On strong Sidon sets of integers*

Yoshiharu Kohayakawa[a], Sang June Lee[b], Carlos Gustavo Moreira[c,d], Vojtěch Rödl[e]

[a] *Instituto de Matemática e Estatística, Universidade de São Paulo, Rua do Matão 1010, 05508–090, São Paulo, Brazil*
[b] *Department of Mathematics, Kyung Hee University, Seoul, South Korea*
[c] *School of Mathematical Sciences, Nankai University, Tianjin, 300071, P. R. China*
[d] *IMPA, Estrada Dona Castorina, 110, 22460-320, Rio de Janeiro, Brazil*
[e] *Department of Mathematics, Emory University, Atlanta, GA, 30322, USA*

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 *α-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 α-strong Sidon sets contained in $[n]$.

Keywords: Sidon sets, random sets of integers, binary expansion
2000 MSC: 11B30, 05D40

*The first author was partially supported by CNPq (311412/2018-1, 423833/2018-9) and FAPESP (2018/04876-1). The second author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2019R1F1A1058860) and by Korea Electric Power Corporation (Grant number:R18XA01). The third author was partially supported by CNPq and FAPERJ. The fourth author was supported by the NSF grant DMS 1764385. This research was partially supported by CAPES (Finance Code 001). FAPESP is the São Paulo Research Foundation. CNPq is the National Council for Scientific and Technological Development of Brazil.

Email addresses: `yoshi@ime.usp.br` (Yoshiharu Kohayakawa), `sjlee242@khu.ac.kr`, `sjlee242@gmail.com` (Sang June Lee), `gugu@impa.br` (Carlos Gustavo Moreira), `vrodl@emory.edu` (Vojtěch Rödl)

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, 4, 5, 12] proved that the maximum cardinality of a Sidon set contained in $[n]$ is $\sqrt{n} + O(n^{1/4})$. 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 $S \subset \mathbb{N}$. We will discuss on this later in the paragraph before Theorem 8.

In connection with the study of Sidon sets contained in randomly generated, infinite sets of integers, we considered the following related concept in [9].

Definition 1 (α-strong Sidon sets)**.** *Fix a constant α with $0 \leq \alpha < 1$. A set $S \subset \mathbb{N}$ is called an* α-strong Sidon set *if*

$$|(x + w) - (y + z)| \geq w^{\alpha} \tag{1}$$

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

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

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

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

$$n^{(1-\alpha)/2} + O\left(n^{(1-3\alpha)/2} + n^{(1-\alpha)/4}\right) \le F(n,\alpha) \le n^{(1-\alpha)/2} + O\big(n^{(1-\alpha)/3}\big).$$

Theorem 4 is proved in Section 2. 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*

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

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

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

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

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

The proof of Theorem 6 is given in Section 3. We now turn to the existence of dense, infinite α-strong Sidon sets. We first consider an analogue of a result of Erdős (see [13, p. 132] or [7, Chapter II, Theorem 9]), who proved that there is a Sidon set $S \subset \mathbb{N}$ such that

$$\limsup_n S(n)n^{-1/2} \ge \frac{1}{2} \tag{2}$$

(see also [10], 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 α-strong Sidon set $S \subset \mathbb{N}$ such that*

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

Theorem 7 is proved in Section 5 (improving the constant $1/2$ in (3) to $1/\sqrt{2}$, in the spirit of [10], 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 $S(n) \ge n^{1/2-\varepsilon}$ for every $n \ge n_0(\varepsilon)$? In this direction, improving a classical result of Ajtai, Komlós and Szemerédi [1], Ruzsa [11] proved the existence of Sidon sets $S \subset \mathbb{N}$ with

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

for every n, where $o(1) \to 0$ as $n \to \infty$ (see also [3]). 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 α-strong Sidon set $S \subset \mathbb{N}$ such that*

$$S(n) \geq n^{(\sqrt{2}-1+o(1))/(1+32\sqrt{\alpha})} \tag{4}$$

for every n.

The proof of Theorem 8, which is partly inspired by Ruzsa's construction in [11], is given in Section 6. Unfortunately, the bound given in (4) gives the best known result only for small values of α. More precisely, the following result, which can be proved with a simple greedy argument (see Section 4), gives a better bound for $\alpha \geq 5.75... \times 10^{-5}$.

Theorem 9. *For every $0 \leq \alpha < 1$, there exists an α-strong Sidon set $S \subset \mathbb{N}$ such that*

$$S(n) \geq \frac{1}{2} n^{(1-\alpha)/3} \tag{5}$$

for every sufficiently large n.

This paper is organised as follows. Sections 2 to 5 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 6. In Section 7, we discuss the connection between strong Sidon sets and an extremal problem on random sets of integers investigated in [9]. 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. Proof of Theorem 4

First, we prove the lower bound. Set

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

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

$$\ell = \left\lfloor \frac{n}{\lceil n^\alpha \rceil} \right\rfloor \geq \frac{n}{n^\alpha + 1} - 1 = n^{1-\alpha} + O\left(n^{1-2\alpha}\right) - 1.$$

Let I be a maximum Sidon set in $[\ell]$. By results of Chowla, Erdős and Turán and Singer [2, 4, 5, 12], we have

$$|I| \geq \sqrt{\ell} + O(\ell^{1/4}) \geq n^{(1-\alpha)/2} + O\left(n^{(1-3\alpha)/2} + n^{(1-\alpha)/4}\right).$$

Set

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

We claim that T is an (n,α)-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 (see Erdős and Turán [5]). Let S be an (n,α)-strong Sidon set. Let

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

where m will be chosen at the end of the proof, and let

$$\mathcal{P} = \Big\{ (I_x, \{a, b\}) \;\Big|\; I_x \cap [n] \neq \emptyset,\ \{a, b\} \subset I_x \cap S \Big\}.$$

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

We can count $\mathcal{P}$ by considering I_x first. We have

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

where $S_x = |I_x \cap S|$. Since $f(t) = \binom{t}{2}$ is convex, by Jensen's inequality, we have

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

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

$$|\mathcal{P}| \geq \frac{m|S|}{2(n + m - 1)} \left(m|S| - (n + m - 1) \right). \tag{6}$$

Next, we count $\mathcal{P}$ 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,

$$|\mathcal{P}| = \sum_{\substack{\{a,b\} \subset S \\ 0 < b-a < m}} (m - (b - a)). \tag{7}$$

Since S is an (n,α)-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^α. Consequently,

$$\sum_{\substack{\{a,b\} \subset S \\ 0 < b-a < m}} (b - a) \geq 0 + n^\alpha + \cdots + kn^\alpha = \frac{k(k+1)}{2} n^\alpha. \tag{8}$$

where k is an integer such that

$$kn^\alpha < m \leq (k + 1)n^\alpha. \tag{9}$$

Inequalities (7) and (8) give that

$$|\mathcal{P}| \leq (k+1)m - \frac{k(k+1)}{2}n^{\alpha} \overset{(9)}{\leq} \frac{m}{2}\left(\frac{m}{n^{\alpha}}+1\right). \tag{10}$$

It follows from (6) and (10) that

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

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,

$$\begin{aligned}
|S| &\leq \frac{n}{m} + \frac{1}{2}\sqrt{\left(\frac{n}{m}+O(1)\right)^2 + 4\left(\frac{n}{m}+O(1)\right)\left(\frac{m}{n^{\alpha}}+1\right)} \\
&\leq \frac{n}{m} + \left(\frac{n}{2m}+O(1)\right) + \sqrt{\left(\frac{n}{m}+O(1)\right)\left(\frac{m}{n^{\alpha}}+1\right)} \\
&\leq \frac{3n}{2m} + n^{(1-\alpha)/2} + \sqrt{\frac{n}{m}} + O\left(\sqrt{\frac{m}{n^{\alpha}}}\right) + O(1),
\end{aligned}$$

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

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

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

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.

