A Complete Annotated Bibliography of Work Related to Sidon Sequences

Kevin O'Bryant*

Department of Mathematics
University of California, San Diego, USA
kevin@member.ams.org

Submitted: May 3, 2004; Accepted: Jul 8, 2004; Published: Jul 26, 2004
MR Subject Classifications: 11B50, 11B83, 05B10

Abstract

A Sidon sequence is a sequence of integers $a_1 < a_2 < \dots$ with the property that the sums $a_i + a_j$ $(i \le j)$ are distinct. This work contains a survey of Sidon sequences and their generalizations, and an extensive annotated and hyperlinked bibliography of related work.

1 Introduction

For a subset $\mathcal{A}$ of an abelian group (usually $\mathbb{Z}$), define

$$\mathcal{A}^*(k) := \#\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} \colon a_1 + a_2 = k\}$$

and

$$\mathcal{A}^\circ(k) := \#\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} \colon a_1 - a_2 = k\}.$$

In 1932, Simon Sidon [3] considered sets of integers with both $\mathcal{A}^*$ and $\mathcal{A}^\circ$ bounded[1]. It is easily shown (and done so in the next section) that $\mathcal{A}^*(k) \le 2$ for all k if and only if $\mathcal{A}^\circ(k) \le 1$ for all $k \ne 0$. This led Sidon to ask Erdős how large a subset of $\{1, 2, \dots, n\}$ can

*The author is a National Science Foundation Postdoctoral Research Fellow at the University of California at San Diego, grant DMS-0202460.

[1]Here is one of his theorems. Suppose that C and g are real numbers. There is a constant $K = K(C, g)$ such that for every set $\mathcal{A}$ of positive integers with $\mathcal{A}^*(k) + \mathcal{A}^\circ(k) \le g$ (for all $k > 0$) and every sequence λ_a with $\sum |\lambda_a|^2 \le C$, there is a function $f : [0, 1] \to \mathbb{C}$ which is bounded by K and $\hat{f}(a) = \lambda_a$ for every $a \in \mathcal{A}$.

be with the property that $\mathcal{A}^*(k) \le 2$ (for all k)? Since that time such sets, e.g., $\{1, 2, 5, 7\}$, have been known as Sidon sets. In other words, $\mathcal{A}$ is a Sidon set if the coefficients of

$$\left(\sum_{a \in \mathcal{A}} z^a \right)^2$$

are bounded by 2.

Unfortunately, many authors call Sidon sets "B_2 sets", and harmonic analysts use the term "Sidon set" to mean something entirely different. These two factors make searching the literature rather difficult. In Math Sci-Net, for example, it is impossible to search for a math expression such as "B_2", and a search for "Sidon" returns almost 700 hits, most concerning the harmonic analysts' Sidon sets. Further, there are several different notations in use, sometimes making it difficult to compare results. For these reasons, I felt that it would be useful to compile a complete annotated bibliography with a consistent notation and to lay out the major avenues of research, past, present and possibly future.

In loose terms, requiring a set to have the Sidon property forces it to be thin, e.g., it cannot contain three consecutive integers. The most basic question is "How thick can a Sidon set be?" There are several ways to make this question explicit, several different settings to explore, and a variety of generalizations. Having only partially solved these problems, researchers have recently begun turning their attention to the question "what is the structure of a maximally thick Sidon set?"

In Section 2, we define the relevant sets and counting functions and fix the terminology used in the annotations. In Section 3, we present the known general constructions of (generalized) Sidon sets. In Sections 4 and 5 we give the state-of-the-art results concerning the density of Sidon sets. In Section 6 we state a few of the results concerning the structure of Sidon sets and their sumsets. In Section 7 we discuss the problem of finding a Sidon subset of a given set, such as Sidon sets whose elements are squares or fifth powers. In Section 9 we list some of the major unsolved questions.

Finally, we give a partially annotated bibliography of works which either develop or apply the theory of Sidon sets. The bibliography is, so far as I know, complete and 100% accurate. The bibliography is heavily hyperlinked (so you lose something if you print it out), and the links to Math Sci-Net reviews require a Math Sci-Net subscription. Please email the author regarding any omissions, additions, errors, or clarifications.

2 Terminology

We begin by defining a generalized Sidon sequence (with parameters h and g) to be a sequence $\mathcal{A}$ such that the coefficients of

$$\left(\sum_{a \in \mathcal{A}} z^a \right)^h \tag{1}$$

are bounded by g. We note that the coefficient of z^k in (1), which we denote $\mathcal{A}^{*h}(k)$, has a number-theoretic interpretation: it is the number of ways to write k as a sum of h

(not necessarily distinct) elements of $\mathcal{A}$. Also note that this definition is sensible for $\mathcal{A}$ a subset of any group G.

Our notation $\mathcal{A}^{*h}(k)$ is motivated by the notation for Fourier convolution: for any functions f, g, we have

$$f * g(k) = \sum_{x \in G} f(x)\overline{g(k-x)}.$$

Thus, if $\mathcal{A}$ is the indicator function of the sequence $\mathcal{A}$ (a common and useful abuse of notation), then $\mathcal{A}^{*h}(k)$ is exactly the convolution of h copies of $\mathcal{A}$ evaluated at k: $\mathcal{A}^{*h}(k) = \mathcal{A} * \cdots * \mathcal{A}(k)$. For brevity, we write $\mathcal{A}^*$ in place of $\mathcal{A}^{*2}$. Likewise, we hijack the notation of Fourier correlation:

$$\mathcal{A}^{\circ}(k) = \sum_x \mathcal{A}(x)\mathcal{A}(k+x) = \#\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} \colon a_2 - a_1 = k\}.$$

While convolution is associative, correlation is not. Thus $\mathcal{A}^{\circ h}$ is ill-defined; we adopt the convention $\mathcal{A}^{\circ h} = \mathcal{A}^{\circ h-1} \circ \mathcal{A}$.

Definition 1 **($B_h^*[g]$ sequence).** *A sequence $\mathcal{A}$ is a $B_h^*[g]$ sequence if the coefficients of $\left(\sum_{a \in \mathcal{A}} z^a\right)^h$ are bounded by g. If $\mathcal{A} \subseteq G \neq \mathbb{Z}$, then we call $\mathcal{A}$ a $B_h^*[g](G)$ sequence. In particular, if G is the additive group of integers modulo n, then we speak of $B_h^*[g] \pmod{n}$ sequences. We use the same notation for the property and for the class of sequences with the property, i.e., if $\mathcal{A}$ is a $B_h^*[g]$ sequence then we write $\mathcal{A} \in B_h^*[g]$.*

Thus, Sidon sequences are exactly the $B_2^*[2]$ sequences. We note that $\mathcal{A}^{\circ}$ is bounded by 1 if and only if $\mathcal{A}^*$ is bounded by 2. For if $\mathcal{A}^{\circ}(k) > 1$ (with $k > 0$), then there are $a_1, a_2, a_3, a_4 \in \mathcal{A}$ with $k = a_1 - a_2 = a_3 - a_4$, and at most two of the a_i are equal. This means that $a_4 + a_1 = a_1 + a_4 = a_2 + a_3 = a_3 + a_2$, so that $\mathcal{A}^*(a_1 + a_4) \geq 3$ (it is possible that $a_2 = a_3$ or $a_4 = a_1$, but not both). Note however that if $\mathcal{A} = \{2^k, 2^k + 1 \colon k \geq 1\}$, then for all k, $\mathcal{A}^*(k) \leq 4$, while $\mathcal{A}^{\circ}(1) = \infty$; and if $\mathcal{A} = \{\pm 2^k \colon k \geq 1\}$ then $\mathcal{A}^{\circ}(k) \leq 3$ for all $k \neq 0$, but $\mathcal{A}^*(0) = \infty$. The upshot is that $B_2^*[2]$ sequences are not only historically important, but they are qualitatively easier to deal with. In essentially all ways, more is known about Sidon sequences than about $B_h^*[g]$ sequences with $h > 2$ or $g > 3$.

We use the notation $[n] := \{1, 2, \ldots, n\}$. Obviously the $B_h^*[g]$ property is invariant under translation and dilation, so a supposition of the type "$\mathcal{A} \subseteq [n]$" can usually be replaced with "$\mathcal{A}$ is a subset of an arithmetic progression of length n".

Definition 2 **(R and C).** *$R_h(g, n)$ is the largest cardinality of a $B_h^*[g]$ sequence contained in $[n]$. $C_h(g, n)$ is the largest cardinality of a $B_h^*[g] \pmod{n}$ sequence.*

Definition 3 **($B_h[g]$ sequence).** *A $B_h[g]$ sequence is a $B_h^*[h!g]$ sequence. If $g = 1$, then we speak simply of B_h sequences.*

We note that many authors define a $B_h[g]$ sequence to be a $B_h^*[h!(g+1) - 1]$ sequence (and so a Sidon sequence, for these authors, is a sequence for which $\mathcal{A}^{*h}(k) \leq 3$). This is not without reason. If $k = a_1 + \cdots + a_h$ and the a_i are distinct, then there are $h!$

rearrangements of the a_i which contribute to $\mathcal{A}^{*h}(k)$. Since there are asymptotically few h-tuples from $\mathcal{A}\times\cdots\times\mathcal{A}$ that have repeated a_i's, one expects that there is little distinction (asymptotically) between $B_h^*[h!g]$ sets and $B_h^*[h!(g+1)-1]$ sets. This expectation, however, has not been proven to hold except for $h=2$, $g=1$.

3 Constructions

3.1 The greedy algorithm

The obvious first attempt at constructing a $B_h^*[g]$ sequence is to be greedy. Set $\gamma_1 = 1$, and define for each $k \geq 1$ the sequence

$$\mathcal{G}_k = \{\gamma_1, \gamma_2, \ldots, \gamma_k\}$$

where γ_k is the least $m > \gamma_{k-1}$ such that $\{\gamma_1, \gamma_2, \ldots, \gamma_k\}$ is a $B_h^*[g]$ sequence. Then

$$\mathcal{G}_h[g] := \bigcup_{k=1}^{\infty} \mathcal{G}_k$$

is an infinite $B_h^*[g]$ sequence.

Mian & Chowla [10] computed the first terms of $\mathcal{G}_2[2]$ (i.e., the greedy Sidon sequence, also called the Mian-Chowla sequence) to be 1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97, ... Stöhr [12] notes that the Mian-Chowla sequence satisfies $\gamma_k < (k-1)^3 + 1$. Even for this most simple case, however, the growth of γ_k is not well understood. See [42]. The points $(k, \log_k(\gamma_k))$ are shown in Figure 3.1.

It is interesting to study the greedy sequence with different seeds. Start by setting $\gamma_1, \ldots, \gamma_r$, and then continue the sequence in the same manner as above. The resulting sequence is denoted $\mathcal{G}_h[g; \gamma_1, \ldots, \gamma_r]$.

Conjecture 4. *For any h and g, there are not positive integers $r, \gamma_1, \ldots, \gamma_r$ such that*

$$\inf_{\mathcal{A} \in B_h^*[g]} \left\{ \sum_{a \in \mathcal{A}} \frac{1}{a} \right\}$$

is achieved with $\mathcal{A} = \mathcal{G}_h[g; \gamma_1, \ldots, \gamma_r]$.

This conjecture is dealt with in [60, 108]; it is known that the infimum in Conjecture 4 (for $g = h = 2$) is between 2.16 and 2.25.

3.2 Ruzsa's sets

A very simple construction of B_2 sequences was given by Ruzsa [59], which is generalized in [127] to $B_2[g^2]$ sequences. Let θ be a generator of the multiplicative group modulo the prime p. For $k, t \in [p-1]$, let $a_{t,k}$ be the congruence class modulo $p^2 - p$ defined by

$$a_{t,k} \equiv t \pmod{p-1} \quad \text{and} \quad a_{t,k} \equiv k\theta^t \pmod{p}.$$

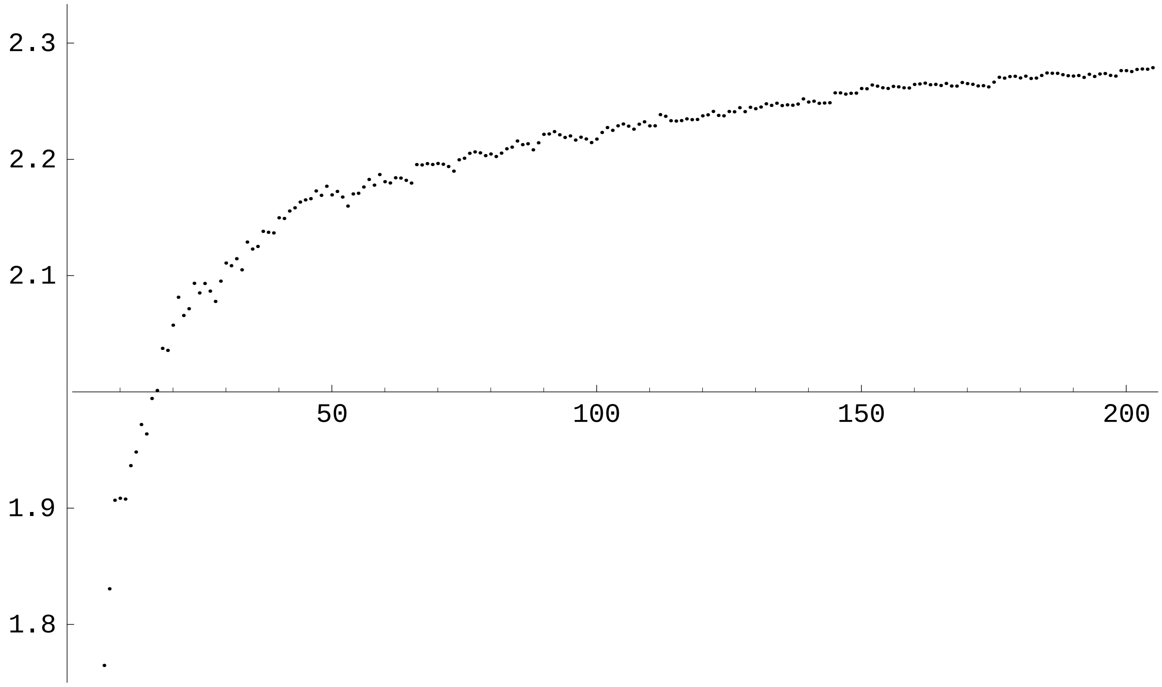

Figure 1: The points $(k, \log_k(\gamma_k))$ for the greedy Sidon set $\mathcal{G}_2[2]$.

Define the set

$$\texttt{Ruzsa}(p, \theta, k) := \{a_{t,k} \colon 1 \leq t < p\} \subseteq \mathbb{Z}/(p^2 - p).$$

If $\mathcal{K}$ is any subset of $[p-1]$, then

$$\texttt{Ruzsa}(p, \theta, \mathcal{K}) := \bigcup_{k \in \mathcal{K}} \texttt{Ruzsa}(p, \theta, k)$$

is a subset of $\mathbb{Z}/(p^2 - p)$ with cardinality $|\mathcal{K}|(p-1)$ and

$$\texttt{Ruzsa}(p, \theta, \mathcal{K}) \in B_2[|\mathcal{K}|^2].$$

An example is given in Figure 3.2: the row labeled k is $\texttt{Ruzsa}(13, 2, k)$. Note that each row is a translate modulo $13^2 - 13$ of the row above (and rotated). This is because

$$a_{t,k\theta} + p \equiv a_{(t+1 \bmod p-1),k} \pmod{p^2 - p},$$

and consequently $\texttt{Ruzsa}(p, \theta, k\theta) + p = \texttt{Ruzsa}(p, \theta, k)$. Since θ is a generator of the multiplicative group modulo p, this implies that for fixed p and θ all of the various $\texttt{Ruzsa}(p, \theta, k)$ are translates of one another.

