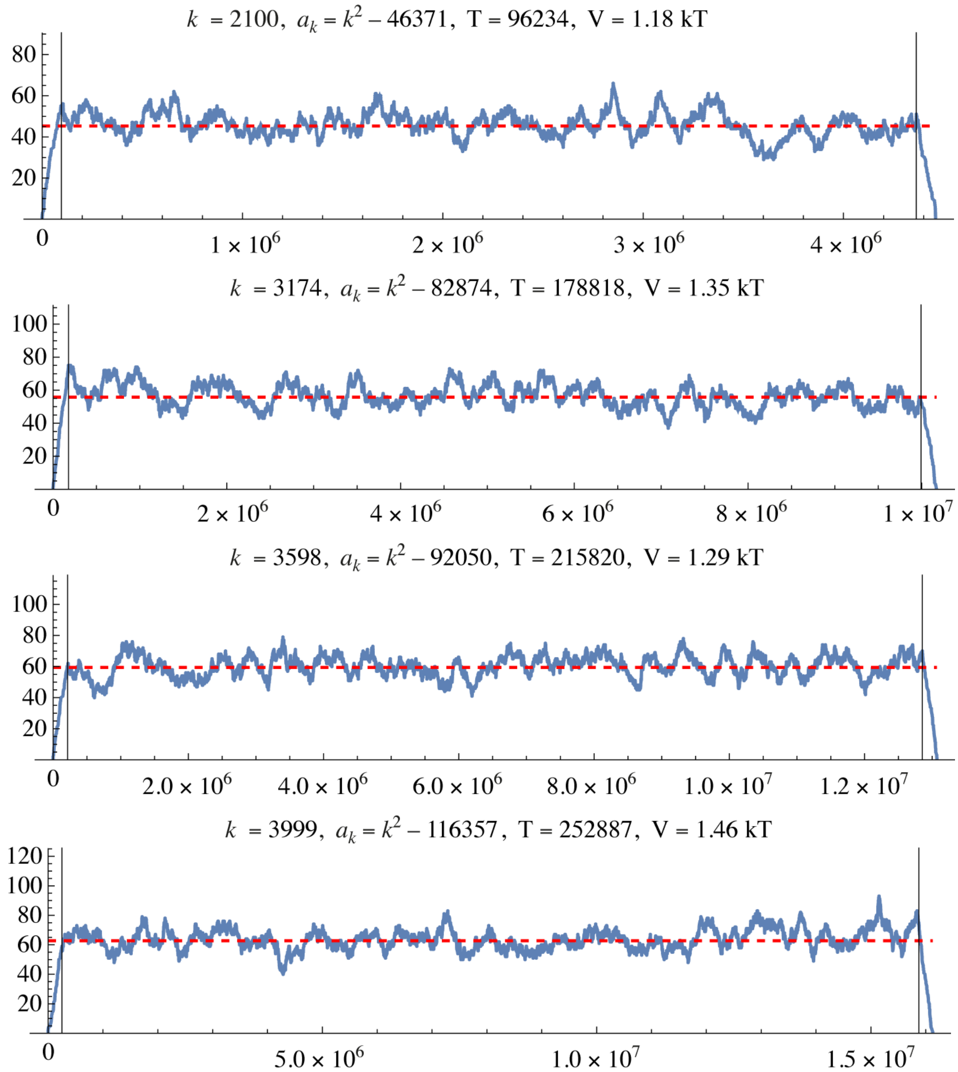


Fig. 6. Plot of A_i as a function of i for four typical thick Sidon sets. The average value of A_i is shown as a horizontal red line, and the values $i = T$ and $i = a_k$ are shown as vertical black lines.

