Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Combinatorial Theory, Series A 113 (2006) 591–607
Journal of Combinatorial Theory Series A
www.elsevier.com/locate/jcta

Constructions of generalized Sidon sets

Greg Martin[a], Kevin O'Bryant[b]

[a] *Department of Mathematics, University of British Columbia, Room 121, 1984 Mathematics Road, Vancouver, BC, Canada V6T 1Z2*
[b] *University of California at San Diego, La Jolla, CA 92093-0112, USA*

Received 4 April 2004

Communicated by R.L. Graham
Available online 23 June 2005

Abstract

We give explicit constructions of sets S with the property that for each integer k, there are at most g solutions to $k = s_1 + s_2$, $s_i \in S$; such sets are called Sidon sets if $g = 2$ and generalized Sidon sets if $g \geqslant 3$. We extend to generalized Sidon sets the Sidon-set constructions of Singer, Bose, and Ruzsa. We also further optimize Kolountzakis' idea of interleaving several copies of a Sidon set, extending the improvements of Cilleruelo, Ruzsa and Trujillo, Jia, and Habsieger and Plagne. The resulting constructions yield the largest known generalized Sidon sets in virtually all cases.

Keywords: Sidon set; B_2 sequence; Sunset; Finite field construction

1. Sidon's Problem

In connection with his study of Fourier series, Sidon [18] was led to ask how dense a set of integers can be without containing any solutions to

$$s_1 + s_2 = s_3 + s_4$$

aside from the trivial solutions $\{s_1, s_2\} = \{s_3, s_4\}$. This, and certain generalizations, have come to be known as *Sidon's Problem*.

Given a set $S \subseteq \mathbb{Z}$, we define the function $S * S$ by

$$S * S(k) := |\{(s_1, s_2)\colon s_i \in S, s_1 + s_2 = k\}|,$$

E-mail addresses: gerg@math.ubc.ca (G. Martin), kevin@member.ams.org (K. O'Bryant).

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2005.04.011

Table 1
Shortest Sidon sets, up to translation and reflection

k	$\mathrm{Min}\{a_k - a_1\}$	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}

which counts the number of ways to write k as a sum of two elements of S. We also set

$$\|S^*\|_\infty := \|S * S\|_\infty = \max_{k\in\mathbb{Z}} \left|\{(s_1, s_2)\colon s_i \in S,\ s_1 + s_2 = k\}\right|.$$

Note that if the set S is translated by c, then the function $S*S$ is translated by $2c$, and $\|S^*\|_\infty$ is unaffected. Similarly, if the set S is dilated by a factor of c, then $\|S^*\|_\infty$ is unaffected.

If $\|S^*\|_\infty \leqslant 2$, then S is called a Sidon set. Table 1 contains the optimally dense Sidon sets with 10 or fewer elements. Erdős and Turàn [8] showed that if $S \subseteq [n] := \{1, 2, \ldots, n\}$ is a Sidon set, then $|S| < n^{1/2} + O(n^{1/4})$, and Singer [19] gave a construction that yields a Sidon set in $[n]$ with $|S| > n^{1/2} - n^{5/16}$, for sufficiently large n. Thus, the maximum density of a finite Sidon set is asymptotically known. The maximum growth rate of $|S \cap [n]|$ for an infinite Sidon set S remains enigmatic. We direct the reader to [15] for a survey of Sidon's Problem.

The object of this paper is to give constructions of large finite sets S satisfying the constraints $S \subseteq [n]$ and $\|S^*\|_\infty \leqslant g$, that is, "large" in terms of n and g. We extend the Sidon set construction of Singer, as well as those of Bose [2] and Ruzsa [16], to allow $\|S^*\|_\infty \leqslant g$ for arbitrary g. The essence of our extension is that although the union of 2 distinct Sidon sets typically has large $\|S^*\|_\infty$, the union of two of Singer's sets will have $\|S^*\|_\infty \leqslant 8$. We also further optimize the idea of Kolountzakis [12] (refined in [5,11]) of controlling $\|S^*\|_\infty$ by interleaving several copies of the *same* Sidon set.

