

PERFECT DIFFERENCE SETS CONSTRUCTED FROM SIDON SETS

JAVIER CILLERUELO AND MELVYN B. NATHANSON

ABSTRACT. A set \mathcal{A} of positive integers is a *perfect difference set* if every nonzero integer has a unique representation as the difference of two elements of \mathcal{A} . We construct dense *perfect difference sets* from dense Sidon sets. As a consequence of this new approach we prove that there exists a perfect difference set \mathcal{A} such that

$$A(x) \gg x^{\sqrt{2}-1-o(1)}.$$

Also we prove that there exists a *perfect difference set* \mathcal{A} such that $\limsup_{x \rightarrow \infty} A(x)/\sqrt{x} \geq 1/\sqrt{2}$.

1. INTRODUCTION

Let \mathbb{Z} denote the integers and \mathbb{N} the positive integers. For nonempty sets of integers \mathcal{A} and \mathcal{B} , we define the *difference set*

$$\mathcal{A} - \mathcal{B} = \{a - b : a \in \mathcal{A} \text{ and } b \in \mathcal{B}\}.$$

For every integer u , we denote by $d_{\mathcal{A},\mathcal{B}}(u)$ the number of pairs $(a, b) \in \mathcal{A} \times \mathcal{B}$ such that $u = a - b$. Let $d_{\mathcal{A}}(u)$ the number of pairs $(a, a') \in \mathcal{A} \times \mathcal{A}$ such that $u = a - a'$. The set \mathcal{A} is a *perfect difference set* if $d_{\mathcal{A}}(u) = 1$ for every integer $u \neq 0$. Note that \mathcal{A} is a perfect difference set if and only $d_{\mathcal{A}}(u) = 1$ for every positive integer u . For perfect difference sets, a simple counting argument shows that

$$A(x) \ll x^{1/2},$$

where the *counting function* $A(x)$ counts the number of positive elements of \mathcal{A} not exceeding x .

It is not completely obvious that perfect difference sets exist, but the greedy algorithm produces [3] a perfect difference set $\mathcal{A} \subseteq \mathbb{N}$ such that

$$A(x) \gg x^{1/3}.$$

At the Workshop on Combinatorial and Additive Number Theory (CANT 2004) in New York in May, 2004, Seva Lev (see also [3]) asked if there exists a perfect difference set \mathcal{A} such that

$$A(x) \gg x^\delta \text{ for some } \delta > 1/3.$$

2000 *Mathematics Subject Classification*. Primary 11B13, 11B34, 11B05, 11A07, 11A41.

Key words and phrases. Difference sets, perfect difference sets, Sidon sets, sumsets, representation functions.

The work of J.C. was supported by Grant MTM 2005-04730 of MYCIT (Spain).

The work of M.B.N. was supported in part by grants from the NSA Mathematical Sciences Program and the PSC-CUNY Research Award Program.

We answer this questions affirmatively by constructing perfect difference sets from classical Sidon sets.

We say that a set \mathcal{B} is a Sidon set if $d_{\mathcal{B}}(u) \leq 1$ for all integer $u \neq 0$.

Theorem 1. *For every Sidon set \mathcal{B} and every function $\omega(x) \rightarrow \infty$, there exists a perfect difference set $\mathcal{A} \subseteq \mathbb{N}$ satisfying*

$$A(x) \geq B(x/3) - \omega(x).$$

It is a difficult problem to construct dense infinite Sidon sets. Ruzsa [6] proved that there exists a Sidon set \mathcal{B} with $B(x) \gg x^{\sqrt{2}-1-o(1)}$. The following result follows easily.

Theorem 2. *There exists a perfect difference set $\mathcal{A} \subseteq \mathbb{N}$ such that*

$$A(x) \gg x^{\sqrt{2}-1+o(1)}.$$

Erdős [7] proved that the lower bound $A(x) \gg x^{1/2}$ does not hold for any Sidon set \mathcal{A} , and so does not hold for perfect difference sets. However, Krückeberg [2] proved that there exists a Sidon set \mathcal{B} such that

$$\limsup_{x \rightarrow \infty} \frac{B(x)}{\sqrt{x}} \geq \frac{1}{\sqrt{2}}.$$

We extend this result to perfect difference sets.

Theorem 3. *There exists a perfect difference set $\mathcal{A} \subseteq \mathbb{N}$ such that*

$$\limsup_{x \rightarrow \infty} \frac{A(x)}{\sqrt{x}} \geq \frac{1}{\sqrt{2}}.$$

Notice that an immediate application of Theorem 1 to Krückeberg's result would give only $\limsup_{x \rightarrow \infty} A(x)x^{-1/2} \geq 1/\sqrt{6}$.