3.3 Bose's sets

Bose [6] constructed Sidon sequences by using finite affine geometry. His construction was extended to B_h sequences (and given in the language of finite fields) in [15], and extended

k \ t	1	2	3	4	5	6	7	8	9	10	11	12
1	145	134	99	16	149	90	115	152	57	10	59	144
2	121	86	3	136	77	102	139	44	153	46	131	132
3	97	38	63	100	5	114	7	92	93	82	47	120
4	73	146	123	64	89	126	31	140	33	118	119	108
5	49	98	27	28	17	138	55	32	129	154	35	96
6	25	50	87	148	101	150	79	80	69	34	107	84
7	1	2	147	112	29	6	103	128	9	70	23	72
8	133	110	51	76	113	18	127	20	105	106	95	60
9	109	62	111	40	41	30	151	68	45	142	11	48
10	85	14	15	4	125	42	19	116	141	22	83	36
11	61	122	75	124	53	54	43	8	81	58	155	24
12	37	74	135	88	137	66	67	56	21	94	71	12

Figure 2: Table of $a_{t,k}$ with $p = 13$, $\theta = 2$. Each row is a Sidon set, the union of any two rows is a $B_2^*[8]$ set, the union of any $|\mathcal{K}|$ rows is a $B_2^*[2|\mathcal{K}|^2]$ set. Specifically, the row labeled k is $\texttt{Ruzsa}(13, 2, k)$.

to $B_2[g^2]$ sequences in [127]. Let q be any prime power, θ a generator of the multiplicative group of $\mathbb{F}_{q^h}$, and $k \in \mathbb{F}_q$, and define the set

$$\texttt{Bose}_h(q, \theta, k) := \{a \in [q^h - 1] \colon \theta^a - k\theta \in \mathbb{F}_q\}.$$

$\texttt{Bose}_h(q, \theta, 1)$ is $B_h \pmod{q^h - 1}$ set, and some work (see [11]) has been done on the question of how quickly these sets can be computed and whether varying θ (with $h = 2$) can help produce a Sidon set with smaller largest element. If $\mathcal{K}$ is any subset of $\mathbb{F}_q \setminus \{0\}$, then

$$\texttt{Bose}_2(q, \theta, \mathcal{K}) := \bigcup_{k \in \mathcal{K}} \texttt{Bose}_2(q, \theta, k)$$

is a $B_2[|\mathcal{K}|^2] \pmod{q^2 - 1}$ sequence.

An example is given in Figure 3.3, with $q = 13$, $h = 2$, $\mathbb{F}_{13^2} = \mathbb{F}_{13}[x]/(x^2 + 2)$, and $\theta = 1 + 3x$. The column labeled c_1 is $\texttt{Bose}_2(13, 1 + 3x \bmod (13, x^2 + 2), c_1)$. Note that, as with Ruzsa's sets, varying k has the effect of translating the set:

$$\texttt{Bose}_h(q, \theta, k) = \texttt{Bose}_h(q, \theta, 1) + \log_\theta(k).$$

We note that, unlike Ruzsa's sets, each *row* (except the one labeled zero) in Figure 3.3 is also a Sidon set.

3.4 Singer's sets

Sidon sequences arose incidentally in Singer's work [4] on finite projective geometry. While Singer's construction gives a slightly thicker Sidon set than Bose's (which is slightly thicker

c_0 \ c_1	0	1	2	3	4	5	6	7	8	9	10	11	12
0		77	147	21	49	35	91	7	119	133	105	63	161
1	168	164	148	1	19	114	87	123	138	79	13	76	116
2	70	25	66	40	50	149	71	83	89	146	16	18	157
3	112	23	58	108	125	31	92	20	67	113	60	82	131
4	140	153	95	159	136	48	110	86	120	88	51	59	141
5	126	96	127	34	45	122	37	145	74	81	106	139	72
6	14	90	93	137	128	15	10	130	27	152	101	33	162
7	98	78	117	17	68	111	46	94	99	44	53	9	6
8	42	156	55	22	165	158	61	121	38	129	118	43	12
9	56	57	143	135	4	36	2	26	132	52	75	11	69
10	28	47	166	144	29	151	104	8	115	41	24	142	107
11	154	73	102	100	62	5	167	155	65	134	124	150	109
12	84	32	160	97	163	54	39	3	30	103	85	64	80

Figure 3: The least positive integer k such that $(1+3x)^k = c_0 + c_1 x \bmod (13, x^2+2)$. The column corresponding to c_1 is the Sidon set $\texttt{Bose}_2(13, 1+3x \bmod (13, x^2+2), c_1)$.

than Ruzsa's), the construction is more complicated — even after the simplification of [15]. Singer's construction was extended to $B_2[g^2]$ sequences in [127]. No computational work has been published for Singer's sets.

Let q be any prime power, and let θ be a generator of the multiplicative group of $\mathbb{F}_{q^{h+1}}$. For each $\vec{k} = \langle k_1, \ldots, k_h \rangle \in \mathbb{F}_q^h$ define the set

$$T(\vec{k}) := \{0\} \cup \left\{ a \in [q^{h+1}-1] \colon \theta^a - \sum_{i=1}^{h} k_i \theta^i \in \mathbb{F}_q \right\}.$$

Then define

$$\texttt{Singer}_h(q, \theta, \vec{k})$$

to be the congruence classes modulo $\frac{q^{h+1}-1}{q-1}$ that intersect $T(\vec{k})$. Also define

$$\texttt{Singer}_h(q, \theta, \mathcal{K}) := \bigcup_{\vec{k} \in \mathcal{K}} \texttt{Singer}_h(q, \theta, \vec{k}),$$

where $\mathcal{K}$ is any subset of $\mathbb{F}_q^h$. The set $\texttt{Singer}_h(q, \theta, \langle 1, 0, 0, \ldots \rangle)$ is a $B_h \pmod{\frac{q^{h+1}-1}{q-1}}$ set. The set $\texttt{Singer}_2(q, \theta, \langle 1, [k], 0 \rangle)$ is a $B_2^*[2k^2]$ set.

3.5 Erdős & Turàn's sets

Erdős & Turàn [5] gave a construction based on quadratic residues. These sets are substantially thinner than the constructions of Ruzsa, Bose, and Singer given above.

Fix a prime p, and let (k^2) be the unique integer in $[p-1]$ congruent to k^2 modulo p. The set $\{2pk+(k^2) : 1 \le k < p\}$ is a B_2 set contained in $[2p+1, 2p(p-1)+1]$.

3.6 Probabilistic Sets

The seminal paper of Erdős & Rényi [13] introducing the probabilistic method to combinatorial number theory contains a small section on B_2g sets. The crucial observation made is that (setting $p_n = 1/\sqrt{n}$) the sum

$$\sum_{n=1}^{N-1} p_n p_{N-n}$$

is bounded independent of N. In particular, they prove the existence of an infinite $B_2^*[g]$ set $a_1 < a_2 < \cdots$ satisfying

$$a_k = \mathcal{O}\left(k^{2(1+2/(g-1))}\right).$$

See the review of [13] for a more detailed explanation.

See [84, 92, 94, 99, 116, 128] for some applications of probability to Sidon sequences, and vice versa.

4 The size of finite Sidon sequences

One of the "most wanted" problems is to asymptotically estimate $R_h(g,n)$ for any h, g with $h > 2$ or $g > 3$. Also on the "most wanted" list is a construction of $B_h^*[g]$ sequences, with $g > h!$, which is dense but is not merely several B_h sets woven together (such sets do exist: [25]).

We measure the thickness of $B_h^*[g]$ sets with the quantity:

$$\sigma_h(g) := \lim_{n\to\infty} \frac{R_h(g,n)}{\sqrt[h]{\lfloor g/h! \rfloor\, n}}.$$

Strictly speaking, this limit is not known to exist for $h > 2$ or for $g > 3$. One should always understand a lower bound on $\sigma_h(g)$ as being a lower bound on the corresponding $\liminf$, and an upper bound as being an upper bound on the $\limsup$. If $g = h!$, then we simply write σ_h.

There are a number of conjectures that are natural to make:

1. The limit in the definition of $\sigma_h(g)$ is in fact well-defined.

2. For each h, $\sigma_h(g)$ is an increasing function of g.

3. For each h, $\lim_{g\to\infty} \sigma_h(g)$ is defined and finite.

4. If $kh! \le g_1 \le g_2 < (k+1)h!$, then $\sigma_h(g_1) = \sigma_h(g_2)$.

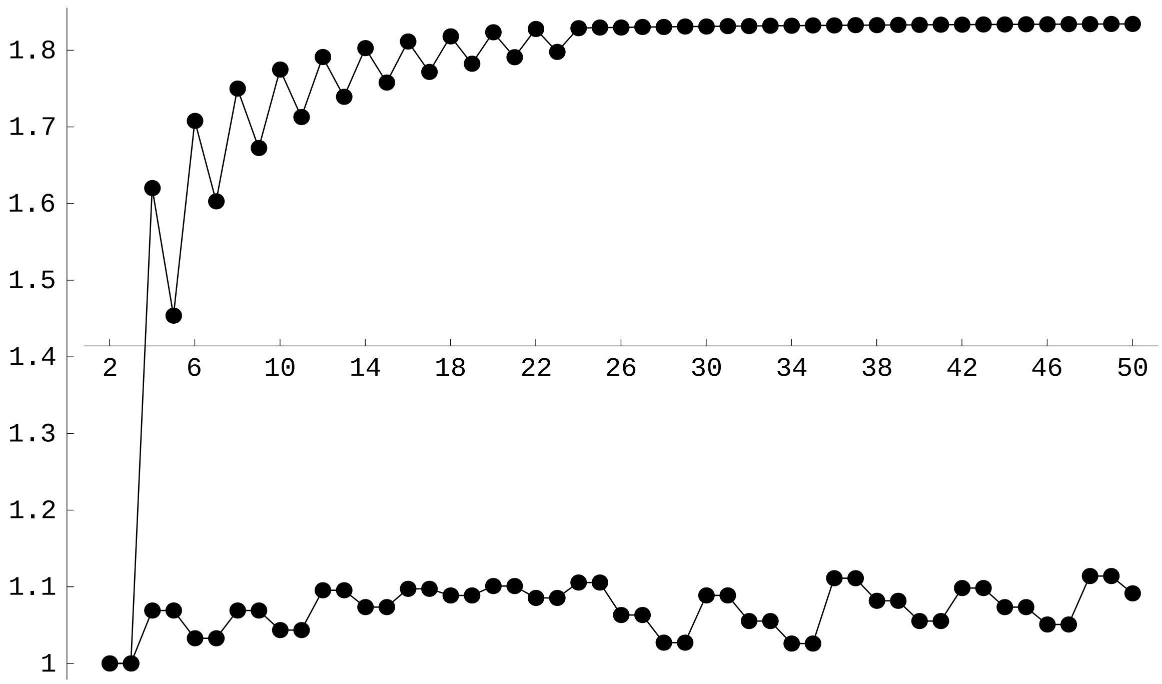

Figure 4: The best known upper and lower bounds on $\sigma_2(g)$.

As basic as these questions may seem, they remain unanswered. Regarding question 3, the limit is known to be bounded between two positive constants. Sadly, there isn't even a conjecture as to growth of σ_h as a function of h (it may well depend on the parity of h).

The only explicit values known are $\sigma_2(2) = \sigma_2(3) = 1$.

4.1 $h = 2$

Erdős offered USD 500 for answer to the question, "Is $R_2(2, n) - \sqrt{n}$ unbounded?" The answer is likely "yes"; it is also likely that $R(2, n) - \sqrt{n}$ is nonnegative. Unfortunately, there has been no progress on these questions since 1941, when it was found that

$$-n^{\alpha/2} < R(2, n) - \sqrt{n} < n^{1/4} + 1,$$

the lower bound holding only for n sufficiently large, with α being a real number such that there is always a prime between $n - n^{\alpha}$ and n (the current record is $\alpha = 0.525$).

The best known upper and lower bounds on $\sigma_2(g)$ are shown in Figure 4.1. The lower bound is

$$\begin{aligned}
\sigma_2(4) &\geq \sqrt{8/7} > 1.069, & \sigma_2(14) &\geq \sqrt{121/105} > 1.073,\\
\sigma_2(6) &\geq \sqrt{16/15} > 1.032, & \sigma_2(16) &\geq \sqrt{289/240} > 1.097,\\
\sigma_2(8) &\geq \sqrt{8/7} > 1.069, & \sigma_2(18) &\geq \sqrt{32/27} > 1.088,\\
\sigma_2(10) &\geq \sqrt{49/45} > 1.043, & \sigma_2(20) &\geq \sqrt{40/33} > 1.100,\\
\sigma_2(12) &\geq \sqrt{6/5} > 1.095, & \sigma_2(22) &\geq \sqrt{324/275} > 1.085,
\end{aligned}$$

and for $g \geq 12$

$$\sigma_2(2g) \geq \sqrt{2}\frac{g + 2\lfloor g/3 \rfloor + \lfloor g/6 \rfloor}{\sqrt{6g^2 - 2g\lfloor g/3 \rfloor + 2g}}.$$

In particular,

$$\lim_{g\to\infty} \sigma_2(g) \geq \sqrt{121/96} > 1.122.$$

The upper bound is a combination of

$$\sigma_2(2g) \leq \sqrt{\tfrac{7}{4}(2 - 1/g)}$$

and

$$\frac{\lfloor g/2 \rfloor}{g}\sigma_2(g)^2 \leq \begin{cases} 1.74043 - 1.00483/g, & g \leq 8 \text{ and even;}\\ 1.58337 - \frac{0.026335}{g} + \sqrt{0.011572 - \frac{0.083397}{g} + \frac{0.00069356}{g^2}}, & g \geq 10 \text{ and even;}\\ 1.74043 - \frac{4.75492}{g}, & g \leq 23 \text{ and odd;}\\ 1.58337 - \frac{0.071949}{g} + \sqrt{0.011572 - \frac{0.22784}{g} + \frac{0.0051768}{g^2}}, & g \geq 25 \text{ and odd.} \end{cases}$$

In particular,

$$\lim_{g\to\infty} \sigma_2(g) \leq 1.839.$$

For $g = 2$, the upper bound is due to Erdős & Turàn [5] and the upper bound is due to Singer [4]. For $g = 3$, the upper bound is Ruzsa's [59], and the lower bound is from $R(g+1, n) \leq R(g, n)$. For $g > 3$ the upper bound is a combination of Green [113] (for small g) and Martin & O'Bryant [126] (for large g). The lower bound for $g = 4$ is due to Habsieger & Plagne [119], the $g = 6$ and $g = 8$ bounds are due to [118], and for all other even g by Martin & O'Bryant [127]. The lower bounds for odd $g > 3$ are just $\sigma_2(2g) \leq \sigma_2(2g+1)$.

The proof of $\sigma_2(2) = 1$ is succinct and elegant; we present it momentarily. The upper bound was found initially in [5] and simplified in [19]. The lower bound was found in [4] and simplified to this form in [59].

Theorem 5. *The largest Sidon subset of* $[n]$ *has* $\sim \sqrt{n}$ *elements, i.e.,* $\sigma_2 = 1$.

Proof. Let $1 \leq a_1 < a_2 < \cdots < a_r \leq n$ be a Sidon sequence, and consider the differences (the parameter u will be set to $\lfloor n^{1/4} \rfloor$):

$$\begin{array}{cccc} a_2 - a_1, & a_3 - a_2, & \ldots, & a_r - a_{r-1} \\ a_3 - a_1, & a_4 - a_2, & \ldots, & a_r - a_{r-2} \\ & \vdots & & \\ a_{u+1} - a_1, & a_{u+2} - a_2, & \ldots, & a_r - a_{r-u} \end{array}$$

The k-th row contains $r-k$ differences, and since $\{a_i\}$ is a Sidon set, these differences are distinct. That's a total of $\sum_{i=1}^{u}(r-i) = ru - \frac{1}{2}u(u+1)$ differences. The sum of all these differences is at least

$$\sum_{i=1}^{ru-u(u+1)/2} i = \frac{1}{2}\left(ru - \tfrac{1}{2}u(u+1)\right)\left(ru - \tfrac{1}{2}u(u+1)+1\right).$$

On the other hand, the sum of the differences in the k-th row telescopes to

$$\sum_{i=r-k+1}^{r} a_i - \sum_{i=1}^{k} a_i < kn,$$

and so the sum of all the differences is less than $\sum_{k=1}^{u} kn = nu(u+1)/2$. Comparing the upper and lower bounds yields an inequality in terms of n, r, and $u = \lfloor n^{1/4} \rfloor$. Calculus implies that $r < n^{1/2} + n^{1/4} + 1$, which in turn implies that $\sigma_2 \le 1$.