3. Proof of Theorem 6

Let $S \subset \mathbb{N}$ be an α-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 4 implies that

$$|S_i| = |S_i - 2^i| \leq F(2^i, \alpha) \leq 2^{i(1-\alpha)/2+1} \tag{11}$$

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

$$\begin{aligned} S(n) &\leq 2^{k_0} + \sum_{k_0 \leq i < k} |S_i| \overset{(11)}{\leq} 2^{k_0} + \sum_{0 \leq i < k} 2^{i(1-\alpha)/2+1} \\ &\leq 2^{(1-\alpha)(k-1)/2} + \frac{2 \cdot 2^{(1-\alpha)k/2}}{2^{(1-\alpha)/2} - 1} \leq c2^{(1-\alpha)(k-1)/2} \leq cn^{(1-\alpha)/2}. \end{aligned}$$

This completes the proof of Theorem 6.

4. Proof of Theorem 9

Theorem 9 follows easily from the following lemma.

Lemma 10. *Fix $0 \leq \alpha < 1$. There is a sequence $a_1 < a_2 < \cdots < a_k < \cdots$ of positive integers with*

$$a_k \leq 6^{1/(1-\alpha)} k^{3/(1-\alpha)} \tag{12}$$

for every $k \geq 1$ such that $S = \{a_k \colon k \geq 1\}$ is an α-strong Sidon set.

To derive Theorem 9 from Lemma 10, it suffices to notice that, for every k, the set S in Lemma 10 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 10.

Proof of Lemma 10. 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 (12). 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

$$a_i \leq t_i \tag{13}$$

We shall define a_k 'greedily'. Let

$$F_k = \{f \in \mathbb{N} \setminus S_{k-1} \colon S_{k-1} \cup \{f\} \text{ contains } x < y \leq z \leq w \text{ violating (1)}\}.$$

Naturally, if $f \in F_k$, then we cannot add f to S_{k-1} to continue our definition of our α-strong Sidon set. Let

$$C_k = \{c \in \mathbb{N} \colon c \notin S_{k-1} \cup F_k\}$$

be the set of 'candidates' to be added to S_{k-1}. It follows from Claim 11 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 α-strong Sidon set $S = \{a_k \colon k \geq 1\}$, with $a_1 < a_2 < \cdots < a_k < \cdots$. Recall that we have assumed that (13) holds for all $1 \leq i < k$. We now prove the following claim.

Claim 11. *We have $a_k \leq t_k$.*

Clearly, once we have established Claim 11, Lemma 10 follows by induction.

Proof of Claim 11. We first note that it suffices to check that

$$t_k \geq |S_{k-1}| + |F_k \cap [t_k]| + 1. \tag{14}$$

Indeed, if (14) holds, then there must be some candidate $c \in C_k$ for our choice of a_k with $c \leq t_k$, and hence $a_k = \min C_k \leq t_k$ follows, as claimed. We now verify (14).

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 $(k-1)\binom{k-1}{2}$ choices for (x, y, z). For each such choice, we have

$$|f - (y + z - x)| \leq f^\alpha \leq t_k^\alpha,$$

as (1) holds and $f \leq t_k$. 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

$$|f - (x + w - y)| \leq w^\alpha \leq t_k^\alpha,$$

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

$$\begin{aligned} |F_k \cap [t_k]| &\leq 4(k-1)\binom{k-1}{2}(2t_k^\alpha + 1) \\ &< 4(k-1)\frac{k^2}{2}3t_k^\alpha = 6k^3 t_k^\alpha - 6k^2 t_k^\alpha \leq 6k^3 t_k^\alpha - k. \end{aligned}$$

Recalling that $|S_{k-1}| = k-1$ and $t_k = 6^{1/(1-\alpha)} k^{3/(1-\alpha)}$, we see that inequality (14) follows. This completes the proof of Claim 11. $\square$

The proof of Lemma 10 is complete. $\square$

5. Proof of Theorem 7

Recall that Theorem 7 asserts that, for any $0 < \alpha < 1$, there is an α-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 [7, Chapter II, Theorem 9]) constructed a Sidon set $A_p \subset \mathbb{N}$ with $|A_p| = p - 1$ such that

(*i*) $2p^2 < a < 4p^2 - p$ for all $a \in A_p$ and

(*ii*) $p < |a - a'| < 2p^2 - p$ for all distinct a and $a' \in A_p$.

Let

$$\eta = \frac{\alpha}{1-\alpha} \quad \text{and} \quad \mu = 4^{\alpha/(1-\alpha)}. \tag{15}$$

Note for later reference that

$$(1+\eta)\alpha = \eta \quad \text{and} \quad \mu = (4\mu)^{\alpha}. \tag{16}$$

Consider also the sets

$$S_p = \{\lfloor \mu p^{2\eta} a \rfloor : a \in A_p\}. \tag{17}$$

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

$$p_1 = \max\{5, 2^{1/(2\eta)}\} \quad \text{and} \quad p_{n+1} > 4\mu p_n^{2+2\eta} + 1 \tag{18}$$

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 (17), we have

$$2\mu p^{2+2\eta} - 1 < x < 4\mu p^{2+2\eta} - \mu p^{1+2\eta}.$$

(*b*) For every $x \in \bigcup_{1\leq j\leq n} S_{p_j}$ and $y \in S_{p_{n+1}}$, owing to (*i*), (17) and (18), we have

$$y - x > 2\mu p_{n+1}^{2+2\eta} - 1 - 4\mu p_n^{2+2\eta} > 2\mu p_{n+1}^{2+2\eta} - p_{n+1}.$$

(*c*) If x and $y \in S_p$ are distinct, then, owing to (*ii*) and (17), we have

$$\mu p^{1+2\eta} - 1 < |y - x| < 2\mu p^{2+2\eta} - \mu p^{1+2\eta} + 1.$$

We are ready to show the following.

Fact 12. *The set $S = \bigcup_{n\geq 1} S_{p_n}$ is an α-strong Sidon set.*

Proof. Suppose x, y, z and $w \in S = \bigcup_{n\geq 1} S_{p_n}$ with $x < y \leq z < w$. Let $n \geq 1$ be such that $w \in S_{p_n}$. For simplicity, let $p = p_n$. We shall consider the four cases in which $|\{x,y,z,w\} \cap S_p| = 1$, 2, 3, and 4, separately.

