# SIDON SETS IN $\mathbb{N}^{d}$ 

JAVIER CILLERUELO

> Abstract. We study finite and infinite Sidon sets in $\mathbb{N}^{d}$. The additive energy of two sets is used to obtain new upper bounds for the cardinalities of finite Sidon subsets of some sets as well as to provide short proofs of already known results. We also disprove a conjecture of Lindstrom on the largest Sidon set in $[1, N] \times[1, N]$ and relate it to a known conjecture of Vinogradov concerning the size of the smallest quadratic residue modulo a prime $p$.

> For infinite Sidon sets $A \subset \mathbb{N}^{d}$, we prove that $\liminf _{n \rightarrow \infty} \frac{\left|A \cap[1, n]^{d}\right|}{\sqrt{n^{d} / \log n}}>0$. Finally, we show how to map infinite Sidon sets in $\mathbb{N}^{d}$ to $\mathbb{N}^{d^{\prime}}$ in an effective way. As an application, we find an explicit Sidon set $A$ such that $A(n) \geq n^{1 / 3+o(1)}$.

## 1. Introduction

A Sidon set is a subset of a semigroup $G$ with the property that all sums of two elements are distinct. Sidon subsets of positive integers are the most common case, but other semigroups $G$ have been considered in the literature. In this paper, we shall deal with Sidon sets in $\mathbb{N}^{d}$. We study both finite and infinite Sidon sets.

A major problem concerning finite Sidon sets is to find the largest cardinality of a Sidon set contained in a given finite set. For $d \geq 1$ we let $F_{d}(n)$ denote the maximal cardinaity of a Sidon set in $[1, n]^{d}$. We omit the subscript when $d=1$.

The trivial counting argument gives $F(n) \ll n^{1 / 2}$. Erdős and Turán [7] proved that $F(n) \leq n^{1 / 2}+O\left(n^{1 / 4}\right)$. This was shapened by Lindstrom [12] who proved that

$$
\begin{equation*}
F(n)<n^{1 / 2}+n^{1 / 4}+1 . \tag{1}
\end{equation*}
$$

[^0]In the $d$-dimensional case, Lindstrom [13] obtained

$$
\begin{equation*}
F_{d}(n)<n^{d / 2}+O\left(n^{d^{2} /(2 d+2)}\right) \tag{2}
\end{equation*}
$$

using the Erdős-Turán approach.
In Section 2, we study $d$-dimensional finite Sidon sets. We use the additive energy of two finite sets to obtain upper bounds for the largest cardinality of a Sidon set contained in the box $\prod_{i=1}^{d}\left[1, n_{i}\right]$. As a particular case, we recover inequality (2). We consider separately the case $d=1$ and obtain the better estimate

$$
F(n)<n^{1 / 2}+n^{1 / 4}+1 / 2 .
$$

We use the additive energy to give a short combinatorial proof of a result of Kolountzakis concerning the distribution of dense Sidon sets in arithmetic progressions. We also study gaps in dense Sidon sets of integers.

An old conjecture of Erdős claims that $F(n)<n^{1 / 2}+O(1)$. It is believed that this is not true and that the right upper bound should be $F(n)<$ $n^{1 / 2}+O\left(n^{\epsilon}\right)$. Lindstrőm made the analogous conjecture to higher dimensions

$$
F_{d}(n)<n^{d / 2}+O(1)
$$

We disprove this conjecture for $d=2$ by proving that the inequality

$$
F_{2}(n)>n+\log n \log \log \log n
$$

holds infinitely often. This result has been obtained independently by Ruzsa [16].

Perhaps the correct conjecture is $F_{2}(n)<n+O\left(n^{\epsilon}\right)$ for any $\epsilon>0$, where the constant implied by the above $O$ depends on both $d$ and $\varepsilon$. To emphasize the difficulty of this problem, we give a quick proof of the fact that the above conjecture implies that the least non quadratic residue in modulo $p$ is $\ll p^{\epsilon}$ for any $\varepsilon>0$, which is a known conjecture of Vinogradov.

As far as lower bounds for the cardinality of finite Sidon sets in higher dimensions go, we show how to map Sidon sets from $\mathbb{N}$ in $d$-dimensional
boxes, and we deduce an asymptotic estimate for the cardinality of the largest Sidon set in the box $\prod_{i=1}^{d}\left[1, n_{i}\right]$, namely that

$$
F\left(n_{1}, \ldots, n_{d}\right) \sim\left(n_{1} \cdots n_{d}\right)^{1 / 2}
$$

as $n_{1} \cdots n_{d} \rightarrow \infty$. In particular, $F_{d}(n) \sim n^{d / 2}$ as $n \rightarrow \infty$.
In Section 3, we move on to infinite Sidon sets. It is a natural problem to ask for infinite Sidon sets in $\mathbb{N}^{d}$ which are as dense as possible. Writing $A(n)=\left|A \cap[1, n]^{d}\right|$ for the counting function of a Sidon set in $\mathbb{N}^{d}$, we trivially have that $A(n) \ll n^{d / 2}$. It is a natural question to ask whether there are infinite Sidon sets $A \subset \mathbb{N}^{d}$ such that $A(n) \gg n^{d / 2}$. We prove that the answer here is no and that, in fact, any Sidon set $A \subset \mathbb{N}^{d}$ satisfies

$$
\liminf _{n \rightarrow \infty} \frac{A(n)}{\sqrt{n^{d} / \log n}}<\infty
$$

The case $d=1$ of the above result was proved by Erdős.
Next define

$$
\alpha_{d}=\sup \left\{\liminf _{n \rightarrow \infty} \frac{\log A(n)}{\log n}\right\},
$$

where the supremum above is taken over all infinite Sidon sets $A \subset \mathbb{N}^{d}$. It is easy to construct an infinite Sidon set of positive integers with $A(n) \gg n^{1 / 3}$. A construction of Ruzsa [15] provides one with $A(n) \geq n^{\sqrt{2}-1+o(1)}$ as $n \rightarrow \infty$. Ruzsa's construction and the trivial upper bound give

$$
\sqrt{2}-1 \leq \alpha_{1} \leq 1 / 2
$$

We describe how to map infinite Sidon sets in $\mathbb{N}$ to Sidon sets in $\mathbb{N}^{d}$ and viceversa in an efficient way. As a consequence, we prove that

$$
\alpha_{d}=d \alpha_{1} .
$$

So, $d(\sqrt{2}-1) \leq \alpha_{d} \leq d / 2$. In other words, the problems of finding dense infinite Sidon sets are equivalent in all dimensions.

We also obtain analogous results when we count in boxes. One of the interests in these results is that it seems easier to construct Sidon sets in higher dimensions. As an application of this approach, we obtain an explicit Sidon sequence of integers with $A(n) \geq n^{1 / 3+o(1)}$ as $n \rightarrow \infty$ by mapping the infinite Sidon set $A=\left\{\left(x, x^{2}\right), x \geq 1\right\} \subset \mathbb{N}^{2}$ to the set of positive integers.

## 2. Finite Sidon Sets

2.1. Additive energy and upper bounds. For any two finite subsets $X, Y$ of a fixed additive semigroup $G$ (usually, $\mathbb{N}$ or $\mathbb{N}^{d}$ ), we write $r_{X+Y}(z)=\#\{(x, y) \in X \times Y, x+y=z\} \quad$ and $\quad X+Y=\{x+y, x \in X, y \in Y\}$.

We will use the trivial identities $r_{X-X}(0)=|X|$ and $\sum_{z} r_{X+Y}(z)=|X||Y|$ throughout the paper.