We now give Ruzsa's construction of a Sidon set contained in $p(p-1)$ with $p-1$ elements (p is any odd prime), from which it follows (using the elementary fact that the ratio between consecutive primes goes to 1) that $\sigma_2 \ge 1$. Let θ be a primitive root modulo p, and consider the set $\mathcal{A}$ of integers a_t ($1 \le t < p-1$) defined by

$$1 \le a_t < p^2 - p \quad \text{and} \quad a_t \equiv t \pmod{p-1} \quad \text{and} \quad a_t \equiv \theta^t \pmod{p}.$$

Now suppose, by way of contradiction, that there are three pairs $(a_{r_m}, a_{v_m}) \in \mathcal{A} \times \mathcal{A}$ satisfying $a_{r_m} + a_{v_m} = k$ (for some fixed $k \in \mathbb{Z}$). Each pair gives rise to a factorization modulo p of

$$x^2 - kx + \theta^k \equiv (x - a_{r_m})(x - a_{v_m}) \pmod{p},$$

using the critical relation $a_{r_m} a_{v_m} \equiv \theta^{r_m + v_m} = \theta^k \pmod{p}$. Factorization modulo p is unique, so it must be that two of the three pairs are congruent modulo p, say

$$a_{r_1} \equiv a_{r_2} \pmod{p}. \tag{2}$$

In this case, $\theta^{r_1} \equiv a_{r_1} \equiv a_{r_2} \equiv \theta^{r_2} \pmod{p}$. Since θ has multiplicative order $p-1$, this tells us that $r_1 \equiv r_2 \pmod{p-1}$. Since $a_{r_m} \equiv r_m \pmod{p-1}$ by definition, we have

$$a_{r_1} \equiv a_{r_2} \pmod{p-1}. \tag{3}$$

Equations (2) and (3), together with $a_{r_1} + a_{v_1} = k = a_{r_2} + a_{v_2}$ imply that the pairs $(a_{r_1}, a_{v_1}), (a_{r_2}, a_{v_2})$ are identical, and so there are *not* three such pairs. Thus, $\mathcal{A}$ is a Sidon set. In particular, $\mathcal{A} = \texttt{Ruzsa}(p, \theta, 1)$. $\square$

k	$\min\{a_k - a_1\}$	Witness
2	1	{0,1}
3	3	{0,1,3}
4	6	{0,1,4,6}
5	11	{0,1,4,9,11}
		{0,2,7,8,11}
6	17	{0,1,4,10,12,17}
		{0,1,4,10,15,17}
		{0,1,8,11,13,17}
		{0,1,8,12,14,17}
7	25	{0,1,4,10,18,23,25}
		{0,1,7,11,20,23,25}
		{0,1,11,16,19,23,25}
		{0,2,3,10,16,21,25}
		{0,2,7,13,21,22,25}
8	34	{0,1,4,9,15,22,32,34}
9	44	{0,1,5,12,25,27,35,41,44}
10	55	{0,1,6,10,23,26,34,41,53,55}
11	72	{0,1,4,13,28,33,47,54,64,70,72}
		{0,1,9,19,24,31,52,56,58,69,72}
12	85	{0,2,6,24,29,40,43,55,68,75,76,85}
13	106	{0,2,5,25,37,43,59,70,85,89,98,99,106}

Figure 5: Shortest Sidon sequences (from [127], extended by John A. Trono of Saint Michael's College [personal communication])

k \ g	2	3	4	5	6	7	8	9	10	11
3	4									
4	7	5								
5	12	8	6							
6	18	13	8	7						
7	26	19	11	9	8					
8	35	25	14	12	10	9				
9	45	35	18	15	12	11	10			
10	56	46	22	19	14	13	12	11		
11	73	58	27	24	17	15	14	13	12	
12	86	≤ 72	31	29	20	18	16	15	14	13
13	107	≤ 101	37	34	24	21	18	17	16	15
14	≤ 140	≤ 128	44	40	28	26	21	19	18	17
15	≤ 163		≤ 52	≤ 47	32	29	24	22	20	19
16	≤ 195				36	34	27	24	22	21
17					≤ 42	≤ 38	30	28	24	23
18							34	32	27	25
19							≤ 38	≤ 36	30	28
20									33	31
21									≤ 37	35
21										≤ 38

Figure 6: $\min\{n\colon R_2(g,n) \geq k\}$ (from [127], extended by John A. Trono of Saint Michael's College [personal communication])

A Sidon sequence $a_1 < a_2 < \cdots < a_k$ is called "short" if $a_k - a_1$ is as small as possible. Figure 4.1 contains (up to reflection and translation) all of the short Sidon sequences with $k \leq 10$, and two of the short Sidon sequences with $k = 11$; I don't know if there are more. It is rumored that Imre Ruzsa has computed that $\min\{a_{14} - a_1\} = 127$.

Figure 4.1 gives the values of n for which $R(g,n) - R(g,n-1) = 1$. This table was computed using the easiest algorithm and a small amount of time. I encourage the interested reader (or her students!) to extend it.

The construction given in [118] is optimized by choosing x so that $R(g,x)/\sqrt{gx}$ is maximized. This appears to happen (for each g) with a fairly small value of x; a formula would lay to rest further optimization efforts (such as those in [119, 127]). Even given a perfect optimization, however, it is unlikely that this construction is optimal in any sense.

4.2 $h > 2$

Very little is understood about B_h sets for $h > 2$. The construction of Bose & Chowla [15] show that $\sigma_h \geq 1$, and we know that $\sigma_2 = 1$. Various improvements on the upper bound on σ_h were given in [14, 20, 32, 39, 58, 61, 82]

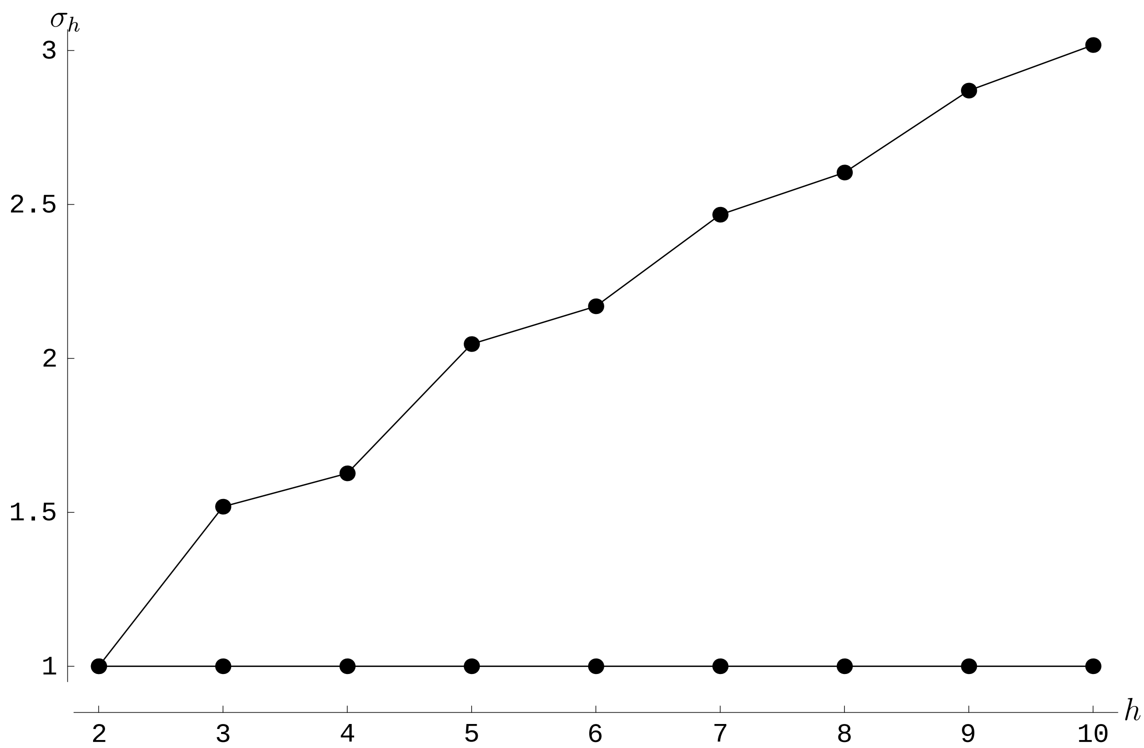

Figure 7: The best known upper and lower bounds on σ_h.

Cilleruelo [110] proved that $\sigma_3 \le 1.576$, $\sigma_4 \le 1.673$, and for $h > 75$,

$$\sigma_h^h \le \frac{5}{2}\left(\tfrac{15}{4} - \tfrac{5}{4\lceil h/2\rceil}\right)^{1/4} \frac{(\lceil h/2\rceil!)^2}{\sqrt{\lceil h/2\rceil}}$$

for odd h, and

$$\sigma_h^h \le \frac{5}{2}\left(\tfrac{15}{4} - \tfrac{5}{2h}\right)^{1/4} ((h/2)!)^2 \sqrt{h/2}$$

for even h. He does give improvements for $h \in [5, 74]$ also.

Ben Green [113] has improved these upper bounds and shown

$$\begin{aligned} \sigma_3 &\le (7/2)^{1/3} < 1.519 \\ \sigma_4 &\le 7^{1/4} < 1.627 \\ \sigma_h &\le \frac{1}{2e}\left(h + \frac{3}{2}\log h + o_h(\log h)\right). \end{aligned}$$

Green's bound for σ_h ultimately relies on the observation that if X_i are independent random variables taking values uniformly in a set of integers $\mathcal{A}$, then the central limit theorem implies that $X_1 + X_2 + \cdots + X_h$ has a normal distribution (for large h). While Green's bound is not given in an effective form, we presume that this could be done in a straightforward manner.

4.3 Cyclic groups

The earliest appearances of Sidon sets were as Monthly problems [1, 2] asking for Sidon subsets of $\mathbb{Z}_n$. If $\mathcal{A}$ is a $B_h^*[g](\text{mod}m)$ set and $\gcd(k,m)=1$, then so is $k\mathcal{A}+r=\{ka+r : a \in \mathcal{A}\}$; we say that $\mathcal{A}$ and $k\mathcal{A}+r$ are equivalent. Veblen and Dickson asked for all inequivalent Sidon subsets of $\mathbb{Z}_n$ for various n. The number of inequivalent modular Sidon sets that arise from the construction of Bose & Chowla is investigated in [16, 17].

The constructions of Ruzsa, Bose, and Singer all give *modular* Sidon sets. This would seem to be a more symmetric setting, and so an easier setting. Unfortunately, while the constructions are naturally modular, the upper bounds on $R_h(g,n)$ sets all seem to fundamentally rely on the *asymmetry* of $[n]$. Progress (beyond the very little in [127]) on bounding $C_h(g,n)$ would be a significant contribution. Here's what is known about $C_2(g,n)$:

Theorem 6. *Let q be a prime power, and let k,g,f,x,y be positive integers with $k<q$.*

i. $\binom{C_2(2,n)}{2} \le \lfloor \frac{n}{2} \rfloor$, *and in particular* $C_2(2,n) \le \sqrt{n}+1$*;*

ii. $C_2(3,n) \le \sqrt{n+9/2}+3$*;*

iii. $C_2(4,n) \le \sqrt{3n}+7/6$*;*

iv. $C_2(g,n) \le \sqrt{gn}$ *for even* g*;*

v. $C_2(g,n) \le \sqrt{1-\frac{1}{g}}\sqrt{gn}+1$, *for odd* g.

vi. If q is a prime, then $C_2(2k^2, q^2-q)) \ge k(q-1)$*;*

vii. $C_2(2k^2, q^2-1) \ge kq$*;*

viii. $C_2(2k^2, q^2+q+1) \ge kq+1$*;*

ix. If $\gcd(x,y)=1$, *then* $C_2(gf,xy) \ge C_2(g,x)C_2(f,y)$*;*

5 The size of infinite Sidon sequences

Let $\mathcal{A} \subseteq \mathbb{Z}$ be a Sidon sequence, and let $A(n)=\#(\mathcal{A}\cap[n])$. Stöhr [12] strengthens an unpublished result of Erdős and proved that

$$\liminf_{n\to\infty} \frac{A(n)}{\sqrt{n/\log(n)}} \ne \infty$$

Stöhr also gave Erdős's proof that there is a Sidon sequence with

$$\limsup_{n\to\infty} \frac{A(n)}{\sqrt{n}} \ge \frac{1}{2};$$

this was improved by Krückeberg [14] to $1/\sqrt{2}$, and taken to $B_2^*[g]$ sequences by Cilleruelo & Trujillo [111]. In [28] a Sidon sequence is constructed with

$$A(n) > 10^{-3}(n \log n)^{1/3}$$

for sufficiently large n. Erdős asked [29] if there is a sequence $a_1 < a_2 < \dots$ with $a_k = o\left(k^{3-\epsilon}\right)$ for any positive ϵ; Ruzsa constructed a Sidon sequence with $A(n) \sim n^{\sqrt{2}-1+o(1)}$.

Sheng Chen [55] conjectures that if $\mathcal{A}$ is a B_h sequence with counting function $A(n)$, then

$$\liminf_{n\to\infty} A(n) \left(\tfrac{\log n}{n}\right)^{1/h}$$

is finite. See also [44, 45, 56, 57, 66, 67, 77, 79, 80]. Neither the results nor the conjectures have been extended to $B_h^*[g]$ sequences.

6 The distribution of $\mathcal{A}$ and $\mathcal{A}+\mathcal{A}$

If $\mathcal{A}_n \subset [n]$ is a sequence of Sidon sets and $|\mathcal{A}| \sim \sqrt{n}$, then $\mathcal{A}_n$ becomes uniformly distributed in $[n]$ (see [49]). Moreover, $\mathcal{A}_n$ becomes uniformly distributed in congruence classes modulo m (for any fixed m) (see [90, 95, 120]). It is shown in [63] that if $\mathcal{A}$ is any finite Sidon sequence, then the sumset $\mathcal{A}+\mathcal{A}$ consists of at least $c|\mathcal{A}|^2$ intervals (for an unspecified constant c). With care this can be improved to $(|\mathcal{A}|^2 - |\mathcal{A}| - 1)/4$. Extensive computations indicate that if $|\mathcal{A}| \sim \sqrt{n}$, then $\mathcal{A}+\mathcal{A}$ consists of $\sim |\mathcal{A}|^2/3$ intervals. Very little is known about the structure of $\mathcal{A}+\mathcal{A}$. Must the size of the longest interval in $\mathcal{A}+\mathcal{A}$ go to infinity as n does (with $|\mathcal{A}| \sim \sqrt{n}$)?

Martin & O'Bryant [126] conjecture that $B_2^*[g]$ sets with maximal size are uniformly distributed. Current computations are insufficient to extend this conjecture to $B_h^*[g]$ sets.

7 Restricted Sidon sequences

A well known conjecture [65] states that the fifth powers $0, 1, 32, 243, \dots$ are a Sidon sequence. Ruzsa [116] shows that there is an α such that $\{n^5 + \lfloor \alpha n^4 \rfloor : n \geq n_0\}$ is a Sidon set. Cilleruelo [69] considered Sidon sequences all of whose terms are squares. Abbot [46] studied the size of Sidon sequences contained in an arbitrary set of integers with cardinality n (there is one with size at least $\frac{2}{25}\sqrt{n}$).

Lindström [21, 23] initiated the study of $B_h^*[g]$ sets in group $\mathbb{Z}^d$.

Erdős [25] investigated Sidon subsets of $B_2^*[g]$ sets. Alon & Erdős [34] considered the problem of decomposing a finite $B_2^*[g]$ into B_2 sets; how many B_2 sets are needed?

8 Generalizations

The graph theorist's analogs of Sidon sets are magic and harmonious labelings. See [26, 27].

The bigger setting for the Sidon question is that of sets which avoid a linear form. Let L be an $m \times n$ matrix of integers. The set $\mathcal{A}$ is said to avoid L if there are no nontrivial solutions to $L\vec{a} = \vec{0}$ with $\vec{a} = (a_1, a_2, \ldots, a_n)^T, a_k \in \mathcal{A}$. Sidon sets are the special case $L = [1, 1, -1, -1]$, sets with 3-term arithmetic progressions are the case $L = [1, -2, 1]$, etc. It is surprising that in such a general setting significant and strong results can be found. Precisely this is done in [22, 24, 59].

