ON STRONG SIDON SETS OF INTEGERS

YOSHIHARU KOHAYAKAWA, SANG JUNE LEE, CARLOS GUSTAVO MOREIRA, AND VOJTĚCH ROŠL

Abstract. A set \( S \subset \mathbb{N} \) of positive integers is a Sidon set if the pairwise sums of its elements are all distinct, or, equivalently, if
\[
|(x + w) - (y + z)| \geq 1
\]
for every \( x, y, z, w \in S \) with \( x < y \leq z < w \). Let \( 0 \leq \alpha < 1 \) be given. A set \( S \subset \mathbb{N} \) is an \( \alpha \)-strong Sidon set if
\[
|(x + w) - (y + z)| \geq w^\alpha
\]
for every \( x, y, z, w \in S \) with \( x < y \leq z < w \). We prove that the existence of dense strong Sidon sets implies that randomly generated, infinite sets of integers contain dense Sidon sets. We derive the existence of dense strong Sidon sets from Ruzsa’s well known result on dense Sidon sets [J. Number Theory 68 (1998), no. 1, 63–71]. We also consider an analogous definition of strong Sidon sets for sets \( S \) contained in \([n]\) = \{1, \ldots, n\}, and give good bounds for \( F(n, \alpha) = \max |S| \) where \( S \) ranges over all \( \alpha \)-strong Sidon sets contained in \([n]\).

1. Introduction

Let \( \mathbb{N} \) be the set of positive integers. A set \( A \subset \mathbb{N} \) is called a Sidon set if all the sums \( a_1 + a_2 \), with \( a_1, a_2 \in S \) and \( a_1 \leq a_2 \), are distinct, or, equivalently, if
\[
|(x + w) - (y + z)| \geq 1
\]
for every \( x, y, z, w \in S \) with \( x < y \leq z < w \).

A well-known problem on Sidon sets is the determination of the maximum size of Sidon sets contained in \([n]\) = \{1, 2, \ldots, n\}. In the 1940s, Chowla, Erdős, Turán, and Singer [2, 5, 6, 11] proved that the maximum cardinality of a Sidon set contained in \([n]\) is \((1 + o(1))\sqrt{n}\). However, how dense a Sidon set contained in \( \mathbb{N} \) can be is not well understood. For \( S \subset \mathbb{N} \), let \( S(n) = |S \cap [n]| \) for all \( n \geq 1 \). A major open problem is to decide how fast \( S(n) \) can grow for a Sidon set \( S \subset \mathbb{N} \).

In connection with the study of Sidon sets contained in randomly generated, infinite sets of integers, we considered the following related concept in [8].

**Definition 1** (\( \alpha \)-strong Sidon sets). Fix a constant \( \alpha \) with \( 0 \leq \alpha < 1 \). A set \( S \subset \mathbb{N} \) is called an \( \alpha \)-strong Sidon set if
\[
|(x + w) - (y + z)| \geq w^\alpha
\]  

(1)
Clearly, a 0-strong Sidon set is a Sidon set. In a way similar to Definition 1, one can define a finite version of strong Sidon sets.

**Definition 2** ($(n, \alpha)$-strong Sidon sets). Fix an integer $n \geq 1$ and a constant $\alpha$ with $0 \leq \alpha < 1$. A set $S \subset [n] = \{1, 2, \ldots, n\}$ is an $(n, \alpha)$-strong Sidon set if

$$|(x+w) - (y+z)| \geq n^\alpha$$

for every $x, y, z, w \in S$ with $x < y \leq z < w$.

Note that there is a conceptual difference between Definitions 1 and 2. While the term $|(x+w) - (y+z)|$ in Definition 1 is compared with a power of $w = \max\{x, y, z, w\}$, the same term in Definition 2 is compared with a power of $n$.

In this paper, we are interested in how dense strong Sidon sets can be. We first consider the ‘finite’ case.

**Definition 3.** Let $F(n, \alpha)$ be the maximal cardinality of an $(n, \alpha)$-strong Sidon set contained in $[n]$.

We have the following upper and lower bounds for $F(n, \alpha)$.

**Theorem 4.** Fix $0 \leq \alpha < 1$. We have

$$n^{(1-\alpha)/2}(1 + o(1)) \leq F(n, \alpha) \leq n^{(1-\alpha)/2} + O(n^{(1-\alpha)/3}).$$

Theorem 4 is proved in Section 3. Next we consider the ‘infinite’ case.

**Definition 5.** For a set $S \subset \mathbb{N}$ of positive integers, we define the counting function $S(n)$ by

$$S(n) = |S[n]| = |S \cap [n]| \quad (n \in \mathbb{N}).$$

We have the following upper bound on $S(n)$ for $\alpha$-strong Sidon sets $S \subset \mathbb{N}$.

**Theorem 6.** Every $\alpha$-strong Sidon set $S \subset \mathbb{N}$ is such that, for every sufficiently large $n$,

$$S(n) \leq cn^{(1-\alpha)/2},$$

where $c = c(\alpha)$ is a constant that depends only on $\alpha$.

The proof of Theorem 6 is given in Section 4. We now turn to the existence of dense, infinite $\alpha$-strong Sidon sets. We first consider an analogue of a result of Erdős (see [12, p. 132] or [7, Chapter II, Theorem 9]), who proved that there is a Sidon set $S \subset \mathbb{N}$ such that

$$\limsup_{n \to \infty} S(n)n^{-1/2} \geq \frac{1}{2}.$$ (2)

(see also [9], where the constant $1/2$ in (2) is improved to $1/\sqrt{2}$). Our result is as follows.

**Theorem 7.** For every $0 < \alpha < 1$, there is an $\alpha$-strong Sidon set $S \subset \mathbb{N}$ such that

$$\limsup_{n \to \infty} S(n)n^{-(1-\alpha)/2} \geq \frac{1}{2}.$$ (3)

Theorem 7 is proved in Section 6 (improving the constant $1/2$ in (3) to $1/\sqrt{2}$, in the spirit of [9], should be possible, but we do not think it would be worth it at this stage). As is well
known, the following is a major open problem: given \( \varepsilon > 0 \), are there Sidon sets \( S = S_\varepsilon \subset \mathbb{N} \) such that \( S(n) \geq n^{1/2-\varepsilon} \) for every \( n \geq n_0(\varepsilon) \)? In this direction, improving a classical result of Ajtai, Komlós and Szemerédi \[1\], Ruzsa \[10\] proved the existence of Sidon sets \( S \subset \mathbb{N} \) with
\[
S(n) \geq n^{\sqrt{2}-1+o(1)}
\]
for every \( n \), where \( o(1) \to 0 \) as \( n \to \infty \) (see, also, \[3, 4\]). The main result of this paper is an attempt to extend Ruzsa’s result to strong Sidon sets.

**Theorem 8.** For every \( 0 \leq \alpha \leq 10^{-4} \), there exists an \( \alpha \)-strong Sidon set \( S \subset \mathbb{N} \) such that
\[
S(n) \geq n^{2 \sqrt{2} - 1 + o(1)}/(1 + 32 \sqrt{\alpha})
\]
for every \( n \).

The proof of Theorem 8, which is partly inspired by Ruzsa’s construction in \[10\], is given in Section 7. Unfortunately, the bound given in (4) gives the best known result only for small values of \( \alpha \). More precisely, the following result, which can be proved with a simple greedy argument (see Section 5), gives a better bound for \( \alpha \geq 5.75 \ldots \times 10^{-5} \).

**Theorem 9.** For every \( 0 \leq \alpha < 1 \), there exists an \( \alpha \)-strong Sidon set \( S \subset \mathbb{N} \) such that
\[
S(n) \geq \frac{1}{2} n^{(1-\alpha)/3}
\]
for every sufficiently large \( n \).

This paper is organised as follows. In Section 2, we discuss the connection between strong Sidon sets and an extremal problem on random sets of integers investigated in \[8\]. Sections 3 to 6 are devoted to the proofs of Theorems 4, 6, 9 and 7. The proof of our main result for infinite strong Sidon sets, Theorem 8, is given in Section 7. We close with some concluding remarks in Section 8.

We shall in general omit floor and ceiling signs when they are not essential, to avoid having to deal with uninteresting, fussy details. Our convention is that \( a/bc \) means \( a/(bc) \).

2. **Sidon sets contained in random sets of integers**

2.1. **An extremal problem on random sets of integers.** In \[8\] we investigated the following question: how dense Sidon sets \( S \) contained in a random set of integers can be? First we describe the probability model for random subsets of \( \mathbb{N} \) that we shall use.

**Definition 10.** Fix a constant \( \alpha \) satisfying \( 0 \leq \alpha < 1 \). Let \( p_m = m^{-\alpha} \) for every positive integer \( m \). Let \( R = R(\alpha) \subset \mathbb{N} \) be a random set obtained by choosing each element \( m \in \mathbb{N} \) independently with probability \( p_m \).

We are interested in two types of results about the growth rate of the counting function \( S(n) \) for Sidon sets \( S \) contained in the random set \( R(\alpha) \) of integers.