We warn the reader that the notation $\|S^*\|_\infty$ is not in wide use. Most authors write "S is a $B_2[g]$ set", sometimes meaning that $\|S^*\|_\infty \leqslant 2g$ and sometimes that $\|S^*\|_\infty \leqslant 2g+1$. Our notation is motivated by the common practice of using the same symbol for a set and

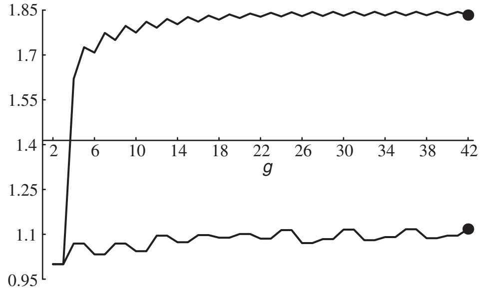

Fig. 1. Upper and lower bounds on $\sigma(g)$.

for its indicator function. With this convention,

$$S * S(k) = \sum_{x \in \mathbb{Z}} S(x)S(k-x)$$

is the Fourier convolution of the function S with itself, and counts representations as a sum of two elements of S. We use the same notation when discussing subsets of $\mathbb{Z}_n$, the integers modulo n, and no ambiguity arises.

Define

$$R(g,n) := \max_S \{|S|: S \subseteq [n],\ \|S^*\|_\infty \leqslant g\}. \tag{1}$$

In words, $R(g,n)$ is the largest possible size of a subset of $[n]$ whose pairwise sums repeat at most g times. We provide explicit lower bounds on $R(g,n)$ which are new for large values of g. Fig. 1 shows the current upper and lower bounds on

$$\sigma(g) := \liminf_{n \to \infty} \frac{R(g,n)}{\sqrt{\lfloor g/2 \rfloor n}}.$$

We comment that it may be possible to replace the lim inf in the definition of σ with a simple lim, but that this has not been proven and is not important for the purposes of this paper. The lower bounds on $\sigma(g)$ are all presented in this paper; some are originally found in [19] ($g = 2, 3$), [11] ($g = 4$), and [5] ($g = 8, 10$) but for other g are new. Other than the precise asymptotics for the $g = 2$ and 3 cases (which were found in 1944 [6] and 1996 [17]), the upper bounds indicated in Fig. 1 are due to Green [9] when $g \leqslant 20$ is even; for all other values of g, the upper bounds are new and are the subject of a work in progress by the authors [14].

Essential to proving these bounds on $\sigma(g)$ is the consideration of

$$C(g,n) := \max_S \{|S|: S \subseteq \mathbb{Z}_n,\ \|S^*\|_\infty \leqslant g\}. \tag{2}$$

The function $C(g,n)$ gives the largest possible size of a subset of the integers modulo n whose pairwise sums (mod n) repeat at most g times. There is a sizable literature on $R(g,n)$, but little work has been done on $C(g,n)$. There is a growing consensus among researchers on Sidon's Problem that substantial further progress on the growth of $R(g,n)$ will require

Table 2
Min$\{n: R(g,n) \geqslant k\}$

	g									
k	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	$\leqslant 92$	$\leqslant 72$	31	29	20	18	16	15	14	13
13			37	34	24	21	18	17	16	15
14			44	40	28	26	21	19	18	17
15			$\leqslant 52$	$\leqslant 47$	32	29	24	22	20	19
16					36	34	27	24	22	21
17					$\leqslant 42$	$\leqslant 38$	30	28	24	23
18							34	32	27	25
19							$\leqslant 38$	$\leqslant 36$	30	28
20									33	31
21									$\leqslant 37$	35
21										$\leqslant 38$

a better understanding of $C(g,n)$. Theorems 1 and 2 below give the state-of-the-art upper and lower bounds.