2. PROOF OF THEOREM 1

2.1. Sketch of the proof. The strategy of the proof is the following:

- Modify any dense Sidon set \mathcal{B} given by dilating it by 3 and removing a suitable *thin* subset of $3 * \mathcal{B}$.
- Complete the remainder set $\mathcal{B}_0 = (3 * \mathcal{B}) \setminus \{\text{removed set}\}$ with a subset of the elements of a very sparse sequence $\mathcal{U} = \{u_s\}$ by adding, if k has not appeared yet in the difference set, two elements u_{2k}, u_{2k+1} in the k -th step such that $u_{2k+1} - u_{2k} = k$.

2.2. The auxiliary sequence \mathcal{U} . For any strictly increasing function $g : \mathbb{N} \rightarrow \mathbb{N}$ and $k \geq 1$, we define integers u_{2k} and u_{2k+1} by

$$\begin{cases} u_{2k} &= 4^{g(k)} + \epsilon_k \\ u_{2k+1} &= 4^{g(k)} + \epsilon_k + k \end{cases}$$

where

$$\epsilon_k = \begin{cases} 1 & \text{if } k \equiv 2 \pmod{3} \\ 0 & \text{otherwise} \end{cases}.$$

For all positive integers k we have

$$u_{2k+1} - u_{2k} = k.$$

Let $\mathcal{U}_k = \{u_{2k}, u_{2k+1}\}$ and $\mathcal{U}_{<\ell} = \bigcup_{k < \ell} \mathcal{U}_k$. It will be useful to state some properties of the sequence $\mathcal{U} = \{u_i\}_{i=2}^{\infty}$.

Lemma 1. *The sequence $\mathcal{U} = \{u_i\}_{i=2}^{\infty}$ satisfies the following properties:*

- (i) For all $i \geq 2$, $u_i \not\equiv 0 \pmod{3}$.
- (ii) For all $k \geq 2$, for $u \in \mathcal{U}_k$, and for all $u', u'', u''' \in \mathcal{U}_{<k}$, we have $u + u' > u'' + u'''$.
- (iii) If $k \geq 2$, $u \in \mathcal{U}_k$, and $u' \in \mathcal{U}_{<k}$, then $u - u' > u/2$.

Proof. (i) By construction.

- (ii) Since $g(k)$ is strictly increasing we have $k \leq g(k)$ and so

$$4k < 4^k \leq 4^{g(k)}$$

for all $k \geq 2$. It follows that

$$\begin{aligned} u'' + u''' &\leq 2u_{2k-1} \leq 2(4^{g(k-1)} + k) \\ &\leq 2 \left(4^{g(k)-1} + k \right) \leq \frac{4^{g(k)}}{2} + 2k \\ &\leq 4^{g(k)} \leq u < u + u'. \end{aligned}$$

- (iii) For $k \geq 2$ we have

$$\begin{aligned} u' &\leq 4^{g(k-1)} + (k-1) + \epsilon_{k-1} \\ &\leq 4^{g(k)-1} + k \\ &< 2 \cdot 4^{g(k)-1} = \frac{4^{g(k)}}{2} \\ &\leq u/2 \end{aligned}$$

and so $u - u' > u/2$. □

2.3. Construction of the Sidon set \mathcal{B}_0 . Take a Sidon set \mathcal{B} and consider the set $\mathcal{B}' = 3 * \mathcal{B} = \{3b : b \in \mathcal{B}\}$. Then \mathcal{B}' is a Sidon set such that $b \equiv 0 \pmod{3}$ for all $b \in \mathcal{B}'$ and $B'(x) = B\left(\frac{x}{3}\right)$.

The set \mathcal{B}_0 will be the set $\mathcal{B}' = 3 * \mathcal{B}$ after we remove all the elements $b \in \mathcal{B}'$ that satisfy at least one of the followings conditions:

- c1:** $b = u - u' + b'$ for some $b' \in \mathcal{B}'$, $b > b'$ and $u, u' \in \mathcal{U}$ such that $u \in \mathcal{U}_r$, $u' \in \mathcal{U}_{<r}$ for some r .
- c2:** $b = u + u' - b'$ for some $b' \in \mathcal{B}$, $b \geq b'$ and $u, u' \in \mathcal{U}$.
- c3:** $b = u + u' - u''$ for some $u \in \mathcal{U}_r$, $u' \in \mathcal{U}$, and $u'' \in \mathcal{U}_{<r}$ with $u' \leq u$.
- c4:** $|b - u_i| \leq i$ for some $u_i \in \mathcal{U}$.