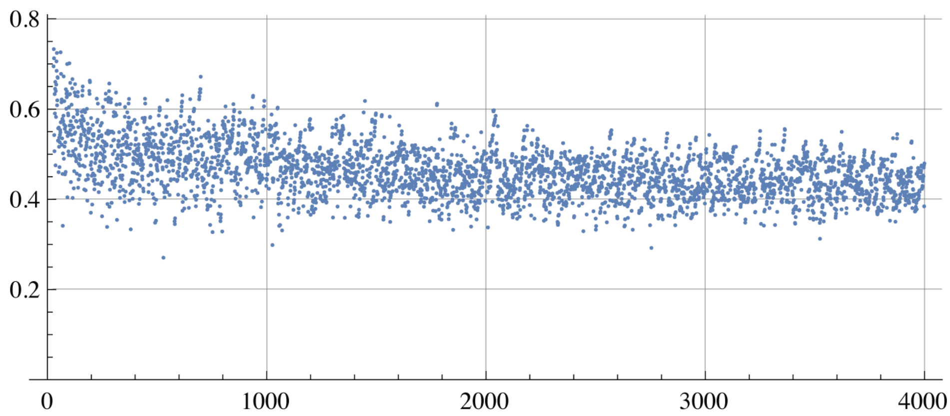


Fig. 7. $V(\mathcal{A}, k^{3/2})$ is defined by a sum with i running from 1 to $a_k + k^{3/2}$. This graph shows the proportion of $V(\mathcal{A}, k^{3/2})$ that comes from $i \leq T$ and $i \geq a_k$.

This paper was the first real improvement in the bounds, upper or lower, of $R(n)$ since 1941. It was the direct inspiration for the current work.

We play the same gambit, but exploit the phenomenon in a different way. Instead of using the Lindström proof, we re-use Theorem 4 on a subset of $\mathcal{A}$. That is, either $\mathcal{A}$ has a large variance (and so a large diameter), or a large subset $\mathcal{M} \subseteq \mathcal{A}$ has a difference set that does not include many small values, and so the small diffs is large, which forces $\mathcal{M}$ to have a large diameter.

3.1. A toy version of our argument. In this subsection, we give a simple argument using the Erdős – Turán Sidon set equation to prove that $b_\infty \le 1.999$. In the next subsection, we engage in a somewhat harder-to-optimize version of this argument with more parameters that leads to a better bound on b_∞ than that given in BFR.

Normalize as above, so that $a_1 = 0$, and set $T = k^{3/2}$ (it needs to be an integer, but we will ignore this issue in this subsection, and we shall also be cavalier about inequalities that may only hold for sufficiently large k). For positive i, set $A_i := |\mathcal{A} \cap [i-T, i)|$ and $A_{-i} := \big|\mathcal{A} \cap [a_k - i + 1, a_k + T + 1 - i)\big|$, and let $\bar{A} := kT/(T + a_k)$, the average value of A_i for $1 \le i \le a_k + T$. If $a_k \le k^2 - T$, then $\bar{A} \sim \sqrt{k}$. We begin by considering $(A_i + A_{-i})/2$ as a function of i; it is monotone increasing for $1 \le i \le T$. Set

$$U_1 := \left\{1 \le j \le T \colon \frac{A_i + A_{-i}}{2} \le \frac{8}{9}\bar{A}\right\},$$

$$U_2 := \left\{1 \le j \le T \colon \frac{8}{9}\bar{A} < \frac{A_i + A_{-i}}{2} < \frac{10}{9}\bar{A}\right\},$$

$$U_3 := \left\{1 \le j \le T \colon \frac{10}{9}\bar{A} \le \frac{A_i + A_{-i}}{2}\right\}.$$

If $|U_1| + |U_3| \ge T/16$, then

$$V(\mathcal{A}, T) := \sum_{i=1}^{T+a_k} (A_i - \bar{A})^2 \ge \sum_{i \in U_1 \cup U_3} \left[(A_i - \bar{A})^2 + (A_{-i} - \bar{A})^2\right]$$

$$\ge \sum_{i \in U_1 \cup U_3} 2\left(\frac{A_i + A_{-i}}{2} - \bar{A}\right)^2 \ge (|U_1 \cup U_2|) \cdot 2\left(\frac{1}{9}\right)^2 \bar{A}^2 \ge \frac{1}{648} kT.$$

We can now appeal to Theorem 4:

$$\operatorname{diam}(\mathcal{A}) \ge \frac{k^2 T^2}{T(T + k - 1) - \frac{1}{16}\frac{2}{81}kT} - T = k^2 - \left(2 - \frac{1}{648}\right)k^{3/2} + O(k).$$

Thus, $b_\infty \le 2 - \dfrac{1}{648} \le 1.999$ if $|U_1| + |U_3| \ge \dfrac{T}{16}$.