- **Case 1:** Suppose first that $\{x,y,z,w\} \cap S_p = \{w\}$. Then

$$w - y \overset{(b)}{>} 2\mu p^{2+2\eta} - p, \text{ while } z - x \overset{(a)}{<} 4\mu p_{n-1}^{2+2\eta} \overset{(18)}{<} p_n = p.$$

  Consequently,

$$|(x+w) - (y+z)| \geq 2\mu p^{2+2\eta} - 2p \geq \mu p^{2\eta} \overset{(16)}{=} \left(4\mu p^{2+2\eta}\right)^{\alpha} \overset{(a)}{\geq} w^{\alpha}.$$

- **Case 2:** Suppose now that $\{x,y,z,w\} \cap S_p = \{z,w\}$. Then

$$w - z \overset{(c)}{>} \mu p^{1+2\eta} - 1, \text{ while, as before, } y - x \overset{(a)}{<} 4\mu p_{n-1}^{2+2\eta} \overset{(18)}{<} p_n = p.$$

  Hence,

$$|(x+w) - (y+z)| > \mu p^{1+2\eta} - 1 - p \overset{(18)}{>} \mu p^{2\eta} \overset{(16)}{=} \left(4\mu p^{2+2\eta}\right)^{\alpha} \overset{(a)}{\geq} w^{\alpha}.$$

- **Case 3:** Suppose $\{x,y,z,w\} \cap S_p = \{y,z,w\}$. Then

$$w - z \overset{(c)}{<} 2\mu p^{2+2\eta} - \mu p^{1+2\eta} + 1, \text{ while } y - x \overset{(b)}{>} 2\mu p^{2+2\eta} - p,$$

  and hence

$$|(x+w) - (y+z)| > \mu p^{1+2\eta} - 1 - p \overset{(18)}{>} \mu p^{2\eta} \overset{(16)}{=} \left(4\mu p^{2+2\eta}\right)^{\alpha} \overset{(a)}{\geq} w^{\alpha}.$$

- **Case 4:** Suppose that $\{x,y,z,w\} \cap S_p = \{x,y,z,w\}$. Since A_p is a Sidon set, we have

$$|(x+w) - (y+z)| \overset{(17)}{\geq} \mu p^{2\eta} - 2 \overset{(16)}{=} \left(4\mu p^{2+2\eta}\right)^{\alpha} - 2 \overset{(a)}{\geq} w^{\alpha}.$$

□

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

$$p - 1 = (1+o(1)) \left(\frac{n}{2\mu}\right)^{1/(2+2\eta)} \overset{(15)}{=} (1+o(1)) \left(\frac{n}{2\mu}\right)^{(1-\alpha)/2}$$
$$= \left(\frac{1}{(4\mu)^{(1-\alpha)/2}} + o(1)\right) (2n)^{(1-\alpha)/2} \overset{(15)}{=} \left(\frac{1}{2} + o(1)\right) (2n)^{(1-\alpha)/2},$$

and (3) follows. □

6. Construction of a dense strong Sidon set

In this section, we construct a dense strong Sidon set for a small α, which implies Theorem 8.

Let
$$b \geq 5 \tag{19}$$
be an integer, fixed throughout this section, and let α be such that
$$b = \Big\lfloor \frac{1}{6\sqrt{\alpha}} \Big\rfloor. \tag{20}$$
Let
$$m_0 = 2^{100b^4}. \tag{21}$$
We shall construct a function $\phi = \phi_b : \mathbb{N}_{\geq m_0} \to \mathbb{N}$ such that, for any Sidon set $S \subset \mathbb{N}_{\geq m_0}$, the set $\phi(S) = \widetilde{S} = \{\widetilde{m} = \phi(m) \colon m \in S\}$ is an α-strong Sidon set. Furthermore, the map ϕ will satisfy the property that $\phi(m) = \widetilde{m} = O(m^{1+5/b})$ (see Fact 16). Therefore, the α-strong Sidon set $\widetilde{S}$ will be denser for larger b and the denser S is, the better. We emphasise that our construction of ϕ is insensitive to the structure of the Sidon set S; it only makes use of the fact that S is a Sidon set. In particular, we can take S to be the Sidon sets of Ruzsa [11] as well the Sidon sets of Cilleruelo [3].

6.1. Construction of ϕ

In order to describe the map $\phi = \phi_b$, we need to introduce several definitions. For a positive integer m, let $a_r a_{r-1} \dots a_2 a_1$ be the binary expansion of m; that is,
$$m = (a_r a_{r-1} \dots a_1)_2 = a_r 2^{r-1} + \dots + a_2 2 + a_1 \tag{22}$$
and $a_r \neq 0$. Note that, in particular, $r = r(m)$ is the number of bits in the binary expansion of m. Observe that
$$2^{r-1} \leq m < 2^r. \tag{23}$$
In what follows, we shall often identify the binary expansion of a positive integer m with the integer m itself. Furthermore, we let $t = t(m)$ be the integer such that
$$2^t \leq \frac{r}{3b} < 2^{t+1},$$
and let
$$s = s(m) = 2^t. \tag{24}$$
Note that
$$\frac{r}{6b} < s \leq \frac{r}{3b}. \tag{25}$$
If $m \geq m_0 = m_0(b)$, then $s = s(m) \geq s_0(b)$ for some $s_0(b)$.

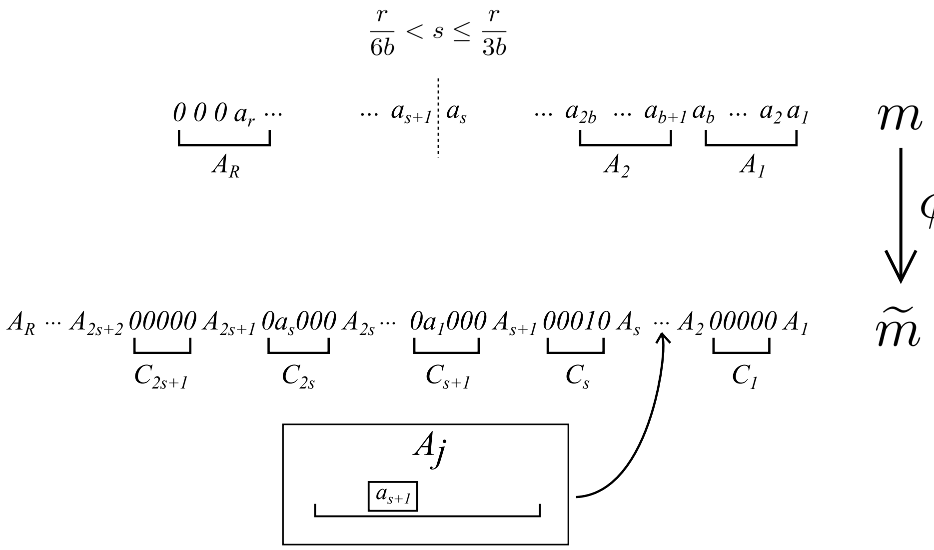

Figure 1: The binary expansions of m and $\widetilde{m}$. The number j is such that the block A_j contains a_{s+1}.