Tables 2 and 3 contain exact values for $R(g,n)$ and $C(g,n)$, respectively, for small values of g and n. These tables have been established by direct (essentially exhaustive) computation. Specifically, Table 2 records, for given values of g and k, the smallest possible value of max S given that $S \subseteq \mathbb{Z}^+$, $|S| = k$ and $\|S^*\|_\infty \leqslant g$; in other words, the entry corresponding to k and g is $\min\{n: R(g,n) \geqslant k\}$. For example, the fact that the $(k,g) = (8,2)$ entry equals 35 records the fact that there exists an 8-element Sidon set of integers from [35] but no 8-element Sidon set of integers from [34].

To show that $R(2,35) \geqslant 8$, for instance, it is only necessary to observe that

$$S = \{1, 3, 13, 20, 26, 31, 34, 35\}$$

has 8 elements and $\|S^*\|_\infty = 2$. To show that $R(2,35) \leqslant 8$, however, seems to require an extensive search.

In the next section, we state our upper bounds on $C(g,n)$, lower bounds on $R(g,n)$ and $C(g,n)$, and constructions that demonstrate our lower bounds. In Section 3 we prove the bounds claimed in Section 2. Since the value of this work is primarily as a synthesis and extension of ideas from a variety of other works, we have endeavored to make this paper self-contained. We conclude in the final section by listing some questions that we would like, but have been unable, to answer.

Table 3
Min$\{n: C(g,n) \geqslant k\}$

	g									
k	2	3	4	5	6	7	8	9	10	11
3	6									
4	12	7								
5	21	11	8							
6	31	19	11	9						
7	48	29	14	13	10					
8	57	43	22	17	12	11				
9	73	57	28	19	16	13	12			
10	91		36	28	19	17	14	13		
11				35	22	21	18	15	14	
12					30	23	21	19	16	15
13						31	24	22	19	17
14							28	25		20

2. Theorems and constructions

2.1. Theorems

Theorem 1. (i) $\binom{C(2,n)}{2} \leqslant \lfloor \frac{n}{2} \rfloor$, *and in particular* $C(2,n) \leqslant \sqrt{n} + 1$;
(ii) $C(3,n) \leqslant \sqrt{n + 9/2} + 3$;
(iii) $C(4,n) \leqslant \sqrt{3n} + 7/6$;
(iv) $C(g,n) \leqslant \sqrt{gn}$ *for even* g;
(v) $C(g,n) \leqslant \sqrt{1 - \frac{1}{g}}\sqrt{gn} + 1$, *for odd* g.

Theorem 2. *Let q be a prime power, and let k, g, f, x, y be positive integers with $k < q$.*
(i) *If p is a prime, then* $C(2k^2, p^2 - p) \geqslant k(p-1)$;
(ii) $C(2k^2, q^2 - 1) \geqslant kq$;
(iii) $C(2k^2, q^2 + q + 1) \geqslant kq + 1$;
(iv) *If* $\gcd(x, y) = 1$, *then* $C(gf, xy) \geqslant C(g, x)C(f, y)$;
(v) $R(gf, xy) \geqslant R(gf, xy + 1 - \lceil \frac{y}{C(f,y)} \rceil) \geqslant R(g, x)C(f, y)$;
(vi) $R(g, 3g - \lfloor g/3 \rfloor + 1) \geqslant g + 2\lfloor g/3 \rfloor + \lfloor g/6 \rfloor$.

Theorem 3.

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

Theorem 4. *For* $g \geqslant 1$,

$$\sigma(2g+1) \geqslant \sigma(2g) \geqslant \frac{g + 2\lfloor g/3 \rfloor + \lfloor g/6 \rfloor}{\sqrt{3g^2 - g\lfloor g/3 \rfloor + g}}.$$

In particular,

$$\liminf_{g\to\infty} \sigma(g) \geqslant \frac{11}{\sqrt{96}}.$$

We note that Martin and O'Bryant have shown [14] that $\limsup_{g\to\infty} \sigma(g) < 1.8391$, whereas $11/\sqrt{96} > 1.1226$. These lower bounds on σ, together with the strongest known upper bounds, are plotted for $2 \leqslant g \leqslant 42$ in Fig. 1.