The quantity $\sum_{x} r_{A+B}^{2}(x)$ is called the additive energy of $A$ and $B$. It counts the number of solutions $a+b=a^{\prime}+b^{\prime}$ with $a, a^{\prime} \in A, b, b^{\prime} \in B$, which is the same as the number of solutions of the equation $a-a^{\prime}=b^{\prime}-b$ with $a, a^{\prime} \in A, b, b^{\prime} \in B$. So,

$$
\begin{equation*}
\sum_{x} r_{A+B}^{2}(x)=\sum_{x} r_{A-A}(x) r_{B-B}(x) . \tag{3}
\end{equation*}
$$

See [19] for more properties and applications of the additive energy of two sets. Here, we exploit relation (3) to obtain several results on Sidon sets. First we state an easy but useful lemma.

Lemma 2.1. Let $A, B \subset G$. Then

$$
\begin{equation*}
|A|^{2} \leq \frac{|A+B|}{|B|^{2}} \sum_{x} r_{A-A}(x) r_{B-B}(x) . \tag{4}
\end{equation*}
$$

In particular, if $r_{A-A}(x) \leq s$ for all $x \neq 0$, then

$$
\begin{equation*}
|A|^{2} \leq|A+B|\left(s+\frac{|A|-s}{|B|}\right) \tag{5}
\end{equation*}
$$

Proof. Cauchy's inequality together with (3) give

$$
\begin{aligned}
(|A||B|)^{2}=\left(\sum_{x \in A+B} r_{A+B}(x)\right)^{2} & \leq|A+B| \sum_{x} r_{A+B}^{2}(x) \\
& =|A+B| \sum_{x} r_{A-A}(x) r_{B-B}(x)
\end{aligned}
$$

For the second assertion, we observe that the sum in (4) is bounded by

$$
r_{A-A}(0) r_{B-B}(0)+s \sum_{g \neq 0} r_{B-B}(g)=|A||B|+s\left(|B|^{2}-|B|\right) .
$$

The inequality (4) appears in [9], which is a nice introduction to additive combinatorics. Ruzsa [14] discovered inequality (5) (for $s=1$ ) by a different method and used it to obtain inequality (2).

Corollary 2.1. Let $A \subset[1, n] \cap \mathbb{N}$ be such that $r_{A-A}(x) \leq s$ for all $x \neq 0$. Then

$$
|A|<(s n)^{1 / 2}+(s n)^{1 / 4}+1 / 2 .
$$

Proof. We take $B=[0, l] \cap \mathbb{Z}$ with $l=\lfloor\sqrt{n(|A|-s) / s}\rfloor$. Then $|A+B| \leq n+l$ and $|B|=l+1$. So,

$$
\begin{aligned}
|A|^{2} \leq & (n+l)\left(s+\frac{|A|-s}{l+1}\right)<s n+s l+\frac{n(|A|-s)}{l+1}+|A|-s \\
& \leq s n+2 \sqrt{s n(|A|-s)}+|A|-s=(\sqrt{s n}+\sqrt{|A|-s})^{2} .
\end{aligned}
$$

Thus, $(|A|-\sqrt{s n})^{2}<|A|-s$. Writing $|A|=\sqrt{s n}+c(s n)^{1 / 4}+1 / 2$, we obtain

$$
c^{2}(s n)^{1 / 2}+c(s n)^{1 / 4}+1 / 4<(s n)^{1 / 2}+c(s n)^{1 / 4}-(s-1 / 2)
$$

which yields a contradiction when $c \geq 1$.
Corollary 2.2. We have $F(n)<n^{1 / 2}+n^{1 / 4}+1 / 2$.
Proof. We take $s=1$ in Corollary 2.1 above.
While Corollary 2.2 is not a huge improvement upon (1), we have included it because it seems to be the limit of counting small differences.

Corollary 2.3. Let $C$ be a convex set contained in $(0,1]^{d}$ with $\mu(C)>0$. Then, any Sidon set $A$ contained in $X_{t}=t \cdot C \cap \mathbb{N}^{d}$ satisfies

$$
|A| \leq t^{d / 2} \mu^{1 / 2}(C)+O\left(t^{d^{2} /(2 d+2)}\right)
$$

Proof. Take $B=X_{s}$ with $s=\left\lfloor t^{(d+2) /(2 d+2)}\right\rfloor$. Then $A+B \subset X_{t+s}=$ $(t+s) \cdot C \cap \mathbb{N}^{d}$, so

$$
|A+B| \leq(t+s)^{d} \mu(C)+O\left(t^{d-1}\right)=t^{d} \mu(C)+O\left(s t^{d-1}\right) .
$$

We now use (5) and the trivial estimate $|A|=O\left(t^{d / 2}\right)$ to obtain

$$
|A|^{2} \leq\left(t^{d} \mu(C)+O\left(s t^{d-1}\right)\right)\left(1+O\left(t^{d / 2} / s^{d}\right)\right)=t^{d} \mu(C)\left(1+O\left(t^{-\frac{d}{2 d+2}}\right)\right)
$$

We observe that by taking $C=(0,1]^{d}$ in Corollary 2.3 above we recover the Lindstrom's upper bound given in (2.5). The next result deals with Sidon sets in general boxes. It is interesting to note the dependence of the error term on the excentricity of the box.

Theorem 2.1. Denote by $F\left(n_{1}, \ldots, n_{d}\right)$ the largest cardinality of a Sidon set in the box $\prod_{i=1}^{d}\left[1, n_{i}\right]$. Let $N_{0}=1, N_{i}=\prod_{j=1}^{i} n_{j}, 1 \leq i \leq d, N=N_{d}$, and let $s$ be the least index such that $n_{s}^{d-s+2} N_{s-1} \geq \sqrt{N}$. Then

$$
\begin{equation*}
F\left(n_{1}, \ldots, n_{d}\right) \leq \sqrt{N}\left(1+O\left(\left(\frac{N_{s-1}}{\sqrt{N}}\right)^{\frac{1}{d-s+2}}\right)\right) \tag{6}
\end{equation*}
$$

Furthermore,

$$
\begin{equation*}
F\left(n_{1}, \ldots, n_{d}\right) \leq \sqrt{N}+O\left(N^{d /(2 d+2)}\right) \tag{7}
\end{equation*}
$$

Proof. We first prove that $N_{i} \leq N^{i /(2 d+2)}$ for all $0 \leq i<s$. This is clear for $i=0$. Suppose that $i \geq 1$ and that it is true for $i-1$. Then, since $i<s$, we have that

$$
\begin{aligned}
N_{i}^{d-i+2}=n_{i}^{d-i+2} N_{i-1}^{d-i+2} & =\left(n_{i}^{d-i+2} N_{i-1}\right) N_{i-1}^{d-i+1} \\
& <N^{\frac{1}{2}}\left(N^{\frac{i-1}{2 d+2}}\right)^{d-i+1}=\left(N^{\frac{i}{2 d+2}}\right)^{d-i+2}
\end{aligned}
$$

In particular, we get $\left(\frac{N_{s-1}}{\sqrt{N}}\right)^{\frac{1}{d-s+2}}<N^{-\frac{1}{2 d+2}}$, so (6) implies (7).
Let $r_{i}=0$ for $i<s$ and $r_{i}=\left\lfloor n_{i}\left(N_{s-1} / \sqrt{N_{d}}\right)^{1 /(d-s+2)}\right\rfloor$ for $s \leq i \leq d$. If we take $B=\left(\left[0, r_{1}\right] \times \cdots\left[0, r_{d}\right]\right) \cap \mathbb{Z}^{d}$, then

$$
\begin{aligned}
|B|=\prod_{i \geq s}\left(r_{i}+1\right) & \geq \prod_{i \geq s}\left(n_{i}\left(\frac{N_{s-1}}{\sqrt{N}}\right)^{\frac{1}{d-s+2}}\right) \\
& =\frac{N}{N_{s-1}}\left(\frac{N_{s-1}}{\sqrt{N}}\right)^{\frac{d-s+1}{d-s+2}}=\sqrt{N}\left(\frac{\sqrt{N}}{N_{s-1}}\right)^{\frac{1}{d-s+2}} . \\
|A+B| \leq \prod_{i=1}^{d}\left(n_{i}+r_{i}\right) & =N \prod_{i \geq s}\left(1+\frac{r_{i}}{n_{i}}\right) \leq N\left(1+O\left(\left(\frac{N_{s-1}}{\sqrt{N}}\right)^{\frac{1}{d-s+2}}\right)\right) .
\end{aligned}
$$