To define $\widetilde{m} = \phi(m)$, we describe the binary expansion of $\widetilde{m}$ from the binary expansion of m. Formally speaking, binary expansions (or representations) of positive integers will be considered to be *words* in $\{0,1\}^* = \bigcup_{l\geq 0}\{0,1\}^l$. 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 $a_r a_{r-1} \dots a_1$. 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

$$A_R A_{R-1} \dots A_2 A_1, \tag{26}$$

where each $A_i = A_i(m)$ is of length b (see Figure 1). Note that A_R contains at least one bit equal to 1. We call (26) the *b-factorization* of m. Note that

$$\frac{r}{b} \leq R < \frac{r}{b} + 1. \tag{27}$$

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

$$c_{2s}c_{2s-1}\dots c_{s+1}c_s \dots c_1 = a_s a_{s-1} \dots a_2 a_1 0^s. \tag{28}$$

Clearly, the word in (28) 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, which gives us 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 $C_i = C_i(m)$ $(1 \le i \le 2s)$. Let us write $C_{i,j}$ for the jth 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 $1 \le i \le 2s$, the definition of the bits of C_i is as follows:

$$\begin{aligned} C_{i,5} &= C_{i,3} = C_{i,1} = 0, \\ C_{i,4} &= c_i \qquad \text{(recall (28))}, \\ C_{i,2} &= \begin{cases} 1 & \text{if } i = s, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{29}$$

Figure 1 may be of some help to see where the $C_i = C_i(m)$ $(1 \le i \le 2s)$ occur in the definition $\widetilde{m} = \phi(m)$. We are now finally able to define the map $\phi : \mathbb{N}_{\ge m_0} \to \mathbb{N}$.

Definition 13. *Let m be any positive integer with $m \ge m_0$. Let* (26) *be its b-factorization. We let*

$$\phi(m) = \widetilde{m} = A_R C_{R-1} A_{R-1} \ldots C_2 A_2 C_1 A_1, \tag{30}$$

where the C_i are as defined above.

For convenience, the 5-bit blocks C_i in (30) are referred to as *C-blocks*, while the b-bit blocks A_i are referred to as *A-blocks*. Note that, when we construct $\widetilde{m}$ 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).

Rationale behind the definition of $\widetilde{m} = \phi(m)$

Very roughly speaking, we define $\widetilde{m} = \phi(m)$ as above because of the following. Suppose S is a Sidon set. Then if we know the sum $m + m'$ of m and $m' \in S$, then we know $\{m, m'\}$. For $\phi(S)$ to be a strong Sidon set, for any m and $m' \in S$, we force the sum $\widetilde{m} + \widetilde{m}' = \phi(m) + \phi(m')$ to determine $\{m, m'\}$ uniquely, *even if we know the value of $\widetilde{m} + \widetilde{m}' = \phi(m) + \phi(m')$ only approximately*. (See Fact 19 and Lemma 22 below.) This is the reason we copy the weak bits of m and m' in "more significant parts" of $\widetilde{m} = \phi(m)$ and $\widetilde{m}' = \phi(m')$. Also, since we have to deal with sums of the form $\widetilde{m} + \widetilde{m}' = \phi(m) + \phi(m')$, we need to consider carries. To overcome difficulties that may arise from such carries, we have some zero bits in the definition of the C-blocks C_i.

6.2. Preliminary remarks on ϕ

We now state some elementary facts about the function ϕ. This section may help the reader get a feeling on how $\phi(m) = \widetilde{m}$ relates to m. However, readers who prefer to see immediately how ϕ is used in the proof of Theorem 8 may consider skipping this section and going directly to Section 6.3.

We start with the following immediate fact.

Fact 14. *If we know all the bits of $\widetilde{m} = \phi(m)$ $(m \geq m_0)$, we can recover m.*

In fact, we are going to observe that one does *not* need to know all bits of $\widetilde{m}$ 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 $\widetilde{m}$ 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 $\widetilde{m}$ 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 $\widetilde{m}$. However, since $j = \lceil (s+1)/b \rceil < s$,

$$\text{all } C_s, C_{s+1}, \ldots, C_{2s} \text{ are on the left from } A_j. \tag{31}$$

Since C_s is the unique C-block with $C_{i,2} = 1$ 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 15. *If we know all the bits of $\widetilde{m} = \phi(m)$ except for the $(1 + 5/b)\, s - 5$ least significant bits of $\widetilde{m}$, 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 $\widetilde{m}$ is $j - 1$, the position of a_{s+1} in $\widetilde{m}$ 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 $\widetilde{m}$ we do not need to know to recover m is at least $(1 + 5/b)\, s - 5$. $\square$

Next we show that $\widetilde{m}$ is not much larger than m if b is large.

Fact 16. *We have $m^{1+5/b}/64 < \widetilde{m} < 4m^{1+5/b}$.*

Proof. Let r be the number of bits in m, and let $\widetilde{r}$ be the number of bits in $\widetilde{m}$. Recalling (23), we have

$$2^{r-1} \le m < 2^r \quad \text{and} \quad 2^{\widetilde{r}-1} \le \widetilde{m} < 2^{\widetilde{r}}. \tag{32}$$

For each factor A_i $(1 \le i \le R-1)$ of m of length b, we add a factor C_j of length 5 to construct $\widetilde{m}$. Hence, we have that $\widetilde{r} = r + 5(R-1)$. Therefore, (27) gives that

$$r\,(1 + 5/b) - 5 \le \widetilde{r} < r\,(1 + 5/b)\,. \tag{33}$$

This together with (32) and $b \ge 5$ completes the proof of Fact 16. $\square$

6.3. Key lemma and proof of Theorem 8

The construction of $\widetilde{m}$ lets us prove the following result.

Lemma 17 (Key lemma)**.** *Let b and $m_0 = m_0(b)$ be as in* (19) *and* (21)*. Let $S \subset \mathbb{N}_{\ge m_0}$ be a Sidon set and let $\widetilde{S} = \{\widetilde{m} \colon m \in S\}$. For $\widetilde{m}_i \in \widetilde{S}$ $(1 \le i \le 4)$ with $\widetilde{m}_1 < \widetilde{m}_2 \le \widetilde{m}_3 < \widetilde{m}_4$, we have*

$$|(\widetilde{m}_1 + \widetilde{m}_4) - (\widetilde{m}_2 + \widetilde{m}_3)| \ge 2^{\ell}, \tag{34}$$

where $\ell = \lfloor (1 + 5/b) r(\widetilde{m}_4)/(36b^2) \rfloor - b - 6$.

The proof of Lemma 17 will be given in Section 6.4. We now show that Lemma 17 may be used to construct strong Sidon sets.

Lemma 18. *Let α with $0 < \alpha \le 10^{-4}$ be given and, following* (19) *and* (20)*, let*

$$b = \lfloor 1/(6\sqrt{\alpha}) \rfloor \ge 5. \tag{35}$$

Let m_0 be as in (21)*. If $S \subset \mathbb{N}_{\ge m_0}$ is a Sidon set, then $\widetilde{S} = \{\widetilde{m} \colon m \in S\}$ is an α-strong Sidon set. Moreover,*

$$\widetilde{S}(n) = S\left(\left\lfloor \left(\frac{n}{4}\right)^{1/(1+5/b)} \right\rfloor \right). \tag{36}$$

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

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

for $\widetilde{m}_1$, $\widetilde{m}_2$, $\widetilde{m}_3$, $\widetilde{m}_4 \in \widetilde{S}$ with $\widetilde{m}_1 < \widetilde{m}_2 \le \widetilde{m}_3 < \widetilde{m}_4$. Indeed, Lemma 17 gives that

$$\log_2\left(|(\widetilde{m}_1 + \widetilde{m}_4) - (\widetilde{m}_2 + \widetilde{m}_3)|\right) \ge \left\lfloor \frac{1 + 5/b}{36b^2} r(\widetilde{m}_4) \right\rfloor - b - 6 \ge \frac{r(\widetilde{m}_4)}{36b^2},$$

where the last inequality follows from (21), i.e., $r(\widetilde{m}_4) \geq r(m_0) \geq 100b^4$. Consequently, in view of $\widetilde{m} < 2^{r(\widetilde{m})}$ and (35), we infer that

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

Next, we consider the counting function $\widetilde{S}(n)$. One can easily check that for any $m \leq (n/4)^{1/(1+5/b)}$ Fact 16 implies that $\widetilde{m} \leq n$. In otherwords, for any $m \in S \cap \left[(n/4)^{1/(1+5/b)}\right]$, its ϕ-image $\phi(m) = \widetilde{m}$ is contained in $[n]$. Since ϕ is one-to-one, we obtain (36), as desired. □

We now prove Theorem 8 combining Ruzsa's theorem [11] and Lemma 18.