2.4. The inductive step. We shall construct the set \mathcal{A} in Theorem 1 by adjoining terms to the *nice* Sidon set \mathcal{B}_0 obtained above. More precisely, the sequence \mathcal{A} satisfying the conditions of the theorem will be

$$\mathcal{A} = \bigcup_{k=0}^{\infty} \mathcal{A}_k$$

where \mathcal{A}_k will be defined by $\mathcal{A}_0 = \mathcal{B}_0$ and for, $k \geq 1$,

$$\mathcal{A}_k = \begin{cases} \mathcal{A}_{k-1} \cup \mathcal{U}_k & \text{if } k \notin \mathcal{A}_{k-1} - \mathcal{A}_{k-1} \\ \mathcal{A}_{k-1} & \text{otherwise.} \end{cases}$$

Lemma 2. *For every positive integer k we have*

$$[-k, k] \subseteq \mathcal{A}_k - \mathcal{A}_k$$

and so

$$d_{\mathcal{A}}(n) \geq 1$$

for all integers n .

Proof. Clear. □

2.5. \mathcal{A} is a Sidon set. First we state two lemmas.

Lemma 3. *Let A_1 and A_2 be nonempty disjoint sets of integers and let $A = A_1 \cup A_2$. For every integer n we have*

$$d_A(n) = d_{A_1}(n) + d_{A_2}(n) + d_{A_1, A_2}(n) + d_{A_2, A_1}(n),$$

where

$$d_{A_i, A_j}(n) = \#\{(a, a') \in A_i \times A_j, a - a' = n\}.$$

Proof. This follows from the identity

$$(A_1 \cup A_2) \times (A_1 \cup A_2) = (A_1 \times A_1) \cup (A_2 \times A_2) \cup (A_1 \times A_2) \cup (A_2 \times A_1).$$

□

Lemma 4. *If $n \in \mathcal{A}_{r-1} - \mathcal{U}_r$ then*

- (i) $|n| > r$, and so $d_{\mathcal{U}_r, \mathcal{A}_{r-1}}(r) = d_{\mathcal{A}_{r-1}, \mathcal{U}_r}(r) = 0$.
- (ii) $d_{\mathcal{A}_{r-1}}(n) = 0$.
- (iii) $d_{\mathcal{U}_r, \mathcal{A}_{r-1}}(n) = 0$.

Proof. Write $n = a - u$, where $a \in \mathcal{A}_{r-1}$ and $u \in \mathcal{U}_r = \{u_{2r}, u_{2r+1}\}$.

(i) If $a = b \in \mathcal{B}_0$ we have that $|b - u| > 2r > r$ because, by condition (c4), we have removed all elements b from \mathcal{B} such that $|b - u_i| \leq i$.

If $a = u' \in \mathcal{U}_{<r}$ then we apply Lemma 1 (iii) to conclude that

$$|u' - u| > \frac{u}{2} \geq \frac{4^{g(r)}}{2} > r.$$

(ii) Since $\mathcal{A}_{r-1} \subseteq \mathcal{B}_0 \cup \mathcal{U}_{<r}$, it follows that

$$d_{\mathcal{A}_{r-1}}(n) \leq d_{\mathcal{B}_0 \cup \mathcal{U}_{<r}}(n) \leq d_{\mathcal{B}_0}(n) + d_{\mathcal{U}_{<r}}(n) + d_{\mathcal{B}_0, \mathcal{U}_{<r}}(n) + d_{\mathcal{U}_{<r}, \mathcal{B}_0}(n).$$

If $a = b \in \mathcal{B}_0$, then $n = b - u$ and

- (1) $b \equiv 0 \pmod{3}$ but $u \not\equiv 0 \pmod{3}$, hence $b - u \not\equiv 0 \pmod{3}$ and $d_{\mathcal{B}_0}(b - u) = 0$ (by Lemma 1 (i)),
- (2) $d_{\mathcal{U}_{<r}}(b - u) = 0$ (by condition (c3)),
- (3) $d_{\mathcal{B}_0, \mathcal{U}_{<r}}(b - u) = 0$ (by condition (c1)),
- (4) $d_{\mathcal{U}_{<r}, \mathcal{B}_0}(b - u) = 0$ (by condition (c2)).

If $a = u' \in \mathcal{U}_{<r}$, then $n = u' - u$ and

- (1) $d_{\mathcal{B}_0}(u' - u) = 0$ (by condition (c1)),
 - (2) $d_{\mathcal{U}_{<r}}(u' - u) = 0$ (by Lemma 1 (ii)),
 - (3) If $u' - u = b - u''$ with $u'' \in \mathcal{U}_{<r}$, then Lemma 1 (iii) implies that $0 < b = u' + u'' - u \leq 0$, and so $d_{\mathcal{B}_0, \mathcal{U}_{<r}}(u' - u) = 0$.
 - (4) $d_{\mathcal{U}_{<r}, \mathcal{B}_0}(u' - u) = 0$ (by condition (c3)).
- (iii) Again, since $\mathcal{A}_{r-1} \subseteq \mathcal{B}_0 \cup \mathcal{U}_{<r}$ we have that

$$d_{\mathcal{U}_r, \mathcal{A}_{r-1}}(n) \leq d_{\mathcal{U}_r, \mathcal{B}_0}(n) + d_{\mathcal{U}_r, \mathcal{U}_{<r}}(n).$$

If $a = b \in \mathcal{B}_0$ then $d_{\mathcal{U}_r, \mathcal{B}_0}(b - u) = 0$ (by condition (c2)) and $d_{\mathcal{U}_r, \mathcal{U}_{<r}}(b - u) = 0$ (by condition (c3)).