Since $A+A \subset\left[1,2 n_{1}\right] \times \cdots \times\left[1,2 n_{d}\right]$ and $|A+A|=\binom{|A|+1}{2}$, we obtain the trivial estimate, $|A| \leq 2^{(d+1) / 2} \sqrt{N}$. Putting these estimates in Lemma 2.1,
we obtain

$$
\begin{aligned}
|A|^{2} & \leq N\left(1+O\left(\left(\frac{N_{s-1}}{\sqrt{N}}\right)^{\frac{1}{d-s+2}}\right)\right)\left(1+\frac{2^{(d+1) / 2} \sqrt{N}}{\sqrt{N}\left(\frac{\sqrt{N}}{N_{s-1}}\right)^{\frac{1}{d-s+2}}}\right) \\
& =N\left(1+O\left(\left(\frac{N_{s-1}}{\sqrt{N}}\right)^{\frac{1}{d-s+2}}\right)\right) .
\end{aligned}
$$

In the next result we show, as an example, how the above Theorem 2.1 specializes when $d=2$.

Corollary 2.4. Denote by $F\left(n_{1}, n_{2}\right)$ the maximum cardinality of a Sidon set $A \subset\left[1, n_{1}\right] \times\left[1, n_{2}\right], n_{1} \leq n_{2}$. Then

$$
\begin{equation*}
F\left(n_{1}, n_{2}\right) \leq\left(n_{1} n_{2}\right)^{1 / 2}+O\left(\min \left(\left(n_{1} n_{2}\right)^{1 / 3},\left(n_{1}^{3} n_{2}\right)^{1 / 4}\right)\right) . \tag{8}
\end{equation*}
$$

Proof. Using the notations of the proof of Theorem 2.1, we have that $s=1$ when $n_{1}^{3} \geq\left(n_{1} n_{2}\right)^{1 / 2}$; that is, when $n_{2} \leq n_{1}^{5}$. In this case,
$F\left(n_{1}, n_{2}\right) \leq\left(n_{1} n_{2}\right)^{1 / 2}\left(1+O\left(\left(\frac{1}{\left(n_{1} n_{2}\right)^{1 / 2}}\right)^{1 / 3}\right)\right)=\left(n_{1} n_{2}\right)^{1 / 2}+O\left(\left(n_{1} n_{2}\right)^{1 / 3}\right)$.
If $n_{2}>n_{1}^{5}$, then $s=2$, therefore
$F\left(n_{1}, n_{2}\right) \leq\left(n_{1} n_{2}\right)^{1 / 2}\left(1+O\left(\left(\frac{n_{1}}{\left(n_{1} n_{2}\right)^{1 / 2}}\right)^{1 / 2}\right)\right)=\left(n_{1} n_{2}\right)^{1 / 2}+O\left(\left(n_{1}^{3} n_{2}\right)^{1 / 4}\right)$.

Although is not our goal to extend this work to the study of $B_{2}[g]$ sets, which are the sets $A$ with $\left|\left\{\left(a, a^{\prime}\right), a+a^{\prime}=x, a \leq a^{\prime}, a, a^{\prime} \in A\right\}\right| \leq g$ for all $x$, we cannot resist the temptation to present an immediate application of the identity (3) to a non trivial upper bound for the largest $B_{2}[g]$ set in $\{1, \ldots n\}$.

Corollary 2.5. If $A \subset\{1, \ldots, n\}$ is a $B_{2}[g]$ set, then $|A| \leq \sqrt{4 g-2} n^{1 / 2}+1$.
Proof. For brevity, we write $r(x)=r_{A+A}(x)$ and $d(x)=r_{A-A}(x)$. Since $A$ is a $B_{2}[g]$ set, we have that $r(x) \leq 2 g$ for all $x$. In the sequel, we will use the
identities $\sum_{x} r(x)=\sum_{x} d(x)=|A|^{2}, d(0)=|A|$ and $\sum_{x} r^{2}(x)=\sum_{x} d^{2}(x)$.
This last identity is (3) when $B=A$. Then

$$
\begin{align*}
\sum_{x \neq 0} d^{2}(x) & =\sum_{x} d^{2}(x)-|A|^{2}=\sum_{x} r^{2}(x)-|A|^{2} \\
& \leq \sum_{x} r(x)(r(x)-2 g)+2 g \sum_{x} r(x)-|A|^{2} \leq(2 g-1)|A|^{2} \tag{9}
\end{align*}
$$

On the other hand,

$$
\begin{equation*}
\sum_{x \neq 0} d^{2}(x)=\sum_{1 \leq|x| \leq n} d^{2}(x) \geq \frac{\left(\sum_{x \neq 0} d(x)\right)^{2}}{2 n}=\frac{\left(|A|^{2}-|A|\right)^{2}}{2 n} \tag{10}
\end{equation*}
$$

The case $g=2$ was proved in [4]. As it was observed in [10], that proof can be generalized to any $g \geq 2$. Indeed, better upper bounds are known. See [6] for a recent survey of the current records.

### 2.2. Distribution in dense Sidon sets.

Corollary 2.6. Let $A$ be a Sidon set contained in $[1, n]$ with size $|A|=n^{1 / 2}-$ $c n^{1 / 4}$. Then, the maximum gap in $A$ (i.e., distance between two consecutive elements) satisfies $g(A) \leq(4+2 c) n^{3 / 4}$.

Proof. Suppose that there exists a gap $[m, m+g-1]$ and consider $X=$ $([1, m-1] \cup[m+g, n]) \cap \mathbb{Z}$ and $B=[0, l] \cap \mathbb{Z}$ with $l=\left\lfloor\sqrt{(n-g) n^{1 / 2}}\right\rfloor$. Since $A \subset X$, we have $|A+B| \leq|X+B| \leq|X|+2|B|-2 \leq n-g+2 l$. We now use Lemma 2.1 and the trivial estimate $|A| \leq 2 n^{1 / 2}$ to get

$$
\begin{aligned}
|A|^{2} & \leq(n-g+2 l)\left(1+\frac{2 n^{1 / 2}}{l+1}\right)=n-g+4 n^{1 / 2}+2 l+\frac{2(n-g) n^{1 / 2}}{l+1} \\
& \leq n-g+4 n^{1 / 2}+4 \sqrt{(n-g) n^{1 / 2}}=\left(\sqrt{n-g}+2 n^{1 / 4}\right)^{2}
\end{aligned}
$$

Thus, $n^{1 / 2}-c n^{1 / 4} \leq \sqrt{n-g}+2 n^{1 / 4}$, which leads to the desired result after obvious algebraic manipulations.

A less precise statement of the Corollary 2.6 above was proved in [3] as a consequence of the well distribution in $[1, n]$ of Sidon sets of large cardinality. We observe that, under the condition $|A|=n^{1 / 2}+O\left(n^{1 / 4}\right)$, the exponent
$3 / 4$ is sharp. To see this, we take a Sidon set $A \subset[1, n]$ with $|A|=n^{1 / 2}$. We slice the interval $[1, n]$ in $n^{1 / 4} / c$ intervals of length $c n^{3 / 4}$. One of them must contain no more than $|A| /\left(n^{1 / 4} / c\right) \leq c n^{1 / 4}$ elements of $A$. Removing these elements from $A$, we get a Sidon set $A^{\prime}$ with $\left|A^{\prime}\right| \geq n^{1 / 2}-c n^{1 / 4}$ and a gap of length $\mathrm{cn}^{3 / 4}$. It is believed that the maximum gap of a Sidon set in $[1, n]$ of maximal cardinality is $O\left(n^{1 / 2+\varepsilon}\right)$.