9 Other open questions

If $\mathcal{A}^*$ is bounded, is it necessarily 0 infinitely often? This is equivalent to a USD 500 question of Erdős [43]: If every positive integer can be written as a sum of two elements of $\mathcal{B} \subseteq \mathbb{N}$ (i.e., $\mathcal{B}$ is a base), must the number of ways to do so go to infinity?

Is there an anti-Freiman theorem: If $|\mathcal{A}+\mathcal{A}|/|\mathcal{A}|^2 > c$, then $\mathcal{A}$ has a large $B_2^*[g]$ subset, where g and 'large' depend only c? This question may be related to the quasi-Sidon sets discussed in [49, 129].

10 Bibliography

[1] Oswald Veblen, *Diophantine analysis: problem 132*, Amer. Math. Monthly **13** (Feb 1906), 46, Solution by F. H. Safford appears in **13** (Nov 1906), 215.

> The problem reads: "From the numbers, $0, 1, 2, \ldots,$ 42, select seven, such that the 42 differences of these seven numbers shall be congruent (mod 43) to the numbers $0, 1, 2, \ldots, 42$. The differences may be both + and −."
>
> The solution concludes: "Hence the problem is impossible."

[2] L. E. Dickson, *Diophantine analysis: Problem 142*, Amer. Math. Monthly **13** (Nov 1906), 219, Solution by L. E. Dickson appears in **14** (May 1907):107 –108.

> The problem reads: "Let n be an integer > 1 and set $p = n(n-1)+1$. Required n integers whose $n(n-1)$ differences are congruent (modulo p) to the numbers $1, 2, \ldots, p-1$. Exhibit at least for $n = 3, 4, 5$, all inequivalent sets of solutions where a set $a_1, a_2, \ldots, a_n$ is called equivalent to the $m(a_1 - d), m(a_2 - d), \ldots, m(a_n - d)$, for any integers m and d (m not divisible by p)."
>
> For $n = 3, 4, 5, 6, 8$ there is a unique set, and for $n = 7$ there are none. The solutions are $n = 3 \Rightarrow \{0, 1, 3\}$, $n = 4 \Rightarrow \{0, 1, 3, 9\}$, $n = 5 \Rightarrow \{0, 1, 6, 8, 18\}$, $n = 6 \Rightarrow \{0, 1, 3, 10, 14, 26\}$, and $n = 8 \Rightarrow \{0, 1, 3, 13, 32, 36, 43, 52\}$.

[3] S. Sidon, *Ein Satz über trigonomietrische Polynome und seine Anwendungen in der Theorie der Fourier-Reihen*, Math. Annalen **106** (1932), 536–539.

[4] James Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385. **MR 1501951**

> Using finite projective geometry, Singer shows that for p a prime power, $C_2(2, p^2 + p + 1) \geq p + 1$. An algebraic outline of his argument follows. Let $\theta \in \mathbb{F}_{p^3}$ be a primitive element. Then $\{1, \theta, \theta^2\}$ is a basis of $\mathbb{F}_{p^3}$ over $\mathbb{F}_p$, hence for each $a \in \mathbb{Z}$, there are unique $r_a, m_a, n_a \in \mathbb{F}_p$ such that $\theta^a = r_a\theta^2 + m_a\theta + n_a$. The set $\{0\} \cup \{a \in [0, p^3 - 1) \colon (r_a, m_a) = (0, 1)\}$, reduced modulo $p^2 + p + 1$, witnesses $C_2(2, p^2 + p + 1) \geq p + 1$.

This article cites [1], [2].

[5] P. Erdös and P. Turàn, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215. **MR 3,270e**

The authors demonstrate that $\forall\epsilon > 0\,\exists n_0$ such that $(\frac{1}{\sqrt{2}} - \epsilon)\sqrt{n} < R_2(2,n) < \sqrt{n} + \mathcal{O}\left(n^{1/4}\right)$ for all $n > n_0$.

The lower bound comes from $R_2(2, 2p^2) \geq p - 1$ (p prime), which is witnessed by $\{2pk+(k^2)\colon 1 \leq k < p\}$, where (k^2) is the unique integer in $[1, p)$ congruent to k^2 modulo p.

The upper bound (the argument can actually be made to give $R_2(2,n) < n^{1/2} + n^{1/4} + 1$) is repeated almost verbatim as Theorem 4 in [31, Chapter II]. Let $S \subset [n]$ be a Sidon set with maximal cardinality, and let $A_u = |S \cap [-n^{3/4} + u, u)|$. The idea is to bound $\sum \binom{A_u}{2}$ above and below. The lower bound uses Cauchy's inequality, and the upper bound uses the observation that $(s_i, s_j) \in S \times S$ is determined by $s_i - s_j$, i.e., Sidon sets not only have distinct sums, but distinct differences as well.

This article cites [3].

[6] R. C. Bose, *An affine analogue of Singer's theorem*, J. Indian Math. Soc. (N.S.) **6** (1942), 1–15. **MR 4,33c**

Using finite affine geometry, Bose demonstrates that for p a prime power, $C_2(2, p^2-1) \geq p$. This theorem is only slightly weaker (in terms of $\frac{C_2(g,n)}{\sqrt{gn}}$) than Singer's [4], while his proof is substantially simpler. His argument, in algebraic form, is as follows. Let $\theta \in \mathbb{F}_{p^2}$ be a primitive element. For each $a \in \mathbb{Z}$, there is a unique $m_a, n_a \in \mathbb{F}_p$ such that $\theta^a = m_a\theta + n_a$. The set $\{a \in [0, p^2 - 1) : m_a = 1\}$ witnesses $C_2(2, p^2 - 1) \geq p$.

This article cites [4].

[7] S. Chowla, *Solution of a problem of Erdös and Turan in additive-number theory*, Proc. Nat. Acad. Sci. India. Sect. A. **14** (1944), 1–2. **MR 7,243b**

Chowla notes that the constructions of Bose [6] or of Singer [4] may be combined with the bound of Erdös & Turàn [5] to give $R_2(2,n) \sim \sqrt{n}$, i.e., $\sigma_2 = 1$. Chowla also notes that $R_2(2,n) \geq C_2(2,n-1) + 1$ by adjoining n to any subset of $[n-1]$ which is a B_2 (mod $n-1$) set and contains 1. Chowla also points out that the error term in the lower bound of $R_2(2,n)$ depends on a result of the form "For sufficiently large n there is a prime between n and $n - n^\theta$."

This article cites [5], [6].

[8] ______, *Solution of a problem of Erdös and Turan in additive-number-theory*, Proc. Lahore Philos. Soc. **6** (1944), 13–14. **MR 7,243c**

[9] P. Erdös, *On a problem of Sidon in additive number theory and on some related problems. Addendum*, J. London Math. Soc. **19** (1944), 208. **MR 7,242f**

Erdős observes that [4] and [5] together imply $R_2(2,n) \sim \sqrt{n}$, i.e., $\sigma_2 = 1$.

This article cites [4], [5].

[10] Abdul Majid Mian and S. Chowla, *On the B_2 sequences of Sidon*, Proc. Nat. Acad. Sci. India. Sect. A. **14** (1944), 3–4. **MR 7,243a**

Nothing is proved here, but the first 11 terms of the greedy Sidon set are reported, and it is noted that this supports the conjecture that $R_2(2,n) \geq \sqrt{n}$ for all n.

The greedy Sidon set begins $a_1 = 1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97, \ldots$. The authors state "It seems likely that

$$\lim_{m\to\infty} \frac{a_{m+1} - a_m}{m} = 2$$

as far as our table goes, we have $\sqrt{a_m} \leq m$." However, $a_{17} = 290 > 17^2$.

This article cites [3], [5].

[11] R. C. Bose and S. Chowla, *On the construction of affine difference sets*, Bull. Calcutta Math. Soc. **37** (1945), 107–112. **MR 7,365g**

This paper considers of the mechanics of converting Bose's construction [6] into actual numbers. Suppose that p is a power of a prime, and $\theta \in \mathbb{F}_{p^2}$ is a primitive element satisfying $\theta^2 + a\theta + b = 0$. Define $f_1 = 0$ and $f_m \equiv \frac{b}{a - f_m} \pmod{p}$. Define also $\log_b(N)$ to be the unique integer $t \in [0, p)$ such that $b^t \equiv N \pmod{p}$. Then the set $\{d_1, \ldots, d_p\}$, defined by $d_1 = 1, d_{m-1} = 1 + d_m - (p+1)\,\mathrm{ind}(f_m - a)$, witnesses $C_2(2, p^2 - 1) \geq p$.

This article cites [4].

[12] Alfred Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I, II*, J. Reine Angew. Math. **194** (1955), 40–65, 111–140. **MR 17,713a**

This survey addresses Sidon sets in §12$a\beta$ on pages 129–135. Two results of Erdős are given: There is an infinite Sidon set whose counting function $A(n)$ satisfies $\limsup \frac{A(n)}{\sqrt{n}} \geq \frac{1}{2}$; Every infinite Sidon set has a counting function $A(n)$ satisfying $\liminf \frac{A(n)}{\sqrt{n}} = 0$.

Stöhr notes that this second result shows that the guess of Mian & Chowla [10] that the n-th term of the greedy Sidon set is at most n^2 is false. He also notes that the second statement (and its proof) can be made more precise: Every infinite Sidon set has a counting function $A(n)$ satisfying $\liminf \frac{A(n)\sqrt{\log n}}{\sqrt{n}} \ll 1$. These results are also reported as Theorems 8 and 9 of [31, Chapter II].

Stöhr then raises the question of how large $\liminf \frac{A(n)\sqrt{\log n}}{\sqrt{n}}$ can be, and if the answer is 0, then what would be a suitable replacement for $\frac{\sqrt{\log n}}{\sqrt{n}}$. He also asks if there is a Sidon set for which $0 < \liminf \frac{A(n)\sqrt{\log n}}{\sqrt{n}} \leq \limsup \frac{A(n)\sqrt{\log n}}{\sqrt{n}} < \infty$. Similar questions are raised for B_h sets.

Stöhr then considers the greedy Sidon set, and notes that its n-th element a_n is at most $(n-1)^3 + 1$.

This article cites [4], [5], [7], [9], [10].

[13] P. Erdős and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. **6** (1960), 83–110. **MR 22:10970**

This papers examines the behavior of $S^*(n)$ for sets S defined by $\mathbb{P}(k \in S) = p_k$, for various sequences p_k. The result relating to Sidon sequences states that for every $\delta > 0$, there exists a $B^*[g]$ sequence $\{a_1, a_2, \ldots\}$ satisfying $a_k = \mathcal{O}\left(k^{2(1+2(g-1)^{-1})}\right)$.

We give the main steps of the proof. Set $p_n = n^{-\frac{1}{2}-\epsilon}$ (with $\epsilon > (g+1)^{-1}$) and $q_n = 1 - p_n$. Define the independent random variables X_n to be 1 with probability p_n and 0 with probability q_n. Define the random function $f(n) = \sum_{k=1}^{n/2} X_k X_{n-k}$; we wish to show that almost surely $f(n) \le \frac{g}{2}$ (with finitely many exceptions). Then

$$\begin{aligned}\mathbb{E}[\exp(tf(n))] &= \prod_{k\le n/2}\left(1+\frac{e^t-1}{(k(n-k))^{1/2+\epsilon}}\right)\\ &\le \prod_{k\le n/2}\exp\left(\frac{e^t-1}{(k(n-k))^{1/2+\epsilon}}\right)\\ &\le \exp\left(\frac{e^t-1}{n^{2\epsilon}}I(\epsilon)\right),\end{aligned}$$

where $I(\epsilon)$ is a constant depending only on ϵ as $n \to \infty$. Set $t = \log(1+n^{2\epsilon})$ and apply the Exponential Chebyshev Theorem to find (with $K = g/2$):

$$\mathbb{P}(f(n) > K) \le \frac{\mathbb{E}[\exp(tf(n))]}{\exp(t(K+1))} \le \frac{C_1}{n^{2\epsilon(K+1)}}.$$

Thus $\sum_{n=1}^{\infty} P(f(n) > K)$ converges, and the Borel-Cantelli Lemma guarantees that $\{n\colon X_n = 1\}$ is almost surely a $B^*[g]$ sequence (at least, after deleting finitely many terms).

This, and other results of this paper, are given in [31, Chapter 3].

This article cites [3], [5].

[14] Fritz Krückeberg, *B_2-Folgen und verwandte Zahlenfolgen*, J. Reine Angew. Math. **206** (1961), 53–60. **MR 23:A3729**

Theorem 1:

$$\frac{1}{h}\sqrt[h]{h} \le \sigma_h \le (h\cdot h!)^{1/h}$$

Theorem 2:

$$\frac{1}{2h^2} \le \sigma_h(h!g) \le (h\cdot h!)^{1/h}.$$

Theorem 3: There is $B^*[2]$ set $\mathcal{A}$ with

$$\limsup_{n\to\infty}\frac{|\mathcal{A}\cap[n]|}{\sqrt{2n}} \ge \frac{1}{2}.$$

The lower bounds in Theorems 1 and 2 are worse than those obtained by the construction of Singer [4] (simplified and generalized to $h > 2$ in [15]), and the upper bounds are from the obvious pigeonhole argument. Theorem 3 is proved in English in [18, Chapter 2].

This article cites [3], [4], [5], [7], [10], [12].

[15] R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962/1963), 141–147. **MR 26:2418**

If m is a prime power, then $C_h(h!, m^h - 1) \ge m$ and $C_h\left(h!, \frac{m^{h+1}-1}{m-1}\right) \ge m+1$. Thus, $\sigma_h \ge 1$.

This article cites [6], [7], [5], [4].

[16] H. Halberstam and R. R. Laxton, *On perfect difference sets*, Quart. J. Math. Oxford Ser. (2) **14** (1963), 86–90. **MR 28:5027**

The authors simplify the construction of [4]. They also consider the problem of identifying those t such that there is an s with $t\mathcal{A} + s \equiv \mathcal{A} \pmod{m}$, where $\mathcal{A}$ is a $B^*[2] \pmod{m}$ set.

This article cites [4].

[17] ———, *Perfect difference sets*, Proc. Glasgow Math. Assoc. **6** (1964), 177–184 (1964). **MR 29:5748**

[18] H. Halberstam and K. F. Roth, *Sequences. Vol. I*, Clarendon Press, Oxford, 1966. **MR 35:1565**

This book is *the* reference for Sidon set research prior to 1969. It also contains the first rigorous treatment of the probabilistic method, and introduction to sieves, and a lengthy discussion of different notions of density and their uses. Making a copy of this oft-referenced text available online would be a valuable service to the community.

[19] Bernt Lindström, *An inequality for B_2-sequences*, J. Combinatorial Theory **6** (1969), 211–212. **MR 38:4436**

This is the book proof that $\sigma_2 \le 1$. The argument is reproduced in the survey accompanying this bibliography.

[20] ———, *A remark on B_4-sequences*, J. Combinatorial Theory **7** (1969), 276–277. **MR 40:2634**

As a consequence of a correlation inequality of van der Corput: $\sigma_4 \le 8^{1/4}$.

[21] ———, *Determination of two vectors from the sum*, J. Combinatorial Theory **6** (1969), 402–407. **MR 38:5641**

Author's abstract: "Let S_m be the set of all vectors of dimension m with all components 0 or 1. Let $\phi(m)$ be the maximum of $|A+B|$ for pairs A, B of subsets of S_m such that the sums $\mathbf{a}+\mathbf{b}$ are different for different pairs $(\mathbf{a},\mathbf{b}), \mathbf{a}\in A, \mathbf{b}\in B$. Let $\lambda(m)$ be the maximum of $|A|, A \subset S_m$, such that the sums $\mathbf{a_1}+\mathbf{a_2}$ are different for different subsets $\{\mathbf{a_1},\mathbf{a_2}\}$ in A. Let $\nu(m)$ be the maximum of $|A|, A\subset S_m$, for A such that the sums $\mathbf{a_1}+\mathbf{a_2}$ are different modulo 2 for different subsets $\{\mathbf{a_1},\mathbf{a_2}\}$ in A, $\mathbf{a_1}\ne\mathbf{a_2}$. The problem is to estimate $\phi(m)^{1/m}$, $\lambda(m)^{1/m}$ and $\nu(m)^{1/m}$ as $m\to\infty$."