If $a = u' \in \mathcal{U}_{<r}$ then $d_{\mathcal{U}_r, \mathcal{B}_0}(u' - u) = 0$ (by condition (c3)). Finally, we have $d_{\mathcal{U}_r, \mathcal{U}_{<r}}(u' - u) = 0$, since if $u' - u = u'' - u'''$, $u'' \in \mathcal{U}_r$, $u''' \in \mathcal{U}_{<r}$, then $0 > u' - u = u'' - u''' > 0$. This completes the proof. \square

Lemma 5. *For every positive integer n we have*

$$d_{\mathcal{A}}(n) \leq 1$$

and so \mathcal{A} is a perfect difference set.

Proof. We will use induction to prove that, for every $r \geq 0$,

$$d_{\mathcal{A}_r}(n) \leq 1 \quad \text{for every nonzero integer } n.$$

This is true for $r = 0$ because $\mathcal{A}_0 = \mathcal{B}_0$ is a subset of a Sidon set.

We assume that the statement is true for $r - 1$ and shall prove it for r .

If $d_{\mathcal{A}_{r-1}}(r) = 1$ then $\mathcal{A}_r = \mathcal{A}_{r-1}$ and there is nothing to prove. Suppose that $d_{\mathcal{A}_{r-1}}(r) = 0$, and so $\mathcal{A}_r = \mathcal{A}_{r-1} \cup \mathcal{U}_r$. Since we have added two new elements u_{2r}, u_{2r+1} to \mathcal{A}_{r-1} , it is possible that there are *new* representations of a positive integer n so that $d_{\mathcal{A}_r}(n) > 1$. We shall prove that this cannot happen.

By Lemma 3, we can write

$$d_{\mathcal{A}_r}(n) = d_{\mathcal{A}_{r-1}}(n) + d_{\mathcal{U}_r}(n) + d_{\mathcal{A}_{r-1}, \mathcal{U}_r}(n) + d_{\mathcal{U}_r, \mathcal{A}_{r-1}}(n)$$

If $n = r$, then Lemma 4 (i) and the relation $u_{2r+1} - u_{2r} = r$ imply that

$$d_{\mathcal{A}_r}(r) = d_{\mathcal{A}_{r-1}}(r) + d_{\mathcal{U}_r}(r) + d_{\mathcal{A}_{r-1}, \mathcal{U}_r}(r) + d_{\mathcal{U}_r, \mathcal{A}_{r-1}}(r) = 0 + 1 + 0 + 0 = 1$$

If $n \neq r$, then

$$d_{\mathcal{A}_r}(n) = d_{\mathcal{A}_{r-1}}(n) + d_{\mathcal{A}_{r-1}, \mathcal{U}_r}(n) + d_{\mathcal{U}_r, \mathcal{A}_{r-1}}(n).$$

If $n \in \mathcal{A}_{r-1} - \mathcal{U}_r$ (the case $n \in \mathcal{U}_r - \mathcal{A}_{r-1}$ is similar), then we can write

$$n = a - u \text{ where } a \in \mathcal{A}_{r-1}, u \in \mathcal{U}_r.$$

Applying Lemma 4 (ii) and Lemma 4 (iii), we obtain

$$d_{\mathcal{A}_r}(n) = d_{\mathcal{A}_{r-1}, \mathcal{U}_r}(n).$$

If $d_{\mathcal{A}_{r-1}, \mathcal{U}_r}(n) \geq 2$, then there exist $a, a' \in \mathcal{A}_{r-1}$ such that $a - u_{2r} = a' - u_{2r+1}$. This implies that

$$a' - a = u_{2r+1} - u_{2r} = r \in \mathcal{A}_{r-1} - \mathcal{A}_{r-1}$$

which is false, so $d_{\mathcal{A}_r}(n) = d_{\mathcal{A}_{r-1}, \mathcal{U}_r}(n) \leq 1$.