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

$$\frac{5}{b} = \frac{5}{\lfloor 1/6\sqrt{b} \rfloor} \leq 32\sqrt{\alpha}. \tag{37}$$

Using (37), we see that the set $\widetilde{S}$ given by Lemma 18 is an α-strong Sidon set with

$$\begin{aligned}\widetilde{S}(n) &= S\big(\lfloor (n/4)^{1/(1+5/b)} \rfloor\big)\\ &\geq n^{(\sqrt{2}-1+o(1))/(1+5/b)} \geq n^{(\sqrt{2}-1+o(1))/(1+32\sqrt{\alpha})},\end{aligned}$$

as required. □

6.4. Proof of Lemma 17

Before addressing inequality (34), we will show that, similarly as in the proof of Fact 15, one can recover $m + m'$ from partial information of $\widetilde{m} + \widetilde{m}' = \phi(m) + \phi(m')$. First, we define notation for binary expansions of sums of the form $\widetilde{m} + \widetilde{m}' = \phi(m) + \phi(m')$, and therefore it will be convenient to describe such expansions explicitly. Suppose $m \geq m'$. Recall (22) and similarly let

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

Consider the b-factorization $A_R A_{R-1} \dots A_2 A_1$ (as in (26)) of m and let the b-factorization of m' be

$$A'_{R'} A'_{R'-1} \dots A'_2 A'_1. \tag{38}$$

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

$$\widetilde{m}' = A'_{R'} C'_{R'-1} A'_{R'-1} \dots C'_2 A'_2 C'_1 A'_1.$$

For convenience, let us set $A'_i = 0^b$ for every $i > R'$ and recall that we let $C'_i = 0^5$ for every $i > 2s(m')$ and hence, in particular, $C'_i = 0^5$ for every $i \geq R'$. For every $1 \leq i \leq R$, we let

$$a_i^+ = \begin{cases} 0 & \text{if } A_i + A'_i < 2^b, \\ 1 & \text{otherwise,} \end{cases} \tag{39}$$

$$C_i^+ = C_i + C'_i + a_{i-1}^+,$$

$$A_i^+ = (A_i + A'_i) \bmod 2^b. \tag{40}$$

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

$$a_R^+ A_R^+ C_{R-1}^+ A_{R-1}^+ \dots C_2^+ A_2^+ C_1^+ A_1^+. \tag{41}$$

It will be convenient to extend the notion of 'C-blocks' to the binary expansion of $\widetilde{m} + \widetilde{m}'$: those are the 5-bit blocks C_i^+ in (41). Similarly, the 'A-blocks' of $\widetilde{m} + \widetilde{m}'$ are the b-bit strings A_i^+ in (41).

The next fact tells that we can recover $m + m'$ from $\widetilde{m} + \widetilde{m}'$. It is a little less trivial than Fact 14 since we need to consider carries.

Fact 19. *If we know all the bits of the sum $\widetilde{m} + \widetilde{m}' = \phi(m) + \phi(m')$, then we can recover $m + m'$.*

Proof. Suppose $\widetilde{m} + \widetilde{m}'$ has binary expansion (41). It is clear that the b-bit string A_1^+ in (41) 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 (41). 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 19 similar to Fact 15: we do not need to know a certain number of the least significant bits of $\widetilde{m} + \widetilde{m}'$ to recover $m + m'$. Recall the notation (38)–(41).

Lemma 20. *Let m and m' be such that $m, m' \geq m_0$ and $\widetilde{m} \geq \widetilde{m}'$. 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 (39)–(40) 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 $\widetilde{m} \geq \widetilde{m}'$ implies that $s \geq s'$. From (31), 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 $C_{i,2}^+ \neq 00$. 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 $C^+_{i,3}C^+_{i,2} = 10$. In this case we can 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 ($1 \le i \le s'$). We distinguish two cases.

- If $s = s'$, then C^+_i ($s = 1 \le i \le 2s$) 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 $1 \le i \le s = s'$.
- If $s > s'$, then we must have $s \ge 2s'$ since s and s' are powers of 2 (recall (24)). Therefore, the C-blocks C_i ($s + 1 \le i \le 2s$) of m and the C-blocks C'_i ($s' + 1 \le i \le 2s'$) of m' do not 'overlap'. Recall that the bits c_i ($1 \le i \le s$) in the definition of the C_i ($1 \le i \le s$) are all 0 (see (28) and (29)). Consequently, we deduce that, examining C^+_i ($s' + 1 \le i \le 2s'$), we are able to recover all the weak bits a'_i ($1 \le i \le s'$) 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 ($1 \le i \le s$) of m by examining C^+_i ($s + 1 \le i \le 2s$). Thus we can recover all the values of $a_i + a'_i$ for all i ($1 \le i \le s'$).

The claim above implies that we can recover A^+_i for every $1 \le i \le j' - 1$. Recall that we know a^+_R, C^+_i and A^+_i ($j' \le i \le R$). A little thought considering carries shows that we can recover $m + m'$, which completes the proof of Lemma 20. □

Lemma 20 easily yields the following.

Lemma 21. *If we know all the bits of $\widetilde{m} + \widetilde{m}' = \phi(m) + \phi(m')$ except for the $(1 + 5/b)\, s' - b - 4$ least significant bits of $\widetilde{m} + \widetilde{m}'$, then we can recover $m + m'$.*

Proof. Lemma 20 implies that the number of least significant bits of $\widetilde{m} + \widetilde{m}'$ we do not need to know to recover $\widetilde{m} + \widetilde{m}'$ is the number of bits in $C_{j'-1}A_{j'-1} \ldots C_1 A_1$, which is equal to

$$(b + 5)(j' - 1),$$

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

$$\begin{aligned}(b + 5)(j' - 1) &= (b + 5)\left(\left\lceil \frac{s' + 1}{b} \right\rceil - 1\right) \\ &\ge (b + 5)\left(\frac{s' + 1}{b} - 1\right) \ge \left(1 + \frac{5}{b}\right) s' - b - 4.\end{aligned}$$

□

In order to show (34) of Lemma 17, the number of least significant bits in $\widetilde{m} + \widetilde{m}'$ we do not need to know to recover $m + m'$ has to be expressed as a parameter of m rather than m'.

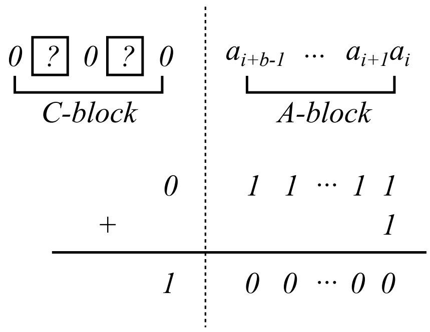

Figure 2: The case in which the number of carries is largest.