The bounds are

$$\sqrt{6} \le \lim_{m\to\infty} \phi(m)^{1/m} \le \sqrt{8},$$

$$\lim_{m\to\infty} \nu(m)^{1/m} = \sqrt{2},$$

$$2^{1/2} \le \liminf_{m\to\infty} \lambda(m)^{1/m}, \quad \limsup_{m\to\infty} \lambda(m)^{1/m} \le 2^{2/3}.$$

The author added (in proof, so their is no proof) that he could improve the $2^{2/3}$ to $2^{3/5}$ using information theory.

[22] János Komlós, Miklós Sulyok, and Endre Szemerédi, *A lemma of combinatorial number theory*, Mat. Lapok **23** (1972), 103–108 (1973). **MR 50:2048** (Hungarian, with English summary)

[23] Bernt Lindström, *On B_2-sequences of vectors*, J. Number Theory **4** (1972), 261–265. **MR 46:3322**

Let $F_h(g,N,d)$ denote the maximum possible size of a $B_h^*[g](\mathbb{Z}^d)$ set contained in $\{0,1,\dots,N-1\}^d$. Theorem 1 states that $F_2(2,N,d) \le N^{d/2} + \mathcal{O}\left(N^{d^2/(2d+2)}\right)$, and Theorem 2 states that $\limsup_{d\to\infty} F_2(2,2,d)^{1/d} \le 2^{3/5}$. The $d=1$ case of Theorem 1 is the main result of [5].

The paper concludes with three open problems: (1) $F_2(2,N,d) = N^{d/2} + \mathcal{O}(1)$, (2) $\lim_{d\to\infty} F_2(2,2,d)^{1/d} = \sqrt{2}$, and (3) Estimate $F_2(3,N,d)$.

This article cites [5], [18], [21], [19], [20], [3].

[24] J. Komlós, M. Sulyok, and E. Szemerédi, *Linear problems in combinatorial number theory*, Acta Math. Acad. Sci. Hungar. **26** (1975), 113–121. **MR 51:342**

[25] P. Erdős, *Some applications of Ramsey's theorem to additive number theory*, European J. Combin. **1** (1980), 43–46. **MR 82a:10067**

Erdős and Donald Newman conjectured (independently) that there is a $B_2[k]$ sequence which is not the union of a finite number of B_2 sequences. He notes that this follows from Ramsey's theorem. Erdős also conjectures that there is $B_2^*[2g]$ set $\mathcal{A}$ such that if $\mathcal{A} = \cup_{i=1}^n \mathcal{A}_i$, then some $\mathcal{A}_i$ is not a $B_2^*[2g-2]$ set. This is proved explicitly for three cases: (1) $h=2$ and $g=1$ (with $\mathcal{A} = \{4^i + 4^j\}$); (2) $g = 2^s$; and (3) $g = \frac{1}{2}\binom{2s}{s}$ with $s \ge 1$. He comments that he is unable to verify the conjecture with $h=2$, $g=5$.

Suppose that the cardinality of the continuum is $> \aleph_1$. There is a set $S \subseteq \mathbb{R}$ with cardinality $\aleph_2$, S is a $B_2^*[4]$ set, and if $S = \cup_{i=1}^\infty S_i$, then some S_i is not a $B_2^*[2]$ set.

Set $L(g,n)$ to be the largest integer ℓ such that every $B_2^*[g]$ set with n elements contains a Sidon subset with ℓ elements. He conjectures that $L(g,n)/\sqrt{n}$ is unbounded (as $n \to \infty$), and speculates that $L(g,n) = \mathcal{O}\left(n^{1/2+\epsilon}\right)$ for every $\epsilon > 0$. He proves that $L(4,n) = \mathcal{O}\left(n^{3/4}\right)$ and $L(8,n) = \mathcal{O}\left(n^{2/3}\right)$.

This article cites [18], [24].

[26] R. L. Graham and N. J. A. Sloane, *On additive bases and harmonious graphs*, SIAM J. Algebraic Discrete Methods **1** (1980), 382–404. **MR 82f:10067a**

Author's abstract: "This paper first considers several types of *additive bases*. A typical problem is to find $n_\gamma(k)$, the largest n for which there exists a set $\{0 = a_1 < a_2 < \cdots < a_k\}$ of distinct integers modulo n such that each r in the range $0 \le r \le n-1$ can be written *at least* once as $r \equiv a_i + a_j$ (modulo n) with $i < j$. For example $n_\gamma(8) = 24$, as illustrated by the set $\{0,1,2,4,8,13,18,22\}$. The other problems arise if *at least* is changed to *at most*, or $i < j$ to $i \le j$, of if the words modulo n are omitted. Tables and bounds are given for each of these problems. Then a closely related graph labeling problem is studied. A connected graph with n edges is called *harmonious* if it is possible to label the vertices with distinct numbers (modulo n) in such a way that the edge sums are also distinct (modulo n). Som infinite families of graphs (odd cycles, ladders, wheels, $\cdots$) are shown to be harmonious while others (even cycles, most complete or complete bipartite graphs, $\cdots$) are not. In fact most graphs are not harmonious. The function $n_\gamma(k)$ is the size of the largest harmonious subgraph of the complete graph on k vertices."

[27] ———, *On constant weight codes and harmonious graphs*, Proceedings of the West Coast Conference on Combinatorics, Graph Theory and Computing (Humboldt State Univ., Arcata, Calif., 1979), Utilitas Math., Winnipeg, Man., 1980, pp. 25–40. **MR 82f:10067b**

The authors apply the construction of [15] to bound the size of constant weight codes and to harmonious graphs. A graph $G = (V, E)$ is harmonious if it is possible to label the $|V|$ vertices with distinct values from $\mathbb{Z}_{|E|}$ so that every element of $\mathbb{Z}_{|E|}$ occurs uniquely as an edge sum of G. The connection to Sidon sets is that $\mathcal{A}$ is Sidon set (modulo $\binom{|\mathcal{A}|}{2}$) exactly if the vertices of the complete graph $K_{|\mathcal{A}|}$ can be labeled (with distinct labels from $\mathcal{A}$) so that the edge sums are distinct.

[28] Miklós Ajtai, János Komlós, and Endre Szemerédi, *A dense infinite Sidon sequence*, European J. Combin. **2** (1981), 1–11. **MR 83f:10056**

I haven't seen this article, but references to it indicate that it contains a proof that there is a Sidon set of positive integers with $\#(\mathcal{A} \cap [n]) \gg (n \log n)^{1/3}$ for all large n. The obvious pigeonhole bound gives only $n^{1/3}$.

[29] Paul Erdős, *Some of my favourite problems which recently have been solved*, Proceedings of the International Mathematical Conference, Singapore 1981 (Singapore, 1981), North-Holland, Amsterdam, 1982, pp. 59–79. **MR 84f:10003**

In §4, Erdős notes that the greedy Sidon sequence satisfies $\gamma_k = \mathcal{O}\left(k^3\right)$, and recalls his conjecture that in fact $\gamma_k = o\left(k^3\right)$. The existence of a $B_2^*[2]$ sequence $a_1, a_2, \ldots$ with $a_k = o\left(k^3\right)$ was shown in [28], but their method does not give a sequence with $a_k = o\left(k^{3-\epsilon}\right)$ for any $\epsilon > 0$.

This article cites [18], [28].

[30] A. Sárközy, *On squares in arithmetic progressions*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **25** (1982), 267–272. **MR 84j:10055**

[31] Heini Halberstam and Klaus Friedrich Roth, *Sequences*, Second, Springer-Verlag, New York, 1983, ISBN 0-387-90801-3. **MR 83m:10094**

From the preface: "Changes from the first edition [18] have been kept to a minimum. Several misprints and some errors that have come to light in the years since the publication of the first edition have been corrected. At several places in the text, and in a short postscript, we have added references to developments that have occurred since the first appearance of Sequences."

[32] A. G. D′yachkov and V. V. Rykov, *B_s-sequences*, Mat. Zametki **36** (1984), 593–601, English translation: Math. Notes **36** (1984), no. 3-4, 794–799. **MR 86m:11016**

I haven't seen this article, but Zentralblatt 567:10041 indicates that it contains the bounds

$$\sigma_{2h} \leq (s_h (h!)^2)^{1/2h}, \quad \sigma_{2h-1} \leq (s_h \cdot h!(h-1)!)^{1/2h-1}$$

where $s_1 = 1, s_2 = 2, s_3 = 3$ and $s_h = \sqrt{125s/36}$ for $h \geq 4$.

[33] P. Erdős and Róbert Freud, *On disjoint sets of differences*, J. Number Theory **18** (1984), 99–109. **MR 85g:11018**

[34] Noga Alon and P. Erdős, *An application of graph theory to additive number theory*, European J. Combin. **6** (1985), 201–203. **MR 87d:11015**

[35] László Babai and Vera T. Sós, *Sidon sets in groups and induced subgraphs of Cayley graphs*, European J. Combin. **6** (1985), 101–114. **MR 87f:05081**

[36] P. Erdős, A. Sárközy, and V. T. Sós, *Problems and results on additive properties of general sequences. IV*, Number Theory (Ootacamund, 1984), Springer, Berlin, 1985, pp. 85–104. **MR 88i:11011a**

[37] ———, *Problems and results on additive properties of general sequences. V*, Monatsh. Math. **102** (1986), 183–197. **MR 88i:11011b**

[38] Andrew D. Pollington, *On the density of B_2-bases*, Discrete Math. **58** (1986), 209–211. **MR 87h:11013**

A B_2-base is a set for which every nonzero integer appears uniquely as a difference. Theorem 1: There is a B_2-basis $\mathcal{A}$ (with counting function $A(n)$) for which $\limsup n^{-1/2}A(n) \geq \frac{1}{2}$. Theorem 2: There exist B_2-bases $\mathcal{A}$ for which $A(n) > (n\log n)^{1/3}/10^3$ for all $n > n_0$.

[39] I. E. Shparlinskiĭ, *On B_s-sequences*, Combinatorial Analysis, No. 7 (Russian), Moskov. Gos. Univ., Moscow, 1986, pp. 42–45, 163. **MR 89j:11008**

[40] Benny Chor and Ronald L. Rivest, *A knapsack-type public key cryptosystem based on arithmetic in finite fields*, IEEE Trans. Inform. Theory **34** (1988), 901–909. **MR 89k:94043**

The system is roughly as follows. Choose a prime power q around 200, h around 25, $k \in \mathbb{F}_q$, and a generator θ of the multiplicative group of $\mathbb{F}_{q^h}$. Publish $\mathtt{Bose}_h(q,\theta,k)$ in sorted order $a_1 < \cdots < a_p$ as Alice's public key. Bob can send a message to Alice by first encoding it as a vector $\vec{x}$ of p nonnegative integers with sum h, and sending the sum $\vec{x}\cdot\langle a_1,\dots,a_p\rangle$. Alice can decode this by using her private information: θ and k. Their are additional contortions recommended to disguise θ and k.

This knapsack cryptosystem was superior to earlier knapsacks in that there was greater density, increasing the information per bit and fortifying against certain attacks. The Chor-Rivest cryptosystem is simplified in [50] (and renamed the powerline cryptosystem), and broken in [75] and [117] using LLL.

[41] D. Hajela, *Some remarks on $B_h[g]$ sequences*, J. Number Theory **29** (1988), 311–323. **MR 90d:11022**

[42] Xing De Jia, *On the distribution of a B_2-sequence*, Qufu Shifan Daxue Xuebao Ziran Kexue Ban **14** (1988), 12–18. **MR 89j:11023**

[43] P. Erdős, *Some old and new problems on additive and combinatorial number theory*, Combinatorial Mathematics: Proceedings of the Third International Conference (New York, 1985), New York Acad. Sci., New York, 1989, pp. 181–186. **MR 90i:11016**

[44] Xing De Jia, *On B_6-sequences*, Qufu Shifan Daxue Xuebao Ziran Kexue Ban **15** (1989), 7–11. **MR 90j:11022**

[45] John C. M. Nash, *On B_4-sequences*, Canad. Math. Bull. **32** (1989), 446–449. **MR 91e:11025**

[46] H. L. Abbott, *Sidon sets*, Canad. Math. Bull. **33** (1990), 335–341. **MR 91k:11022**

Author's abstract: "Denote by $g(n)$ be the largest integer m such that every set of integers of size n contains a subset of size m whose pairwise sums are distinct. It is shown that $g(n) > cn^{1/2}$ for any constant $c < \frac{2}{25}$ and all sufficiently large n."

[47] J. Cilleruelo, *B_2-sequences whose terms are squares*, Acta Arith. **55** (1990), 261–265. **MR 91i:11023**

A B_2 sequence $\{a_1^2, a_2^2, \dots, a_k^2, \dots\}$ is constructed such that $a_k \ll k^2$. The sequence $\{a_1, a_2, \dots\}$ is almost $I = \cup_{j=1}^{\infty} = \cup_{j=1}^{\infty}\{a\colon 6^j \leq a < 6^j + 6^{j/2},\ a \equiv 2 \pmod 6\}$, but some elements needs to be removed.

[48] P. Erdős, *Some applications of probability methods to number theory. Successes and limitations*, Sequences (Naples/Positano, 1988), Springer, New York, 1990, pp. 182–194. **MR 91d:11084**

[49] P. Erdős and R. Freud, *On sums of a Sidon-sequence*, J. Number Theory **38** (1991), 196–205. **MR 92g:11028**

This nicely written article begins with a proof that a Sidon subset of $[n]$ with $\sqrt{n}$ elements is uniformly distributed as $n \to \infty$. This is used to study how unbalanced the sumset $\mathcal{S} = \{a_i + a_j : a_i, a_j \in \mathcal{A}\}$ of a Sidon set $\mathcal{A} \subseteq [n]$ (not necessarily maximal) can be. They show that $\#(\mathcal{S} \cap [n])$ cannot be larger than n/π (as $n \to \infty$), but can be as large as $n(1 - 1/\sqrt{2})$. This improves the trivial bounds of $n/2$ and $n/4$ to $0.318n$ and $0.293n$.

The authors then consider a couple of generalizations of Sidon sets, the most interesting being that of a *quasi-Sidon sequence*, i.e., a sequence of $\mathcal{A}$ integers whose sumset $\mathcal{S}$ has cardinality $(1 + o(1))\binom{|\mathcal{A}|}{2}$. Loosely, $\mathcal{A}^*(x) \leq 2$ for almost all integers x. They note that a quasi-Sidon subset of $[n]$ can have cardinality $\sim \sqrt{4n/3}$, but cannot have cardinality $\sim \sqrt{3.93n}$. Curiously, if one uses the "distinct difference" description of Sidon sets, then the corresponding quasi-Sidon sets cannot be substantively larger than a classic Sidon set.

[50] H. W. Lenstra Jr., *On the Chor-Rivest knapsack cryptosystem*, J. Cryptology **3** (1991), 149–155. **MR 92j:94012**

Author's abstract: "Among all public-key cryptosystems that depend on the knapsack problem, the system proposed by B. Chor and R. L. Rivest [40] is one of the few that have not been broken. The main difficulty in implementing their system is the computation of discrete logarithms in large finite fields. In this note we describe the 'powerline system', which is a modification of the Chor-Rivest system that does not have this shortcoming. The powerline system, which is not a knapsack system, is at least as secure as the original Chor-Rivest system."

See also [75] and [117].

[51] An Ping Li, *On B_3-sequences*, Acta Math. Sinica **34** (1991), 67–71. **MR 92f:11037**

[52] Vera T. Sós, *An additive problem in different structures*, Graph Theory, Combinatorics, Algorithms, and Applications (San Francisco, CA, 1989), SIAM, Philadelphia, PA, 1991, pp. 486–510. **MR 92k:11026**

[53] Torleiv Kløve, *Constructions of $B_h[g]$-sequences*, Acta Arith. **58** (1991), 65–78. **MR 92f:11033**

[54] Javier Cilleruelo and Antonio Córdoba, *$B_2[\infty]$-sequences of square numbers*, Acta Arith. **61** (1992), 265–270. **MR 93g:11014**

[55] Sheng Chen, *On Sidon sequences of even orders*, Acta Arith. **64** (1993), 325–330. **MR 94h:11015**

Let $A(n)$ be the counting function of the B_{2k} sequence A. Then $\liminf_{n\to\infty} A(n) \left(\frac{\log n}{n}\right)^{1/2k} < \infty$. Chen conjectures that for all $h \geq 2$, A a B_h sequence, $\liminf_{n\to\infty} A(n) \left(\frac{\log n}{n}\right)^{1/h} < \infty$.