If $n \notin (\mathcal{A}_{r-1} - \mathcal{U}_r) \cup (\mathcal{U}_r - \mathcal{A}_{r-1})$ then

$$d_{\mathcal{A}_r}(n) = d_{\mathcal{A}_{r-1}}(n) \leq 1.$$

This completes the proof. \square

2.6. The counting function $A(x)$. We have

$$A(x) \geq B_0(x) = B(x) - R(x) = B(x/3) - R(x)$$

where $R = R_1 \cup R_2 \cup R_3 \cup R_4$ and R_i denotes the set of elements of B removed by condition (c_i), $i = 1, 2, 3, 4$.

Lemma 6. *Let $U(x)$ denote the counting function of the set \mathcal{U} . For the sets R_1, R_2, R_3, R_4 defined above, we have*

- (i) $R_1(x) \leq U^2(2x)$.
- (ii) $R_2(x) \leq U^2(2x)$.
- (iii) $R_3(x) \leq U^3(2x)$.
- (iv) $R_4(x) \leq 2U^2(2x) + U(2x)$.

Proof. (i) We have

$$R_1(x) = \#\{b \in B : b \leq x \text{ and } b \text{ satisfies condition (c1)}\}.$$

Because B is a Sidon set, for every pair of integers $u, u' \in \mathcal{U}$ there exists at most one pair of integers $b, b' \in \mathcal{B}$ such that $b - b' = u - u'$. The condition $x \geq b > b'$ implies that $0 < u - u' \leq x$. On the other hand Lemma 1 (iii) implies that $u - u' > u/2$ and so $u < 2x$ and

$$R_1(x) \leq \#\{(u, u'), u' < u, u < 2x\} \leq U^2(2x).$$

(ii) Again, because B is a Sidon set, for every pair $u, u' \in \mathcal{U}$ there exists at most one pair $b, b' \in \mathcal{B}$ such that $b + b' = u + u'$. The condition $x \geq b \geq b'$ implies $u, u' \leq 2x$ and so

$$R_2(x) \leq \#\{(u, u') \in \mathcal{U} \times \mathcal{U} : u \leq 2x, u' \leq 2x\} \leq U^2(2x).$$

(iii) If $u \in \mathcal{U}_r$, $u'' \in \mathcal{U}_{<r}$, then Lemma 1 (iii) implies that $b = u + u' - u'' > u - u'' > u/2$ and so

$$\begin{aligned} R_3(x) &= \#\{b \in B : b \leq x \text{ and } b \text{ satisfies condition (c3)}\} \\ &\leq \#\{(u, u', u'') \in \mathcal{U} \times \mathcal{U} \times \mathcal{U} : u < 2x, u'' < u, u' \leq u\} \\ &\leq U(2x)^3. \end{aligned}$$

(iv) We have

$$\begin{aligned} R_4(x) &= \#\{b \in B : b \leq x \text{ and } |b - u_i| \leq i \text{ for some } u_i \in \mathcal{U}\} \\ &\leq \#\{n \in \mathbb{N} : n \leq x \text{ and } |n - u_i| \leq i \text{ for some } i\}. \end{aligned}$$

If $n \leq x$ and $|n - u_i| \leq i$, then $u_i \leq n + i \leq x + i$. Since $u_2 = 4^{g(1)} \geq 4$, $u_3 = 4^{g(1)+1} \geq 16$, and, for $i \geq 4$,

$$u_i \geq 4^{g((i-1)/2)} \geq 4^{(i-1)/2} = 2^{i-1} \geq 2i.$$

Therefore, $u_i \leq x + i \leq x + u_i/2$ and so $u_i \leq 2x$. It follows that $i \leq U(2x)$ and so

$$\begin{aligned} R_4(x) &\leq \#\{n \leq x : |n - u_i| \leq U(2x) \text{ and } u_i \leq 2x\} \\ &\leq (2U(2x) + 1)U(2x) = 2U(2x)^2 + U(2x). \end{aligned}$$

This completes the proof of the lemma. \square

Finally, given any function $\omega(x) \rightarrow \infty$ we have that

$$A(x) \geq B(x/3) - (U(2x)^3 + 4U^2(2x) + U(2x)) \geq B(x/3) - \omega(x)$$

for any function $g : \mathbb{N} \rightarrow \mathbb{N}$ and sequence \mathcal{U} growing fast enough. This completes the proof of Theorem 1.

3. PROOF OF THEOREM 3

Lemma 7. *If C_1 and C_2 are Sidon sets such that $(C_i - C_i) \cap (C_j - C_j) = \{0\}$, $(C_i + C_i) \cap (C_j + C_j) = \emptyset$ and $(C_i + C_i - C_i) \cap C_j = \emptyset$ for $i \neq j$, then $C_1 \cup C_2$ is a Sidon set.*

Proof. Obvious. \square

Lemma 8. *For each odd prime p there exist a Sidon set \mathcal{B}_p such that*

- (i) $\mathcal{B}_p \subseteq [1, p^2]$.
- (ii) $(\mathcal{B}_p - \mathcal{B}_p) \cap [-\sqrt{p}, \sqrt{p}] = \emptyset$.
- (iii) $|\mathcal{B}_p| > p - 2\sqrt{p}$.