Lemma 22. *Let m and m' be such that $m, m' \geq m_0$ and $\widetilde{m} \geq \widetilde{m}'$. If we know all the bits of $\widetilde{m} + \widetilde{m}'$, except for the $\lfloor (1+5/b)r(\widetilde{m})/(36b^2) \rfloor - b - 6$ least significant ones, then we can recover $m + m'$.*

Proof. We consider two cases depending on the values of $\widetilde{m}'$ and $\widetilde{m}$. 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

$$\log_2 \widetilde{m}' \leq (1+5/b)s - b - 5$$

for $s = s(m)$. Since the number of bits in A_i is 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 $\log_2 \widetilde{m}' \leq (1+5/b)s - b - 5$, the binary expansion of $\widetilde{m} + \widetilde{m}'$ is the same as $\widetilde{m}$ except for $(1+5/b)s - 5$ least significant bits. Hence, Fact 15 implies that we can recover m. Thus we can obtain $\widetilde{m}$, and then we recover $\widetilde{m}' = (\widetilde{m} + \widetilde{m}') - \widetilde{m}$. Fact 14 gives that $\widetilde{m}'$ determines m', and hence, we can determine $m + m'$.

- **Case 2:** We suppose that

$$\log_2 \widetilde{m}' > (1+5/b)s - b - 5.$$

Inequalities (23) and (25) give that

$$\log_2 \widetilde{m}' \leq \widetilde{r}' \leq 6bs',$$

and hence,

$$s' > \frac{1+5/b}{6b}s - 1. \tag{42}$$

Lemma 21 implies that the number of least significant bits of $\widetilde{m} + \widetilde{m}'$ we do not need to know to recover $m + m'$ is

$$\left(1+\frac{5}{b}\right)s' - b - 4 \overset{(42)}{>} \frac{(1+5/b)^2}{6b}s - b - 6$$
$$\overset{(25)}{\geq} \left(\frac{1+5/b}{6b}\right)^2 r - b - 6 \overset{(33)}{\geq} \frac{1+5/b}{36b^2}\widetilde{r} - b - 6,$$

which completes the proof of Lemma 22. $\square$

It only remains to show that Lemma 22 implies Lemma 17.

Proof of Lemma 17. Fix $\widetilde{m}_i \in \widetilde{S}$ $(1 \leq i \leq 4)$ with $\widetilde{m}_1 < \widetilde{m}_2 \leq \widetilde{m}_3 < \widetilde{m}_4$ and let m, μ, μ', $m' \in S$ be such that

$$\widetilde{m} = \widetilde{m}_4, \quad \widetilde{\mu} = \widetilde{m}_3, \quad \widetilde{\mu}' = \widetilde{(\mu')} = \widetilde{m}_2 \quad \text{and} \quad \widetilde{m}' = \widetilde{(m')} = \widetilde{m}_1.$$

Recall that

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

Suppose, for a contradiction, that

$$\big|\,(\widetilde{m}_1 + \widetilde{m}_4) - (\widetilde{m}_2 + \widetilde{m}_3)\,\big| = \big|\,\big(\widetilde{m} + \widetilde{m}'\big) - \big(\widetilde{\mu} + \widetilde{\mu}'\big)\,\big| < 2^{\ell}.$$

In other words, $\widetilde{m} + \widetilde{m}'$ and $\widetilde{\mu} + \widetilde{\mu}'$ have the same binary expansion except possibly for the ℓ least significant bits. Lemma 22 gives that $m + m' = \mu + \mu'$, which contradicts the assumption that S is a Sidon set. $\square$

7. Sidon sets contained in random sets of integers

7.1. An extremal problem on random sets of integers

In [9] 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 23. *Fix a constant α 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 of integers obtained by including each $m \in \mathbb{N}$ independently with probability p_m.*

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

(*i*) Find some constant $f(\alpha)$ such that, with probability 1, there is a Sidon set S contained in $R(\alpha)$ such that, for all n,

$$S(n) \geq n^{f(\alpha)+o(1)}. \tag{43}$$

(*ii*) Find some 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 [9] are the following (see Figure 7.1):[1]

(*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, while we know the best possible $f(\alpha)$ and $g(\alpha)$ for $1/3 \leq \alpha \leq 1$, this is not the case for $0 \leq \alpha < 1/3$. The goal of this section is to show that the existence of dense α-strong Sidon sets implies lower bounds for $f(\alpha)$ in (43). To this end, we use the following modification of Definition 1.

Definition 24 ((α, c)-strong Sidon sets)**.** *Let constants $c > 0$ and α with $0 \leq \alpha < 1$ be given. A set $S \subset \mathbb{N}$ is called an* (α, c)-strong Sidon set *if*

$$|(x + w) - (y + z)| \geq cw^{\alpha}$$

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

We shall consider (α, c)-strong Sidon sets for $c = 1$ and $c = 16$ only ($c = 1$ corresponds to α-strong Sidon sets and Theorem 25 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 25. *Let $0 \leq \alpha \leq 1/2$ be given. If there exists an $(\alpha, 16)$-strong Sidon set $S \subset \mathbb{N}$ with*

$$S(n) \geq n^{h(\alpha)+o(1)}, \tag{44}$$

then, with probability 1, the random subset $R = R(\alpha)$ of $\mathbb{N}$ contains a Sidon set S^* such that

$$S^*(n) \geq n^{h(\alpha)+o(1)}.$$

[1]We remark that, in [9], 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 [9] to the present context, one has to take the constant α in [9] to be 1 and the constant δ in [9] to be $1 - \alpha$. Thus, for instance, to interpret Figure 1 in [9] one should have in mind that $\delta = 1 - \alpha$ (where α is the α in Definition 23, that is, it is the α in the present paper).

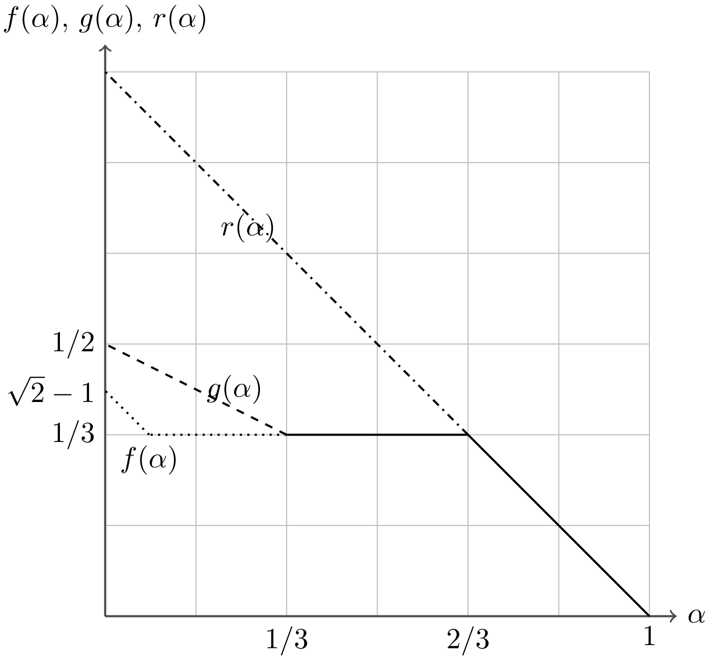

Figure 3: The graphs of the functions $f(\alpha)$, $g(\alpha)$ and $r(\alpha) = 1 - \alpha$. The slope of the dashed line is $-1/2$, while the slope of the non-horizontal dotted line is -1.