Now suppose that $|U_1| + |U_3| \le \dfrac{T}{16}$, so that $|U_2| \ge \dfrac{15}{16}T$. Set

$$\mathcal{M} := \mathcal{A} \cap \big[|U_1| + |U_2|,\ a_k - |U_1| - |U_2|\big].$$

Clearly,

$$|\mathcal{M}| = k - A_{|U_1|+|U_2|} - A_{-(|U_1|+|U_2|)} \geq k - \frac{20}{9}\bar{A}.$$

Set $L = \mathcal{A} \cap [0, |U_1|)$ and $R = \mathcal{A} \cap (a_k - |U_1|, a_k]$. By the definition of U_1, we see that

$$|L \cup R| \geq 2 \cdot \frac{8}{9}\bar{A}.$$

We also see that $L \cup R$ has $\binom{|L|}{2} + \binom{|R|}{2}$ pairs of elements whose difference is at most $|U_1|$. We have

$$\binom{|L|}{2} + \binom{|R|}{2} \geq \left(\frac{8}{9}\bar{A}\right)^2 - \left(\frac{8}{9}\bar{A}\right) \sim \frac{64}{81}k$$

differences, each at most $T/16$. Set $T_2 = \frac{3}{8}T$, which is larger than $T/16$, so that

$$S(\mathcal{M}, T_2) := \sum_{\substack{r=1 \\ r \notin \mathcal{M}-\mathcal{M}}}^{T_2-1} (T_2 - r) \geq \sum_{\substack{r=1 \\ r \in (L-L)\cup(R-R)}}^{T_2-1} (T_2 - r) \geq \frac{64}{81}k \cdot \left(\frac{3}{8}T - |U_1|\right).$$

Theorem 4 now gives

$$\begin{aligned}
\operatorname{diam}(\mathcal{A}) &= (\min \mathcal{M} - a_1) + \operatorname{diam}(\mathcal{M}) + (a_k - \max \mathcal{M}) \\
&\geq 2(|U_1| + |U_2|) + \frac{|\mathcal{M}|^2 T_2^2}{T_2(T_2 + |\mathcal{M}| - 1) - 2 \cdot \left(\frac{64}{81}k \cdot \left(\frac{3}{8}T - |U_1|\right)\right)} - T_2 \\
&= k^2 - \left(\frac{6734}{729}\frac{|U_1|}{T} - 2\frac{|U_2|}{T} + \frac{6361}{1944}\right)k^{3/2}.
\end{aligned}$$

The extremal values for $|U_1|$, $|U_2|$ are $\frac{1}{16}T$ and $\frac{15}{16}T$, respectively, whence

$$b_\infty \leq \frac{11515}{5832} < 1.999.$$

To get better numbers, we should have more levels than just $8/9$, $10/9$, and we should allow $T = \tau k^{3/2}$ to vary. We pursue this in the next subsection.

3.2. More parameters leads to a better bound. We begin by fixing real numbers $\tau > 0$, $\alpha \in (0,1)$, $\beta \in (0,1)$, $\delta \in (0, 1/2)$, $\tau_2 > 0$. Specific values that work out well are:

$$\tau = \frac{59}{58} \approx 1.017, \tag{5}$$

$$\alpha = \frac{80}{319} \approx 0.2508, \tag{6}$$

$$\beta = \frac{195}{356} \approx 0.5478, \tag{7}$$

$$\delta = \frac{398773753333438270}{2448810518987915261} \approx 0.1628, \tag{8}$$

$$\tau_2 = \frac{51}{223} \approx 0.2287. \tag{9}$$

The reason for the ridiculous-looking value of δ is that it makes two bounds that we will encounter exactly equal.

To better wrangle the equations, set $\min \mathcal{A} = 0$, $|\mathcal{A}| = k$, $T = \tau k^{3/2} + \epsilon_1$ (all of the ϵ variables are chosen in $[0,1)$ to make some other variable an integer), and $\bar{A} = \dfrac{kT}{a_k + T}$, and assume that $s_k = a_k \leq k^2 - T$, so that $\tau\sqrt{k} \leq \bar{A} < \tau\sqrt{k} + \epsilon_1/k$.