[56] Martin Helm, *On B_{2k}-sequences*, Acta Arith. **63** (1993), 367–371. **MR 95c:11029**

[57] ———, *Some remarks on the Erdős-Turán conjecture*, Acta Arith. **63** (1993), 373–378. **MR 94c:11012**

[58] Xing De Jia, *On finite Sidon sequences*, J. Number Theory **44** (1993), 84–92. **MR 94k:11014**

Author's abstract: "A set A of integers is called a B_h-sequence if all sums $a_1 + \cdots + a_h$, where $a_i \in A$, are distinct up to rearrangement of the summands. Let $F_h(n)$ [resp. $f_h(n)$] denote the size of a largest B_h-sequence [resp. B_h-sequence for $\mathbf{Z}/(n)$]. It is proved that, for every $r \geq 1$ as $n \to \infty$, $F_{2r}(n) \leq r^{1/2r}(r!)^{1/r} n^{1/2r} + O(n^{1/4r})$, $f_{2r}(n) \leq (r!)^{1/r} n^{1/2r} + O(n^{1/4r})$. Some open problems concerning B_h-sequences are also discussed in this paper."

Translating into the notation of this survey, that says $\sigma_h \leq (h/2 \cdot ((h/2)!)^2)^{1/h}$ for even h.

[59] Imre Z. Ruzsa, *Solving a linear equation in a set of integers. I*, Acta Arith. **65** (1993), 259–282. **MR 94k:11112**

Fix integers $a_1, \ldots, a_k, b$. Ruzsa considers sets S for which $b = \sum s_i a_i$ has no solutions with $s_i \in S$ with and without the stipulation that the s_i be distinct. Sum-free sets, 3-term-AP-free sets [65, Problem E10], and Sidon sequences are some of the special cases studied.

Ruzsa gives an interesting spin on the Erdős/Turàn [5] bound, giving $R(2,n) \leq \sqrt{n} + n^{1/4} + 1$ and $R(3,n) \leq \sqrt{n} + 4n^{1/4} + 11$. He also shows that $\{s \in [0, p(p-1)) \colon s \equiv i \pmod{p-1}, s \equiv g^i \pmod{p}, g \text{ a primitive root}\}$ witnesses $C(2, p(p-1)) = p - 1$.

He also shows that one may take at most $(1 + o(1))h^{2-1/h} n^{1/h}$ numbers from $[0, n)$ such that the h-fold sums of distinct elements (up to rearrangements of the summands) are distinct.

Part II is [74].

[60] Zhen Xiang Zhang, *A B_2-sequence with larger reciprocal sum*, Math. Comp. **60** (1993), 835–839. **MR 93m:11012**

Author's abstract: "A sequence of positive integers is called a B_2-sequence if the pairwise differences are all distinct. The Mian-Chowla sequence is the B_2-sequence obtained by the greedy algorithm. Its reciprocal sum S^* has been conjectured to be the maximum over all B_2-sequences. In this paper we give a B_2-sequence which disproves this conjecture. Our sequence is obtained as follows: the first 14 terms are obtained by the greedy algorithm, the 15th term is 229, from the 16th term on, the greedy algorithm continues. The reciprocal sum of the first 300 terms of our sequence is larger than S^*."

[61] Sheng Chen, *On the size of finite Sidon sequences*, Proc. Amer. Math. Soc. **121** (1994), 353–356. **MR 94h:11016**

Author's abstract: "Let $h \geq 2$ be an integer. A set of positive integers B is called a B_h-sequence, or a Sidon sequence of order h, if all sums $a_1 + a_2 + \cdots + a_h$, where $a_i \in B$ $(i = 1, 2, \ldots, h)$, are distinct up to rearrangements of the summands. Let $F_h(n)$ be the size of the maximum B_h-sequence contained in $\{1, 2, \ldots, n\}$. We prove that

$$F_{2r-1}(n) \leq ((r!)^2 n)^{1/(2r-1)} + \mathcal{O}\left(n^{1/(4r-2)}\right).$$

"

In the terminology of this survey, this is $\sigma_h^h \leq (\lceil h/2 \rceil !)^2$ for odd h.

[62] Paul Erdős, *Some problems in number theory, combinatorics and combinatorial geometry*, Math. Pannon. **5** (1994), 261–269. **MR 95j:11018**

[63] P. Erdős, A. Sárközy, and T. Sós, *On sum sets of Sidon sets. I*, J. Number Theory **47** (1994), 329–347. **MR 95e:11030**

This article gives bounds for the number of intervals in the sumset of a Sidon set. Define

$$\mathcal{B}(\mathcal{A}+\mathcal{A},d) := \{s\colon s-d \notin \mathcal{A}+\mathcal{A}, s \in \mathcal{A}+\mathcal{A}\},$$

and denote its counting function by $\mathcal{B}(\mathcal{A}+\mathcal{A},d,n)$. The following theorems are proved: Theorem 1: There is an absolute constant $c_1 > 0$ such that for every finite Sidon set $\mathcal{A}$ and integer $d > 0$,

$$|\mathcal{B}(\mathcal{A}+\mathcal{A},d)| > c_1|\mathcal{A}|^2.$$

Theorem 2: There is an absolute constant c_2 such that for every Sidon set $\mathcal{A}$ and integer $d > 0$,

$$\limsup_{N\to\infty} \frac{\mathcal{B}(\mathcal{A}+\mathcal{A},d,n)}{A^2(N)} > c_2 > 10^{-7}.$$

Theorem 3: For $n > n_0$, there is a Sidon set in $[n]$ whose sumset does not contain a gap of length $3\sqrt{n}$. Theorem 4: $\forall\epsilon > 0$ there is a Sidon set (let $s_1 < s_2 < \dots$ be its sumset) and integer i_0 such that $\forall i > i_0$

$$s_{i+1} - s_i < s_i^{\frac{1}{2}} (\log s_i)^{\frac{3}{2}+\epsilon}.$$

Theorem 5: There is an absolute constant $c_4 > 0$ such that if $\mathcal{A}$ is a finite Sidon set with $|\mathcal{A}| \geq 2$ and sumset $s_1 < s_2 < \cdots < s_u$, then

$$\max_{1\leq i<u} (s_{i+1} - s_i) > c_4 \log|\mathcal{A}|.$$

I remark that with a little care one may prove the inequality

$$|\mathcal{B}(\mathcal{A}+\mathcal{A},d)| \geq \tfrac{1}{4}(|\mathcal{A}|^2 - |\mathcal{A}| - 1)$$

in Theorem 1, and one may take $c_2 = \frac{1}{62} > 0.0162$.

The paper concludes with some interesting open problems. Does the number of "length one" intervals in the sumset of a finite Sidon set go to infinity as the size of the set does? Does

$$\tfrac{1}{t}\sum_{i=1}^{t-1}(s_{i+1} - s_i)^2 \to \infty$$

where $s_1 < s_2 < \cdots < s_t$ is the sum set of a finite Sidon set? If $\mathcal{A}$ is a dense finite Sidon set, must $\mathcal{A}+\mathcal{A}$ be well-distributed w.r.t. small moduli?

[64] P. Erdős, A. Sárközy, and V. T. Sós, *On additive properties of general sequences*, Discrete Math. **136** (1994), 75–99, Trends in discrete mathematics. **MR 96d:11014**

Author's abstract: "The authors give a survey of their papers on additive properties of general sequences and they prove several further results on the range of additive representation functions and on difference sets. Many related unsolved problems are discussed."

[65] Richard K. Guy, *Unsolved problems in number theory*, Second, Springer-Verlag, New York, 1994, ISBN 0-387-94289-0, Unsolved Problems in Intuitive Mathematics, I. **MR 96e:11002**

[66] Martin Helm, *A remark on B_{2k}-sequences*, J. Number Theory **49** (1994), 246–249. **MR 96b:11024**

Author's abstract: "Improving a result of Chen [A note on B2k-sequences, preprint] in this paper we prove that

$$\liminf_{n\to\infty} \frac{A(n)}{n^{1/2k}} (\log n)^{1/(3k-1)} < \infty$$

holds for every infinite B_{2k}-sequence A."

[67] Xing De Jia, *On B_{2k}-sequences*, J. Number Theory **48** (1994), 183–196. **MR 95d:11027**

If $\mathcal{A}$ is a B_{2k} sequence whose counting function satisfies $A(n^2) \ll A(n)^2$, then

$$\liminf_{n\to\infty} \frac{A(n)}{\sqrt[2k]{n/\log(n)}} < \infty.$$

[68] Zhen Xiang Zhang, *Finding finite B_2-sequences with larger $m - a_m^{1/2}$*, Math. Comp. **63** (1994), 403–414. **MR 94i:11109**

The set $(m\mathtt{Bose}_2(p,\theta,k)+r) \cup \{0\}$ is a Sidon set modulo p^2-1 provided p is a prime power, θ generates the multiplicative group of $\mathbb{F}_{p^2}$, $1 \le k < p$, and $\gcd(m, p^2-1) = 1$. This paper considers the algorithmic difficulties of computing

$$\min_{\theta,r} \max \left\{\mathtt{Bose}_2(p,\theta,1)+r\right\},$$

where $\mathtt{Bose}_2(p,\theta,1)+r$ is reduced modulo p^2-1. As an application of the algorithm, it is noted that for $p = 829$, there are θ and r such that $\max\{\mathtt{Bose}_2(p,\theta,1)+r\} = 829^2 - 16939$, whence $R(2, 670303) - \sqrt{670303} > 10$. The algorithm is simplified and made faster in [89].

[69] J. Cilleruelo, *$B_2[g]$ sequences whose terms are squares*, Acta Math. Hungar. **67** (1995), 79–83. **MR 95m:11032**

[70] P. Erdős, A. Sárközy, and V. T. Sós, *On sum sets of Sidon sets. II*, Israel J. Math. **90** (1995), 221–233. **MR 96f:11034**

Author's abstract: "It is proved that there is no Sidon set in $[n]$ whose sumset contains $c_1 n^{1/2}$ consecutive integers, but it may contain $c_2 n^{1/3}$ consecutive integers. Moreover, it is shown that a finite Sidon set cannot be well-covered by generalized arithmetic progressions."

[71] Mihail N. Kolountzakis, *An effective additive basis for the integers*, Discrete Math. **145** (1995), 307–313. **MR 96m:11010**

Author's abstract: "We give an algorithm for the enumeration of a set E of nonnegative integers with the property that each nonnegative integer x can be written as a sum of two elements of E in at least $C_1 logx$ and at most $C_2 logx$ ways, where C_1, C_2 are positive constants. Such a set is called a basis and its existence has been established by Erdős. Our algorithm takes time polynomial in n to enumerate all elements of E not greater than n. We accomplish this by derandomizing a probabilistic proof which is slightly different than that given by Erdős."

[72] Hanno Lefmann and Torsten Thiele, *Point sets with distinct distances*, Combinatorica **15** (1995), 379–408. **MR 96h:52016**

[73] Carl Pomerance and András Sárközy, *Combinatorial number theory*, Handbook of Combinatorics, Vol. 1, 2, Elsevier, Amsterdam, 1995, pp. 967–1018. **MR 97e:11032**

[74] Imre Z. Ruzsa, *Solving a linear equation in a set of integers. II*, Acta Arith. **72** (1995), 385–397. **MR 96j:11128**

[75] C. P. Schnorr and H. H. Hörner, *Attacking the Chor-Rivest cryptosystem by improved lattice reduction*, Advances in Cryptology—EUROCRYPT '95 (Saint-Malo, 1995), Lecture Notes in Comput. Sci., vol. 921, Springer, Berlin, 1995, pp. 1–12. **MR 96k:94014**

Author's abstract: "Summary: "We introduce algorithms for lattice basis reduction that are improvements of the famous L^3-algorithm. If a random L^3-reduced lattice basis $b_1, \cdots, b_n$ is given such that the vector of reduced Gram-Schmidt coefficients ($\{\mu_{i,j}\}$, $1 \le j < i \le n$) is uniformly distributed in $[0,1)^{\binom{n}{2}}$, then the pruned enumeration finds with positive probability a shortest lattice vector. We demonstrate the power of these algorithms by solving random subset sum problems of arbitrary density with 74 and 82 weights, by breaking the Chor-Rivest cryptoscheme in dimensions 103 and 151 and by breaking Damgård's hash function.""

This paper breaks the Chor-Rivest cryptosystem [40] with a few days computation. The followup attack in [117] is more efficient.

[76] Joel Spencer and Prasad Tetali, *Sidon sets with small gaps*, Discrete Probability and Algorithms (Minneapolis, MN, 1993), Springer, New York, 1995, pp. 103–109. **MR 97g:05163**

[77] Sheng Chen, *A note on B_{2k} sequences*, J. Number Theory **56** (1996), 1–3. **MR 97a:11035**

Let $\mathcal{A} = \{a_1 < a_2 < \dots\}$ be a B_{2k} sequence ($k \ge 2$) with counting function $A(n)$. Then

$$\liminf_{n\to\infty} \frac{A(n)}{n^{1/(2k)}(\log n)^{1/(4k-4)}} < \infty$$

and

$$\limsup_{n\to\infty} \frac{a_n}{n^{2k}\sqrt{\log n}} = \infty.$$

[78] S. W. Graham, *B_h sequences*, Analytic Number Theory, Vol. 1 (Allerton Park, IL, 1995), Birkhäuser Boston, Boston, MA, 1996, pp. 431–449. **MR 97h:11019**

[79] Martin Helm, *On B_3-sequences*, Analytic Number Theory, Vol. 2 (Allerton Park, IL, 1995), Progr. Math., vol. 139, Birkhäuser Boston, Boston, MA, 1996, pp. 465–469. **MR 97d:11040**

[80] ———, *On the distribution of B_3-sequences*, J. Number Theory **58** (1996), 124–129. **MR 97d:11041**

Author's abstract: "An infinite set of natural numbers is called a B_3-sequence if all sums $a_1 + a_2 + a_3$ with $a_j \in \mathcal{A}$ and $a_1 \le a_2 \le a_3$ are distinct. Let $A(n)$ be the number of positive elements $\le n$ in $\mathcal{A}$. P. Erdős conjectures that every B_3-sequence $\mathcal{A}$ satisfies $\liminf_{n\to\infty} A(n)n^{-1/3} = 0$. In this paper we prove that no sequence satisfying $A(n) \sim \alpha n^{1/3}$ can be a B_3-sequence. We also give other necessary conditions for a B_3-sequence."

[81] Xingde Jia, *$B_h[g]$-sequences with large upper density*, J. Number Theory **56** (1996), 298–308. **MR 96k:11009**

The analysis in this article is flawed; see [105] for an explanation and correction.

[82] Mihail N. Kolountzakis, *The density of $B_h[g]$ sequences and the minimum of dense cosine sums*, J. Number Theory **56** (1996), 4–11. **MR 96k:11026**

Author's abstract: "A set E of integers is called a $B_h[g]$ set if every integer can be written in at most g different ways as a sum of h elements of E. We give an upper bound for the size of a $B_h[1]$ subset $\{n_1, \ldots, n_k\}$ of $\{1, \ldots, n\}$ whenever $h = 2m$ is an even integer:

$$k \leq (m(m!)^2)^{1/h} n^{1/h} + \mathcal{O}\left(n^{1/2h}\right).$$

For the case $h = 2$ ($h = 4$) this has already been proved by Erdős and Turán (by Lindström). It has been independently proved for all even h by Jia who used an elementary combinatorial argument. Our method uses a result, which we prove, related to the minimum of dense cosine sums which roughly states that if $1 \leq \lambda_1 < \cdots < \lambda_N \leq (2 - \epsilon)N$ are N different integers then

$$\left| \min_x \sum_1^N \cos \lambda_j x \right| \geq C\epsilon^2 N.$$

Finally we exhibit some dense finite and infinite $B_2[2]$ sequences."

