INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7 (2007), #A11

INTEGER SETS HAVING THE MAXIMUM NUMBER OF DISTINCT DIFFERENCES

Oleg Pikhurko[1]
Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15213
http://www.math.cmu.edu/~pikhurko

Tomasz Schoen[2]
Department of Discrete Mathematics, Adam Mickiewicz University, Poznań, Poland
schoen@amu.edu.pl

Received: 9/12/06, Revised: 1/27/07, Accepted: 2/3/07, Published: 2/19/07

Abstract

In this paper we study the function $D(k,n)$ which is the maximum of $|A-A| = \big|\{a-b : a,b \in A\}\big|$ over all k-subsets A of $\{0,\dots,n\}$. We prove that for any fixed real $c \ge 0$ and any function $k(n) = (c+o(1))\sqrt{n}$, the limit

$$d(c) = \lim_{n\to\infty} \frac{D(k(n),n)}{n}$$

exists, as well as present some upper and lower bounds on $d(c)$.

1. Introduction

For $A \subset \mathbb{Z}$ let its *difference set* $A-A$ be $\{a-b : a,b \in A\}$. We say that A is a *difference basis* for a set $I \subset \mathbb{Z}$ if $A-A \supset I$. If, moreover, $A \subset I$, then A is called a *restricted difference basis* for I.

Here we study the function $D(k,n)$ which is the maximum size of $A-A$ over all k-subsets A of $[0,n] = \{0,\dots,n\}$. In other words, of all k-subsets of $[0,n]$ we want to choose one with the maximum number of distinct differences. The analogous problem for *sums* has been considered by Pikhurko [7].

One trivial upper bound is $D(k,n) \le k^2-k+1$. (Note that 0 is represented k times as a difference in $A-A$.) This bound is sharp if and only if $[0,n]$ contains a Sidon k-set. Let s_n

[1]Partially supported by the Berkman Faculty Development Fund, Carnegie Mellon University, and the National Science Foundation, Grant DMS-0457512.
[2]Partially supported by KBN Grant 1 P03A 029 30.

be the largest such k. As it was shown by Erdős and Turán [3], we have $s_n = (1+o(1))\sqrt{n}$. Getting good estimates on the error term is a well-known open problem. For example, the \$500 prize of Erdős [1] for proving or disproving that $s_n = \sqrt{n} + O(1)$ is still unclaimed.

Another trivial bound $D(k,n) \le 2n+1$ is obtained by observing that $A - A$ is a subset of $[-n, n]$. This bound is sharp if and only if $[0,n]$ has a restricted difference basis $A \subset [0,n]$ of size k. Let b_n be the smallest possible k with this property. The parameter b_n is not known even asymptotically. The best known upper bound $b_n \le (\sqrt{3}+o(1))\sqrt{n}$ is due to Wichmann [10]. A result of Rédei and Rényi [8] implies that

$$b_n \ge (c + o(1))\sqrt{n}, \tag{1}$$

where $c = \sqrt{2+4/(3\pi)} = 1.5570\ldots$. Leech [4] observed that the choice $\theta = 4.4934\ldots$ in Rédei and Rényi's argument (instead of $\theta = 3\pi/2$ used in [8]) improves the lower bound (1) to $b_n \ge (1.5602\cdots + o(1))\sqrt{n}$.

Given these well-known unsolved problems, the exact computation of $D(k,n)$ for all k and n seems out of reach. Therefore, we settle for proving some reasonable general bounds as n tends to infinity and $k = k(n)$ is an integer-valued function of n.

It follows from the above that, for all sufficiently large n, $D(k(n),n) = (k(n))^2 - k(n) + 1$ if $\limsup_{n\to\infty} k(n)/\sqrt{n} < 1$ and $D(k(n),n) = 2n-1$ if $\liminf_{n\to\infty} k(n)/\sqrt{n} > \sqrt{3}$. This prompts us to define, for any constant c,

$$d(c) = \lim_{\substack{n\to\infty \\ k(n)=(c+o(1))\sqrt{n}}} \frac{D(k(n),n)}{n}. \tag{2}$$

In Section 2 we show that this definition is correct, that is, the limit exists and is independent of the choice of the function $k(n)$. It follows (see Corollary 4) that $d(c)$ is a continuous function. Thus we have $d(c) = c^2$ if $0 \le c \le 1$ and $d(c) = 2$ if $c \ge \sqrt{3}$.