Combining Theorems 8 and 25 implies that (43) holds with $f(\alpha) = (\sqrt{2}-1)/(1+32\sqrt{\alpha})$, which, unfortunately, does not improve the value obtained for $f(\alpha)$ in [9]. As it turns out, our strategy to obtain a better value for $f(\alpha)$ has been recently vindicated: Fabian, Rué and Spiegel [6] succeeded in obtaining dense enough strong Sidon sets by different methods, which, together with the strategy put forward here, gives a value for $f(\alpha)$ that supersedes the one in [9]. The reader is referred to [6] for details.

The next section is devoted to the proof of Theorem 25.

7.2. Proof of Theorem 25

Theorem 25 trivially holds for $\alpha = 0$, and hence throughout Section 7.2 we assume that $0 < \alpha \le 1/2$. The proof of Theorem 25 is based on two auxiliary lemmas, Lemmas 26 and 29. In order to formulate these lemmas, we introduce some notation. Let

$$\beta = \frac{1}{1-\alpha} \quad \text{so that} \quad \alpha = 1 - \frac{1}{\beta}.$$

Note that

$$\alpha\beta = \beta - 1, \;\; 0 < \alpha \le 1/2, \;\; 1 < \beta \le 2. \tag{45}$$

For every integer $i \ge 1$, let

$$I_i = \mathbb{N} \cap \big[i^\beta, (i+1)^\beta\big).$$

For a, $b \in \mathbb{N}$, write

$$a \sim b \tag{46}$$

if a, $b \in I_i$ for some $i \in \mathbb{N}$. The following holds.

Lemma 26. *For every sufficiently large $i \in \mathbb{N}$, say $i \geq i_0(\alpha)$, we have*

$$\mathbb{P}\left(|R \cap I_i| \geq 1\right) \geq \frac{1}{3}. \tag{47}$$

Proof. Let X_i be the size of a random set obtained by choosing each element in I_i independently with probability

$$\left((i+1)^{\beta}\right)^{-\alpha} = (i+1)^{-\alpha\beta} = (i+1)^{-(\beta-1)}. \tag{48}$$

Since each element in I_i is chosen to be in R independently with probability at least $\left((i+1)^{\beta}\right)^{-\alpha}$, we have that $\mathbb{P}\left(|R \cap I_i| \geq 1\right) \geq \mathbb{P}\left(X_i \geq 1\right)$. Therefore, to prove (47), it suffices to prove that $\mathbb{P}(X_i = 0) \leq 2/3$.

Let us first note that, as $\beta > 1$, we have

$$(i+1)^{\beta} - i^{\beta} \geq \beta i^{\beta-1}. \tag{49}$$

Moreover, for $\beta > 1$ and $i \geq i_0(\beta)$, we have

$$\beta\left(\frac{i}{i+1}\right)^{\beta-1} - \left(\frac{1}{i+1}\right)^{\beta-1} \geq \frac{\beta}{2}. \tag{50}$$

Using (48), (49) and (50), we see that

$$\begin{aligned}
\mathbb{P}(X_i = 0) &\leq \left(1 - \left(\frac{1}{i+1}\right)^{\alpha\beta}\right)^{(i+1)^{\beta} - i^{\beta} - 1} = \left(1 - \left(\frac{1}{i+1}\right)^{\beta-1}\right)^{(i+1)^{\beta} - i^{\beta} - 1} \\
&\leq \exp\left(-\left(\frac{1}{i+1}\right)^{\beta-1}\left((i+1)^{\beta} - i^{\beta} - 1\right)\right) \\
&\leq \exp\left(-\left(\frac{1}{i+1}\right)^{\beta-1}\left(\beta i^{\beta-1} - 1\right)\right) \\
&= \exp\left(-\beta\left(\frac{i}{i+1}\right)^{\beta-1} + \left(\frac{1}{i+1}\right)^{\beta-1}\right) \\
&\leq \exp\left(-\frac{\beta}{2}\right) \leq \mathrm{e}^{-\frac{1}{2}} < \frac{2}{3},
\end{aligned}$$

and (47) follows. $\square$

For the proof of Lemma 29, it is convenient to have the following.

Claim 27. *Let $S \subset \mathbb{N}$ be an $(\alpha, 16)$-strong Sidon set, where $0 < \alpha \leq 1/2$. 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 β and x with $1 < \beta \leq 2$ and $x \geq 1$, we have

$$(x+1)^\beta - x^\beta \leq 2\beta x^{\beta-1}. \tag{51}$$

Observe that (51) is equivalent to

$$(1+z)^\beta - 2\beta z \leq 1, \tag{52}$$

which is true in view of the fact that the derivative of LHS of (52) is negative.

We now start the proof of Claim 27. 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 (51), we see that

$$\begin{aligned}|x+w-(y+z)| &\leq |w-z| + |y-x| \leq |I_j| + |I_i| \leq 2|I_j| \\ &= 2\big((j+1)^\beta - j^\beta\big) \leq 4\beta j^{\beta-1} \leq 4\beta (j^\beta)^\alpha < 4\beta w^\alpha.\end{aligned}$$

By (45), we have

$$|x+w-(y+z)| < 8w^\alpha.$$

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,

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

which again contradicts the assumption on S. Therefore, Claim 27 is proved. □

In the proof of Theorem 25, it will be convenient to consider $(\alpha, 16)$-strong Sidon sets S with the property that S meets every I_i ($i \geq 1$) in at most one element.

Definition 28. *Let $0 < \alpha \leq 1/2$ 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 27 allows us to discard at most 1 element 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 (44) 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 (46)).

Lemma 29. *Let $0 < \alpha \leq 1/2$ be given and let $S = \{s_1 < s_2 < \dots\} \subset \mathbb{N}$ 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 $S' = \{s'_1, s'_2, \dots\}$. 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

$$\begin{aligned} i^\beta &\leq a < (i+1)^\beta, & j^\beta &\leq b < (j+1)^\beta, \\ k^\beta &\leq c < (k+1)^\beta, & \ell^\beta &\leq d < (\ell+1)^\beta. \end{aligned}$$

Hence,

$$i^\beta + \ell^\beta \leq a + d < (i+1)^\beta + (\ell+1)^\beta$$

and

$$j^\beta + k^\beta \leq b + c < (j+1)^\beta + (k+1)^\beta.$$

Since $a + d = b + c$ holds, the two intervals $\left[i^\beta + \ell^\beta, (i+1)^\beta + (\ell+1)^\beta\right)$ and $\left[j^\beta + k^\beta, (j+1)^\beta + (k+1)^\beta\right)$ are not disjoint. Firstly, if $j^\beta + k^\beta \leq i^\beta + \ell^\beta$, then necessarily $i^\beta + \ell^\beta < (j+1)^\beta + (k+1)^\beta$ since otherwise the two intervals would be disjoint. Thus,

$$j^\beta + k^\beta \leq i^\beta + \ell^\beta < (j+1)^\beta + (k+1)^\beta. \tag{53}$$

On the other hand, if $i^\beta + \ell^\beta \leq j^\beta + k^\beta$, then $j^\beta + k^\beta < (i+1)^\beta + (\ell+1)^\beta$, and thus,

$$i^\beta + \ell^\beta \leq j^\beta + k^\beta < (i+1)^\beta + (\ell+1)^\beta. \tag{54}$$