For $1 \leq j \leq a_k + T$, we have $A_j := |\mathcal{A} \cap [j-T, j)|$. For negative subscripts, we set $A_{-j} := A_{a_k+T+1-j}$. For example, $A_1 = |\{0\}| = 1$ and $A_{-1} = |\{a_k\}| = 1$. As a function of j, we see that $(A_j + A_{-j})/2$ is nondecreasing for $1 \leq j \leq T$, and increases by at most 1 as j increases by 1.

We partition the interval $[1,T]$ into 5 parts[1]:

$$U_1 := \left\{ j \in [1,T] \colon \frac{A_j + A_{-j}}{2} \leq (1-\alpha)\bar{A} \right\},$$

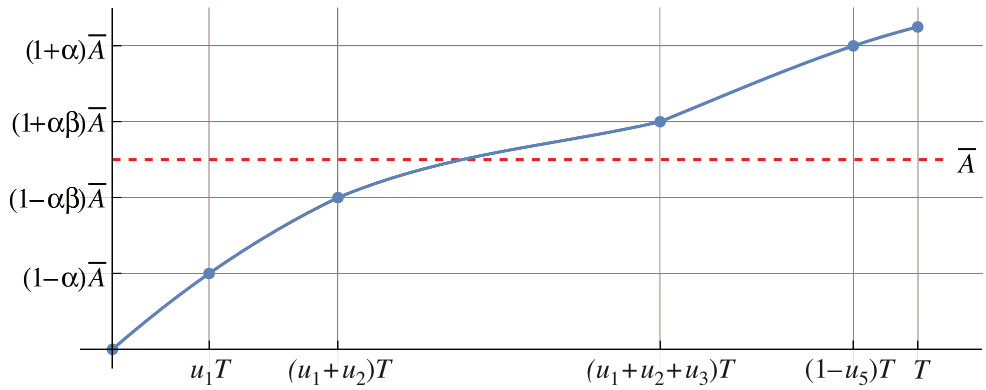
$$U_2 := \left\{ j \in [1,T] \colon (1-\alpha)\bar{A} < \frac{A_j + A_{-j}}{2} \leq (1-\alpha\beta)\bar{A} \right\},$$

$$U_3 := \left\{ j \in [1,T] \colon (1-\alpha\beta)\bar{A} < \frac{A_j + A_{-j}}{2} \leq (1+\alpha\beta)\bar{A} \right\},$$

$$U_4 := \left\{ j \in [1,T] \colon (1+\alpha\beta)\bar{A} \leq \frac{A_j + A_{-j}}{2} \leq (1+\alpha)\bar{A} \right\},$$

$$U_5 := \left\{ j \in [1,T] \colon (1+\alpha)\bar{A} < \frac{A_j + A_{-j}}{2} \right\}.$$

We set u_i by $u_i T = |U_i|$, and set $y := u_1 + u_5$, $x := u_2 + u_4$. For example, $x + y + u_3 = 1$ and $u_1 + u_2 + u_3 \geq 1 - x - y$. The following graph, an imagined plot of $(A_j + A_{-j})/2$ as a function of j, helps to understand the meaning of u_1, u_2, u_3, u_4, u_5.



[1]Setting $\beta = 1$ forces $U_2 = U_4 = \varnothing$, and is thereby substantially simpler, but leads merely $b_\infty \leq 1.999$.

Claim 1. *If $y+\beta^2x \ge \beta^2\delta$, then $V(\mathcal{A},T) \ge 2\alpha^2\beta^2\tau^2\, kT$.*

Proof. We have

$$\begin{aligned}
V(\mathcal{A},T) &\ge \sum_{j=1}^{T}(A_j-\bar{A})^2+(A_{-j}-\bar{A})^2 \\
&\ge \sum_{j=1}^{T} 2\left(\frac{A_j+A_{-j}}{2}-\bar{A}\right)^2 = 2\sum_{i=1}^{5}\sum_{j\in U_i}\left(\frac{A_j+A_{-j}}{2}-\bar{A}\right)^2 \\
&\ge 2(|U_1|+|U_5|)\alpha^2\bar{A}^2+2(|U_2|+|U_4|)(\alpha\beta)^2\bar{A}^2 \\
&\ge 2\alpha^2\tau^2(y+\beta^2x)\, kT.
\end{aligned}$$

By hypothesis of this claim, $y+\beta^2x\ge\beta^2\delta$, and so $V(\mathcal{A},T)\ge 2\alpha^2\beta^2\tau^2\delta\, kT$.