In Section 3 we improve the trivial upper bound $d(c) \le \min(c^2, 2)$ for a range of c as follows.

Theorem 1 *For any $c \ge 1$ we have $d(c) \le \min\left(2c-1,\ c^2/2+1-2/(3\pi)\right)$ Thus, if we define $c_0 = 2 - 2/\sqrt{3\pi} = 1.3485\ldots$ and $c_1 = \sqrt{2+4/(3\pi)} = 1.5570\ldots$, then*

$$d(c) \le \begin{cases} 2c-1, & 1 \le c \le c_0, \\ \frac{c^2}{2} + 1 - \frac{2}{3\pi}, & c_0 \le c \le c_1, \\ 2, & c \ge c_1. \end{cases}$$

Let us turn to lower bounds. Recall that we know $d(c)$ for any c except for $1 < c < \sqrt{3}$.

Theorem 2 *For any real γ with $0 \le \gamma \le 2$ we have*

$$d\left(\frac{4-\gamma}{\sqrt{7-\gamma}}\right) \ge \frac{13 - 6\gamma + \gamma^2/2}{7-\gamma}. \tag{3}$$

Also, let $c_2 = 4/\sqrt{7} = 1.5118\ldots$, *and* $c_3 = \sqrt{39/14} = 1.6690\ldots$. *Then we have*

$$d(c) \geq \begin{cases} 2 - \frac{1}{c^2}, & 1 \leq c \leq \sqrt{2}, \\ \frac{13}{7}, & c_2 \leq c \leq c_3, \\ \frac{2c^2}{3}, & c_3 \leq c \leq \sqrt{3}. \end{cases} \qquad (4)$$

Remark. The first bound in (4) is larger than the parametric bound (3) for c between 1 and $c_4 = 1.3028\ldots$. The bound (3) takes over for $c_4 \leq c \leq c_2$, which corresponds to γ ranging from $0.7405\ldots$ down to 0.

The graphical summary of our findings is presented in Figure 1, where the upper (gray) graph corresponds to the upper bound of Theorem 1 and the lower (black) graph corresponds to the lower bound of Theorem 2. For the reader's convenience, we present two plots, with the second plot zooming into the range where $d(c)$ is still unknown.

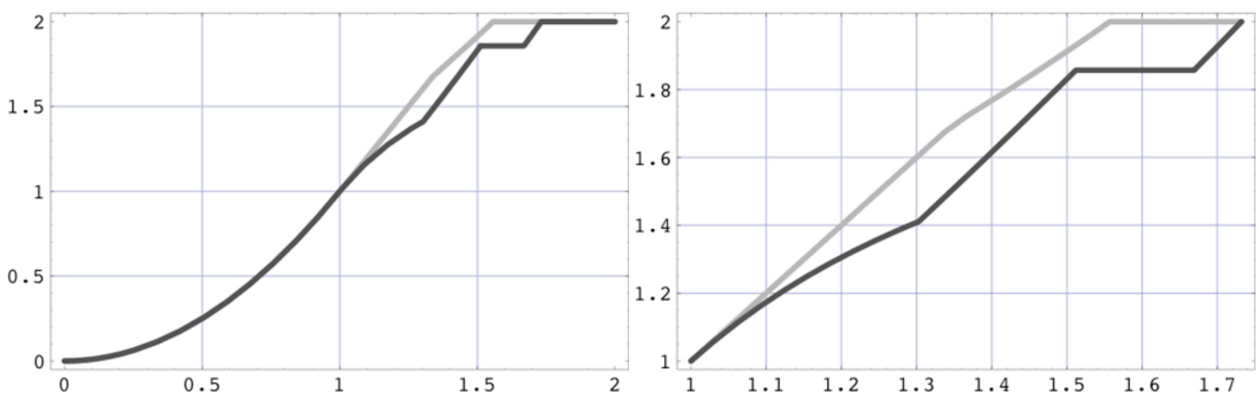

Figure 1: Our bounds on $d(c)$.