(a) Find the largest possible constant \( f(\alpha) \) such that, with probability 1, there is a Sidon set \( S \) contained in \( R(\alpha) \) such that, for all \( n \),
\[
S(n) \geq n^{f(\alpha)+o(1)}.
\]
(b) Find the smallest possible constant \( g(\alpha) \) such that, with probability 1, every Sidon set \( S \) contained in \( R(\alpha) \) is such that, for all \( n \),
\[
S(n) \leq n^{g(\alpha)+o(1)}.
\]

The constants \( f(\alpha) \) and \( g(\alpha) \) obtained in [8] are the following:

(a) \( f(\alpha) = g(\alpha) = 1 - \alpha \) for \( 2/3 \leq \alpha < 1 \).
(b) \( f(\alpha) = g(\alpha) = 1/3 \) for \( 1/3 \leq \alpha \leq 2/3 \).
(c) \( f(\alpha) = \max\{1/3, \sqrt{2} - 1 - \alpha\} \) and \( g(\alpha) = (1 - \alpha)/2 \) for \( 0 \leq \alpha \leq 1/3 \).

Thus, there is a gap between \( f(\alpha) \) and \( g(\alpha) \) if \( 0 \leq \alpha \leq 1/3 \). The goal of this section is to show that the existence of certain \( \alpha \)-strong Sidon sets implies lower bounds for \( f(\alpha) \) in (6). To this end, we use the following modification of Definition 1.

**Definition 11** ((\( \alpha, c \))-strong Sidon sets). Let constants \( c > 0 \) and \( \alpha \) with \( 0 \leq \alpha < 1 \) be given. A set \( S \subseteq \mathbb{N} \) is called an \( (\alpha, c) \)-strong Sidon set if
\[
|(x + w) - (y + z)| \geq cw^\alpha
\]
for every \( x, y, z, w \in S \) with \( x < y < z < w \).

We shall consider \((\alpha, c)\)-strong Sidon sets for \( c = 1 \) and \( c = 16 \) only (\( c = 1 \) corresponds to \( \alpha \)-strong Sidon sets and Theorem 12 below concerns the case \( c = 16 \)). The existence of an \( (\alpha, 16) \)-strong Sidon set with \( S(n) \) satisfying (4) follows from Theorem 8.

We prove the following.

**Theorem 12.** Let \( 0 \leq \alpha \leq 1/2 \) be given. If there exists an \( (\alpha, 16) \)-strong Sidon set \( S \subseteq \mathbb{N} \) with
\[
S(n) \geq n^{h(\alpha)+o(1)},
\]
then, with probability 1, the random subset \( R = R(\alpha) \) of \( \mathbb{N} \) contains a Sidon set \( S^* \) such that
\[
S^*(n) \geq n^{h(\alpha)+o(1)}.
\]

The next section is devoted to the proof of Theorem 12.

2.2. **Proof of Theorem 12** The proof of Theorem 12 is based on two auxiliary lemmas, Lemmas 13 and 16. In order to formulate these lemmas, we introduce some notation. Let
\[
\beta = \frac{1}{1 - \alpha} \quad \text{so that} \quad \alpha = 1 - \frac{1}{\beta}.
\]
For every integer \( i \geq 1 \), let
\[
I_i = \mathbb{N} \cap [i^\beta, (i + 1)^\beta).
\]
For \( a, b \in \mathbb{N} \), write
\[
a \sim b
\]
if \( a, b \in I_i \) for some \( i \in \mathbb{N} \). The following holds.

**Lemma 13.** For every sufficiently large \( i \in \mathbb{N} \), say \( i \geq i_0(\alpha) \), we have
\[
P(|R \cap I_i| \geq 1) \geq \frac{1}{3}.
\]

\(^1\)We remark that, in [8], the random set \( R \) is generated by selecting each natural number \( m \) with probability \( p_m = \min\{\alpha m^{\delta - 1}, 1\} \). Thus, to translate the results in [8] to the present context, one has to take the constant \( \alpha \) in [8] to be 1 and the constant \( \delta \) in [8] to be \( 1 - \alpha \). Thus, for instance, to interpret Figure 1 in [8] one should have in mind that \( \delta = 1 - \alpha \) (where \( \alpha \) is the \( \alpha \) in Definition 10 that is, it is the \( \alpha \) in the present paper).
Proof. Let $X_i$ be the size of a random set obtained by choosing each element in $I_i$ independently with probability
\[(i + 1)^\beta - i^\beta = (i + 1)^\beta - (i + 1)^\beta = (i + 1)^\beta - i^\beta. \tag{10}\]
Since each element in $I_i$ is chosen to be in $R$ independently with probability at least $((i + 1)^\beta - i^\beta, \alpha$, we have that $P(|R \cap I_i| \geq 1) \geq P(X_i \geq 1)$. Therefore, to prove $\ref{lem16}$, it suffices to prove that $P(X_i = 0) \leq 2/3$.

Let us first note that, as $\beta \geq 1$, we have
\[(1 + i)^\beta - i^\beta \geq \beta i^\beta - 1. \tag{11}\]
Moreover, for $i \geq i_0(\beta)$, we have
\[\beta \left(\frac{i}{i + 1}\right)^{\beta - 1} - \left(\frac{1}{i + 1}\right)^{\beta - 1} \geq \frac{\beta}{2}. \tag{12}\]
Using $\ref{eq10}, \ref{eq11}$ and $\ref{eq12}$, we see that
\[
P(X_i = 0) \leq \left(1 - \left(\frac{1}{1 + i}\right)^{\alpha \beta}ight)^{(1 + i)^\beta - i^\beta - 1} \leq \exp \left(-\left(\frac{1}{1 + i}\right)^{\beta - 1} - (1 + i)^\beta - i^\beta - 1\right) \leq \exp \left(-\left(\frac{1}{1 + i}\right)^{\beta - 1}\beta - 1\right) \leq \exp \left(-\left(\frac{\beta}{2}\right)^{1 + i}\right) \leq e^{-\frac{\beta}{2}} < \frac{2}{3}, \tag{13}\]
and $\ref{lem16}$ follows. $\square$

For the proof of Lemma $\ref{lem16}$, it is convenient to have the following.

Claim 14. Let $S \subset \mathbb{N}$ be an $(\alpha, 16)$-strong Sidon set, where $0 \leq \alpha \leq 1/2$. Then the elements of $S$ are contained in distinct intervals of $I_i$, with possibly only one exceptional interval containing two elements of $S$.

Proof. In what follows, we shall make use of the following inequality: for all reals $\beta$ and $x$ with $1 \leq \beta < 2$ and $x \geq 1$, we have
\[(x + 1)^\beta - x^\beta \leq 2\beta x^\beta - 1. \tag{13}\]
We now start the proof of Claim $\ref{claim14}$. Let us first show that there is at most one interval $I_i$ that contains at least two elements of $S$. Suppose for a contradiction that $i < j$ $(i, j \in \mathbb{N})$ and $x, y, z, w \in S$ are such that $x < y < z < w$, and $x, y \in I_i$ and $z, w \in I_j$. Using $\ref{eq13}$, we see that
\[
|x + w -(y + z)| \leq |w - z| + |y - x| \leq |I_j| + |I_i| \leq 2|I_j| \leq 2(j + 1)^\beta - j^\beta \leq 4\beta j^\beta - 1 \leq 4\beta(j^\beta)^\alpha < 4\beta w^\alpha.
\]
Because of the assumption $0 \leq \alpha \leq 1/2$, we have that
\[1 \leq \beta = \frac{1}{1 - \alpha} \leq 2. \tag{14}\]
Hence,
\[|x + w -(y + z)| < 8w^\alpha.
\]
This contradicts the assumption that $S$ is an $(\alpha, 16)$-strong Sidon set.
Next, we show that there is no interval with three elements of $S$. Suppose for a contradiction that $i \in \mathbb{N}$ and $x, y, z \in S$ are such that $x < y < z$ and $x, y, z \in I_i$. Then,

$$|x + z - (y + y)| \leq |z - y| + |y - x| < 2|I_i| \leq 4\beta \alpha^6 \leq 8\alpha,$$

which again contradicts the assumption on $S$. Therefore, Claim 14 is proved.

In the proof of Theorem 12, it will be convenient to consider $(\alpha, 16)$-strong Sidon sets $S$ with the property that $S$ meets every $I_i$ ($i \geq 1$) at most one element.

**Definition 15.** Let $0 \leq \alpha < 1/2$ be given and let $S$ be an $(\alpha, 16)$-strong Sidon set. If the elements of $S$ are all contained in distinct intervals $I_i$ ($i \geq 1$), we say that $S$ is a canonical $(\alpha, 16)$-strong Sidon set.

Claim 14 allows us to discard a bounded number of elements of any $(\alpha, 16)$-strong Sidon set $S$ to obtain a canonical $(\alpha, 16)$-strong Sidon set. Clearly, this process does not decrease the density of $S$ (that is, the exponent $h(\alpha)$ in (7) does not change).

We now show that certain perturbations of strong Sidon sets are Sidon sets. Recall that we write $a \sim b$ if $a$ and $b$ belong to the same interval $I_i$ (see (8)).

**Lemma 16.** Let $0 \leq \alpha \leq 1/2$ be given and let $S = \{s_1 < s_2 < \ldots\} \subset \mathbb{N}$ be a canonical $(\alpha, 16)$-strong Sidon set. For every $i \geq 1$, let $s'_i$ be an integer such that $s'_i \sim s_i$, and let $S' = \{s'_1, s'_2, \ldots\}$.