Kolountzakis [11] used analytic methods and a theorem on the minimum value of a sum of cosines to prove that dense Sidon sets in $[1, n]$ are well distributed in residues classes $(\bmod q)$ when $q=o\left(n^{1 / 2}\right)$ as $n \rightarrow \infty$. We now give a short combinatorial proof of this result.

Theorem 2.2 (Kolountzakis). Let $A \subset\{1, \ldots, n\}$ be a Sidon set with $|A| \geq$ $n^{1 / 2}-l$. Given $q$, we write $A_{i}=\{a \in A, a \equiv i(\bmod q)\}$. Then
i) $\sum_{i=0}^{q-1}\left(\left|A_{i}\right|-\frac{|A|}{q}\right)^{2} \leq \frac{4 \ln n^{1 / 2}}{q}+\frac{8 n^{3 / 4}}{q^{1 / 2}}$.
ii) $\left|A_{i}\right|=\frac{|A|}{q}+\theta\left(\frac{\max \{0, l\}^{1 / 2} n^{1 / 4}}{q^{1 / 2}}+\frac{n^{3 / 8}}{q^{1 / 4}}\right)$, for some $|\theta|<3$.
iii) If $q<\frac{n^{1 / 6}}{100}$ and $l<n^{1 / 3}$, then $A$ contains all residues $(\bmod q)$.

Proof. We split $A$ in residues classes, $A=\cup_{i=1}^{q}\left(q \cdot A_{i}+i\right)$ with $A_{i} \subset[0,\lfloor n / q\rfloor]$. We let $B=[0,|B|-1] \cap \mathbb{Z}$, so $\left|A_{i}+B\right| \leq\lfloor n / q\rfloor+|B|$. We observe also that if $a_{i}-a_{i}^{\prime}=a_{j}-a_{j}^{\prime} \neq 0$, then $\left(q a_{i}+i\right)-\left(q a_{i}^{\prime}+i\right)=\left(q a_{j}+j\right)-\left(q a_{j}^{\prime}+j\right)$, which is impossible since $A$ is a Sidon set. So, $\sum_{i=1}^{q} r_{A_{i}-A_{i}}(g) \leq 1$ for $g \neq 0$.

Using Lemma 2.1 for each $A_{i}$ and summing up the inequality (5) over all $i=1, \ldots, q$, we get that

$$
\begin{aligned}
\sum_{i=1}^{q}\left|A_{i}\right|^{2} & \leq \sum_{i=1}^{q} \frac{\left|A_{i}+B\right|}{|B|^{2}} \sum_{g} r_{A_{i}-A_{i}}(g) r_{B-B}(g) \\
& \leq \frac{\lfloor n / q\rfloor+|B|}{|B|^{2}}\left(\sum_{i=0}^{q}\left|A_{i}\right||B|+\sum_{g \neq 0}\left(\sum_{i=1}^{q} r_{A_{i}-A_{i}}(g)\right) r_{B-B}(g)\right) \\
& \leq \frac{\lfloor n / q\rfloor+|B|}{|B|^{2}}\left(|A||B|+\sum_{g \neq 0} r_{B-B}(g)\right) \\
& =\frac{\lfloor n / q\rfloor+|B|}{|B|^{2}}\left(|A||B|+|B|^{2}-|B|\right) \\
& =\lfloor n / q\rfloor+|A|-1+|B|+(|A|-1)\lfloor n / q\rfloor /|B|
\end{aligned}
$$

Taking $|B|=\lceil\sqrt{|A| n / q}\rceil$, we obtain

$$
\sum_{i=1}^{q}\left|A_{i}\right|^{2}<\frac{n}{q}+|A|+2 \sqrt{|A| n / q}
$$

We now write $|A|=n^{1 / 2}-l$ and use the trivial estimate $|A| \leq 3 n^{1 / 2}$, to get

$$
\begin{aligned}
\sum_{i}\left(\left|A_{i}\right|-|A| / q\right)^{2} & =\sum_{i}\left|A_{i}\right|^{2}-|A|^{2} / q<\frac{n-|A|^{2}}{q}+|A|+2 \sqrt{|A| n / q} \\
& <\frac{4 l n^{1 / 2}}{q}+4 n^{1 / 2}+\frac{4 n^{3 / 4}}{q^{1 / 2}}<\frac{4 l n^{1 / 2}}{q}+\frac{8 n^{3 / 4}}{q^{1 / 2}}
\end{aligned}
$$

which is i). To deduce ii) from i), we observe that

$$
\left|A_{i}-|A| / q\right| \leq\left(\sum_{i}\left(\left|A_{i}\right|-|A| / q\right)^{2}\right)^{1 / 2} \leq \frac{2 l^{1 / 2} n^{1 / 4}}{q^{1 / 2}}+\frac{2 \sqrt{2} n^{3 / 8}}{q^{1 / 4}}
$$

Finally, iii) follows easily from ii).
We observe that iii) is tight up to constants. Take a Sidon set $A$ with $n^{1 / 2}$ elements, which is possible for infinitely many values of $n$. Consider $q=\left[n^{1 / 6}\right]$. There exists $r$ such that $|\{a \in A, a \equiv r(\bmod q)\}| \leq n^{1 / 2} / q \leq$ $n^{1 / 3}$. Now we remove these elements from $A$. The new set $A^{\prime}$ satisfies that $\left|A^{\prime}\right| \geq n^{1 / 2}-n^{1 / 3}$ and one of the residues $(\bmod q)$ with $q \sim n^{1 / 6}$ doesn't appear in $A^{\prime}$.
2.3. Lindstrom's conjecture. Erdős and Turan asked if $F(n)<n^{1 / 2}+$ $O(1)$ holds for all $n$. This unsolved question was generalized by Lindstrom [12] in 1969 for any $d$ who asked whether

$$
\begin{equation*}
F_{d}(n)<n^{d / 2}+O(1) \tag{11}
\end{equation*}
$$

holds for all $n$ and $d$, where the constant in $O$ may depend on $d$.
We answer this question in the negative for $d=2$. Ruzsa [16] has also proved the result below independently by a similar construction.

Theorem 2.3. There exists a constant $c>0$ and infinitely many integers $n$ such that

$$
F_{2}(n)>n+c \log n \log \log \log n .
$$

Proof. Let $n_{p}$ be the least quadratic non-residue $(\bmod p)$, where $p$ is an odd prime. It is known [8] that there exists a constant $c_{0}>0$ such that the inequality $n_{p}>c_{0} \log p \log \log \log p$ holds for infinitely many primes $p$. For one of these primes $p$, consider the set

$$
A_{p}=\left\{\left(\left(n_{p} k^{2}\right)_{p},\left(n_{p}(k+1)^{2}\right)_{p}\right), k=1, \ldots p\right\}
$$