[83] ———, *Problems in the additive number theory of general sets, I: sets with distinct sums* (1996), 15 pages, unpublished.

This delightful review of problems—including for each a summary of what's known and an outline of how it is known—is a must-read for researchers in the area. The three sections are entitled "Finite $B_h[g]$ sets", "Infinite $B_h[g]$ sets with large lower density", and "Infinite $B_h[g]$ with large upper density".

[84] ———, *Some applications of probability to additive number theory and harmonic analysis*, Number Theory (New York, 1991–1995), Springer, New York, 1996, pp. 229–251. **MR 98i:11061**

Author's abstract: "We present some applications of the probabilistic method in additive number theory and harmonic analysis. We describe two general approaches to the probabilistic construction of certain objects. The question of whether one can actually "construct" these is also discussed and several examples of "derandomized" probabilistic proofs are given."

[85] Imre Z. Ruzsa, *Sumsets of Sidon sets*, Acta Arith. **77** (1996), 353–359. **MR 97j:11013**

This paper follows [63, 70] in the consideration of the length of the longest interval contained in the sumset of a Sidon set, and the length of the longest interval *not* contained in $\mathcal{A}$. For example, a set $\mathcal{A} \subseteq [n]$ is given such that $\mathcal{A} + \mathcal{A}$ contains an interval of length $c\sqrt{n}$, showing that this is the correct size up to the constant factor.

[86] A. Sárközy and V. T. Sós, *On additive representation functions*, The Mathematics of Paul Erdős, I, Springer, Berlin, 1997, pp. 129–150. **MR 97m:11019**

[87] Béla Bajnok, *Constructions of spherical 3-designs*, Graphs Combin. **14** (1998), 97–107. **MR 99f:05020**

Author's abstract: "Spherical t-designs are Chebyshev-type averaging sets on the d-sphere $S^d \subset R^{d+1}$ which are exact for polynomials of degree at most t. This concept was introduced in 1977 by Delsarte, Goethals, and Seidel, who also found the minimum possible size of such designs, in particular, that the number of points in a 3-design on S^d must be at least $n \geq 2d+2$. In this paper we give explicit constructions for spherical 3-designs on S^d consisting of n points for $d = 1$ and $n \geq 4$; $d = 2$ and $n = 6, 8, \geq 10$; $d = 3$ and $n = 8, \geq 10$; $d = 4$ and $n = 10, 12, \geq 14$; $d \geq 5$ and $n \geq 5(d+1)/2$ odd or $n \geq 2d+2$ even. We also provide some evidence that 3-designs of other sizes do not exist. We will introduce and apply a concept from additive number theory generalizing the classical Sidon-sequences. Namely, we study sets of integers S for which the congruence $\varepsilon_1 x_1 + \varepsilon_2 x_2 + \cdots + \varepsilon_t x_t \equiv 0$ mod n, where $\varepsilon_i = 0, \pm 1$ and $x_i \in S$ $(i = 1, 2, \ldots, t)$, only holds in the trivial cases. We call such sets Sidon-type sets of strength t, and denote their maximum cardinality by $s(n, t)$. We find a lower bound for $s(n, 3)$, and show how Sidon-type sets of strength 3 can be used to construct spherical 3-designs. We also conjecture that our lower bound gives the true value of $s(n, 3)$ (this has been verified for $n \leq 125$)."

[88] D. Frank Hsu and Xingde Jia, *Some nonexistence results on perfect addition sets*, Proceedings of the Twenty-Ninth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, Fl, 1998), vol. 134, 1998, pp. 131–137. **MR 2000a:11021**

[89] Bernt Lindström, *Finding finite B_2-sequences faster*, Math. Comp. **67** (1998), 1173–1178. **MR 98m:11012**

Lindström shows that for any two generators θ, θ' of $\mathbb{F}_{p^2}$ (p an odd prime power), there is an m and an r such that

$$\mathtt{Bose}_2(p, \theta, 1) = m\,\mathtt{Bose}_2(p, \theta', 1) - r.$$

In other words, varying the generator does not generate "new" Bose sets. (It is easy to extend this to show the uselessness of varying k in $\mathtt{Bose}_2(p, \theta, k)$.) He also gives a criterion (in terms of u and v) for the existence of a generator θ satisfying $\theta^2 = u\theta + v$. These two results greatly improve the efficiency of Zhang's algorithm [68].

[90] ———, *Well distribution of Sidon sets in residue classes*, J. Number Theory **69** (1998), 197–200. **MR 99c:11021**

Author's abstract: "A set $\mathcal{A}$ of non-negative integers is a Sidon set if the sums $a + b$ $(a, b \in A, a \leq b)$ are distinct. Assume that $a \subseteq [1, n]$ and that $|A| = (1 + o(1)))n^{1/2}$. Let $m \geq 2$ be an integer. In Theorem 1 I prove that asymptotically $1/m$ of all elements in $\mathcal{A}$ fall into each residue class modulo m. When $m = 2$ I prove a sharper result in Theorem 2. Assume that $|A| \geq n^{1/2}$. Then the difference between the number of odd and the number of even elements in $\mathcal{A}$ is $\mathcal{O}\left(n^{3/8}\right)$. If the interval $[1, n]$ is divided into m equal parts and the number of elements from $\mathcal{A}$ in each part is counted, then similar results hold for these counts."

[91] Imre Z. Ruzsa, *An infinite Sidon sequence*, J. Number Theory **68** (1998), 63–71. **MR 99a:11014**

Author's abstract: "We show the existence of an infinite Sidon sequence such that the number of elements in $[1, N]$ is $N^{\sqrt{2}-1+o(1)}$."

[92] ———, *A small maximal Sidon set*, Ramanujan J. **2** (1998), 55–58, Paul Erdős (1913–1996). **MR 99g:11026**

Author's abstract: "We construct a Sidon set $\mathcal{A} \subset [1, N]$ which has $\ll (N \log N)^{1/3}$ elements and which is maximal in the sense that the inclusion of any other integer from $[1, N]$ destroys the Sidon property."

[93] Andreas Baltz, Tomasz Schoen, and Anand Srivastav, *Probabilistic construction of small strongly sum-free sets via large Sidon sets*, Randomization, Approximation, and Combinatorial Optimization (Berkeley, CA, 1999), Lecture Notes in Comput. Sci., vol. 1671, Springer, Berlin, 1999, pp. 138–143. **MR 2001e:68137**

[94] Anant P. Godbole, Svante Janson, Nicholas W. Locantore Jr., and Rebecca Rapoport, *Random Sidon sequences*, J. Number Theory **75** (1999), 7–22. **MR 2000c:11031**

Author's abstract: "A subset $\mathcal{A}$ of the set $[n] = \{1, 2, \ldots, n\}$, $|\mathcal{A}| = k$ is said to form a Sidon (or B_h) sequence $h \geq 2$, if each of the sums $a_1 + a_2 + \cdots + a_h$, $a_1 \leq a_2 \leq \cdots \leq a_h$; $a_i \in \mathcal{A}$, are distinct. We investigate threshold phenomena for the Sidon property, showing that if $\mathcal{A}_n$ is a random subset of $[n]$, then the probability that $\mathcal{A}_n$ is a B_h sequence tends to unity as $n \to \infty$ if $k_n = |\mathcal{A}_n| \ll n^{1/2h}$, and that $\mathbf{P}(\mathcal{A}_n \text{ is Sidon}) \to 0$ provided that $k_n \gg n^{1/2h}$. The main tool employed is the Janson exponential inequality. The validity of the Sidon property *at* the threshold is studied as well. We prove, using the Stein-Chen method of Poisson approximation, that $\mathbf{P}(\mathcal{A}_n \text{ is Sidon}) \to \exp -\lambda$ $(n \to \infty)$ if $k_n \sim \Lambda \cdot n^{1/2h}$ $(\Lambda \in \mathbf{R}^+)$, where λ is a constant that depends in a well-specified way on Λ. Multivariate generalizations are presented."

[95] Mihail N. Kolountzakis, *On the uniform distribution in residue classes of dense sets of integers with distinct sums*, J. Number Theory **76** (1999), 147–153. **MR 2000a:11028**

Author's abstract: "A set $\mathcal{A} \subseteq \{1, \ldots, N\}$ is of the type B_2 if all sums $a+b$, with $a \geq b$, $a, b \in \mathcal{A}$, are distinct. It is well known that the largest such set is of size asymptotic to $N^{1/2}$. For a B_2 set $\mathcal{A}$ of this size we show that, under mild assumptions on the size of the modulus m and on the difference $N^{1/2} - |\mathcal{A}|$ (these quantities should not be too large), the elements of $\mathcal{A}$ are uniformly distributed in the residue classes mod m. Quantitative estimates on how uniform the distribution is are also provided. This generalizes recent results of Lindström whose approach was combinatorial. Our main tool is an upper bound on the minimum of a cosine sum of k terms, $\sum_1^k \cos \lambda_j x$, all of whose positive integer frequencies j are at most $(2 - \epsilon)k$ in size. "

[96] B. Lindström, *Primitive quadratics reflected in B_2-sequences*, Portugal. Math. **56** (1999), 257–263. **MR 2000j:11029**

[97] Bernt Lindström, *Computing B_3-sequences*, Proceedings of the Seventh Nordic Combinatorial Conference (Turku, 1999), Turku Cent. Comput. Sci., Turku, 1999, pp. 65–68. **MR 2000k:11027**

[98] Imre Z. Ruzsa, *Erdős and the integers*, J. Number Theory **79** (1999), 115–163. **MR 2002e:11002**

A brief recounting of the state-of-the-art on several aspects of Sidon sets.

[99] Andreas Baltz, Tomasz Schoen, and Anand Srivastav, *Probabilistic construction of small strongly sum-free sets via large Sidon sets*, Colloq. Math. **86** (2000), 171–176. **MR 2001k:05197**

[100] T. Banakh, O. Verbitsky, and Ya. Vorobets, *A Ramsey treatment of symmetry*, Electron. J. Combin. **7** (2000), Research Paper 52, 25 pp. (electronic). **MR 2001m:05255**

Author's abstract: "Given a space Ω endowed with symmetry, we define $ms(\Omega, r)$ to be the maximum of m such that for any r-coloring of Ω there exists a monochromatic symmetric set of size at least m. We consider a wide range of spaces Ω including the discrete and continuous segments $\{1, \ldots, n\}$ and $[0, 1]$ with central symmetry, geometric figures with the usual symmetries of Euclidean space, and Abelian groups with a natural notion of central symmetry. We observe that $ms(\{1, \ldots, n\}, r)$ and $ms([0, 1], r)$ are closely related, prove lower and upper bounds for $ms([0, 1], 2)$, and find asymptotics of $ms([0, 1], r)$ for r increasing. The exact value of $ms(\Omega, r)$ is determined for figures of revolution, regular polygons, and multi-dimensional parallelopipeds. We also discuss problems of a slightly different flavor and, in particular, prove that the minimal r such that there exists an r-coloring of the k-dimensional integer grid without infinite monochromatic symmetric subsets is $k + 1$."

[101] Javier Cilleruelo, *An upper bound for $B_2[2]$ sequences*, J. Combin. Theory Ser. A **89** (2000), 141–144. **MR 2001d:11026**

Cilleruelo gives a combinatorial proof that $R(4, n) \leq \sqrt{6n} + 1$, whence $\sigma_2(4) \leq \sqrt{3}$.

[102] ______, *Gaps in dense Sidon sets*, Integers **0** (2000), Paper A11, 6pp. (electronic). **MR 2001m:11129**

Author's abstract: "We prove that if $\mathcal{A} \subset [1, N]$ is a Sidon set with $N^{1/2} - L$ elements, then any interval $I \subset [1, N]$ of length cN contains $c|\mathcal{A}| + E_I$ elements of $\mathcal{A}$, with $|E_I| \leq 52N^{1/4}(1 + c^{1/2}N^{1/8})(1 + L_+^{1/2})N^{-1/8}$, $L_+ = \max\{0, L\}$. In particular, if $|A| = N^{1/2} + \mathcal{O}\left(N^{1/4}\right)$, and $g(A)$ is the maximum gap in $\mathcal{A}$, we deduce that $g(A) \ll N^{3/4}$. We also prove that, under this condition, the exponent $3/4$ is sharp."

[103] Javier Cilleruelo and Jorge Jiménez-Urroz, *$B_h[g]$ sequences*, Mathematika **47** (2000), 109–115 (2002). **MR 1924491**

Author's abstract: "We give new upper and lower bounds for $F_h(g, N)$, the maximum size of a $B_h[g]$ sequence contained in $[1, N]$. We prove

$$F_h(g, N) \leq (\sqrt{3h}h!gN)^{1/h},$$

and for any $\epsilon > 0$ and $g > g(\epsilon, h)$,

$$F_h(g, N) \geq \left((1 - \epsilon)\sqrt{\frac{\pi}{6}}\sqrt{h}gN\right)^{1/h} + o\left(()\, N^{1/h}\right).$$

"

This means that $\sigma_h(h!g) \leq (h!\sqrt{3h})^{1/h}$ (an improvement for $h > 7$) and $\liminf_{g\to\infty} \sigma_h(h!g)h^{-1/(2h)} \geq \sqrt{\pi/6}$.

[104] B. Lindström, *A translate of Bose-Chowla B_2-sets*, Studia Sci. Math. Hungar. **36** (2000), 331–333. **MR 2001j:11005**

[105] Bernt Lindström, *$B_h[g]$-sequences from B_h-sequences*, Proc. Amer. Math. Soc. **128** (2000), 657–659. **MR 2000e:11022**

If $\mathcal{A}$ is a B_h set and $\mathcal{B} = \{0, 1, \ldots, m\}$, then

$$m\mathcal{A} + \mathcal{B} = \{ma + b \colon a \in \mathcal{A}, b \in \mathcal{B}\}$$

is a $B_h[g]$ set. Consequently, $R_h(h!m^{h-1}, n) \geq (m^{h-1}n)^{1/h}(1 + o(1))$.

This is the same construction of [81], but here it is analyzed correctly.

[106] Melvyn B. Nathanson, *N-graphs, modular Sidon and sum-free sets, and partition identities*, Ramanujan J. **4** (2000), 59–67. **MR 2001c:05011**

> **Author's abstract:** "Using a new graphical representation for partitions, the author obtains a family of partition identities associated with partitions into distinct parts of an arithmetic progression, or, more generally, with partitions into distinct parts of a set that is a finite union of arithmetic progressions associated with a modular sum-free Sidon set. Partition identities are also constructed for sets associated with modular sum-free sets."

[107] Oriol Serra and Gilles Zémor, *On a generalization of a theorem by Vosper*, Integers **0** (2000), Paper A10, 10 pp. (electronic). **MR 2001f:11178**

> **Author's abstract:** "Let S, T be subsets of $\mathbb{Z}/p\mathbb{Z}$ with $\min\{|S|, |T|\} > 1$. The Cauchy-Davenport theorem states that $|S + T| \geq \min\{p, |S| + |T| - 1\}$. A theorem by Vosper characterizes the critical pair in the above inequality. We prove the following generalization of Vosper's theorem. If $|S + T| \leq \min\{p - 2, |S| + |T| + m\}$, $2 \leq |S|, |T|$, and $|S| \leq p - \binom{m+4}{2}$, then S is a union of at most $m + 2$ arithmetic progressions with the same difference. The term $\binom{m+4}{2}$ is best possible, i.e. cannot be replaced by a smaller number. "

[108] H. Taylor and G. S. Yovanof, *B_2-sequences and the distinct distance constant*, Comput. Math. Appl. **39** (2000), 37–42, Sol Golomb's 60th Birthday Symposium (Oxnard, CA, 1992). **MR 2001j:11007**

> **Author's abstract:** "A sequence of positive integers $1 < \alpha_1 < \alpha_2 < \ldots$ with the property that all differences $\alpha_j - \alpha_i$, $i < j$ are distinct is called a B_2-sequence. Denote by DDC (distinct difference constant) the maximum over all possible B_2-sequences of the sum $\sum(1/\alpha_i)$. Previously known upper and lower bounds for the DDC are $2.1597 < DDC < 2.374$. We have estimated the following sharper bounds on DDC: $2.1600383 < DDC < 2.2473$. We have further proved that any B_2-sequence which achieves the maximum reciprocal sum must start with the terms $1, 2, 4$."