2. The Existence of the Limit

Theorem 3 *Let* $c \geq 0$ *be a fixed real. Let* $k(n)$ *be any integer-valued function such that* $k(n) = (c + o(1))\sqrt{n}$. *Then the ratio* $D(k(n), n)/n$ *tends to a limit as* n *tends to infinity, and this limit depends only on* c *(and not on the choice of the function* $k(n)$*).*

Proof. We use the method of Rédei and Rényi [8]. Given $k(n)$, let $\lambda = \limsup_{n\to\infty} \dfrac{D(k(n), n)}{n}$. Fix some small $\varepsilon > 0$. Let N be such that $|k(n) - c\sqrt{n}| < \varepsilon\sqrt{n}$ for all $n \geq N$. Choose $n_0 \geq \max(N, \varepsilon^{-1})$ such that $D(k(n_0), n_0) \geq (\lambda - \varepsilon)n_0$. Let n be sufficiently large, depending on ε, N, n_0.

The assumptions that $n_0 > \varepsilon^{-1}$ and n is large guarantee that there is a prime q with

$$(1 - \varepsilon)\sqrt{\frac{n}{n_0}} < q < \sqrt{\frac{n}{n_0 + 1}} - 1$$

(see, for instance, Lou and Yao [5] for results on the distribution of primes). Letting $m = q^2 + q + 1$ we have that $m(n_0 + 1) < (q + 1)^2(n_0 + 1) < n$ and $mn_0 > q^2 n_0 > (1 - 2\varepsilon)n$.

A construction of Singer [9] gives us numbers $a_0, \ldots, a_q \in [0, m - 1]$ such that the differences $a_i - a_j$, $i \neq j$, are pairwise distinct non-zero residues modulo m. It follows that these differences cover each non-zero residue modulo m precisely once.

Take any set $B_0 \subset [0, n_0]$ with $|B_0| = k(n_0)$ and $|B_0 - B_0| \geq (\lambda - \varepsilon)n_0$. Consider the set

$$B' = \{a_i + bm : i \in [0, q],\, b \in B_0\}.$$

Let us observe that $B' \subset [0, n]$ by the choice of q. If $|B'| \leq k(n)$, let $B = B'$; otherwise let B consist of arbitrary $k(n)$ elements of B'.

First, let us estimate $|B' - B'|$. If $h \in B_0 - B_0$, say $h = b_1 - b_2$, then $B' - B'$ contains the elements

$$a_i + b_1 m - (a_j + b_2 m) = (a_i - a_j) + hm, \quad i, j \in [0, q].$$

Moreover, different choices of the ordered triple (i, j, h) with $i \neq j$ produce distinct differences: the choice of i, j determines a non-zero residue modulo m and then h is determined uniquely. Furthermore, these elements are different from hm, which are obtained by taking $a_i = a_j$. Thus

$$|B' - B'| \geq |B_0 - B_0| \times ((q + 1)q + 1) \geq (\lambda - \varepsilon)n_0 m \geq (\lambda - \varepsilon)(1 - 2\varepsilon)n \geq (\lambda - O(\varepsilon))n. \tag{5}$$

Now, let us estimate $|B' \setminus B|$. We have

$$|B'| \leq (q + 1)|B_0| \leq (q + 1)(c + \varepsilon)\sqrt{n_0} < (c + \varepsilon)\sqrt{n},$$

so that $|B' \setminus B| = |B'| - |B| \leq 2\varepsilon\sqrt{n}$ in view $k(n) \geq (c - \varepsilon)\sqrt{n}$.

But by deleting $O(\varepsilon\sqrt{n})$ elements from B', we can destroy at most $O(\varepsilon n)$ differences, that is,

$$\frac{D(k(n), n)}{n} \geq \frac{|B - B|}{n} \geq \lambda - O(\varepsilon)$$

for all large n. As ε was arbitrary, the existence of the limit follows.