where $(x)_{p}$ denotes the least positive integer which is congruent with $x$ $(\bmod p)$. First we will prove that $A_{p}$ is a Sidon set in $\mathbb{Z}_{p} \times \mathbb{Z}_{p}$. Suppose that $\left(n_{p} k_{1}^{2}, n_{p}\left(k_{1}+1\right)^{2}\right)+\left(n_{p} k_{2}^{2}, n_{p}\left(k_{2}+1\right)^{2}\right) \equiv\left(n_{p} k_{3}^{2}, n_{p}\left(k_{3}+1\right)^{2}\right)+\left(n_{p} k_{4}^{2}, n_{p}\left(k_{4}+1\right)^{2}\right) \quad(\bmod p)$.
Then $\left\{\begin{array}{l}k_{1}^{2}+k_{2}^{2} \equiv k_{3}^{2}+k_{4}^{2}(\bmod p) \\ \left(k_{1}+1\right)^{2}+\left(k_{2}+1\right)^{2} \equiv\left(k_{3}+1\right)^{2}+\left(k_{4}+1\right)^{2}(\bmod p),\end{array}\right.$ and we easily obtain that $\left\{\begin{array}{l}k_{1} \equiv k_{3}(\bmod p) \\ k_{2} \equiv k_{4}(\bmod p)\end{array}\right.$ or $\left\{\begin{array}{l}k_{1} \equiv k_{4}(\bmod p) \\ k_{2} \equiv k_{3}(\bmod p)\end{array}\right.$. Thus, $A_{p}$ is a Sidon set in $\mathbb{Z}_{p} \times \mathbb{Z}_{p}$, and since that $n_{p} k^{2}$ and $n_{p}(k+1)^{2}$ are quadratic non-residues $(\bmod p)$, we have that $A_{p} \subset\left[n_{p}, p\right]^{2}$. Hence, the set $A_{p}-\left(n_{p}-1, n_{p}-1\right)$ is a Sidon set with $p$ elements included in $\left[1, p-n_{p}+1\right]^{2}$. Then

$$
F_{2}\left(p-n_{p}+1\right) \geq p=p-n_{p}+1+n_{p}-1,
$$

and the theorem follows taking $n=p-n_{p}+1$.

It is believed that the correct conjecture is the following:
Conjecture: For any $\varepsilon>0$, we have $F_{2}(n)<n+O\left(n^{\varepsilon}\right)$.
Theorem 2.4. The estimate $F_{2}(n)<n+O\left(n^{\varepsilon}\right)$ implies that the least quadratic non-residue modulo $p$ is of size $O\left(p^{\varepsilon}\right)$, which is a known conjecture of Vinogradov.

Proof. Using the same construction as in Theorem 2.3, we have with the notations from its proof that

$$
p \leq F_{2}\left(p-n_{p}\right)<p-n_{p}+O\left(\left(p-n_{p}\right)^{\varepsilon}\right),
$$

and the result follows.
2.4. Lower bounds. Three different constructions of maximal Sidon sets which show that $F(n) \geq n^{1 / 2}(1+o(1))$ are known ([1], [14] and [17]). In particular, they all imply that

$$
\begin{equation*}
F(n) \sim n^{1 / 2} \tag{12}
\end{equation*}
$$

There is a natural way to map one dimensional Sidon sets to $d$-dimensional Sidon sets. The next lemma will help us in this respect.

Lemma 2.2. Let $n_{1}, \ldots, n_{d}$ be positive integers and write

$$
N_{0}=1, \quad N_{i}=\prod_{1 \leq k \leq i} n_{k}, \quad i=1, \ldots, d
$$

For each integer $a, 0 \leq a \leq N_{d}-1$, let $a_{1}, \ldots, a_{d}$ be integers such that

$$
\begin{equation*}
a=\sum_{i=1}^{d} a_{i} N_{i-1}, \quad \text { and } \quad 0 \leq a_{i} \leq n_{i}-1, \quad i=1, \ldots, d \tag{13}
\end{equation*}
$$

Proof. Notice that $0 \leq a \leq \sum_{i=1}^{d}\left(n_{i}-1\right) N_{i-1}=\sum_{i=1}^{d} N_{i}-N_{i-1}=N_{d}-1$. Then, to conclude the proof, it is enough to prove that all the representations in (13) are distinct.

Suppose that $\sum_{i=1}^{d} a_{i} N_{i-1}=\sum_{i=1}^{d} a_{i}^{\prime} N_{i-1}$ and let $j$ denote the lowest index such that $a_{j} \neq a_{j}^{\prime}$. Then $\sum_{i=j}^{d} a_{i} N_{i-1}=\sum_{i=j}^{d} a_{i}^{\prime} N_{i-1}$. Dividing by $N_{j-1}$ we obtain that $a_{j} \equiv a_{j}^{\prime}\left(\bmod n_{j}\right)$. But the condition $1 \leq a_{j}, a_{j}^{\prime} \leq n_{j}$ forces $a_{j}=a_{j}^{\prime}$.

Theorem 2.5. Let $n_{1}, \ldots, n_{d}$ be positive integers. If we denote by $F\left(n_{1}, \ldots, n_{d}\right)$ the largest size of a Sidon set contained in the box $\left[1, n_{1}\right] \times \cdots \times\left[1, n_{d}\right]$, then

$$
F\left(n_{1}, \ldots, n_{d}\right) \geq F\left(n_{1} \cdots n_{d}\right)
$$

In particular,

$$
\begin{equation*}
F_{d}(n) \geq F\left(n^{d}\right) \tag{14}
\end{equation*}
$$

Proof. Let $\varphi_{d}$ denote the function defined by $\varphi_{d}(a)=\left(a_{1}, \ldots, a_{d}\right)$, where $a_{1}, \ldots, a_{d}$ are defined in (13). This function maps Sidon sets to Sidon sets. To see it, suppose that $A$ is a Sidon set and for $a, a^{\prime}, a^{\prime \prime}, a^{\prime \prime \prime} \in A$ we have that

$$
\varphi_{d}(a)+\varphi_{d}\left(a^{\prime}\right)=\varphi_{d}\left(a^{\prime \prime}\right)+\varphi_{d}\left(a^{\prime \prime \prime}\right) .
$$

Then,

$$
a_{i}+a_{i}^{\prime}=a_{i}^{\prime \prime}+a_{i}^{\prime \prime \prime}, \quad \text { for } i=1, \ldots, d
$$

Thus,

$$
\sum_{i=1}^{d} a_{i} N_{i-1}+\sum_{i=1}^{d} a_{i}^{\prime} N_{i-1}=\sum_{i=1}^{d} a_{i}^{\prime \prime} N_{i-1}+\sum_{i=1}^{d} a_{i}^{\prime \prime} N_{i-1},
$$

therefore, $a+a^{\prime}=a^{\prime \prime}+a^{\prime \prime \prime}$. Since $A$ is a Sidon set, we have that $\left\{a, a^{\prime}\right\}=$ $\left\{a^{\prime \prime}, a^{\prime \prime \prime}\right\}$, so $\left\{\varphi_{d}(a), \varphi_{d}\left(a^{\prime}\right)\right\}=\left\{\varphi_{d}\left(a^{\prime \prime}\right), \varphi_{d}\left(a^{\prime \prime \prime}\right)\right\}$. Hence, we have showed that the set $\varphi_{d}(A)$ is also a Sidon set.

Let $A \subset\left[1, n_{1} \cdots n_{d}\right]$ be a Sidon set. If $A$ is a Sidon set in $\left[1, n_{1} \cdots n_{d}\right]$, then $A-1$ is a Sidon set in $\left[0, n_{1} \cdots n_{d}-1\right]$. Then $\varphi_{d}(A-1)$ is Sidon set in $\left[0, n_{1}-1\right] \times \cdots \times\left[0, n_{d}-1\right]$, so the set $\varphi_{d}(A-1)+(1, \ldots, 1)$ is a Sidon set in $\left[1, n_{1}\right] \times \cdots \times\left[1, n_{d}\right]$.

Corollary 2.7. For all positive integers $d$, we have that

$$
F_{d}(n) \sim n^{d / 2} \quad \text { as } \quad n \rightarrow \infty
$$

Proof. This is a consequence of (2), (12) and (14).