We claim that inequality (53) implies that $0 \leq i^\beta + \ell^\beta - (j^\beta + k^\beta) < 4\beta\ell^{\beta-1}$. Indeed,

$$\begin{aligned} 0 \leq i^\beta + \ell^\beta - (j^\beta + k^\beta) &< (j+1)^\beta + (k+1)^\beta - j^\beta - k^\beta \\ &\leq 2\beta j^{\beta-1} + 2\beta k^{\beta-1} < 4\beta\ell^{\beta-1}, \end{aligned}$$

where the next to last inequality follows from (45) and (51). Similarly, inequality (54) implies

$$0 \leq j^\beta + k^\beta - (i^\beta + \ell^\beta) < 4\beta\ell^{\beta-1}.$$

Consequently, we have

$$\left|i^\beta + \ell^\beta - (j^\beta + k^\beta)\right| < 4\beta\ell^{\beta-1}. \tag{55}$$

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 $w \in I_\ell$, 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 $\ell \le w^{1/\beta} < \ell + 1$, i.e.,

$$w^{1/\beta} - 1 < \ell \le w^{1/\beta}. \tag{56}$$

Raising all terms of (56) to the power of β and using the inequality $\xi^\beta - (\xi - 1)^\beta - \beta\xi^{\beta-1} < 0$ with $\xi = w^{1/\beta}$, we infer that

$$w - \beta w^\alpha < (w^{1/\beta} - 1)^\beta < \ell^\beta \le w.$$

Similarly, we have

$$x - \beta x^\alpha < i^\beta \le x, \quad y - \beta y^\alpha < j^\beta \le y \quad \text{and} \quad z - \beta z^\alpha < k^\beta \le z.$$

Consequently, in view of the fact that

$$\ell^{\beta-1} = \ell^{\beta\beta^{-1}(\beta-1)} \le w^{(\beta-1)/\beta} = w^\alpha,$$

we conclude that

$$\begin{aligned} \big|x + w - (y + z)\big| &\le \big|i^\beta + \ell^\beta - (j^\beta + k^\beta)\big| + 4\beta w^\alpha \\ &\overset{(55)}{<} 4\beta\ell^{\beta-1} + 4\beta w^\alpha \le 8\beta w^\alpha \le 16 w^\alpha, \end{aligned}$$

where the last inequality follows from (45). This contradicts the assumption that S is an $(\alpha, 16)$-strong Sidon set. This contradiction implies that S' is indeed a Sidon set. □

We are now ready to prove Theorem 25.

Proof of Theorem 25. Recall that Theorem 25 trivially holds for $\alpha = 0$, and that, hence, we assume that $0 < \alpha \le 1/2$. Let $S = \{s_1 < s_2 < \cdots\} \subset \mathbb{N}$ be an $(\alpha, 16)$-strong Sidon set such that

$$S(n) \ge n^{h(\alpha)+o(1)}.$$

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 23, and let i_0 be the integer from Lemma 26. Set

$$J = \{j : i_j \ge i_0 \text{ and } R \cap I_{i_j} \ne \emptyset\}.$$

For each such $j \in J$, we select an arbitrary element $s_j^* \in R \cap I_{i_j}$ and let $S^* = \{s_1^* < s_2^* < \cdots\}$. Since $s_j^* \sim s_j$, Lemma 29 implies that S^* is a Sidon set.

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

$$|S(n)| - i_0 \ge n^{h(\alpha)+o(1)}$$

intervals I_{i_j} with $S \cap I_{i_j} \neq \emptyset$. Moreover, by Lemma 26, we have

$$\mathbb{P}\left(R \cap I_{i_j} \neq \emptyset\right) \geq 1/3$$

for every $j \geq i_0$. Thus, Chernoff's bound (see, e.g., [8, Corollary 2.3]) gives that, for any fixed $\varepsilon > 0$ and $n \geq n(\varepsilon)$,

$$\mathbb{P}\left[S^*(n) < n^{h(\alpha)-\varepsilon}\right] \leq 2\exp\left(-n^{h(\alpha)-\varepsilon}\right) \leq \frac{1}{n^2}. \tag{57}$$

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

Lemma 30 (Borel–Cantelli Lemma)**.** *Let $\{F_n\}_{n\in\mathbb{N}}$ be a sequence of events in a probability space. If $\sum_{n=1}^{\infty}\mathbb{P}[F_n] < \infty$, then, with probability 1, only finitely many F_n occur, i.e.,*

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

Since $\sum 1/n^2 < \infty$, inequality (57) and the Borel–Cantelli Lemma gives that, with probability 1, the random set R is such that, for every $n \geq n_0 = n_0(R,\varepsilon)$,

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

This completes the proof of Theorem 25. $\square$

8. Concluding remarks

Erdős proved that 'lim sup' in (2) cannot be replaced by 'lim'. Indeed, he showed that any Sidon set $S \subset \mathbb{N}$ is such that

$$\liminf_n S(n)n^{-1/2}\sqrt{\log n} < \infty$$

(see [13, 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 α-strong Sidon set $S \subset \mathbb{N}$ ($0 \leq \alpha < 1$), we have

$$\liminf_n S(n)n^{-(1-\alpha)/2} = 0?$$

Our approach for producing strong Sidon sets is based on the construction of a function ϕ such that $\phi(S)$ is a strong Sidon set for *any* Sidon set S. In contrast, Fabian, Rué, and Spiegel [6] obtained denser strong Sidon sets by nicely elaborating on a construction of Cilleruelo [3]. It would be very interesting to see whether there is a "black box" approach that can do numerically at least as well as the approach in [6].

We close by mentioning that the approach of Fabian, Rué, and Spiegel [6] allowed them to investigate "strong B_h-sets".

References

[1] M. Ajtai, J. Komlós, and E. Szemerédi, *A dense infinite Sidon sequence*, European J. Combin. **2** (1981), no. 1, 1–11. 1

[2] S. Chowla, *Solution of a problem of Erdős and Turán in additive-number theory*, Proc. Nat. Acad. Sci. India. Sect. A. **14** (1944), 1–2. 1, 2

[3] J. Cilleruelo, *Infinite Sidon sequences*, Adv. Math. **255** (2014), 474–486. 1, 6, 8

[4] P. Erdős, *On a problem of Sidon in additive number theory and on some related problems. Addendum*, J. London Math. Soc. **19** (1944), 208. 1, 2

[5] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215. 1, 2

[6] D. Fabian, J. Rué, and C. Spiegel, *On strong infinite Sidon and B_h sets and random sets of integers*, arXiv: 1812.05167. 7.1, 8

[7] H. Halberstam and K. F. Roth, *Sequences*, second ed., Springer-Verlag, New York, 1983. 1, 5, 8

[8] S. Janson, T. Łuczak, and A. Ruciński, *Random graphs*, Wiley-Interscience, New York, 2000. 7.2

[9] 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. 1, 1, 7.1, 7.1, 1, 7.1

[10] F. Krückeberg, *B_2-Folgen und verwandte Zahlenfolgen*, J. Reine Angew. Math. **206** (1961), 53–60. 1, 1

[11] I. Z. Ruzsa, *An infinite Sidon sequence*, J. Number Theory **68** (1998), no. 1, 63–71. 1, 1, 6, 6.3

[12] 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, 2

[13] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. II*, J. Reine Angew. Math. **194** (1955), 111–140. 1, 8