Also, the value of the limit depends only on c but not on the choice of the function $k(n)$. Indeed, if two different choices $k_1(n)$ and $k_2(n)$ produced different limiting values, then the function $k(n)$ defined by $k(2l - 1) = k_1(2l - 1)$ and $k(2l) = k_2(2l)$, $l \in \mathbb{N}$, would contradict the first part of the theorem. □

Remark. The proof gives in fact a stronger claim as follows. Suppose that we have some k_0-set $B_0 \subset [0, n_0]$. Let $b_0 = |B_0 - B_0|$ and let n be sufficiently large. Then by choosing an appropriate $q \approx \sqrt{n/(n_0 + 1)}$, we obtain, as above, a set $B \subset [0, n]$ such that $|B| \approx k_0 q$ and

$|B-B| \gtrapprox b_0q^2$. It follows that $d(k_0/\sqrt{n_0+1}) \geq b_0/(n_0+1)$. This inequality (combined with the deletion method) can be used for proving lower bounds on the function $d(c)$, see Section 4 for examples.

Corollary 4 *$d(c)$ is a continous function of c.*

Proof. Suppose that the claim is not true. Since $d(c)$ is non-decreasing, this means that there are c_0 and $\varepsilon > 0$ such that $d(c) > d(c_0) + \varepsilon$ for all $c > c_0$. Find two sequences $n_1 < n_2 < \dots$ and $k_1, k_2, \dots$ of positive integers with

$$c_0\sqrt{n_i} \leq k_i \leq (c_0 + 1/i)\sqrt{n_i} \quad \text{and} \quad D(k_i, n_i) \geq (d(c_0) + \varepsilon/2)n_i, \quad \text{for all } i \in \mathbb{N}.$$

Let $k(n)$ be an arbitrary function such that $k(n_i) = k_i$ for all $i \in \mathbb{N}$ and $k(n) = (c_0+o(1))\sqrt{n}$. By Theorem 3,

$$\lim_{n\to\infty} \frac{D(k(n), n)}{n} = d(c_0).$$

However, by the definition,

$$\limsup_{n\to\infty} \frac{D(k(n), n)}{n} \geq \limsup_{i\to\infty} \frac{D(k_i, n_i)}{n_i} \geq d(c_0) + \frac{\varepsilon}{2},$$

which is a contradiction. □

3. Upper Bounds

Here we prove Theorem 1. We will not need the constants c_0, c_1 here; these constants simply mark the values of c when one bound starts superseding another. So, fix constant c and take any function $k(n) = (c+o(1))\sqrt{n}$. Let n be sufficiently large and let the corresponding value $k(n)$ be denoted by k. Let A be an arbitrary subset of $[0, n]$ of size k.

We start by showing that $d(c) \leq 2c - 1$ for any $c \geq 1$. The case $c = 1$ has already been settled. Also, we know that $d(c) \leq 2$ for any c. So let us assume that $1 < c < 3/2$. Define $t := \lfloor (c-1)n \rfloor$, $A_i := A \cap [i, i+t-1]$, and $a_i := |A_i|$, $\quad i \in [1-t, n]$.

Let $\mathcal{X}$ consist of all quadruples (a, b, i, x) such that $x = a - b > 0$ and $a, b \in A_i$. Using the identity $\sum_{i=1-t}^{n} a_i = kt$ and the quadratic-arithmetic mean inequality, we obtain

$$|\mathcal{X}| = \sum_{i=1-t}^{n} \binom{a_i}{2} = \frac{1}{2}\sum_{i=1-t}^{n} a_i^2 \; - \frac{kt}{2} \geq (1+o(1))\frac{(kt)^2}{2(n+t)}. \tag{6}$$

For $x \in \mathbb{Z}$, let $\nu(x)$ be the number of representations $x = a - b$ with $a, b \in A$. Then, each $x \in [1, t-1]$ is included in precisely $(t-x)\nu(x)$ quadruples. Hence,

$$|\mathcal{X}| = \sum_{x=1}^{t-1}(t-x)\nu(x) \leq \sum_{x=1}^{t-1}(t-x) + \sum_{x=1}^{t-1}(t-x) \times \max(\nu(x)-1, 0). \tag{7}$$

The first sum is $t(t-1)/2$, while the second sum can be bounded from above by

$$t\sum_{x=1}^{n}\max(\nu(x)-1,0)=t\sum_{x=1}^{n}\nu(x)-t\left|(A-A)\cap[1,n]\right|=t\binom{k}{2}-t\,\frac{|A-A|-1}{2}.$$

Putting all together we obtain:

$$\frac{(kt)^2}{2(n+t)}\le\frac{t^2}{2}+\frac{t(k^2-|A-A|)}{2}+o(n^2).$$

Routine simplifications yield the desired bound on $|A-A|$.