Proof. Ruzsa [5] constructed, for each prime p , a Sidon set $R_p \subseteq [1, p^2 - p]$ with $|R_p| = p - 1$. We consider the subset \mathcal{B}_p of R_p that we obtain by removing all elements $b \in R_p$ such that $0 < |b - b'| \leq \sqrt{p}$ for some $b' \in R_p$. Since R_p is a Sidon set, it follows that we have removed at most \sqrt{p} elements from R_p , and so $|\mathcal{B}_p| \geq |R_p| - \sqrt{p} = p - \sqrt{p} - 1 > p - 2\sqrt{p}$. \square

Proof of Theorem 3. We shall construct an increasing sequence of finite set $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ such that $\mathcal{A} = \cup_{k=1}^{\infty} A_k$ is a perfect difference set satisfying Theorem 3.

In the following, l_k will denote the largest integer in the set A_{k-1} , and p_k the least prime greater than $4l_k^2$. Let

$$A_1 = \{0, 1\}.$$

Then $l_2 = 1$ and $p_2 = 5$. We define

$$A_k = \begin{cases} A_{k-1} \cup (\mathcal{B}_{p_k} + p_k^2 + 2l_k) & \text{if } k \in A_{k-1} - A_{k-1} \\ A_{k-1} \cup (\mathcal{B}_{p_k} + p_k^2 + 2l_k) \cup \{4p_k^2, 4p_k^2 + k\} & \text{otherwise.} \end{cases}$$

We shall prove that the set $\mathcal{A} = \cup_{k=1}^{\infty} A_k$ satisfies the theorem.

By construction, $[1, k] \subseteq A_k - A_k$ for every positive integer k and so $\mathcal{A} - \mathcal{A} = \mathbb{Z}$.

We must prove that A_k is a Sidon set for every $k \geq 1$.

This is clear for $k = 1$. Suppose that A_{k-1} is a Sidon set. Let $C_1 = A_{k-1}$ and $C_2 = \mathcal{B}_{p_k} + p_k^2 + 2l_k$. We shall show that

$$C_1 \cup C_2 = A_{k-1} \cup (\mathcal{B}_{p_k} + p_k^2 + 2l_k)$$

is a Sidon set. Notice that

$$\begin{aligned} C_1 - C_1 &\subseteq [-l_k, l_k] \subseteq [-\sqrt{p_k}, \sqrt{p_k}] \\ C_2 - C_2 &= \mathcal{B}_{p_k} - \mathcal{B}_{p_k} \\ [-\sqrt{p_k}, \sqrt{p_k}] \cap (\mathcal{B}_{p_k} - \mathcal{B}_{p_k}) &= \{0\}. \end{aligned}$$

Then

$$(C_1 - C_1) \cap (C_2 - C_2) = \{0\}.$$

Notice also that if $x \in C_2 + C_2$ then $x \geq 2p_k^2 + 4l_k$, but $C_1 + C_1 \subset [1, 2l_k]$. Then

$$(C_1 + C_1) \cap (C_2 + C_2) = \emptyset.$$

If $x \in (C_1 + C_1 - C_1)$, then $x \leq 2l_k$, but if $x \in C_2$, then $x > 2l_k$. Thus,

$$(C_1 + C_1 - C_1) \cap C_2 = \emptyset.$$

If $x \in C_2 + C_2 - C_2$, then $x \geq 2(p_k^2 + 2l_k + 1) - (p_k^2 + p_k^2 + 2l_k) = 2l_k + 1$, and if $x \in C_1$, then $x \leq l_k$. Therefore,

$$(C_2 + C_2 - C_2) \cap C_1 = \emptyset.$$

Then $A_{k-1} \cup (\mathcal{B}_{p_k} + p_k^2 + 2l_k)$ is a Sidon set.

Now we must distinguish two cases:

If $k \in A_{k-1} - A_{k-1}$ then $A_k = A_{k-1} \cup (\mathcal{B}_{p_k} + p_k^2 + 2l_k)$ and we have proved that it is a Sidon set.