Claim 2. *If $y+\beta^2x\ge\beta^2\delta$, then*

$$b_\infty \le \tau+\frac{1}{\tau}-2\alpha^2\beta^2\delta\tau \le \frac{38692477564867759220242645 45}{19404057077873190546069259 42} \le 1.99405.$$

Proof. Theorem 4 gives (under the hypothesis that $y+\beta^2x\ge\beta^2\delta$)

$$\operatorname{diam}(\mathcal{A}) \ge \frac{k^2T^2}{T(T+k-1)-2\alpha^2\tau^2\delta kT}-T = k^2-\left(\tau+\frac{1}{\tau}-2\alpha^2\beta^2\delta\tau\right)k^{3/2}+O(k).$$

With the values of $\tau,\ \alpha,\ \delta$ given on lines (5), (6), and (8) above, this gives the claimed number.

We now work under the hypothesis that $y+\beta^2x\le\beta^2\delta$. Note that $|U_1|+|U_2|\le yT+xT\le \left(\frac{y}{\beta^2}+x\right)\le\delta T<T$, so that necessarily U_3 is not empty. It can happen that $U_4,\ U_5$ are empty.

Let $X-X$ be the set of positive differences of elements of X. In particular, if X is a subset of a Sidon set, then $|X-X|=\binom{|X|}{2}$. We set

$$\mathcal{M} := \mathcal{A}\cap(\max U_3, a_k-\max U_3).$$

We will find that $|\mathcal{M}|\approx|\mathcal{A}|$, but that if x,y are small then $\mathcal{M}-\mathcal{M}$ is missing a substantial number of small integers, so that $S(\mathcal{M},T_2)$ is $\Omega(k^{5/2})$, which forces the diameter of $\mathcal{M}$ to be large. This, in turn, forces $\operatorname{diam}(\mathcal{A})\ge 2\max U_3+\operatorname{diam}(\mathcal{M})$ to be large, and this gives a bound on b_∞.

Claim 3. *Suppose that $y+\beta^2x\le\beta^2\delta$. Then $|\mathcal{M}|\ge k-2(1+\alpha\beta)\tau\sqrt{k}+O(1)$.*

Proof. As $y+\beta^2x\le\beta^2\delta$, we know that U_3 is nonempty. Let $z=\max U_3$. By the definition of U_3, we know that $\frac{A_z+A_{-z}}{2}\le(1+\alpha\beta)\bar{A}$. Therefore,

$$|\mathcal{M}|\ge k-2(1+\alpha\beta)\bar{A}-2 = k-2(1+\alpha\beta)\tau\sqrt{k}+O(1).$$

We set $L_i := \mathcal{A}\cap(U_i-1)$ and $R_i := \mathcal{A}\cap(a_k+T+1-U_i)$. Note that $L_1,\ L_2,\ R_1,\ R_2$ are disjoint, and disjoint from $\mathcal{M}$. But they are all subsets of the Sidon set $\mathcal{A}$, so any difference in $(L_1\cup L_2)-(L_1\cup L_2)$ or $(R_1\cup R_2)-(R_1\cup R_2)$ is necessarily missing from $\mathcal{M}-\mathcal{M}$, and so contributes to $S(\mathcal{M},T_2)$ (provided T_2 is large enough).

Claim 4. *Suppose that* $y + \beta^2 x \le \beta^2\delta$.
There are at least $(1-\alpha)^2\tau^2 k + O\big(\sqrt{k}\,\big)$ *elements of* $(L_1 - L_1) \cup (R_1 - R_1)$, *each at most* yT.
There are at least $\alpha^2(1-\beta)^2\tau^2 k + O\big(\sqrt{k}\,\big)$ *elements of* $(L_2 - L_2) \cup (R_2 - R_2)$, *each at most* xT.
There are at least $(1-\alpha\beta)^2\tau^2 k + O\big(\sqrt{k}\,\big)$ *elements of* $\big((L_1\cup L_2) - (L_1 \cup L_2)\big) \cup \big((R_1\cup R_2) - (R_1 \cup R_2)\big)$, *each at most* $(x+y)T$.