Our proof of the other bound of Theorem 1 uses some ideas from [8] and works for an abritrary $c>0$. Let n, k, and A be as before. Let $b=|A-A|$. For a real x define

$$f(x)=\sum_{a\in A}\mathrm{e}^{\mathrm{i}ax},$$

where i is a square root of -1. We have

$$|f(x)|^2=\left(\sum_{a\in A}\mathrm{e}^{\mathrm{i}ax}\right)\left(\sum_{a\in A}\mathrm{e}^{-\mathrm{i}ax}\right)=\sum_{a_1,a_2\in A}\mathrm{e}^{\mathrm{i}(a_1-a_2)x}\ge 0. \tag{8}$$

The difference $|f(x)|^2-\sum_{r=-n}^{n}\mathrm{e}^{\mathrm{i}rx}$ can be written as a sum of $2n+1-b$ terms of the form $-\mathrm{e}^{\mathrm{i}rx}$ and k^2-b (not necessarily distinct) terms of the form $\mathrm{e}^{\mathrm{i}rx}$. Thus, by taking the real part of (8) we obtain

$$(2n+1-b)+(k^2-b)+D_n(x)\ge 0, \tag{9}$$

where

$$D_n(x)=1+2\sum_{r=1}^{n}\cos(rx).$$

The function $D_n(x)/(2\pi)$ is called the *Dirichlet kernel*. It is well-known (and easy to show by induction on n) that

$$1+2\sum_{r=1}^{n}\cos(rx)=\frac{\sin(\frac{2n+1}{2}x)}{\sin(\frac{x}{2})}.$$

Let us take $x=3\pi/(2n+1)$. Then $D_n(x)\le -4n/(3\pi)+o(n)$. Plugging this into (9) we obtain the required bound on $b=|A-A|$.

4. Lower Bounds

First, we prove the lower bound (3). We apply the idea of the remark after Theorem 3 to the set $B_0=\{0,1,4,6\}$. Namely, we pick a large prime q. As in Theorem 3, let $A=\{a_0,\dots,a_q\}$ be the Singer subset of $[0,m-1]$, where $m=q^2+q+1$. Let $C=C_0\cup C_1\cup C_4\cup C_6$, where $C_i = A + im = \{a + im : a \in A\}$. Note that $|B_0 - B_0| = 13$. As in (5), we have $|C - C| \geq 13m$.

Given γ, let C'_0 consist of the first $\lfloor \gamma q/2 \rfloor$ elements of C_0 and let C'_6 consist of the last $\lfloor \gamma q/2 \rfloor$ elements of C_6. Let $B = C \setminus (C'_0 \cup C'_6)$. Note that

$$(C_0 - C'_0) \cup (C'_6 - C_6) \subset C_1 - C_1 \subset B - B.$$

So by removing $C'_0 \cup C'_6$ from C we destroy at most

$$\begin{aligned} 2 \quad &\times \quad \Big(|C'_0| \times |C_1 \cup C_4 \cup C_6| + |C'_6| \times |(C_0 \setminus C'_0) \cup C_1 \cup C_4| \Big) \\ &= \quad 2 \left(\frac{\gamma q}{2} \times 3q + \frac{\gamma q}{2} \times \left(3 - \frac{\gamma}{2}\right) q + o(q^2) \right) \quad = \quad \left(6\gamma - \frac{\gamma^2}{2} + o(1) \right) m \end{aligned}$$

differences. Thus,

$$|B - B| \geq \left(13 - 6\gamma + \frac{\gamma^2}{2} + o(1) \right) m. \tag{10}$$