If $k \notin A_{k-1} - A_{k-1}$ then $A_k = A_{k-1} \cup (\mathcal{B}_{p_k} + p_k^2 + 2l_k) \cup \{4p_k^2, 4p_k^2 + k\}$ and we have to prove that it is also a Sidon set. In this case we take $C_1 = A_{k-1} \cup (\mathcal{B}_{p_k} + p_k^2 + 2l_k)$ and $C_2 = \{4p_k^2, 4p_k^2 + k\}$. We can write

$$\begin{aligned} C_1 - C_1 &= (A_{k-1} - A_{k-1}) \cup (\mathcal{B}_{p_k} - \mathcal{B}_{p_k}) \\ &\quad \cup (A_{k-1} - (\mathcal{B}_{p_k} + p_k^2 + 2l_k)) \\ &\quad \cup ((\mathcal{B}_{p_k} + p_k^2 + 2l_k) - A_{k-1}). \end{aligned}$$

If $x \in (A_{k-1} - (\mathcal{B}_{p_k} + p_k^2 + 2l_k)) \cup ((\mathcal{B}_{p_k} + p_k^2 + 2l_k) - A_{k-1})$, then $|x| \geq p_k^2 + l_k > k$.

If $x \in (\mathcal{B}_{p_k} - \mathcal{B}_{p_k})$ then $x = 0$ or $|x| > \sqrt{p_k} > k$, then, since $C_2 - C_2 = \{-k, 0, k\}$, we have

$$(C_1 - C_1) \cap (C_2 - C_2) = \{0\}.$$

On the other hand if $x \in C_2 + C_2$ then $x \geq 8p_k^2$ but

$$C_1 + C_1 \subset [1, 2((p_k^2 - p_k) + p_k^2 + 2l_k)] \subset [1, 4p_k^2].$$

Then

$$(C_1 + C_1) \cap (C_2 + C_2) = \emptyset.$$

If $x \in C_1 + C_1 - C_1$ then $x \leq 3p_k^2 + 2l_k < 4p_k^2$. Thus,

$$(C_1 + C_1 - C_1) \cap C_2 = \emptyset.$$

Also we have that $C_2 + C_2 - C_2 = 4p_k^2 + \{-k, 0, k, 2k\}$, but if $x \in C_1$ we have that $x < 2p_k^2 + 2l_k < 2p_k^2 + \sqrt{p_k} < 4p_k^2 - k$. Thus

$$(C_2 + C_2 - C_2) \cap C_1 = \emptyset.$$

To finish the proof of the theorem note that

$$\begin{aligned} \limsup_{x \rightarrow \infty} \frac{\mathcal{A}(x)}{\sqrt{x}} &\geq \limsup_{k \rightarrow \infty} \frac{\mathcal{A}(2p_k^2 - p_k + l_k)}{\sqrt{2p_k^2 - p_k + l_k}} \geq \\ \limsup_{k \rightarrow \infty} \frac{|\mathcal{B}_{p_k}|}{\sqrt{2p_k^2 - p_k + l_k}} &\geq \limsup_{k \rightarrow \infty} \frac{p_k - 2\sqrt{p_k}}{\sqrt{2p_k^2 - p_k + \sqrt{p_k}/2}} = \frac{1}{\sqrt{2}}. \end{aligned}$$

□

4. REMARKS AND OPEN PROBLEMS

4.1. The sequence $t(\mathcal{A})$ associated to a perfect difference set. Any translation of a perfect difference set intersects to itself in exactly one element, and so we can define, for every perfect difference set \mathcal{A} , a sequence $t(\mathcal{A})$ whose elements are given by $t_n = \mathcal{A} \cap (\mathcal{A} - n)$ for all $n \geq 1$. The sequence t_n is very irregular, but the greedy algorithm used in [3] generates a perfect difference set such that $t_n \ll n^3$. Our method generates a dense Sidon set \mathcal{A} , but gives a very poor upper bound for the sequence t_n .

Problem 1. *Does there exists perfect difference set such that $t_n = o(n^3)$?*

4.2. Sidon sets included in perfect difference sets. We have proved that any Sidon set can be perturbed slightly to become a subset of a perfect difference set. Every subset of a perfect difference set is a Sidon set. It is natural to ask if *every* Sidon set is a subset of a perfect difference set. The answer is negative. To construct a counterexample, we take a perfect difference set \mathcal{A} and consider the set $\mathcal{B} = 2 * \mathcal{A} = \{2a : a \in \mathcal{A}\}$. The set \mathcal{B} has the following properties:

- (i) \mathcal{B} is a Sidon set.
- (ii) If n is an even integer not in \mathcal{B} , then $\mathcal{B} \cup \{n\}$ is not a Sidon set.

- (iii) If m and m' are distinct odd integers not in \mathcal{B} , then $\mathcal{B} \cup \{m, m'\}$ is not a Sidon set.

The Sidon set \mathcal{B} is not a subset of a perfect difference set. Since this construction is rather artificial, we wonder if almost all Sidon sets are subsets of perfect difference sets.