Then $S'$ is a Sidon set.

**Proof.** Suppose for a contradiction that $S'$ is not a Sidon set. In other words, suppose that there are $a, b, c, d \in S'$ with $a < b \leq c < d$ such that $a + d = b + c$. Let $a \in I_i, b \in I_j, c \in I_k$ and $d \in I_\ell$. Since we assume that $S$ is canonical, we have that $i < j \leq k < \ell$.

We clearly have that

$$i^\beta \leq a < (i + 1)^\beta, \quad j^\beta \leq b < (j + 1)^\beta,$$

$$k^\beta \leq c < (k + 1)^\beta, \quad \ell^\beta \leq d < (\ell + 1)^\beta.$$

Hence,

$$i^\beta + \ell^\beta \leq a + d < (i + 1)^\beta + (\ell + 1)^\beta \quad \text{and} \quad j^\beta + k^\beta \leq b + c < (j + 1)^\beta + (k + 1)^\beta.$$

Since $a + d = b + c$ holds, the two intervals $[i^\beta + \ell^\beta, (i + 1)^\beta + (\ell + 1)^\beta]$ and $[j^\beta + k^\beta, (j + 1)^\beta + (k + 1)^\beta]$ are not disjoint, and hence one of the following holds:

$$j^\beta + k^\beta \leq i^\beta + \ell^\beta < (j + 1)^\beta + (k + 1)^\beta \quad (15)$$

or

$$i^\beta + \ell^\beta \leq j^\beta + k^\beta < (i + 1)^\beta + (\ell + 1)^\beta. \quad (16)$$

We claim that inequality (15) implies that $0 \leq i^\beta + \ell^\beta - (j^\beta + k^\beta) < 4\beta \ell^\beta - 1$. Indeed, (15) yields

$$0 \leq i^\beta + \ell^\beta - (j^\beta + k^\beta) \leq (j + 1)^\beta + (k + 1)^\beta - j^\beta - k^\beta$$

$$\leq \beta(j + 1)^\beta - 1 + \beta(k + 1)^\beta - 1 \leq \beta(2j)^\beta - 1 + \beta(2k)^\beta - 1 < 4\beta \ell^\beta - 1,$$

where the last inequality follows from $\alpha \leq 1/2$ Similarly, inequality (16) implies

$$0 \leq j^\beta + k^\beta - (i^\beta + \ell^\beta) < 4\beta \ell^\beta - 1.$$
Consequently, we have

\[ |i^\beta + \ell^\beta - (j^\beta + k^\beta)| < 4\beta \ell^{\beta-1}. \] (17)

Let \( x, y, z, w \in S \) be such that \( x \sim a, y \sim b, z \sim c \) and \( w \sim d \). Since \( S \) is canonical, we have \( x < y \leq z < w \). Since \( x \in I_i, y \in I_j, z \in I_k \) and \( w \in I_l \), we have that \( i = \lfloor x^{1/\beta} \rfloor, j = \lfloor y^{1/\beta} \rfloor, k = \lfloor z^{1/\beta} \rfloor, \) and \( \ell = \lfloor w^{1/\beta} \rfloor \). Note that \( \ell \leq w^{1/\beta} < \ell + 1 \), i.e.,

\[ w^{1/\beta} - 1 < \ell \leq w^{1/\beta}. \] (18)

Raising all terms of (18) to the power of \( \beta \) and using the inequality \( \xi^\beta - (\xi - 1)^\beta - \beta \xi^{\beta-1} < 0 \) with \( \xi = w^{1/\beta} \), we infer that

\[ w - \beta w^\alpha < (w^{1/\beta} - 1)^\beta < \ell^\beta \leq w. \]

Similarly, we have

\[ x - \beta x^\alpha < i^\beta \leq x, \quad y - \beta y^\alpha < j^\beta \leq y, \quad \text{and} \quad z - \beta z^\alpha < k^\beta \leq z. \]

Consequently, in view of the fact that

\[ \ell^\beta - 1 = \ell^{\beta-1}(\beta - 1) \leq w^{(\beta-1)/\beta} = w^\alpha, \]

we conclude that

\[ |x + w - (y + z)| \leq |i^\beta + \ell^\beta - (j^\beta + k^\beta)| + 4\beta w^\alpha \leq 4\beta \ell^{\beta-1} + 4\beta w^\alpha \leq 8\beta w^\alpha \leq 16w^\alpha, \]

where the last inequality follows from (14). This contradicts the assumption that \( S \) is an \((\alpha, 16)\)-strong Sidon set. This contradiction implies that \( S' \) is indeed a Sidon set.

\[ \square \]

We are now ready to prove Theorem 12.

**Proof of Theorem 12.** Let \( S = \{s_1 < s_2 < \ldots \} \subset \mathbb{N} \) be an \((\alpha, 16)\)-strong Sidon set such that

\[ S(n) \geq n^{h(\alpha) + o(1)}. \]

We may suppose that \( S \) is canonical.

Let \( i_j \) be such that \( s_j \in I_{i_j} \). Let \( R = R(\alpha) \) be the random set introduced in Definition 10 and let \( i_0 \) be the integer from Lemma 13. Set

\[ J = \{j : i_j \geq i_0 \text{ and } R \cap I_{i_j} \neq \emptyset\}. \]

For each such \( j \in J \), we select an arbitrary element \( s_j^* \in R \cap I_{i_j} \) and let \( S^* = \{s_j^* \leq s_j < \ldots \} \).

Since \( s_j^* \sim s_j \), Lemma 16 implies that \( S^* \) is a Sidon set.

Next, we estimate \( S^*(n) \). Since \( S \) is canonical, between 1 and \( n \), there are at least

\[ |S(n)| - i_0 \geq n^{h(\alpha) + o(1)} \]

intervals \( I_{i_j} \) with \( S \cap I_{i_j} \neq \emptyset \). Moreover, by Lemma 13, we have

\[ \mathbb{P}(R \cap I_{i_j} \neq \emptyset) \geq 1/3 \]

for every \( j \geq i_0 \). Thus, Chernoff’s bound gives that, for any fixed \( \varepsilon > 0 \) and \( n \geq n(\varepsilon) \),

\[ \mathbb{P}\left[ S^*(n) < n^{h(\alpha) - \varepsilon} \right] \leq 2 \exp \left( -\frac{1}{3} n^{h(\alpha) - \varepsilon} \right) \leq \frac{1}{n^2}. \] (19)

We now recall the well-known Borel–Cantelli lemma.

7
Lemma 17 (Borel–Cantelli Lemma). Let \( \{ F_n \}_{n \in \mathbb{N}} \) be a sequence of events in a probability space. If \( \sum_{n=1}^{\infty} P[F_n] < \infty \), then, with probability 1, only finitely many \( F_n \) occur, i.e.,

\[
P \left( \bigcap_{i \geq 1} \bigcup_{n \geq i} F_n \right) = 0.
\]

Since \( \sum 1/n^2 < \infty \), inequality (19) and the Borel–Cantelli Lemma gives that, with probability 1, the random set \( R \) is such that, for every \( n \geq n_0 = n_0(R) \),

\[
S^*(n) \geq n^{h(\alpha) - \varepsilon}.
\]

This completes the proof of Theorem 12. \( \square \)

3. Proof of Theorem 14

First, we prove the lower bound. Set

\[
J_i = \{ k \in \mathbb{N} : i \lceil n^\alpha \rceil \leq k < (i + 1) \lceil n^\alpha \rceil \},
\]

for \( i \geq 0 \), and let \( \ell \) be the number of intervals \( J_i \) such that \( J_i \subset [n] \). We have

\[
\ell = \left\lfloor \frac{n}{\lceil n^\alpha \rceil} \right\rfloor = n^{1-\alpha}(1 + o(1)).
\]

Let \( I \) be a maximum Sidon set in \( [\ell] \). By results of Chowla, Erdős and Turán and Singer [2, 5, 6, 11], we have

\[
|I| \geq \sqrt{\ell}(1 + o(1)).
\]

Set

\[
T = \{ i \lceil n^\alpha \rceil : i \in I \}.
\]

We claim that \( T \) is an \( (n, \alpha) \)-strong Sidon set. Indeed, if \( a_1, a_2, a_3, a_4 \) are in \( T \), then there are \( j_1, j_2, j_3, j_4 \) with \( a_i = j_i \lceil n^\alpha \rceil \), for \( i = 1, 2, 3, 4 \). Since \( |(j_1 + j_2) - (j_3 + j_4)| \geq 1 \), the statement follows.

Next, we consider the upper bound. We will use a double counting argument. Let \( S \) be an \( (n, \alpha) \)-strong Sidon set. Let

\[
I_x = [x + 1, x + m],
\]

and

\[
P = \left\{ (I_x, \{a, b\}) \mid I_x \cap [n] \neq \emptyset, \{a, b\} \subset I_x \cap S \right\}.
\]

Note that \( I_x \cap [n] \neq \emptyset \) if and only if \( 1 - m \leq x \leq n - 1 \).