## 3. Infinite Sidon sets

Dealing with infinite Sidon sequences is a much more complicated matter both for the case for $d=1$ as well as when $d>1$. Futhermore, there is no known natural way to map infinite Sidon sets in $\mathbb{N}$ to Sidon sets in $\mathbb{N}^{d}$ or viceversa. Doing it in an economical way is part of this work. Let $A \subset \mathbb{N}^{d}$ be an infinite Sidon set and let

$$
A(n)=\#\left\{a=\left(a_{1}, \ldots, a_{d}\right) \in A, a_{i} \leq n, \text { for all } i=1, \ldots, d\right\}
$$

denote, as usual, the natural counting function of $A$. In general, given positive numbers $t_{1}, \ldots, t_{d}$, we let

$$
A\left(n^{t_{1}}, \ldots, n^{t_{d}}\right)=\#\left\{a=\left(a_{1}, \ldots, a_{d}\right) \in A, a_{i} \leq n^{t_{i}}, \text { for all } i=1, \ldots, d\right\}
$$

3.1. Upper bounds. Obviously, for any Sidon set $A$ in $\mathbb{N}^{d}$, we have that

$$
\begin{equation*}
A(n) \leq F_{d}(n) \ll n^{d / 2} \tag{15}
\end{equation*}
$$

It is a natural question to ask whether there exist infinite Sidon sets $A$ such that $A(n) \gg n^{d / 2}$ holds for all $n$. Erdős [18] answered this question in the negative for $d=1$ by proving that

$$
\liminf _{n \rightarrow \infty} \frac{A(n)}{\sqrt{n / \log n}} \ll 1
$$

Trujillo [20] studied the 2-dimensional case and gave a partial answer to this question by proving that

$$
\lim _{N \rightarrow \infty} \inf _{n, m>N} \frac{A(n, m)}{\sqrt{n m / \log (n m)}} \ll 1
$$

where $A(n, m)$ is the size of $A \cap[1, n] \times[1, m]$. Unfortunately this estimate is not strong enough to prove that $\lim _{\inf }^{n \rightarrow \infty}$ $\frac{A(n)}{n}=0$ for any infinite Sidon set $A \subset \mathbb{N}^{2}$. We solve this question for any $d \geq 1$.

Theorem 3.1. For any positive integer $d \geq 1$ and for any infinite Sidon set $A$ in $\mathbb{N}^{d}$, we have

$$
\liminf _{n \rightarrow \infty} \frac{A(n)}{\sqrt{n^{d} / \log n}} \ll 1
$$

Proof. Let $\tau(N)=\inf _{n>N} \frac{A(n)(\log n)^{1 / 2}}{n^{d / 2}}$ and consider the $d$-dimensional box $\left(0, N^{2}\right]^{d}$. For any $\overrightarrow{\mathrm{i}}=\left(i_{1}, \ldots, i_{d}\right), 0 \leq i_{j}<N$, let denote by $C_{\overrightarrow{\mathrm{r}}}$ the number of elements of $A$ lying in the small box $N \cdot \overrightarrow{1}+(0, N]^{d}$. For each $l=0,1, \ldots$, let $D_{l}=\sum_{\mid \overrightarrow{1}=l} C_{\overrightarrow{1}}$, where $|\overrightarrow{\mathrm{i}}|=\max _{1 \leq j \leq d} i_{j}$. Then

$$
D_{l}^{2} \leq d(l+1)^{d-1} \sum_{|\vec{i}|=l} C_{\mathrm{r}}^{2},
$$

so,

$$
\frac{1}{d} \sum_{0 \leq l<N} \frac{D_{l}^{2}}{(l+1)^{d-1}} \leq \sum_{0 \leq|\mathrm{i}|<N} C_{\overrightarrow{\mathrm{r}}}+\sum_{0 \leq|\mathrm{i}|<N} C_{\overrightarrow{\mathrm{r}}}\left(C_{\overrightarrow{\mathrm{r}}}-1\right) .
$$

By (15), we have that

$$
\sum_{0 \leq|\mathrm{r}|<N} C_{\overrightarrow{\mathrm{r}}}=A\left(N^{2}\right) \ll_{d} N^{d} .
$$

Observe that all the differences $\bar{a}-\bar{a}^{\prime}$ with $\bar{a} \neq \bar{a}^{\prime}$ both in the same small box belong to $(-N, N)^{d}$. This property together with the Sidon property give

$$
\sum_{\overrightarrow{\mathrm{r}}} C_{\overrightarrow{\mathrm{r}}}\left(C_{\overrightarrow{\mathrm{r}}}-1\right) \leq(2 N)^{d} .
$$

So,

$$
\sum_{0 \leq l<N} \frac{D_{l}^{2}}{(l+1)^{d-1}} \ll d_{d} N^{d} .
$$

On the other hand, we can write

$$
\left(\sum_{0 \leq l<N} \frac{D_{l}}{(l+1)^{d / 2}}\right)^{2} \leq \sum_{0 \leq l<N} \frac{D_{l}^{2}}{(l+1)^{d-1}} \sum_{0 \leq l<N} \frac{1}{(l+1)} \ll_{d} N^{d} \log N .
$$

Now we sum by parts to obtain

$$
\begin{array}{r}
\sum_{0 \leq l<N} \frac{D_{l}}{(l+1)^{d / 2}}=\sum_{1 \leq l \leq N} \frac{D_{l-1}}{l^{d / 2}} \gg d \int_{1}^{N} \frac{\sum_{l \leq t} D_{l-1}}{t^{d / 2+1}} d t= \\
\int_{1}^{N} \frac{A(t N)}{t^{d / 2+1}} d t \gg_{d} \int_{1}^{N} \frac{\tau(N)(t N)^{d / 2}}{(\log (t N))^{1 / 2}} \frac{1}{t^{d / 2+1}} d t \ggg_{d} \tau(N) N^{d / 2}(\log N)^{1 / 2} .
\end{array}
$$

From (9), (10) and (12), we obtain that $\lim _{N \rightarrow \infty} \tau(N) \ll_{d} 1$.
3.2. Lower bounds. It is time to consider lower bounds for infinite Sidon sequences in $\mathbb{N}^{d}$. We introduce the quantity

$$
\alpha_{d}=\sup _{A \text { Sidon set in } \mathbb{N}^{d}} \liminf _{n \rightarrow \infty} \frac{\log A(n)}{\log n}
$$

It is known that $\sqrt{2}-1 \leq \alpha_{1} \leq 1 / 2$. The upper bound follows trivially from (1), and the lower bound cames from a clever construction by Ruzsa [15]. It is believed that $\alpha_{1}=1 / 2$.

To deal with more general counting functions for infinite Sidon sets in $\mathbb{N}^{d}$, we introduce the quantity

$$
\alpha^{t_{1}, \ldots, t_{d}}=\sup _{A \text { Sidon set in } \mathbb{N}^{d}} \liminf _{n \rightarrow \infty} \frac{\log A\left(n^{t_{1}}, \ldots, n^{t_{d}}\right)}{\log n}
$$

Notice that $\alpha^{\overbrace{1, \ldots, 1}}=\alpha_{d}$. Here, we prove the following result.

Theorem 3.2. For all positive numbers $t_{1}, \ldots, t_{d}$, we have that

$$
\begin{equation*}
\alpha^{t_{1}, \ldots, t_{d}}=\left(t_{1}+\cdots+t_{d}\right) \alpha_{1} \tag{16}
\end{equation*}
$$

In particular, $\alpha_{d}=d \alpha_{1}$.

Proof. To prove that $\alpha^{t_{1}, \ldots, t_{d}} \leq\left(t_{1}+\cdots+t_{d}\right) \alpha_{1}$, we map $\mathbb{N}^{d}$ to $\mathbb{N}$ by using an injective function $\phi$ with the following two properties:
i) $\phi$ maps Sidon sets in $\mathbb{N}^{d}$ to Sidon sets in $\mathbb{N}$.
ii) $\phi\left(\left(\left[1, n^{t_{1}}\right] \times \cdots \times\left[1, n^{t_{d}}\right]\right) \cap \mathbb{N}^{d}\right) \subset\left[1, n^{t_{1}+\cdots+t_{d}+\epsilon(n)}\right]$, with $\epsilon(n) \rightarrow 0$ as $n \rightarrow \infty$.