Erdős and Freud [2] proved that any almost optimal Sidon subset of $[0, n]$, that is, having size $(1 + o(1))\sqrt{n}$, is almost uniformly distributed in the interval. This, of course, applies to the Singer set A. It follows that the diameter of C'_0 and of C'_6 is $(\gamma/2 + o(1))m$, where the *diameter* of a finite set $X \subset \mathbb{Z}$ is $\operatorname{diam} X = \max X - \min X$. Thus

$$\operatorname{diam} B = \operatorname{diam} C - \frac{\gamma}{2} m - \frac{\gamma}{2} m + o(m) = (7 - \gamma + o(1))m.$$

By translating B, we can ensure that $B \subset [0, \operatorname{diam} B]$. Let us denote $k_q = |B|$ and $n_q = \operatorname{diam}(B)$.

Thus we have an infinite sequence of pairs (k_q, n_q) with $k_q = (4 - \gamma + o(1))q$, $n_q = (7 - \gamma + o(1))q^2$, and $D(k_q, n_q) \geq (13 - 6\gamma + \gamma^2/2 + o(1))\, q^2$. Let P be an infinite set of primes such that $n_p \neq n_q$ for all distinct $p, q \in P$. Take any function $k(n)$ such that $k(n_q) = k_q$ for all $q \in P$ and $k(n) = ((4 - \gamma)/\sqrt{7 - \gamma} + o(1))\sqrt{n}$ as $n \to \infty$. The desired bound follows from Theorem 3:

$$d\left(\frac{4 - \gamma}{\sqrt{7 - \gamma}} \right) \geq \liminf_{\substack{q \to \infty \\ q \in P}} \frac{D(k_q, n_q)}{n_q} \geq \frac{13 - 6\gamma + \gamma^2/2}{7 - \gamma}.$$

In order to prove the first bound in (4), we proceed similarly to above. Namely, let q, m, A, C_0, and C_1 be as before. Define $B_0 = \{0, 1\}$, $C = C_0 \cup C_1 = A \cup (A + m)$, and let C'_0 (resp. C'_1) consist of the first (resp. last) $\lfloor \gamma q/2 \rfloor$ elements of C, where we set $\gamma = 2 - c^2$. We allow c to range between 1 and $\sqrt{2}$, so $0 \leq \gamma \leq 1$. Let $B = C \setminus (C'_0 \cup C'_1)$. Then $|B| = (2 - \gamma + o(1))q$ and $\operatorname{diam} B = (2 - \gamma + o(1))m$, so we indeed have $|B| = (c + o(1))\sqrt{\operatorname{diam} B}$.

By (5), $|C - C| \geq 3m$. Let us estimate the number of destroyed differences, that is, the size of $(C - C) \setminus (B - B)$. The analysis here is a bit more complicated. Let us remove C_0' first. Since $C_0 - C_0' \subset C_1 - C_1$, when we remove C_0', we destroy at most

$$2 \times |C_0'| \times |C_1| = (\gamma + o(1))m$$

differences. Now, let us remove C_1'. We have

$$C_1' - C_1' = (C_1' - m) - (C_1' - m) \subset (C_0 \setminus C_0') - (C_0 \setminus C_0')$$

because $\gamma \leq 1$. Also, $C_1' - (C_1 \setminus (C_1' \cup (C_0' + m)) \subset (C_1' - m) - (C_0 \setminus C_0')$. Thus, by removing C_1' we destroy at most

$$2 \times |C_1'| \times |(C_0' + m) \cup (C_0 \setminus C_0')| = \gamma(\gamma/2 + (1 - \gamma/2) + o(1))m = (\gamma + o(1))m$$

differences. Therefore, $\big|(C - C) \setminus (B - B)\big| \leq (2\gamma + o(1))m$, and $|B - B| \geq (3 - 2\gamma + o(1))m$. Putting all estimates together we obtain by Theorem 3 the required bound

$$d(c) \geq \frac{3 - 2\gamma}{2 - \gamma} = 2 - \frac{1}{c^2}, \quad 1 \leq c \leq \sqrt{2}.$$

The second bound in (4) follows from the case $\gamma = 0$ of (3) and the trivial observation that $d(c)$ is a non-decreasing function of c.