We can count \( P \) by considering \( I_x \) first. We have

\[
|P| = \sum_{1 - m \leq x \leq n - 1} \binom{S_x}{2},
\]

where \( S_x = |I_x \cap S| \). Since \( f(t) = \binom{t}{2} \) is convex, we have

\[
|P| \geq (n + m - 1) \binom{\sum S_x}{2}/(n + m - 1).
\]

Since each element in \( S \) appears exactly \( m \) intervals \( I_x \), we have \( \sum S_x = m|S| \). Consequently,

\[
|P| \geq \frac{m|S|}{2(n + m - 1)} (m|S| - (n + m - 1)). \quad (20)
\]
Next, we count \( P \) by considering \( \{a, b\} \) first. A pair \( \{a, b\} \subset S \), with \( 0 < b - a < m \), is contained in \((m - (b - a))\) intervals of \( I_x \). Hence,

\[
|P| = \sum_{\{a, b\} \subset S \atop 0 < b - a < m} (m - (b - a)). \tag{21}
\]

Since \( S \) is an \((n, \alpha)\)-strong Sidon set, each \( b - a \) \((a, b \in S, \ 0 < b - a < m)\) differs from all other \( b' - a' \) \((a', b' \in S, \ 0 < b' - a' < m)\) by at least \( n^\alpha \). Consequently,

\[
\sum_{\{a, b\} \subset S \atop 0 < b - a < m} (b - a) \geq 0 + n^\alpha + \cdots + kn^\alpha = \frac{k(k + 1)}{2} n^\alpha. \tag{22}
\]

where \( k \) is an integer such that

\[
k \alpha < m \leq (k + 1) n^\alpha. \tag{23}
\]

Inequalities (21) and (22) give that

\[
|P| \leq (k + 1) m - \frac{k(k + 1)}{2} n^\alpha \leq \frac{m}{2} \left( \frac{m}{n^\alpha} + 1 \right). \tag{24}
\]

It follows from (20) and (24) that

\[
\frac{m}{2(n + m - 1)} (m|S| - (n + m - 1)) \leq \frac{m}{2} \left( \frac{m}{n^\alpha} + 1 \right),
\]

that is,

\[
|S|^2 - \frac{n + m - 1}{m} |S| - \frac{n + m - 1}{m} \left( \frac{m}{n^\alpha} + 1 \right) \leq 0.
\]

Hence,

\[
|S| \leq \frac{n}{m} + \frac{1}{2} \sqrt{\left( \frac{n}{m} + O(1) \right)^2 + 4 \left( \frac{n}{m} + O(1) \right) \left( \frac{m}{n^\alpha} + 1 \right)}
\]

\[
\leq \frac{n}{m} + \left( \frac{n}{2m} + O(1) \right) + \sqrt{\left( \frac{n}{m} + O(1) \right) \left( \frac{m}{n^\alpha} + 1 \right)}
\]

\[
\leq \frac{3n}{2m} + n^{(1-\alpha)/2} + \sqrt{\frac{n}{m}} + O \left( \sqrt{\frac{m}{n^\alpha}} \right) + O(1),
\]

where the last two inequalities follow from \( \sqrt{x + y} \leq \sqrt{x} + \sqrt{y} \).

By taking \( m = n^{(2+\alpha)/3} \), we have

\[
\frac{n}{m} = n^{1-(2+\alpha)/3} = n^{(1-\alpha)/3} \quad \text{and} \quad \sqrt{\frac{n}{m}} = \sqrt{n^{(2+\alpha)/3-\alpha}} = n^{(1-\alpha)/3}.
\]

Thus,

\[
|S| \leq n^{(1-\alpha)/2} + O \left( n^{(1-\alpha)/3} \right),
\]

which completes the proof of the upper bound in Theorem 4.

4. PROOF OF THEOREM 6

Let \( S \subset \mathbb{N} \) be an \( \alpha \)-strong Sidon set. For all integers \( i \geq 0 \), let

\[
S_i := S \cap (2^i, 2^{i+1}].
\]

Clearly, \( S_i \) is a \((2^i, \alpha)\)-strong Sidon set. Since

\[
S_i - 2^i := \{ s - 2^i : s \in S_i \} \subset [2^i]
\]
is also a \((2^i, \alpha)\)-strong Sidon set, Theorem 14 implies that
\[
|S_i| = |S_i - 2^i| \leq F(2^i, \alpha) \leq 2^{(1-\alpha)/2+1}
\] (25)
for all \(i\) sufficiently large, say, \(i \geq k_0\). Set
\[
c = c(\alpha) = 1 + \frac{2^{(1-\alpha)/2+1}}{2^{(1-\alpha)/2} - 1}.
\]
We infer that, for \(k\) satisfying \((1-\alpha)(k-1)/2 \geq k_0\), we have
\[
S(n) \leq 2^{k_0} + \sum_{k_0 \leq i < k} |S_i| \leq 2^{k_0} + \sum_{0 \leq i < k} 2^{i(1-\alpha)/2+1}
\]
\[
\leq 2^{(1-\alpha)(k-1)/2} + \frac{2 \cdot 2^{(1-\alpha)k/2}}{2^{(1-\alpha)/2} - 1} \leq c 2^{(1-\alpha)(k-1)/2} \leq cn (1-\alpha)/2.
\]
This completes the proof of Theorem 6.

5. Proof of Theorem 9

Lemma 18. Fix \(0 \leq \alpha < 1\). There is a sequence \(a_1 < a_2 < \cdots < a_k < \cdots\) of positive integers with
\[
a_k \leq 6^{1/(1-\alpha)} k^{3/(1-\alpha)}
\] (26)
for every \(k \geq 1\) such that \(S = \{a_k : k \geq 1\}\) is an \(\alpha\)-strong Sidon set.

To derive Theorem 9 from Lemma 18, it suffices to notice that, for every \(k\), the set \(S\) in Lemma 18 is such that \(S(n) \geq S(a_k) = k\) for every \(n \geq 6^{1/(1-\alpha)} k^{3/(1-\alpha)} \geq a_k\). Inequality 5 follows for all large enough \(n\). We now proceed to prove Lemma 18.

Proof of Lemma 18. For simplicity, for every \(k \geq 1\), let \(t_k = 6^{1/(1-\alpha)} k^{3/(1-\alpha)}\) be the value on the right-hand side of (26) and observe for later reference that
\[
t_k = 6k^{3/\alpha} \geq k + 4(k-1)\left(\frac{k-1}{2}\right)(2t_k^{\alpha} + 1).
\] (27)
Let \(a_1 = 1\). Now let \(k \geq 2\) and suppose that we have already have defined \(a_i\) for all \(1 \leq i < k\) in such a way that \(S_{k-1} = \{a_1, \ldots, a_{k-1}\}\) does not contain \(x < y \leq z < w\) violating (1) and, for all \(1 \leq i < k\), we have
\[
a_i \leq t_i
\] (28)
We shall define \(a_k\) ‘greedily’. Let
\[
F_k = \{f \in \mathbb{N} \setminus S_{k-1} : S_{k-1} \cup \{f\}\text{ contains }x < y \leq z < w\text{ violating (1)}\}.
\]
Naturally, if \(f \in F_k\), then we cannot add \(f\) to \(S_{k-1}\) to continue our definition of our \(\alpha\)-strong Sidon set. Let
\[
C_k = \{c \in \mathbb{N} : c \notin S_{k-1} \cup F_k\}
\]
be the set of ‘candidates’ to be added to \(S_{k-1}\). It follows from Claim 19 below that \(C_k\) is non-empty and hence \(\min C_k\) exists. We set \(a_k = \min C_k\). It follows by induction that this procedure defines an infinite \(\alpha\)-strong Sidon set \(S = \{a_k : k \geq 1\}\), with \(a_1 < a_2 < \cdots < a_k < \cdots\). Recall that we have assumed that (28) holds for all \(1 \leq i < k\). We now prove the following claim.
Claim 19. We have \(a_k \leq t_k\).

Clearly, once we have established Claim 19, Lemma follows by induction.

Proof of Claim 19. We first note that it suffices to check that
\[
t_k \geq |S_{k-1}| + |F_k \cap [t_k]| + 1. \tag{29}
\]
Indeed, if (29) holds, then there must be some candidate \(c \in C_k\) for our choice of \(a_k\) with \(c \leq t_k\), and hence \(a_k = \min \{C \leq t_k\}\) follows, as claimed. We now verify (29).

Since \(|S_{k-1}| = k - 1\), our task is to give a suitable upper bound for \(|F_k \cap [t_k]|\). Recall that \(S_{k-1}\) contains no elements \(x < y \leq z < w\) violating (1). On the other hand, if \(f \in F_k \cap [t_k]\), then \(S_{k-1} \cup \{f\}\) does contain such elements \(x < y \leq z < w\), and hence one of \(x, y, z\) or \(w\) must be \(f\). Suppose for instance that \(f = w\). We have at most \((k-1)(k-1)\) choices for \((x, y, z)\). For each such choice, we have
\[
f = y + z - x + f^\alpha = y + z - x + t_k^\alpha,
\]
as \(f \leq t_k\). Thus, the triple \((x, y, z)\) contributes at most \(2t_k^\alpha + 1\) elements \(f\) to the set \(F_k \cap [t_k]\).