Proof. Note that $|L_1| = A_{\max U_1}$, $|R_1| = A_{-\max U_1}$, and the definition of U_1 $\Bigg($together with the nonemptiness of U_2, which is implied by $\dfrac{y}{\beta^2} + x \le \delta\Bigg)$ gives

$$A_{\max U_1} + A_{-\max U_1} \le 2(1-\alpha)\bar{A} < A_{1+\max U_1} + A_{-1-\max U_1} \le A_{\max U_1} + A_{-\max U_1} + 2,$$

and so

$$2(1-\alpha)\bar{A} - 2 \le |L_1 \cup R_1| \le 2(1-\alpha)\bar{A}.$$

Similarly,

$$|L_2 \cup R_2| = 2\alpha(1-\beta)\bar{A} + O(1),$$
$$|L_1 \cup L_2 \cup R_2 \cup R_1| = 2(1-\alpha\beta)\bar{A} + O(1).$$

For a Sidon set X, the size of $X - X$ is exactly $\dbinom{|X|}{2}$. For example, $(L_1 - L_1) \cup (R_1 - R_1)$ has

$$\binom{|L_1|}{2} + \binom{|R_1|}{2} \ge 2\binom{(1-\alpha)\bar{A}}{2} = \big((1-\alpha)\bar{A}\big)^2 + O\big(\sqrt{k}\,\big) = (1-\alpha)^2\tau^2 k + O\big(\sqrt{k}\,\big)$$

elements, each at most $\operatorname{diam}(U_1) = u_1 T$, which is at most yT.
Essentially identical computations give the other assertions of this claim.
We set $T_2 := \tau_2 T + \epsilon_2$, with $\epsilon_2 \in [0,1)$ chosen to make T_2 an integer.
Claim 5. *Suppose that* $y + \beta^2 x \le \beta^2 \delta$ *and* $\tau_2 > x + y$. *Then* $S(\mathcal{M}, T_2)$ *is at least* $kT \cdot \tau^2 \cdot w$, *where*

$$\begin{aligned} w &:= \tau_2(1-\alpha\beta)^2 - y(1-\alpha)(1+\alpha-2\alpha\beta) - x\alpha(1-\beta)(2-\alpha-\alpha\beta) \\ &= \frac{30590263131}{179748900463} - \frac{6622929}{9056729}y - \frac{5081160}{27794789}x. \end{aligned}$$

Proof. By hypothesis, $T_2 = \tau_2 T > (x+y)T$, so all of the differences described in Claim 4 contribute to

$$S(\mathcal{M}, T_2) := \sum_{\substack{r=1 \\ r \in \mathcal{M}-\mathcal{M}}}^{T_2 - 1} (T_2 - r) \ge \sum_{r \in ((L_1\cup L_2)-(L_1\cup L_2))\cup((R_1\cup R_2)-(R_1\cup R_2))} (T_2 - r).$$

For example, the $(1-\alpha)^2\tau^2 k$ differences in $(L_1 - L_1)\cup(R_1 - R_1)$ contribute at least

$$(T_2 - yT)\big((1-\alpha)^2\tau^2 k + O\big(\sqrt{k}\,\big)\big) = (\tau_2 - y)(1-\alpha)^2\tau^2 kT + O(k^2)$$

to $S(\mathcal{M}, T_2)$. Similarly, the

$$\alpha^2(1-\beta)^2\bar{A}^2 + O(\sqrt{k}\,)$$

differences in $(L_2 - L_2) \cup (R_2 - R_2)$, each at most $\operatorname{diam}(U_2) = u_2 T < xT$, contribute at least

$$(T_2 - \operatorname{diam}(U_2))\Big(\alpha^2(1-\beta)^2\bar{A}^2 + O(\sqrt{k}\,)\Big) = (\tau_2 - x)\alpha^2(1-\beta)^2\tau^2 kT + O(k^2)$$

to $S(\mathcal{M}, T_2)$. Finally, $(L_1 \cup L_2) - (L_1 \cup L_2)$ and $(R_1 \cup R_2) - (R_1 \cup R_2)$ have many differences that haven't been counted already. They get