To prove the last bound in (4) we modify the construction of Wichmann [10]. Let $A_{k,r}$ be the set of $4r + k + 3$ integers with the smallest element 0 and the differences between consecutive elements being

$$\underbrace{1, \ldots, 1}_{r}, r + 1, \underbrace{2r + 1, \ldots, 2r + 1}_{r}, \underbrace{4r + 3, \ldots, 4r + 3}_{k}, \underbrace{2r + 2, \ldots, 2r + 2}_{r+1}, \underbrace{1, \ldots, 1}_{r}.$$

Thus, for example, the largest element of $A_{k,r}$ is

$$n = r + (r + 1) + r(2r + 1) + k(4r + 3) + (r + 1)(2r + 2) + r = 4r^2 + 4kr + O(k + r).$$

As it is stated in [10], for all $k, r \geq 1$ we have $A_{k,r} - A_{k,r} = [-n, n]$, that is, $A_{k,r}$ is a restricted difference basis for $[0, n]$ (see Miller [6, Apendix A] for a rigorous proof of this fact). Given fixed $c \leq \sqrt{3}$, let r tend to infinity. Let $k = \lceil (9/c^2 - 1)r \rceil$, $l = k - 2r \geq 0$, and $A = A_{k,r}$. Then $n = \operatorname{diam} A = (36/c^2 + o(1))r^2$ and $|A - A| = (72/c^2 + o(1))r^2$.

Partition $A = X \cup Y \cup Z$, where X (resp. Z) consists of the first $2r + 1$ (resp. last $2r + 1$) elements of A. Let L consist of the first l elements of Y and let $B = A \setminus L$.

Let us estimate the number of differences destroyed by removing L. Since Y and $L \subset Y$ are arithmetic progressions, we have $|Y - L| \leq |Y| + |L| - 1 = o(r^2)$. Also $(X - L) \cup (Z - L)$ has size at most $|L| \times |X \cup Z| = (36/c^2 - 12 + o(1))r^2$. So,

$$|B - B| \geq (72/c^2 - 2(36/c^2 - 12) + o(1))r^2 = (24 + o(1))r^2.$$

Since $|B|/\sqrt{n} = c + o(1)$, Theorem 3 implies that $d(c) \geq 24/(36/c^2) = 2c^2/3$, as required.

5. Final Remarks

Some of our bounds can be improved. Unfortunately, all the improvements that we could find are very small (hardly visible on the plots) while the resulting formulas become very complicated. Therefore, we settled for the present simpler bounds.

The value of $d(c)$ remains unknown for $1 < c < \sqrt{3}$ when $1 < d(c) \leq 2$. We state the following challenge:

Problem. Compute $d(c)$ exactly for at least one value of c with $1 < d(c) < 2$.

Acknowledgement

We thank the referee for many helpful suggestions that improved the presentation of this paper.

References

[1] P. Erdős, *A survey of problems in combinatorial number theory*, Ann. Discrete Math. **6** (1980), 89–115.

[2] P. Erdős and R. Freud, *On sums of a Sidon-sequence*, J. Number Theory **38** (1991), 196–205.

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

[4] J. Leech, *On the representation of* $1, 2, \ldots, n$ *by differences*, J. Lond. Math. Soc. **31** (1956), 160–169.

[5] S. Lou and Q. Yao, *A Chebyshev's type of prime number theorem in a short interval II*, Hardy-Ranamujan J. **15** (1992), 1–33.

[6] J. C. P. Miller, *Difference bases. Three problems in additive number theory*, Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), Academic Press, 1971, pp. 299–322.

[7] O. Pikhurko, *Dense edge-magic graphs and thin additive bases*, Discrete Math. **306** (2006), 2097–2107.

[8] I. Redéi and A. Rényi, *On the representation of integers* $1, 2, \ldots, n$ *by differences*, Mat. Sbornik **24** (1949), 385–389.

[9] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–85.

[10] B. Wichmann, *A note on restricted difference bases*, J. Lond. Math. Soc. **38** (1963), 465–466.