We now estimate the number of \(f\) that are included in \(F_k \cap [t_k]\) because they play the role of \(z\) in some quadruple \((x, y, z, w)\) violating (1), where \(x, y\) and \(w\) belong to \(S_{k-1}\). We have
\[
f = x + w - y + w^\alpha = x + w - y + t_k^\alpha,
\]
where we used that \(w \in S_{k-1}\) and hence \(w \leq a_{k-1} \leq t_{k-1} < t_k\). Thus, again, the triple \((x, y, w)\) forbids at most \(2t_k^\alpha + 1\) elements. The analysis is similar for the cases in which \(f = x\) and \(f = y\).

It follows that
\[
|F_k \cap [t_k]| \leq 4(k-1)\left(\frac{k-1}{2}\right)(2t_k^\alpha + 1). \tag{30}
\]
Recalling that \(|S_{k-1}| = k - 1\), we see that inequality (29) follows from (27) and (30). This completes the proof of Claim 19.

The proof of Lemma is complete.

6. PROOF OF THEOREM 7

Recall that Theorem asserts that, for any \(0 < \alpha < 1\), there is an \(\alpha\)-strong Sidon set \(S\) such that, for any \(\varepsilon > 0\), there are arbitrary large \(n\) for which \(S(n)n^{-(1-\alpha)/2} \geq 1/2 - \varepsilon\). That is, (3) holds.

Proof of Theorem 7. Let \(p\) be an odd prime. Erdős (see Chapter II, Theorem 9) constructed a Sidon set \(A_p \subset \mathbb{N}\) with \(|A_p| = p - 1\) such that

1. \(2p^2 < a < 4p^2 - p\) for all \(a \in A_p\), and
2. \(p < |a - a'| < 2p^2 - p\) for all distinct \(a\) and \(a' \in A_p\).

Let
\[
\eta = \frac{\alpha}{1 - \alpha} \quad \text{and} \quad \mu = 4^{\alpha/(1-\alpha)}.
\]
Note for later reference that
\[
(1 + \eta)\alpha = \eta \quad \text{and} \quad \mu = (4\mu)^\alpha. \tag{32}
\]
Consider also the sets
\[
S_p = \{\mu p^2 \eta a: a \in A_p\}. \tag{33}
\]
In order to construct the set $S$ as required in the theorem, we fix a rapidly increasing sequence $(p_n)_{n \geq 1}$ of primes, say, with
\[ p_{n+1} > 4 \mu p_n^{2+2\eta} \quad (34) \]
for all $n \geq 1$, and set
\[ S = \bigcup_{n \geq 1} S_{p_n}. \]
We now state three facts concerning the sets $S_p$ and $S = \bigcup_{n \geq 1} S_{p_n}$.

(a) For every $x \in S_p$, owing to \((i)\) and \((33)\), we have
\[ 2 \mu p^{2+2\eta} < x < 4 \mu p^{2+2\eta} - \mu p^{1+2\eta}. \]

(b) For every $x \in \bigcup_{1 \leq j \leq n} S_{p_j}$ and $y \in S_{p_{n+1}}$, owing to \((i)\) \((33)\) and \((34)\), we have
\[ y - x > 2 \mu p_n^{2+2\eta} - 4 \mu p_n^{2+2\eta} > 2 \mu p_n^{2+2\eta} - p_{n+1}. \]

(c) If $x$ and $y \in S_p$ are distinct, then, owing to \((ii)\) and \((33)\), we have
\[ \mu p^{1+2\eta} < |y - x| < 2 \mu p^{2+2\eta} - \mu p^{1+2\eta}. \]

We now state and prove the following fact, which says that the sets $S_{p_n}$ $(n \geq 1)$ do not 'interact' with one another, in the sense that no 'bad' quadruple $(x, y, z, w)$ can come from distinct sets $S_{p_n}$.

**Fact 20.** Suppose $x, y, z$ and $w \in S = \bigcup_{n \geq 1} S_{p_n}$ with $x < y \leq z < w$ violate the required inequality
\[ |(x + w) - (y + z)| \geq w^\alpha. \] (35)
Let $n \geq 1$ be such that $w \in S_{p_n}$. Then $x, y$ and $z$ belong to $S_{p_n}$ as well.

With Fact 20 at hand, we conclude that no quadruple $(x, y, z, w)$ of elements of $S$ with $x < y \leq z < w$ can violate \((35)\). Indeed, Fact 20 tells us that, for such a violation to happen, there must be $p = p_n$ such that all of $x, y, z$ and $w$ belong to $S_p$. Since $A_p$ is a Sidon set, we have
\[ |(x + w) - (y + z)| \geq \mu p^{2+2\eta} \quad (4 \mu p^{2+2\eta})^\alpha \geq w^\alpha, \]
verifying \((35)\). We conclude that $S = \bigcup_{n \geq 1} S_{p_n}$ is an $\alpha$-strong Sidon set. We now prove Fact 20.

**Proof of Fact 20.** For simplicity, let $p = p_n$ so that $w \in S_{p_n}$. We shall rule out the three cases in which $\{|x, y, z, w| \cap S_p\} = 1, 2$ and 3. Suppose first that $\{x, y, z, w\} \cap S_p = \{w\}$.

Then $w - y > 2 \mu p^{2+2\eta} - p$, while $z - x < 4 \mu p_n^{2+2\eta} < p_n = p$. Consequently, $|(x + w) - (y + z)| > 2 \mu p^{2+2\eta} - 2p \geq \mu p^{2+2\eta} \quad (4 \mu p^{2+2\eta})^\alpha \geq w^\alpha$. Suppose now that $\{x, y, z, w\} \cap S_p = \{z, w\}$.

Then $w - z > 2 \mu p^{1+2\eta}$, while, as before, $y - x < 4 \mu p_n^{2+2\eta} < p_n = p$. Hence, $|(x + w) - (y + z)| > \mu p^{1+2\eta} - p > \mu p^{2+2\eta} \quad (4 \mu p^{2+2\eta})^\alpha \geq w^\alpha$. Finally, suppose $\{x, y, z, w\} \cap S_p = \{y, z, w\}$. Then
\[ w - z < 2 \mu p^{2+2\eta} - \mu p^{1+2\eta}, \quad \text{while} \quad y - x > 2 \mu p^{2+2\eta} - p, \quad \text{and hence} \quad |(x + w) - (y + z)| > \mu p^{1+2\eta} - p > \mu p^{2+2\eta} \quad (4 \mu p^{2+2\eta})^\alpha \geq w^\alpha. \]

It now remains to prove \((3)\). Note that \((a)\) above implies that, in an interval of the form $(n, (2 + o(1))n)$, where $n = 2 \mu p^{2+2\eta}$ and $o(1) \rightarrow 0$ as $n \rightarrow \infty$, we have $p - 1$ elements of $S$.  

12
However,
\[ p - 1 = (1 + o(1)) \left( \frac{n}{2\mu} \right)^{1/(2+2\eta)} (1 + o(1)) \left( \frac{n}{2\mu} \right)^{(1-\alpha)/2} \]
\[ = \left( \frac{1}{(4\mu)^{(1-\alpha)/2}} + o(1) \right) (2n)^{(1-\alpha)/2} (1 + o(1)) (2n)^{(1-\alpha)/2}, \]
and (3) follows. \( \square \)

7. CONSTRUCTION OF A DENSE STRONG SIDON SET

In this section, we construct a dense strong Sidon set for a small \( \alpha \), which implies Theorem 8.

Let \( b \geq 5 \) (36) be an integer, fixed throughout this section, and let \( \alpha \) be such that
\[ b = \left\lfloor \frac{1}{6\sqrt{\alpha}} \right\rfloor. \] (37)

For \( m_0 = 2^{10064} \), (38) we are going to construct a mapping \( \phi : \mathbb{N} \geq m_0 \rightarrow \mathbb{N} \) such that, for a Sidon set \( S \subset \mathbb{N} \geq m_0 \), the set \( \tilde{S} = \{ \tilde{m} = \phi(m) : m \in S \} \) is an \( \alpha \)-strong Sidon set. Furthermore, the map \( \phi \) will satisfy the property that \( \phi(m) = \tilde{m} = O(m^{1+5/b}) \) (see Fact 24). Therefore, the \( \alpha \)-strong Sidon set \( \tilde{S} \) will be denser for larger \( b \).

7.1. Construction of \( \phi \). In order to describe the map \( \phi = \phi(b) \), we need to introduce several definitions. For a positive integer \( m \), let \( a_r a_{r-1} \ldots a_2 a_1 \) be its binary expansion:
\[ m = (a_r a_{r-1} \ldots a_2 a_1)_2 = a_r 2^{r-1} + \cdots + a_2 2 + a_1, \] (39)
where \( a_r \neq 0 \). Note that
\[ 2^{r-1} \leq m < 2^r. \] (40)

In what follows, we shall often identify the binary expansion of a positive integer \( m \) with the integer \( m \) itself. We shall write \( r = r(m) \) for the number of bits in the binary expansion of \( m \). Furthermore, we let \( t = t(m) \) be the largest integer such that
\[ 2^t \leq \frac{r}{3b} < 2^{t+1}, \]
and let
\[ s = s(m) = 2^t. \] (41)

Note that
\[ \frac{r}{6b} < s \leq \frac{r}{3b}. \] (42)

If \( m \geq m_0 = m_0(b) \), then \( s = s(m) \geq s_0(b) \) for some \( s_0(b) \).