Suppose that we have constructed such a function $\phi$. Then, given $\varepsilon>0$, let $A \in \mathbb{N}^{d}$ be an infinite Sidon set such that

$$
\begin{equation*}
\alpha^{t_{1}, \ldots, t_{d}}-\varepsilon \leq \liminf _{n \rightarrow \infty} \frac{\log A\left(n^{t_{1}}, \ldots, n^{t_{d}}\right)}{\log n} \tag{17}
\end{equation*}
$$

By ii), we have that

$$
\begin{equation*}
A\left(n^{t_{1}}, \ldots, n^{t_{d}}\right) \leq \phi(A)\left(n^{t_{1}+\cdots+t_{d}+\epsilon(n)}\right) \tag{18}
\end{equation*}
$$

Then, by i), (18) and (17), we obtain

$$
\begin{aligned}
& \frac{\alpha^{t_{1}, \ldots, t_{d}}-\varepsilon}{t_{1}+\cdots+t_{d}} \leq \liminf _{n \rightarrow \infty} \frac{\log A\left(n^{t_{1}}, \ldots, n^{t_{d}}\right)}{\log \left(n^{t_{1}+\cdots+t_{d}+\epsilon(n)}\right)} \\
& \leq \liminf _{n \rightarrow \infty} \frac{\log \left(\phi(A)\left(n^{t_{1}+\cdots+t_{d}+\epsilon(n)}\right)\right)}{\log \left(n^{t_{1}+\cdots+t_{d}+\epsilon(n)}\right)} \leq \alpha_{1} .
\end{aligned}
$$

Since this is true for all $\varepsilon>0$, we have that

$$
\alpha^{t_{1}, \ldots, t_{d}} \leq\left(t_{1}+\cdots+t_{d}\right) \alpha_{1} .
$$

Next, we will construct explicitly the function $\phi$ and prove its properties i) and ii). Given $\left(a_{1}, \ldots, a_{d}\right) \in \mathbb{N}^{d}$ write the binary expansion of $a_{i}$ using binary strings $\Delta_{k}^{i}$ of length $\left[k t_{i}\right], k \geq 1$ as

$$
\begin{array}{r}
a_{1}=\Delta_{1}^{1} \Delta_{2}^{1} \ldots \Delta_{k}^{1} \ldots \\
a_{2}=\Delta_{1}^{2} \Delta_{2}^{2} \ldots \Delta_{k}^{2} \ldots \\
\ldots \\
a_{d}=\Delta_{1}^{d} \Delta_{2}^{d} \ldots \Delta_{k}^{d} \ldots
\end{array}
$$

We define $\phi\left(a_{1}, \ldots, a_{d}\right)$ as the integer whose binary expansion is
$\Delta_{1}^{1} 0 \Delta_{1}^{2} 0 \cdots 0 \Delta_{1}^{d} 0 \Delta_{2}^{1} 0 \Delta_{2}^{2} 0 \cdots 0 \Delta_{2}^{d} 0 \cdots \cdots 0 \Delta_{k}^{1} 0 \Delta_{k}^{2} 0 \cdots 0 \Delta_{k}^{d} 0 \cdots$
To prove property i), we will show that if $A \in \mathbb{N}^{d}$ is a Sidon set, then $\phi(A)$ is also a Sidon set. Suppose that

$$
\phi\left(a_{1}, \ldots, a_{d}\right)+\phi\left(a_{1}^{\prime}, \ldots, a_{d}^{\prime}\right)=\phi\left(a_{1}^{\prime \prime}, \ldots, a_{d}^{\prime \prime}\right)+\phi\left(a_{1}^{\prime \prime \prime}, \ldots, a_{d}^{\prime \prime \prime}\right),
$$

where $\left(a_{1}, \ldots, a_{d}\right),\left(a_{1}^{\prime}, \ldots, a_{d}^{\prime}\right),\left(a_{1}^{\prime \prime}, \ldots, a_{d}^{\prime \prime}\right),\left(a_{1}^{\prime \prime \prime}, \ldots, a_{d}^{\prime \prime \prime}\right) \in A$. Thanks to the inserted zeroes between blocks, we have that for all $i=1, \ldots, d$ and $j \geq 1$,

$$
\Delta_{j}^{i}\left(a_{i}\right)+\Delta_{j}^{i}\left(a_{i}^{\prime}\right)=\Delta_{j}^{i}\left(a_{i}^{\prime \prime}\right)+\Delta_{j}^{i}\left(a_{i}^{\prime \prime \prime}\right) .
$$

Then, for any $i=1, \ldots, d$,
$\Delta_{1}^{i}\left(a_{i}\right) \Delta_{2}^{i}\left(a_{i}\right) \cdots+\Delta_{1}^{i}\left(a_{i}^{\prime}\right) \Delta_{2}^{i}\left(a_{i}^{\prime}\right) \cdots=\Delta_{1}^{i}\left(a_{i}^{\prime \prime}\right) \Delta_{1}^{i}\left(a_{i}^{\prime \prime}\right) \cdots+\Delta_{1}^{i}\left(a_{i}^{\prime \prime \prime}\right) \Delta_{2}^{i}\left(a_{i}^{\prime \prime \prime}\right) \cdots$.

So,

$$
\left(a_{1}, \ldots, a_{d}\right)+\left(a_{1}^{\prime}, \ldots, a_{d}^{\prime}\right)=\left(a_{1}^{\prime \prime}, \ldots, a_{d}^{\prime \prime}\right)+\left(a_{1}^{\prime \prime \prime}, \ldots, a_{d}^{\prime \prime \prime}\right)
$$

Since $A$ is a Sidon set, we have that

$$
\left\{\left(a_{1}, \ldots, a_{d}\right),\left(a_{1}^{\prime}, \ldots, a_{d}^{\prime}\right)\right\}=\left\{\left(a_{1}^{\prime \prime}, \ldots, a_{d}^{\prime \prime}\right),\left(a_{1}^{\prime \prime \prime}, \ldots, a_{d}^{\prime \prime \prime}\right)\right\}
$$

SO

$$
\left\{\phi\left(a_{1}, \ldots, a_{d}\right), \phi\left(a_{1}^{\prime}, \ldots, a_{d}^{\prime}\right)\right\}=\left\{\phi\left(a_{1}^{\prime \prime}, \ldots, a_{d}^{\prime \prime}\right), \phi\left(a_{1}^{\prime \prime \prime}, \ldots, a_{d}^{\prime \prime \prime}\right)\right\}
$$

therefore $\phi(A)$ is a Sidon set.

To prove ii), suppose that $a_{i} \leq n^{t_{i}}$. Then the length of the binary expansion of $a_{i}$ is bounded by $t_{i} \log _{2} n$. Let $k$ the greatest integer such that $\Delta_{k}^{i} \neq 0$ for some $i$. Then

$$
\left[t_{i}\right]+\left[2 t_{i}\right]+\cdots+\left[(k-1) t_{i}\right] \leq t_{i} \log _{2} n
$$

which gives $k \leq \sqrt{2 \log _{2} n}+O(1)$.
On the other hand, the length of the binary expansion of $\phi\left(a_{1}, \ldots, a_{d}\right)$ is bounded by

$$
\sum_{i=1}^{d} \sum_{j=1}^{k}\left(\left[j t_{i}\right]+1\right) \leq \frac{k^{2}}{2}\left(t_{1}+\cdots+t_{d}\right)+O(k)
$$

Then

$$
\phi\left(a_{1}, \ldots, a_{d}\right) \leq 2^{\frac{k^{2}}{2}\left(t_{1}+\cdots+t_{d}\right)+O(k)} \leq n^{t_{1}+\cdots t_{d}+\epsilon(n)}
$$

where $\epsilon(n)=O(1 / \sqrt{\log n})$.