2.2. *Constructions*

Theorem 2 rests on the constructions given in the following four subsections. We denote the finite field with q elements by $\mathbb{F}_q$, and its multiplicative group by $\mathbb{F}_q^\times$.

2.2.1. *Ruzsa's construction*

Let θ be a generator of the multiplicative group modulo the prime p. For $1 \leqslant i < p$, let $a_{t,i}$ be the congruence class modulo $p^2 - p$ defined by

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

Define the set

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

Ruzsa [16] showed that $\texttt{Ruzsa}(p,\theta,1)$ is a Sidon set. We show that 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

$$\|\texttt{Ruzsa}(p,\theta,\mathcal{K})^*\|_\infty \leqslant 2|\mathcal{K}|^2.$$

For example, $\texttt{Ruzsa}(11,2,\{1,2\})$ is

$$\{7, 39, 58, 63, 65, 86, 92, 100, 101, 104\} \cup \{28, 47, 52, 54, 75, 81, 89, 90, 93, 106\}$$

and one may directly verify that $\|\texttt{Ruzsa}(11,2,\{1,2\})^*\|_\infty = 8$.

2.2.2. *Bose's construction*

Let q be any prime power, θ a generator of $\mathbb{F}_{q^2}$, $k \in \mathbb{F}_q$, and define the set

$$\texttt{Bose}(q,\theta,k) := \{a \in [q^2-1]\colon \theta^a - k\theta \in \mathbb{F}_q\}.$$

Bose [2] showed that for $k \neq 0$, $\texttt{Bose}(q, \theta, k)$ is Sidon set. We show that if $\mathcal{K}$ is any subset of $\mathbb{F}_q \setminus \{0\}$, then

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

is a subset of $\mathbb{Z}_{q^2-1}$, has $|\mathcal{K}|q$ elements, and

$$\|\texttt{Bose}(q, \theta, \mathcal{K})^*\|_\infty \leqslant 2|\mathcal{K}|^2.$$

For example, $\texttt{Bose}(11, x \bmod (11, x^2 + 3x + 6), \{1, 2\})$ is

$$\{1, 30, 38, 55, 56, 65, 69, 71, 76, 99, 118\}$$
$$\cup\{18, 26, 43, 44, 53, 57, 59, 64, 87, 106, 109\}.$$

2.2.3. *Singer's construction*

Sidon sets arose incidentally in Singer's work [19] on finite projective geometry. While Singer's construction gives a slightly thicker Sidon set than Bose's (which is slightly thicker than Ruzsa's), the construction is more complicated—even after the simplification of Bose and Chowla [3].

Let q be any prime power, and let θ be a generator of the multiplicative group of $\mathbb{F}_{q^3}$. For each $k_1, k_2 \in \mathbb{F}_q$ define the set

$$T(\langle k_1, k_2\rangle) := \{0\} \cup \{a \in [q^3 - 1]\colon \theta^a - k_2\theta^2 - k_1\theta \in \mathbb{F}_q\}.$$

Then define

$$\texttt{Singer}(q, \theta, \langle k_1, k_2\rangle)$$

to be the congruence classes modulo $q^2 + q + 1$ that intersect $T(\langle k_1, k_2\rangle)$. Singer proved that for $k_2 = 0$, $k_1 \neq 0$, $\texttt{Singer}(q, \theta, \langle k_1, k_2\rangle)$ is a Sidon set. We show that if $\mathcal{K} \subseteq \mathbb{F}_q \times \mathbb{F}_q$ does not contain two pairs with one an $\mathbb{F}_q$-multiple of the other, then

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

is a subset of $\mathbb{Z}_{q^2+q+1}$ with $|\mathcal{K}|q + 1$ elements and

$$\|\texttt{Singer}(q, \theta, \mathcal{K})^*\|_\infty \leqslant 2|\mathcal{K}|^2.$$