To define \( \tilde{m} = \phi(m) \), we describe the binary expansion of \( \tilde{m} \) from the binary expansion of \( m \).

Formally speaking, binary expansions (or representations) of positive integers will be considered to be words in \( \{0, 1\}^* = \bigcup_{t \geq 0} \{0, 1\}^t \). Given a word \( w \), we shall write \( \|w\| \) for the length of \( w \).

We shall sometimes add 0s to the left of the binary expansion of a number to make it have a suitable length.
Let $m$ have binary expansion $a_ra_{r-1}\ldots a_1$. Add a suitable number $x$, with $0 \leq x < b$, of 0
bits to the left of the expansion of $m$ to obtain a word whose length is a multiple of $b$. We now
factor this word as

$$A_RA_{R-1}\ldots A_2A_1,$$

where each $A_i = A_i(m)$ is of length $b$ (see Figure 1). Note that $A_R$ contains a 1 bit. We call
the $b$-factorization of $m$. Note that $r \leq R < r + 1$.

To describe the binary expansion of $\tilde{m}$, we first define $2s$ bits $c_j$. Let $c_j \in \{0, 1\}$ ($1 \leq j \leq 2s$)
be defined by

$$c_{2s}c_{2s-1}\ldots c_{s+1}c_s\ldots c_1 = a_s a_{s-1} \ldots a_2 a_1 0^s.$$  

Note that the word in (45) is obtained as follows: we first write the $s$ least significant bits of $m$
and then we add a string of 0s of length $s$. Clearly, we thus obtain a word of length $2s$. It will
be convenient to refer to the $s$ least significant bits $a_s, \ldots, a_1$ of $m$ as the weak bits of $m$. The
remaining bits of $m$ will be referred to as the strong bits of $m$. As it turns out, we shall often
be interested in the bit $a_{s+1}$, that is, in the weakest strong bit of $m$.

Next we define the 5-bit words $C_i = C_i(m)$ ($1 \leq i \leq 2s$). Let us write $C_{i,j}$ for the $j$th bit
of $C_i$, that is, let

$$C_i = C_{i,5}C_{i,4}C_{i,3}C_{i,2}C_{i,1},$$

For $i > 2s$, we let $C_i = 0^5 = 00000$. For $1 \leq i \leq 2s$, the definition of the bits of $C_i$ is as follows:

$$C_{i,5} = C_{i,3} = C_{i,1} = 0,$$

$$C_{i,4} = c_i \quad \text{(recall (45))},$$

$$C_{i,2} = \begin{cases} 1 & \text{if } i = s, \\ 0 & \text{otherwise.} \end{cases}$$

Figure 1. The binary expansions of $m$ and $\tilde{m}$.
We now define the map \( \phi : \mathbb{N}_{\geq m_0} \to \mathbb{N} \).

**Definition 21.** Let \( m \) be any positive integer with \( m \geq m_0 \). Let \( [13] \) be its \( b \)-factorization. We let

\[
\phi(m) = \tilde{m} = A_R C_{R-1} A_{R-1} \ldots C_2 A_2 C_1 A_1,
\]

where the \( C_i \) are as defined above.

For convenience, the 5-bit blocks \( C_i \) in \([47]\) are referred to as \( C \)-blocks, while the \( b \)-bit blocks \( A_i \) are referred to as \( A \)-blocks. Note that, when we construct \( \tilde{m} \) from \( m \), the bits \( a_i \) of \( m \) are placed in ‘new positions’, with every bit moved some positions to the left, because of the insertion of the \( C \)-blocks: the bits in \( A_1 \) stay in the same positions, the bits in \( A_2 \) move 5 positions to the left, and, more generally, the bits in \( A_j \) move \( 5(j - 1) \) positions to the left. Also, the weak bits of \( m \) are copied in the middle of \( \phi(m) \) (see Figure 1).

7.2. Preliminary remarks on \( \phi \). We now state some elementary facts about the function \( \phi \). This section may help the reader get a feeling on how \( \phi(m) = \tilde{m} \) relates to \( m \). However, readers who prefer to see immediately how \( \phi \) is used in the proof of Theorem 8 may consider skipping this section and going directly to Section 7.3.

We start with the following immediate fact.

**Fact 22.** If we know all the bits of \( \tilde{m} = \phi(m) \) \((m \geq m_0)\), we can recover \( m \).

In fact, we are going to observe that one does not need to know all bits of \( \tilde{m} \) to recover \( m \). In order to formulate our claim, consider the \( A \)-block \( A_j \) containing the weakest strong bit \( a_{s+1} \) and observe that

\[
j = \lceil (s + 1)/b \rceil < s.
\]

We will observe that if we are given a word \( \tilde{m} \) with some (but possibly not all) bits on the right from the image of \( a_{s+1} \) “erased” (i.e., instead of 0 or 1 on the bit’s spot, we see the “neutral” symbol *), we can still recover \( m \).

To this end, we first observe that \( \tilde{m} \) has length \( r + 10s \), however, since all we know about the relation of \( r \) and \( s \) is that \( 3bs \leq r < 6bs \), we cannot recover the value of \( r \) and \( s \) just from the information about the length of \( \tilde{m} \). However, since \( j = \lceil (s + 1)/b \rceil < s \),

\[
\text{all } C_s, C_{s+1}, \ldots, C_{2s} \text{ are on the left from } A_j.
\]

Since \( C_s \) is the unique \( C \)-block with \( C_{1:2} = 1 \) and nothing was erased from \( C_s \), we can determine the value of \( s \) from its location (see Figure 1). This allows us to find the value \( a_{s+1} \) as well as all \( a_i \) for \( i \geq s + 1 \). On the other hand, the information about \( a_1, a_2, \ldots, a_s \) is encoded in \( C_{s+1}, C_{s+2}, \ldots, C_{2s} \), and consequently we can recover \( m \). This implies the following.

**Fact 23.** If we know all the bits of \( \tilde{m} = \phi(m) \) except for the \((1 + 5/b) s - 5 \) least significant bits of \( \tilde{m} \), then we can recover \( m \).

**Proof.** Recall that \( A_j \) is the \( A \)-block containing the weakest strong bit \( a_{s+1} \) of \( m \). Since the number of \( C \)-blocks to the right of \( a_{s+1} \) in \( \tilde{m} \) is \( j - 1 \), the position of \( a_{s+1} \) in \( \tilde{m} \) is

\[
(s + 1) + 5(j - 1) = s + 5j - 4 \geq s + \frac{5(s + 1)}{b} - 4 \geq \left(1 + \frac{5}{b}\right)s - 4,
\]

where \( j = \lceil (s + 1)/b \rceil \). Hence, the number of least significant bits in \( \tilde{m} \) we need not know to recover \( m \) is at least \((1 + 5/b) s - 5\). \( \square \)
Next we show that $\tilde{m}$ is not much larger than $m$ if $b$ is large.

**Fact 24.** We have $m^{1+5/b}/64 < \tilde{m} < 4m^{1+5/b}$.

*Proof.* Let $r$ be the number of bits in $m$, and let $\tilde{r}$ be the number of bits in $\tilde{m}$. Recalling (40), we have

$$2^{r-1} \leq m < 2^r \quad \text{and} \quad 2^{\tilde{r}-1} \leq \tilde{m} < 2^{\tilde{r}}. \quad (49)$$

For each factor $A_i$ ($1 \leq i \leq R - 1$) of $m$ of length $b$, we add a factor $C_j$ of length 5 to construct $\tilde{m}$. Hence, we have that $\tilde{r} = r + 5(R - 1)$. Therefore, (44) gives that

$$r (1 + 5/b) - 5 \leq \tilde{r} < r (1 + 5/b). \quad (50)$$

This together with (49) and $b \geq 5$ completes the proof of Fact 24. □

**7.3. Key lemma and proof of Theorem 8.** The construction of $\tilde{m}$ lets us prove the following result.

**Lemma 25** (Key lemma). Let $b$ and $m_0 = m_0(b)$ be as in (36) and (38). Let $S \subset \mathbb{N}_{\geq m_0}$ be a Sidon set and let $\tilde{S} = \{\tilde{m}: m \in S\}$. For $\tilde{m}_i \in \tilde{S}$ ($1 \leq i \leq 4$) with $\tilde{m}_1 < \tilde{m}_2 < \tilde{m}_3 < \tilde{m}_4$, we have

$$|\tilde{m}_4 - (\tilde{m}_3 - \tilde{m}_2)| \geq 2^\ell, \quad (51)$$

where $\ell = [(1 + 5/b)r(\tilde{m}_4)/(36b^2)] - b - 6$.

The proof of Lemma 25 will be given in Section 7.4. We now show that Lemma 25 may be used to construct strong Sidon sets.