[109] Peter J. Cameron and Paul Erdős, *Notes on sum-free and related sets*, Recent Trends in Combinatorics (Mátraháza, 1995), Cambridge Univ. Press, Cambridge, 2001, pp. 95–107. **MR 2000c:05144**

> Fix h and g, and Let $f_{\max}(n)$ be the number of maximal $B_h^*[g]$ sets contained in $[n]$. Then $\limsup_{n\to\infty} f_{\max}(n) = \infty$.

[110] Javier Cilleruelo, *New upper bounds for finite B_h sequences*, Adv. Math. **159** (2001), 1–17. **MR 2002g:11023**

$$\sigma_3 \leq \left(\frac{4}{1 + (\frac{2}{\pi+2})^4}\right)^{1/3} < 1.576,$$
$$\sigma_4 \leq \left(\frac{8}{1 + (\frac{2}{\pi+2})^4}\right)^{1/4} < 1.673.$$

> For $3 \leq m < 38$

$$\sigma_{2m-1} \leq \left(\frac{(m!)^2}{1 + \cos^{2m}(\pi/m)}\right)^{1/(2m-1)},$$
$$\sigma_{2m} \leq \left(\frac{m(m!)^2}{1 + \cos^{2m}(\pi/m)}\right)^{1/(2m)}.$$

For $38 \le m$

$$\sigma_{2m-1} \le \left(\frac{5}{2} \left(\frac{15}{4} - \frac{5}{4m} \right)^{1/4} \frac{(m!)^2}{\sqrt{m}} \right)^{1/(2m-1)},$$
$$\sigma_{2m} \le \left(\frac{5}{2} \left(\frac{15}{4} - \frac{5}{4m} \right)^{1/4} \sqrt{m}(m!)^2 \right)^{1/(2m)}.$$

[111] Javier Cilleruelo and Carlos Trujillo, *Infinite $B_2[g]$ sequences*, Israel J. Math. **126** (2001), 263–267. **MR 2003d:11032**

Author's abstract: "We exhibit, for any integer $g \ge 2$, an infinite sequence $\mathcal{A} \in B_2[g]$ such that $\limsup_{x\to\infty} A(x)x^{-1/2} = \frac{3}{2\sqrt{2}}\sqrt{g-1}$. In addition, we obtain better estimates for small values of g. For example, we exhibit an infinite sequences $\mathcal{A} \in B_2[2]$ such that $\limsup_{x\to\infty} A(x)x^{-1/2} = \sqrt{3/2}$."

[112] Gérard Cohen, Simon Litsyn, and Gilles Zémor, *Binary B_2-sequences: a new upper bound*, J. Combin. Theory Ser. A **94** (2001), 152–155. **MR 2002a:94019**

Author's abstract: "We show that the maximum size of a B_2-sequence of binary n-vectors for large enough n is at most $2^{0.5753n}$, thus improving on the previous bound $2^{0.6n}$ due to B. Lindström."

[113] Ben Green, *The number of squares and $B_h[g]$ sets*, Acta Arith. **100** (2001), 365–390. **MR 2003d:11033**

This paper contains a substantial jump in sophisticatedness-of-technique over essentially all earlier work on the density of finite $B_h^*[g]$ sets. The techniques used in [118] to get upper bounds are incorporated and extended.

The central problem here is to bound

$$\underline{M}(n) := \inf_{f:[n]\to\mathbb{R}, \sum f(x)=n} \sum_{a+b=c+d} f(a)f(b)f(c)f(d).$$

As the summation has 3 degrees of freedom, it is not surprising that there are positive constants c_1, c_2 with $c_1 n^3 \lesssim \underline{M}(n) \lesssim c_2 n^3$. Green shows that we may take $c_1 = 4/7$ and $c_2 = 0.64074$. He also shows that the infimum is obtained for a unique function f, and $(f \circ f) \circ f(x)$ is constant for $x \in [n]$.

A substantive amount of additional work gives the bounds

$$\begin{aligned}
\sigma_3 &\le (7/2)^{1/3} < 1.519\\
\sigma_4 &\le 7^{1/4} < 1.627\\
\sigma_{2h}((2h)!) &\le \pi^{1/2} h^{1/2} (h!)^2 (1+\epsilon(h))/((2h)!)\\
\sigma_{2h-1}((2h-1)!) &\le \pi^{1/2} h^{-1/2} (h!)^2 (1+\epsilon(h))/((2h-1)!).
\end{aligned}$$

The function $\epsilon(h)$ tends to 0 as $h \to \infty$, but it is not computed explicitly. Also, Green shows that $\sigma_2(g) \le 7/4(1-1/g)$ and $\sigma_2(g) \le 1.6999$.

While the main theorems are proven in full detail, but there are number of comments about generalizations that are neither proven nor straightforward.

[114] Alain Plagne, *A new upper bound for $B_2[2]$ sets*, J. Combin. Theory Ser. A **93** (2001), 378–384. **MR 2001k:11035**

$\sigma_2(4) \le 1.67131$.

[115] ______, *Recent progress on finite $B_h[g]$ sets*, Proceedings of the Thirty-Second Southeastern International Conference on Combinatorics, Graph Theory and Computing (Baton Rouge, LA, 2001), vol. 153, 2001, pp. 49–64. **MR 2003a:05146**

[116] I. Z. Ruzsa, *An almost polynomial Sidon sequence*, Studia Sci. Math. Hungar. **38** (2001), 367–375. **MR 2002k:11030**

There is a real number α and integer n_0 such that $\{n^5 + \lfloor \alpha n^4 \rfloor : n > n_0\}$ is a Sidon set.

[117] Serge Vaudenay, *Cryptanalysis of the Chor-Rivest Cryptosystem*, Journal of Cryptology **14** (January 2001), 87 –100.

Author's abstract: "Knapsack-based cryptosystems used to be popular in the beginning of public key cryptography before all but the ChorRivest cryptosystem being broken. In this paper we show how to break this one with its suggested parameters: $\mathbb{F}_{197^{24}}$ and $\mathbb{F}_{256^{25}}$. We also give direction on possible extensions of our attack."

[118] Javier Cilleruelo, Imre Z. Ruzsa, and Carlos Trujillo, *Upper and lower bounds for finite $B_h[g]$ sequences*, J. Number Theory **97** (2002), 26–34. **MR 2003i:11033**

This nine page article inaugurated the modern era of Sidon-set research, containing significant advances in dealing with both g and h in getting both upper and lower bounds. In many cases, this was the first progress over the trivial bounds. The results here have all received substantial further refinement and generalization. We note that this article was submitted 31 months before publication, and the preprint was influencing other workers as early as 2000.

They prove that $R_2(2g,n) \le 1.319(2gn)^{1/2} + 1$ and, whence $\sigma_2(2g) \le 1.319$. They prove that $\sigma_2(2g) \ge \frac{g+\lfloor g/2 \rfloor}{\sqrt{g^2+2g\lfloor g/2 \rfloor}}$, whence $\sigma_2(4) \ge \sqrt{3/2} > 1.224$. For $h > 2$, they prove that $R_h(h!g,n) \le \frac{(h(h!)^2 gN)^{1/h}}{(1+\cos^h(\pi/h))^{1/h}}$, whence

$$\sigma_h(h!g)^h \le \frac{h(h!)^2}{1+\cos^h(\pi/h)}.$$

[119] Laurent Habsieger and Alain Plagne, *Ensembles $B_2[2]$: l'étau se resserre*, Integers **2** (2002), Paper A2, 20 pp. (electronic). **MR 2002m:11010** (French)

Author's abstract: "Let $F_2(N,2)$ denote the maximal cardinality of any $B_2[2]$ set included in $\{1,2,\dots,N\}$ It is a well known fact that the ratio $F_2(N,2)/\sqrt{N}$ $(N \ge 1)$ is bounded from below and from above by two positive constants. However, one still ignores whether this quantity has a limit as N tends toward infinity. This explains the huge amount of work that was produced in order to improve the best lower and upper asymptotic bounds for $F_2(N,2)/\sqrt{N}$. In this paper, we obtain the following asymptotic bounds

$$\frac{4}{\sqrt{7}} \lesssim \frac{F_2(N,2)}{\sqrt{N}} < 2.3218\dots.$$

"

[120] Tomasz Schoen, *The distribution of dense Sidon subsets of $\mathbb{Z}_m$*, Arch. Math. (Basel) **79** (2002), 171–174. **MR 2003f:11022**

Author's abstract: "Let $S \subseteq \mathbb{Z}_m$ be a Sidon set of cardinality $|S| = m^{1/2} + \mathcal{O}(1)$. It is proved, in particular, that for any interval $\mathcal{I} = \{a, a+1, \ldots, a+\ell-1\}$ in $\mathbb{Z}_m$, $0 \leq \ell$ ¡ m, we have $||S \cap \mathcal{I}| - |S|\ell/m| = \mathcal{O}\left(|S|^{1/2} \log m\right)$."

[121] David R. Wood, *On vertex-magic and edge-magic total injections of graphs*, Australas. J. Combin. **26** (2002), 49–63. **MR 2003e:05121**

Author's abstract: "The study of graph labellings has focused on finding classes of graphs which admit a particualr type of labelling. Here we consider variations of the well-known edge-magic and vertex-magic total labellings for which all graphs admit such a labelling. In particular, we consider two types of injections of the vertices and edges of a graph with positive integers: (1) for every edge the sum of its label and those of its end-vertices is some *magic* constant (*edge-magic*); and (2) for every vertex the sum of its label and those of the edges incident to it is some *magic* constant (*vertex-magic*). Our aim is to minimise the maximum label or the magic constant associated with the injection. We present upper bounds on these parameters for complete graphs, forests and arbitrary graphs, which in a number of cases are within a constant factor of being optimal. Our results are based on greedy algorithms for computing an antimagic injection, which is then extended to a magic total injection. Of independent interst is our result that every forest has an edge-antinmagic vertex labelling."

[122] M. Chateauneuf, A. C. H. Ling, and D. R. Stinson, *Slope packings and coverings, and generic algorithms for the discrete logarithm problem*, J. Combin. Des. **11** (2003), 36–50. **MR 2003j:05035**

[123] Fan Chung, Paul Erdős, and Ronald Graham, *On sparse sets hitting linear forms*, Number Theory for the Millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 257–272. **MR 2003k:11012**

[124] Béla Bollobás and Oleg Pikhurko, *Integer Sets with Prescribed Pairwise Differences Being Distinct*, January 19, 2004, The website http://www.math.cmu.edu/ pikhurko/Papers/index.html links to the preprint, which it notes as "to appear in Europ J Comb."

Author's abstract: "We label the vertices of a given graph G with positive integers so that the pairwise differences over its edges are all distinct. Let $\mathcal{D}(G)$ be the smallest value that the largest label can have.

For example, for the complete graph K_n, the labels must form a Sidon set. Hence $\mathcal{D}(K_n) = (1 + o(1))n^2$. Rather surprisingly, we demonstrate that there are gaphs with only $n^{3/2+o(1)}$ edges achieving this bound.

More generally, we study the maximum value of $\mathcal{D}(G)$ that a graph G of the given order n and size m can have. We obtain bounds which are sharp up to a logarithmic multiplicative factor. The analogous problem for pairwise sums is considered as well. Our results, in particular, disprove a conjecture of Wood."

[125] M. Helm, *Upper bounds for $B_2[g]$-sets*, unpublished.

I have not seen this article, but it reportedly contains a proof that $R(4, n) \leq \sqrt{6n} + \mathcal{O}(1)$.

[126] Greg Martin and Kevin O'Bryant, *Continuous Ramsey theory and Sidon sets*, 2002, arXiv:math.NT/0210041.

Author's abstract: "A symmetric subset of the reals is one that remains invariant under some reflection $x \mapsto c - x$. Given $0 < \epsilon \leq 1$, there exists a real number $\Delta(\epsilon)$ with the following property: if $0 \leq \delta < \Delta(\epsilon)$, then every subset of $[0, 1]$ with measure ϵ contains a symmetric subset with measure δ, while if $\delta > \Delta(\epsilon)$, then there exists a subset of $[0, 1]$ with measure ϵ that does not contain a symmetric subset with measure δ. In this paper we establish upper and lower bounds for $\Delta(\epsilon)$ of the same order of magnitude: for example, we prove that $\Delta(\epsilon) = 2\epsilon - 1$ for $\frac{11}{16} \leq \epsilon \leq 1$ and that $0.59\epsilon^2 < \Delta(\epsilon) < 0.8\epsilon^2$ for $0 < \epsilon \leq \frac{11}{16}$.

This continuous problem is intimately connected with a corresponding discrete problem. A set S of integers is called a $B^*[g]$ set if for any given m there are at most g ordered pairs $(s_1, s_2) \in S \times S$ with $s_1 + s_2 = m$; in the case $g = 2$, these are better known as Sidon sets. We also establish upper and lower bounds of the same order of magnitude for the maximal possible size of a $B^*[g]$ set contained in $\{1, \ldots, n\}$, which we denote by $R(g, n)$. For example, we prove that $R(g, n) < 1.31\sqrt{gn}$ for all $n \geq g \geq 2$, while $R(g, n) > 0.79\sqrt{gn}$ for sufficiently large integers g and n.

These two problems are so interconnected that both continuous and discrete tools can be applied to each problem with surprising effectiveness. The harmonic analysis methods and inequalities among various L^p norms we use to derive lower bounds for $\Delta(\epsilon)$ also provide uniform upper bounds for $R(g, n)$, while the techniques from combinatorial and probabilistic number theory that we employ to obtain constructions of large $B^*[g]$ sets yield strong upper bounds for $\Delta(\epsilon)$."

[127] ———, *Constructions of Generalized Sidon Sets*, August 5, 2004, `http://www.math.ubc.ca/~gerg/`.

Author's abstract: "We give explicit constructions of sets S with the property that for each integer k, there are at most g solutions to $k = s_1 + s_2, a_i \in S$; such sets are called Sidon sets if $g = 2$ and generalized Sidon sets if $g \geq 3$. We extend to generalized Sidon sets the Sidon-set constructions of Singer, Bose, and Ruzsa. We also further optimize Koulantzakis' idea of interleaving several copies of a Sidon set, extending the improvements of Cilleruelo & Ruzsa & Trujillo, Jia, and Habsieger & Plagne."

[128] Melvyn Nathanson, *On the ubiquity of Sidon sets*, May 1, 2003, arXiv:math.NT/0304496.

Author's abstract: "It is proved that almost all small subsets of $[n]$ are $B_2[g]$ sets, in the sense that if $B_2[g](k, n)$ denotes the number of $B_2[g]$ sets of cardinality k contained in the interval $[n]$, then $\lim_{n\to\infty} B_2[g](k, n)/\binom{n}{k} = 1$ if $k = o\left(n^{g/(2g+2)}\right)$."

[129] Oleg Pikhurko, *Dense edge magic graphs and thin additive bases*, November 8, 2003, `http://www.dpmms.cam.ac.uk/~oleg/Papers/EdgeMagic.ps`.

Author's abstract: "A graph G of ornder n and size m is *edge-magic* if there is a bijection $\ell\colon V(G) \cup E(G) \to [n + m]$ such that all sums $\ell(a) + \ell(b) + \ell(ab)$, $ab \in E(G)$, are the same. We present new lower and upper bounds on $\mathcal{M}(n)$, the maximum size of an edge-magic graph of order n, being the first to show an upper bound of the form $\mathcal{M}(n) \leq (1 - \epsilon)\binom{n}{2}$. Concrete estimates for ϵ can be obtained by knowing $s(k, n)$, the maximum number of distinct pairwise sums that a k-subset of $[n]$ can have.

So, we also study $s(k, n)$, motivated by the above connections to edge-magic graphs and by the fact that a few known functions from additive number theory can be expressed via $s(k, n)$. For example, our estimate

$$s(k, n) \leq n + k^2 \left(\frac{1}{4} - \frac{1}{(\pi + 2)^2} + o\,(1)\right)$$

implies new bounds on the maximum size of quasi-Sidon sets, a problem pose by Erdős and Freud [49]. The related problem for differences is considered as well."