To prove that the inequality $\alpha^{t_{1}, \ldots, t_{d}} \geq\left(t_{1}+\cdots+t_{d}\right) \alpha_{1}$ holds, we construct another function $\varphi$ with analogous properties:
i) $\varphi$ maps Sidon sets in $\mathbb{N}$ to Sidon sets in $\mathbb{N}^{d}$.
ii) $\varphi\left(\left[1, n^{t_{1}+\cdots+t_{d}}\right] \cap \mathbb{N}\right) \subset\left[1, n^{t_{1}+\epsilon_{1}(n)}\right] \times \cdots \times\left[1, n^{t_{d}+\epsilon_{d}(n)}\right]$, with $\epsilon_{i}(n) \rightarrow 0$ as $n \rightarrow \infty$ for $i=1, \ldots, d$,
and we follow a similar argument. We omit the details, but provide the function $\varphi$ :

Given $a \in \mathbb{N}$, write the binary expansion of $a$ in the following way

$$
a=\Delta_{1}^{1} \Delta_{1}^{2} \cdots \Delta_{1}^{d} \Delta_{2}^{1} \Delta_{2}^{2} \cdots \Delta_{2}^{d} \cdots \cdots \Delta_{k}^{1} \Delta_{k}^{2} \cdots \Delta_{k}^{d} \cdots
$$

where the length of $\Delta_{j}^{i}$ is $\left[j t_{i}\right]$. We define $\varphi(a)=\left(a_{1}, \ldots, a_{d}\right)$, where the binary expansion of $a_{i}$ is

$$
\Delta_{1}^{i} 0 \Delta_{2}^{i} 0 \cdots 0 \Delta_{k}^{i} 0 \cdots
$$

The set $A=\left\{\left(n, n^{2}\right), n \geq 1\right\}$ is a Sidon set such that $A\left(n, n^{2}\right)=n$. It shows that $\alpha^{1,2} \geq 1$, so $\alpha_{1} \geq 1 / 3$. Of course, we can obtain this lower bound using the greedy algorithm to construct Sidon sets of integers, but the construction provided by the theorem above is explicit (we don't need to know the previous elements of the sequence to compute $a_{n}$ ). More precisely,

Corollary 3.1. The sequence of integers defined by

$$
\begin{equation*}
a_{n}=\sum_{j \geq 1} 2^{\frac{3 j^{2}+j}{2}-2}\left(\left\lfloor 2^{-j(j-1) / 2}(n)_{2^{j(j+1) / 2}}\right\rfloor+2^{j+1}\left\lfloor 2^{-j(j-1)}\left(n^{2}\right)_{2^{j(j+1)}}\right\rfloor\right), \tag{20}
\end{equation*}
$$

where $(x)_{m}$ is the least non negative residue which is congruent with $x$ $(\bmod m)$, is a Sidon set which satisfies $a_{n}=O\left(n^{3+o(1)}\right)$.

Proof. We will check that $a_{n}=\phi\left(n, n^{2}\right)$ where $\phi$ is the function defined in (19) for the special case $d=2, t_{1}=1, t_{2}=2$. Looking at that definition we observe that

$$
\begin{align*}
\Delta_{j}^{1} & =2^{-j(j-1) / 2} \sum_{j(j-1) / 2 \leq i<j(j+1) / 2} \varepsilon_{i} 2^{i}=\left\lfloor 2^{-j(j-1) / 2}(n)_{2^{j(j+1) / 2}}\right\rfloor  \tag{21}\\
\Delta_{j}^{2} & =2^{-j(j-1)} \sum_{j(j-1) \leq i<j(j+1)} \varepsilon_{i} 2^{i}=\left\lfloor 2^{-j(j-1)}\left(n^{2}\right)_{2^{j(j+1)}}\right\rfloor .
\end{align*}
$$

Then

$$
\Delta_{j}^{1} 0 \Delta_{j}^{2} 0=\left\lfloor 2^{-j(j-1) / 2}(n)_{2^{j(j+1) / 2}}\right\rfloor+2^{j+1}\left\lfloor 2^{-j(j-1)}\left(n^{2}\right)_{2^{j(j+1)}}\right\rfloor,
$$

so,

$$
\begin{aligned}
a_{n} & =\phi\left(n, n^{2}\right)=\Delta_{1}^{1} 0 \Delta_{1}^{2} 0 \Delta_{2}^{1} 0 \Delta_{2}^{2} 0 \cdots \cdots 0 \Delta_{k}^{1} 0 \Delta_{k}^{2} 0 \cdots \\
& =\sum_{j \geq 1} 2^{\frac{3 j^{2}+j}{2}-2}\left(\left\lfloor 2^{-j(j-1) / 2}(n)_{2^{j(j+1) / 2}}\right\rfloor+2^{j+1}\left\lfloor 2^{-j(j-1)}\left(n^{2}\right)_{2^{j(j+1)}}\right\rfloor\right) .
\end{aligned}
$$

## References

[1] R. C. Bose, An analogue of Singer's theorem, J. Indian Math. Soc. (N.S.) 6 (1942), 115.
[2] S. Chowla, Solution of a problem of Erdős and Turán in additive-number theory, Proc. Nat. Acad. Sci. India. Sect. A. 14 (1944), 12.
[3] J. Cilleruelo, Gaps in dense Sidon sets. Integers (2000), A11, 6pp. (electronic).
[4] J. Cilleruelo, An upper bound for $B_{2}[2]$ sequences, J. Combin. Theory Ser. A 89 (2000), no. 1, 141-144.
[5] J. Cilleruelo and M. Nathanson, Dense sets of integers with prescribed representation function. arXiv:0708.2853 .
[6] J. Cilleruelo and C. Vinuesa, $B_{2}[g]$ sets and a conjecture of Schinzel and Schmidt, Preprint, (2008).
[7] 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.
[8] S.W. Graham and C. J. Ringrove, Lower bounds for least quadratic nonresidues, Progress in Math. 85, (1990).
[9] A. Granville, An introducttion to additive combinatorics, Additive combinatorics, 1-27, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007
[10] B. Green, The number of squares and $B_{h}[g]$ sets. Acta Arith. 100 (2001), no. 4, 365-390
[11] M. L. Kolountzakis, On the uniform distribution in residue classes of dense sets of integers with distinct sums. J. Number Theory 76 (1999), no. 1, 147153
[12] B. Lindstrőm, An inequality for $B_{2}$-sequences. J. Comb. Theory Ser. A 6 (1969), 211-212.
[13] B. Lindstrőm, On $B_{2}$-sequences of vectors. J. Number Theory 4 (1972), 261265.
[14] I. Z. Ruzsa, Solving a linear equation in a set of integers. I. Acta Arith. 65 (1993), no. 3, 259-282.
[15] I. Z. Ruzsa, An infinite Sidon sequence. J. Number Theory 68 (1998), 63-71.
[16] I. Z. Ruzsa, Personal comunication.
[17] J. Singer, A theorem infinite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938), 377385.
[18] A. Stőr, Gelőste und ungelőste Fragen űber Basen der natűrlichen Zahlenreihe. I, II, J. Reine Angew. Math 194 (1955), 40-65, 111-140.
[19] T. Tao and V. Vu, Additive Combinatorics. Cambridge Studies in Advanced Mathematics, 105 (2006).
[20] C. Trujillo, Sucesiones de Sidon, Ph. D thesis, (1998) Universidad Politécnica de Madrid.

Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid, Spain
E-mail address: franciscojavier.cilleruelo@uam.es


[^0]:    2000 Mathematics Subject Classification. Primary 11B13, 11B34, 11B05.
    Key words and phrases. Sidon sets.
    The work of J.C. was supported by grants and MTM 2005-04730 of MYCIT (Spain).