**Lemma 26.** Let $\alpha$ with $0 < \alpha \leq 10^{-4}$ be given. Let $m_0$ be as in (38). Let

$$b = \lceil 1/(6\sqrt{\alpha}) \rceil \geq 5. \quad (52)$$

If $S \subset \mathbb{N}_{\geq m_0}$ is a Sidon set, then $\tilde{S} = \{\tilde{m}: m \in S\}$ is an $\alpha$-strong Sidon set. Moreover,

$$\tilde{S}(n) = S \left( \left\lfloor \frac{n}{4} \right\rfloor ^{1/(1+5/b)} \right). \quad (53)$$

*Proof.* Before we start, we note that the assumption $0 < \alpha \leq 10^{-4}$ guarantees that $1/(6\sqrt{\alpha}) \geq 5$, with plenty of room. We claim that $\tilde{S}$ is an $\alpha$-strong Sidon set, i.e.,

$$|\tilde{m}_1 + \tilde{m}_4 - (\tilde{m}_2 + \tilde{m}_3)| \geq \tilde{m}_4^\alpha$$

for $\tilde{m}_1, \tilde{m}_2, \tilde{m}_3, \tilde{m}_4 \in \tilde{S}$ with $\tilde{m}_1 < \tilde{m}_2 \leq \tilde{m}_3 < \tilde{m}_4$. Indeed, Lemma 25 gives that

$$\log_2 (|\tilde{m}_1 + \tilde{m}_4 - (\tilde{m}_2 + \tilde{m}_3)|) \geq \left\lceil \frac{1 + 5/b}{36b^2} r(\tilde{m}_4) \right\rceil - b - 6 \geq \frac{r(\tilde{m}_4)}{36b^2},$$

where the last inequality follows from (38), i.e., $r(\tilde{m}_4) \geq r(m_0) \geq 100b^4$. Consequently, in view of $\tilde{m} < 2r(\tilde{m})$ and (52), we infer that

$$|\tilde{m}_1 + \tilde{m}_4 - (\tilde{m}_2 + \tilde{m}_3)| \geq \tilde{m}_4^{1/(36b^2)} \geq \tilde{m}_4^\alpha.$$

Next, we consider the counting function $\tilde{S}(n)$. One can easily check that for any $m \leq (n/4)^{b/(b+5)}$ Fact 24 implies that $\tilde{m} \leq n$. In otherwords, for any $m \in S \cap [(n/4)^{b/(b+5)]}$, its $\phi$-image $\phi(m) = \tilde{m}$ is contained in $[n]$. Since $\phi$ is one-to-one, we obtain (53), as desired. □

We now prove Theorem 8 combining Ruzsa’s theorem [10] and Lemma 26.
Proof of Theorem 8. Ruzsa’s theorem guarantees the existence of a Sidon set $S$ satisfying

$$S(n) \geq n^{\sqrt{2-1+o(1)}}.$$ 

Recall (37) and note that, for $\alpha \leq 10^{-4}$, we have

$$\frac{5}{b} = \frac{5}{[1/6\sqrt{\alpha}]} \leq 32\sqrt{\alpha}.$$ 

Using (54), we see that the set $\tilde{S}$ given by Lemma 26 is an $\alpha$-strong Sidon set with

$$\tilde{S}(n) = S\left(\left\lfloor \frac{n}{4} \right\rfloor^{1/(1+5/b)} \right) \geq n^{(\sqrt{2-1+o(1)})/(1+5/b)} \geq n^{(\sqrt{2-1+o(1)})/(1+32\sqrt{\alpha})},$$

as required. □

7.4. Proof of Lemma 25. Before addressing inequality (51), we will show that, similarly as in the proof of Fact 22, one can recover $m+m'$ from partial information of $\bar{m}+\bar{m}' = \phi(m)+\phi(m')$. First, we define notation for binary expansions of sums of the form $\bar{m}+\bar{m}' = \phi(m)+\phi(m')$, and therefore it will be convenient to describe such expansions explicitly. Suppose $m \geq m'$.

Recall (39) and similarly let

$$m' = a'_r a'_{r-1} \ldots a'_1.$$ 

Consider the $b$-factorization $A_R A_{R-1} \ldots A_2 A_1$ (as in (43)) of $m$ and let the $b$-factorization of $m'$ be

$$A'_R A'_{R-1} \ldots A'_2 A'_1.$$ 

Since we suppose $m \geq m'$, we have $R \geq R'$. Now let $C'_i$ be the $C$-blocks in the binary expansion of $\bar{m}'$, so that

$$\bar{m}' = A'_R C'_{R-1} A'_{R-1} \ldots A'_2 C'_1 A'_1.$$ 

For convenience, let us set $A'_i = 0^b$ for every $i > R'$ and recall that we let $C'_i = 0^b$ for every $i > 2s(m')$ and hence, in particular, $C'_i = 0^b$ for every $i \geq R'$. For every $1 \leq i \leq R$, we let

$$a_i^+ = \begin{cases} 
0 & \text{if } A_i + A_i' < 2^b, \\
1 & \text{otherwise,}
\end{cases}$$

$$C_i^+ = C_i + C_i' + a_i'^{-1},$$

$$A_i^+ = (A_i + A_i') \mod 2^b.$$ 

Note that $a_i^+$ is a carry. One sees that the binary expansion of $\bar{m}+\bar{m}'$ is

$$a_R^+ A_R^+ C_{R-1}^+ A_{R-1}^+ \ldots A_2^+ C_1^+ A_1^+.$$ 

It will be convenient to extend the notion of ‘$C$-blocks’ to the binary expansion of $\bar{m}+\bar{m}'$: those are the $5$-bit blocks $C_i^+$ in (58). Similarly, the ‘$A$-blocks’ of $\bar{m}+\bar{m}'$ are the $b$-bit strings $A_i^+$ in (58).

The next fact tells that we can recover $m+m'$ from $\bar{m}+\bar{m}'$. It is a little less trivial than Fact 22 since we need to consider carries.

Fact 27. If we know all the bits of the sum $\bar{m}+\bar{m}' = \phi(m)+\phi(m')$, then we can recover $m+m'$.

Proof. Suppose $\bar{m}+\bar{m}'$ has binary expansion (58). It is clear that the $b$-bit string $A_i^+$ in (58) is formed by the $b$ least significant bits of $m+m'$. Moreover, we can tell whether there is a carry to the $(b+1)$st bit when we add the $b$ least significant bits of $m$ and $m'$ by examining the rightmost
bit of $C_{1}^{+}$ in (55). This information and $A_{2}^{+}$ let us determine the next least significant $b$ bits of $m + m'$. Proceeding this way, we are able to determine all the bits of $m + m'$.

We will prove a strengthened version of Fact 27 similar to Fact 23: we need not know a certain number of the least significant bits of $\tilde{m} + \tilde{m}'$ to recover $m + m'$. Recall the notation (55)–(58).

**Lemma 28.** Let $m$ and $m'$ be such that $m, m' \geq m_0$ and $\tilde{m} \geq \tilde{m}'$. Let $A_{j}'$, be the $A$-block of $m'$ that contains the weakest strong bit of $m'$. Then $a_{R}^{+}$, $C_{i}^{+}$ and $A_{i}^{+}$ ($j' \leq i \leq R$) as defined in (56)–(57) determine $m + m'$ uniquely.

**Proof.** Suppose we know $a_{R}^{+}$, $C_{i}^{+}$ and $A_{i}^{+}$ ($j' \leq i \leq R$). We have to recover the bits of $m + m'$ from this data. First we claim that we can determine $s = s(m)$ and $s' = s(m')$. Note first that $\tilde{m} \geq \tilde{m}'$ implies that $s \geq s'$. From (48), observe that the C-blocks $C_{s}^{+}$ and $C_{s'}^{+}$ are placed in the left of $A_{j}'$. Moreover, it follows from the definition of $C_{i,2}$ (1 $\leq i \leq 2s$) and $C_{i,2}'$ (1 $\leq i \leq 2s'$) that there are at most two indices $i$ such that $C_{i,2}^{+} \neq 0$. If $s \neq s'$, then there are exactly two indices $i$ such that $C_{i,2}^{+} = 1$. In this case, one is $s$ and the other is $s'$. On the other hand, if $s = s'$, then there is only one index $i$ such that $C_{i,3}^{+} = 1$. In this case we have $s = s' = i$. In either case, we can thus recover $s$ and $s'$ from the given data.

Next we claim that one can recover the value of $a_{i} + a_{i}'$ for all $i$ (1 $\leq i \leq s'$). We distinguish two cases.

- If $s = s'$, then $C_{i}^{+}$ ($s = 1 \leq i \leq 2s$) determines $a_{1} + a_{1}'$, $a_{2} + a_{2}'$, $\ldots$, $a_{s} + a_{s}'$. This is because $C_{i}$ and $C_{i}'$ contain $a_{i}$ and $a_{i}'$ for all $1 \leq i \leq s = s'$.
- If $s > s'$, then we must have $s \geq 2s'$ since $s$ and $s'$ are powers of 2 (recall (41)). Therefore, the C-blocks $C_{i}$ ($s + 1 \leq i \leq 2s$) of $m$ and the C-blocks $C_{i}'$ ($s' + 1 \leq i \leq 2s'$) of $m'$ do not 'overlap’. Recall that the bits $c_{i}$ (1 $\leq i \leq s$) in the definition of the $C_{i}$ (1 $\leq i \leq s$) are all 0 (see (45) and (46)). Consequently, we deduce that, examining $C_{1}^{+}$ ($s' + 1 \leq i \leq 2s'$), we are able to recover all the weak bits $a_{i}'$ (1 $\leq i \leq s'$) of $m'$. On the other hand, since $C_{i}' = 0^{5}$ for every $i > 2s'$, we can also recover all the weak bits $a_{i}$ (1 $\leq i \leq s$) of $m$ by examining $C_{1}^{+}$ ($s + 1 \leq i \leq 2s$). Thus we can recover all the values of $a_{i} + a_{i}'$ for all $i$ (1 $\leq i \leq s'$).