$$\big((1-\alpha\beta)\bar{A}\big)^2 + O(\sqrt{k}\,) = (1-\alpha\beta)^2\tau^2 k + O(\sqrt{k}\,)$$

elements, but only

$$(1-\alpha\beta)^2\tau^2 k - (1-\alpha)^2\tau^2 k - \alpha^2(1-\beta)^2\tau^2 k + O(\sqrt{k}\,) = 2\alpha(1-\alpha)(1-\beta)\tau^2 k + O(\sqrt{k}\,),$$

each at most $\operatorname{diam}(U_1 \cup U_2) = |U_1| + |U_2| - 1 < (u_1 + u_2)T \le (y + x)T$, have not been accounted for already. These contribute an additional

$$(\tau_2 - (y + x)) \cdot 2\alpha(1-\alpha)(1-\beta)\tau^2 kT + O(k^2)$$

to $S(\mathcal{M}, T_2)$. After some algebra to rearrange terms, this claim is confirmed.

Claim 6. *Suppose that $y + \beta^2 x \le \beta^2\delta$. Then*

$$\begin{aligned} b_\infty &\le \frac{\tau^2\big(2\tau_2^2\big(2\alpha\beta + \beta^2\delta + 1\big) + 2(\alpha-1)\beta^2\delta(\alpha(2\beta-1)-1) - 2\tau_2(\alpha\beta-1)^2 + \tau_2^3\big) + \tau_2}{\tau\tau_2^2} \\ &\le \frac{38692477564867759220242645 45}{19404057077873190546069259 42} \le 1.99405. \end{aligned}$$

Proof. We begin with

$$\begin{aligned} \operatorname{diam}(\mathcal{A}) &= \min\mathcal{M} + \operatorname{diam}(\mathcal{M}) + a_k - \max\mathcal{M} \\ &\ge 2(T - xT - yT) + \frac{|\mathcal{M}|^2 T_2^2}{T_2(T_2 + |\mathcal{M}| - 1) - 2\tau^2 wkT} - T_2, \end{aligned}$$

where we have used Theorem 4 and Claim 5. The first term contributes $2\tau(1 - x - y)$ to the $k^{3/2}$ coefficient, and the last term contributes $-\tau_2$. The middle term can be converted to a geometric series:

$$\begin{aligned} &\frac{|\mathcal{M}|^2 T_2^2}{T_2(T_2 + |\mathcal{M}| - 1) - 2\tau^2 wkT} \\ &\qquad = \frac{|\mathcal{M}|^2}{1 + \dfrac{|\mathcal{M}| - 1}{\tau\tau_2 k^{3/2}} - 2\dfrac{\tau w}{\tau_2^2 k^{1/2}}} \\ &\qquad = |\mathcal{M}|^2\left(1 + \left(\frac{2\tau w}{\tau_2^2 k^{1/2}} - \frac{|\mathcal{M}| - 1}{\tau\tau_2 k^{3/2}}\right) + \left(\frac{2\tau w}{\tau_2^2 k^{1/2}} - \frac{|\mathcal{M}| - 1}{\tau\tau_2 k^{3/2}}\right)^2 + \ldots\right) \end{aligned}$$

$$= |\mathcal{M}|^2 \left(1 + \frac{2\tau w}{\tau_2^2 k^{1/2}} - \frac{|\mathcal{M}| - 1}{\tau \tau_2 k^{3/2}} + O(1/k)\right).$$

Defining μ by $|\mathcal{M}| = k - \mu\sqrt{k}$, we get

$$\begin{aligned} &|\mathcal{M}|^2 \left(1 + \frac{2\tau w}{\tau_2^2 k^{1/2}} - \frac{|\mathcal{M}| - 1}{\tau \tau_2 k^{3/2}} + O(1/k)\right) \\ &\quad = (k - \mu\sqrt{k})^2 \left(1 + \frac{2\tau w}{\tau_2^2 k^{1/2}} - \frac{k - \mu\sqrt{k}}{\tau \tau_2 k^{3/2}}\right) + O(k) \\ &\quad = k^2 + \left(\frac{2\tau w}{\tau_2^2} - 2\mu - \frac{1}{\tau \tau_2}\right) k^{3/2} + O(k). \end{aligned}$$