Problem 2. *Determine when a Sidon set is a subset of a perfect difference set.*

4.3. Perfect h -sumsets. Let \mathcal{A} be a set of integers. For every integer u , we denote by $r_{\mathcal{A}}^h(u)$ the number of h -tuples $(a_1, \dots, a_h) \in \mathcal{A}^h$, such that

$$a_1 \leq \dots \leq a_h$$

and

$$a_1 + \dots + a_h = u.$$

We say that \mathcal{A} is a *perfect h -sumset* or a *unique representation basis of order h* if $r_{\mathcal{A}}^h(u) = 1$ for every integer u . Nathanson [4] proved that for every $h \geq 2$ and for every function $f : \mathbb{Z} \rightarrow \mathbb{N}_0 \cup \{\infty\}$ such that $\limsup_{|u| \rightarrow \infty} f(u) \geq 1$ there exists a set of integers \mathcal{A} such that

$$r_{\mathcal{A}}^h(u) = f(u)$$

for every integer u . In particular, the *perfect h -sumsets* correspond to the representation function $f \equiv 1$. Nathanson's construction produces a *perfect h -sumset* \mathcal{A} with

$$A(x) \gg x^{1/(2h-1)}$$

and he asked for denser constructions.

It is easy to modify our approach to get a perfect 2-sumset \mathcal{A} with $A(x) \gg x^{\sqrt{2}-1+o(1)}$. But for $h \geq 3$ our method cannot be adapted easily, and a more complicated construction is needed. We shall study perfect h -sumsets in a forthcoming paper [1].

4.4. Sums and differences. Let \mathcal{A} be a set of integers. For every integer u , we denote by $d_{\mathcal{A}}(u)$ and $s_{\mathcal{A}}(u)$ the number of solutions of

$$u = a - a' \text{ with } a, a' \in \mathcal{A}$$

and

$$u = a + a' \text{ with } a, a' \in \mathcal{A} \text{ and } a \leq a',$$

respectively. We say that \mathcal{A} is a *perfect difference sumset* if $d_{\mathcal{A}}(n) = 1$ for all $n \in \mathbb{N}$ and if $s_{\mathcal{A}}(n) = 1$ for all $n \in \mathbb{Z}$.

We can extend Theorem 1 and Theorem 3 to perfect difference sumsets. Then it is natural to ask if, for any two functions $f_1 : \mathbb{N} \rightarrow \mathbb{N}$ and $f_2 : \mathbb{Z} \rightarrow \mathbb{N}$, there exists a set \mathcal{A} such that $d_{\mathcal{A}}(n) = f_1(n)$ for all $n \in \mathbb{N}$ and $s_{\mathcal{A}}(n) = f_2(n)$ for all $n \in \mathbb{Z}$. (Note that perfect difference sumsets correspond to the functions $f_1 \equiv 1$ and $f_2 \equiv 1$.) It is not difficult to guess that the answer is no. For example, if $s_{\mathcal{A}}(n) = 2$ for infinitely many integers n , it is easy to see that $d_{\mathcal{A}}(n) \geq 2$ for infinitely many integers n .

Problem 3. Give general conditions for functions f_1 and f_2 to assure that there exists a set \mathcal{A} such that $d_{\mathcal{A}}(n) \equiv f_1(n)$ and $s_{\mathcal{A}}(n) \equiv f_2(n)$.

Is the condition $\liminf_{u \rightarrow \infty} f_1(u) \geq 2$ and $\liminf_{|u| \rightarrow \infty} f_2(u) \geq 2$ sufficient?

REFERENCES

- [1] J. Cilleruelo and M. B. Nathanson, *Dense sets of integers with prescribed representation functions*, Preprint., 2006.
- [2] F. Krückeberg, *B₂-Folgen und verwandte Zahlenfolgen*, J. Reine Angew. Math. **206** (1961), 53–60.
- [3] V. F. Lev, *Reconstructing integer sets from their representation functions*, Electron. J. Combin. **11** (2004), no. 1, Research Paper 78, 6 pp. (electronic).
- [4] M. B. Nathanson, *Every function is the representation function of an additive basis for the integers*, Port. Math. (N.S.) **62** (2005), no. 1, 55–72.
- [5] I. Z. Ruzsa, *Solving a linear equation in a set of integers. I*, Acta Arith. **65** (1993), no. 3, 259–282.
- [6] ———, *An infinite Sidon sequence*, J. Number Theory **68** (1998), no. 1, 63–71.
- [7] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I, II*, J. Reine Angew. Math. **194** (1955), 40–65, 111–140.

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD AUTÓNOMA DE MADRID, 28049 MADRID, SPAIN

E-mail address: `franciscojavier.cilleruelo@uam.es`

DEPARTMENT OF MATHEMATICS, LEHMAN COLLEGE (CUNY), BRONX, NEW YORK 10468

E-mail address: `melvyn.nathanson@lehman.cuny.edu`