The claim above implies that we can recover $A_{1}^{+}$ for every 1 $\leq i \leq j' - 1$. Recall that we know $a_{R}^{+}$, $C_{i}^{+}$ and $A_{i}^{+}$ ($j' \leq i \leq R$). A little thought considering carries shows that we can recover $m + m'$, which completes the proof of Lemma 28.

**Lemma 28** easily follows the following.

**Lemma 29.** If we know all the bits of $\tilde{m} + \tilde{m}' = \phi(m) + \phi(m')$ except for the $(1 + 5/b) s' - b - 4$ least significant bits of $\tilde{m} + \tilde{m}'$, then we can recover $m + m'$.

**Proof.** Lemma 28 implies that the number of least significant bits of $\tilde{m} + \tilde{m}'$ we need not know to recover $\tilde{m} + \tilde{m}'$ is

$$||C_{j'-1}A_{j'-1} \ldots C_{1}A_{1}|| = (b + 5)(j' - 1),$$

where $s' = s(m')$ and $j' = \lceil (s' + 1)/b \rceil$. Consequently,

$$(b + 5)(j' - 1) = (b + 5) \left( \left\lceil \frac{s' + 1}{b} \right\rceil - 1 \right) \geq (b + 5) \left( \frac{s' + 1}{b} - 1 \right) \geq \left( 1 + \frac{5}{b} \right) s' - b - 4.$$
In order to show (51) of Lemma 25, the number of least significant bits in \( \tilde{m} + \tilde{m}' \) we need not know to recover \( m + m' \) has to be expressed as a parameter of \( m \) rather than \( m' \).

**Lemma 30.** Let \( m \) and \( m' \) be such that \( m, m' \geq m_0 \) and \( \tilde{m} \geq \tilde{m}' \). If we know all the bits of \( \tilde{m} + \tilde{m}' \), except for the \( \lfloor (1 + 5/b) r(\tilde{m})/(36b^2) \rfloor - b - 6 \) least significant ones, then we can recover \( m + m' \).

**Proof.** We consider two cases depending on the values of \( \tilde{m}' \) and \( \tilde{m} \). Roughly speaking, the first case is when \( \log m' \lesssim (\log m)/b \), and the second case is when \( \log m' \gtrsim (\log m)/b \).

- **Case 1:** First we suppose that
  \[
  \log_2 \tilde{m}' \leq (1 + 5/b) s - b - 5
  \]
  for \( s = s(m) \). Since \( \|A_i\| = b \) and the least significant bit of a \( C \)-block is 0, carries may happen in a row at most \( b \) times (see Figure 2).

  Since \( \log_2 \tilde{m}' \leq (1 + 5/b) s - b - 5 \), the binary expansion of \( \tilde{m} + \tilde{m}' \) is the same as \( \tilde{m} \) except for \( (1 + 5/b) s - 5 \) least significant bits. Hence, Fact 23 implies that we can recover \( m \). Thus we can obtain \( \tilde{m} \), and then we recover \( \tilde{m}' = (\tilde{m} + \tilde{m}') - \tilde{m} \). Fact 22 gives that \( \tilde{m}' \) determines \( m' \), and hence, we can determine \( m + m' \).

- **Case 2:** We suppose that
  \[
  \log_2 \tilde{m}' > (1 + 5/b) s - b - 5.
  \]
  Inequalities (40) and (42) give that
  \[
  \log_2 \tilde{m}' \leq \tilde{r}' \leq 6bs',
  \]
  and hence,
  \[
  s' > \frac{1 + 5/b}{6b} s - 1.
  \]
  Lemma 29 implies that the number of least significant bits of \( \tilde{m} + \tilde{m}' \) we need not know to recover \( m + m' \) is
  \[
  \left( 1 + \frac{5}{b} \right) s' - b - 4 \geq \frac{(1 + 5/b)^2}{6b} (s - b - 6) \geq \left( 1 + \frac{5/b}{6b} \right)^2 r - b - 6 \geq \frac{1 + 5/b}{36b^2} r - b - 6,
  \]
  which completes the proof of Lemma 30. \( \Box \)

It only remains to show that Lemma 30 implies Lemma 25.
Proof of Lemma 24. Fix \( \tilde{m}_i \in \tilde{S} \) (1 ≤ \( i \) ≤ 4) with \( \tilde{m}_1 < \tilde{m}_2 \leq \tilde{m}_3 < \tilde{m}_4 \) and let \( m, \mu, \mu', m' \in S \) be such that

\[
\tilde{m} = \tilde{m}_4, \quad \tilde{\mu} = \tilde{m}_3, \quad \tilde{\mu}' = (\tilde{\mu}') = \tilde{m}_2 \quad \text{and} \quad \tilde{m}' = (\tilde{m}') = \tilde{m}_1.
\]

Recall that

\[
\ell = \left\lfloor \frac{1 + 5/b}{36b^2} - r(\tilde{m}) \right\rfloor - b - 6.
\]

Suppose, for a contradiction, that

\[
| (\tilde{m}_1 + \tilde{m}_4) - (\tilde{m}_2 + \tilde{m}_3) | = | (\tilde{m}_1 + \tilde{m}') - (\tilde{\mu} + \tilde{\mu}') | < 2^\ell.
\]

In other words, \( \tilde{m} + \tilde{m}' \) and \( \tilde{\mu} + \tilde{\mu}' \) have the same binary expansion except possibly for the \( \ell \) least significant bits. Lemma 30 gives that \( m + m' = \mu + \mu' \), which contradicts the assumption that \( S \) is a Sidon set. \( \square \)

8. CONCLUDING REMARKS

Erdős proved that ‘\( \limsup \)’ in \(^1\) cannot be replaced by ‘\( \lim \)’. Indeed, he showed that any Sidon set \( S \subset \mathbb{N} \) is such that

\[
\liminf_{n \to \infty} S(n)n^{-1/2}\sqrt{\log n} < \infty
\]

(see \(^{12} \) p. 133 or \(^7 \) Chapter II, Theorem 8)). It is natural to ask whether a similar result holds for strong Sidon sets: is it true that, for any \( \alpha \)-strong Sidon set \( S \subset \mathbb{N} \) (0 ≤ \( \alpha < 1 \)), we have

\[
\liminf_{n \to \infty} S(n)n^{-(1-\alpha)/2} = 0?
\]

Although we have been able to transfer Ruzsa’s result for Sidon sets to \( \alpha \)-strong Sidon sets, the density of our resulting \( \alpha \)-strong Sidon set decreases fast as \( \alpha \) increases. It would be interesting to obtain better constructions that would yield a much slower density degradation as \( \alpha \) increases. As discussed in Section \(^2\) this would have an interesting consequence concerning the density of Sidon sets contained in infinite random sets of integers.

REFERENCES

4. J. Cilleruelo and R. Tesoro, Dense infinite \( B_h \) sequences, Publ. Mat. 59 (2015), no. 1, 55–73. \(^1\)
5. P. Erdős, On a problem of Sidon in additive number theory and on some related problems. Addendum, J. London Math. Soc. 19 (1944), 208. \(^3\) \(^3\)
6. P. Erdős and P. Turán, On a problem of Sidon in additive number theory, and on some related problems, J. London Math. Soc. 16 (1941), 212–215. \(^3\) \(^3\)
7. H. Halberstam and K. F. Roth, Sequences, second ed., Springer-Verlag, New York, 1983. \(^3\) \(^3\)
8. Y. Kohayakawa, S. J. Lee, C. G. Moreira, and V. Rödl, Infinite Sidon sets contained in sparse random sets of integers, SIAM J. Discrete Math. 32 (2018), no. 1, 410–449. \(^3\) \(^3\) \(^3\) \(^3\)
9. F. Krückeberg, \( B_2 \)-Folgen und verwandte Zahlenfolgen, J. Reine Angew. Math. 206 (1961), 53–60. \(^1\)
10. I. Z. Ruzsa, An infinite Sidon sequence, J. Number Theory 68 (1998), no. 1, 63–71. \(^1\) \(^1\) \(^7\) \(^3\)
11. J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938), no. 3, 377–385. \(^1\) \(^1\)

Instituto de Matemática e Estatística, Universidade de Säo Paulo, Rua do Matão 1010, 05508–090 Säo Paulo, Brazil.

Email address: yoshi@ime.usp.br

Department of Mathematics, DukSung Women’s University, Seoul, South Korea.

Email address: sanglee242@duksung.ac.kr, sjlee242@gmail.com

Instituto de Matemática Pura e Aplicada, Rio de Janeiro, Brazil.

Email address: gugu@impa.br

Department of Mathematics, Emory University, Atlanta, GA 30322, USA.

Email address: rodl@mathcs.emory.edu