Thus,

$$b_\infty \le \tau\tau_2 - 2\tau(1 - x - y) + 2\mu + \frac{1}{\tau\tau_2} - \frac{2\tau w}{\tau_2^2}. \tag{10}$$

From Claim 3, we know that μ is at most $2(1 + \alpha\beta)\tau$. The right-hand side of (10) is a linear expression in x and y, which we must maximize in the region $x \ge 0,\ y \ge 0,\ y + \beta^2 x \le \beta^2\delta$. The maximum occurs[2] at the vertex $(x, y) = (0, \beta^2\delta)$, and is

$$b_\infty \le \frac{38692477564867759220242645 45}{19404057077873190546069259 42}.$$

Claims 2 and 6 complete the proof of Theorem 2. The value of δ was chosen so as to make the two bounds exactly equal. In general, one sets

$$\delta = -\frac{\tau_2\left(-2\alpha^2\beta^2\tau^2 + 4\alpha\beta\tau^2\tau_2 + 4\alpha\beta\tau^2 + \tau^2\tau_2^2 + \tau^2\tau_2 - 2\tau^2 - \tau_2 + 1\right)}{2\tau^2\left(\alpha^2\beta^2\tau_2^2 + \alpha^2\beta^2 - \alpha^2 - 2\alpha\beta + 2\alpha + \tau_2^2\right)}$$

to accomplish this.

In reality, the bounds were first worked out symbolically using Mathematica, and then optimized using simulated annealing. Having good estimates of where the optimal value occurs then allowed certain streamlining of the argument.

Acknowledgements. I wish to thank Melvyn B. Nathanson and Yin Choi Cheng, who independently showed great patience while I explained early versions of this work.

Conflict of interest. The author declares that he has no potential conflict of interest in relation to the study in this paper.

Funding. This research was supported by a PSC – CUNY Award, jointly funded by The Professional Staff Congress and The City University of New York.

[2] Ideally, we would set

$$\tau_2 = \sqrt{\frac{-2\alpha^2\beta^3 + 2\alpha^2\beta^2 - \alpha^2 + 2\alpha\beta^3 - 2\alpha\beta + 2\alpha - \beta^2}{\beta^2 - 1}},$$

and then this expression has a factor of $y + \beta^2 x$, which we could replace with $\beta^2\delta$. The author didn't realize this until after the optimization work was complete, and including it would make some intermediate optimization steps more delicate.

References

1. J. Balogh, Z. Füredi, S. Roy, *An upper bound on the size of Sidon sets* (2021); available at https://arxiv.org/abs/2103.15850.
2. Y. Caicedo, C. A. Martos, A. Trujillo, *g-Golomb rulers*, Rev. Integr. Temas Mat., **33**, № 2, 161 – 172 (2015).
3. J. Cilleruelo, *Sidon sets in $\mathbb{N}^d$*, J. Combin. Theory Ser. A, **117**, № 7, 857 – 871 (2010); DOI 10.1016/j.jcta.2009.12.003.
4. *Distributed.net: Completion of OGR-28 project* (2022); https://blogs.distributed.net/2022/11/23/03/28/bovine/.
5. G. Dogon, T. Rokicki, *Larger Golomb rulers, gathering 4 gardner 12 (Atlanta, Georgia, April 1)* (2016), Exchange Book: Art, Games, Magic, and Math., vol. 1 (2017), p. 155 – 166; http://cube20.org/golomb/.
6. P. Erdös, P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc., **16**, 212 – 215 (1941); DOI 10.1112/jlms/s1-16.4.212.
7. B. Lindström, *An inequality for B_2-sequences*, J. Combin. Theory, **6**, 211 – 212 (1969).
8. K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electron. J. Combin., **DS11**, 39 (2004).
9. J. Shearer, *This webpage is devoted to Golomb rulers* (1999); https://web.archive. org/web/20171225101048/http://www.research.ibm.com/people/s/shearer/grule.html.
10. S. Sidon, *Ein Satz über trigonometrische Polynome und seine Anwendungen in der Theorie der Fourier – Reihen*, Math. Ann., **106**, 536 – 539 (1932).
11. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., **43**, № 3, 377 – 385 (1938).

Received 07.10.23