For example, $\texttt{Singer}(11, x \bmod (11, x^3 + x^2 + 6x + 4), \{\langle 1, 1\rangle, \langle 1, 2\rangle\})$ is

$$\{0, 9, 57, 59, 63, 81, 86, 97, 100, 112, 125, 132\}$$
$$\cup\{3, 15, 28, 35, 36, 45, 93, 95, 99, 117, 122\}.$$

2.2.4. The Cilleruelo, Ruzsa and Trujillo construction

Kolountzakis observed that if S is a Sidon set, and $S+1 := \{s+1: s \in S\}$, then $\|(S \cup (S+1))^*\|_\infty \leqslant 4$. This idea of interleaving several copies of the same Sidon set was extended incorrectly by Jia (but fixed by Lindström), and then correctly by Cilleruelo, Ruzsa and Trujillo and Habsieger and Plagne (to $h > 2$).

Let $S \subseteq \mathbb{Z}_x$ and $M \subseteq \mathbb{Z}_y$ have $\|S^*\|_\infty \leqslant g$ and $\|M^*\|_\infty \leqslant f$. Let $S' \subseteq [x]$ and $M' \subseteq [y]$ be corresponding sets of integers, i.e., $S = \{s \bmod x: s \in S'\}$. Now, let

$$M' + yS' := \{m + ys: m \in M', s \in S'\} \subseteq \mathbb{Z}.$$

The set

$$M + yS := \{t \bmod xy: t \in M' + yS'\} \subseteq \mathbb{Z}_{xy}$$

satisfies $\|(M + yS)^*\|_\infty \leqslant gf$.

3. Proofs

If S is a set of integers (or congruence classes), we use $S(x)$ to denote the corresponding indicator function. Also, we use the standard notations for convolution and correlation of two real-valued functions

$$S * T(x) = \sum_y S(y)T(x-y) \quad \text{and} \quad S \circ T(x) = \sum_y S(y)T(x+y).$$

For sets S, T of integers, $S * T(x)$ is the number of ways to write x as a sum $s+t$ with $s \in S$ and $t \in T$. Likewise, $S \circ T(x)$, is the number of ways to write x as a difference $t - s$.

3.1. Theorem 1

Part (i) is just the combination of the pigeonhole principle and the fact (which we prove below) that if $\|S*S\|_\infty \leqslant 2$, then for $k \neq 0$, $S \circ S(k) \leqslant 1$. Part (ii) follows from the observation that if $\|S * S\|_\infty \leqslant 3$, then $S \circ S(k) \leqslant 2$ for $k \neq 0$, and in fact $S \circ S(k) \leqslant 1$ for almost all k. Part (iii) follows an idea of Cilleruelo: if $\|S * S\|_\infty \leqslant 4$, then $S \circ S$ is small on average. For $g > 4$, the theorem is a straightforward consequence of the pigeonhole principle. We consider (iii) to be the interesting contribution.

Proof. (i) We show that $\binom{C(2,n)}{2} \leqslant \lfloor n/2 \rfloor$, whence $C(2,n) < \sqrt{n} + 1$. Let $S \subseteq [n]$ have $\|S^*\|_\infty \leqslant 2$. If $\{s_1, s_2\}$, $\{s_3, s_4\}$ are distinct pairs of distinct elements of S, and

$$s_1 - s_2 \equiv s_3 - s_4 \pmod{n}, \tag{3}$$

then $s_4 + s_1 \equiv s_1 + s_4 \equiv s_3 + s_2 \equiv s_3 + s_2$, contradicting the supposition that $\|S^*\|_\infty \leqslant 2$. Therefore, the map $\{s_1, s_2\} \mapsto \{\pm(s_1 - s_2)\}$ is 1-1 on pairs of distinct elements of S, and the image is contained in $\{\{\pm 1\}, \{\pm 2\}, \ldots, \{\pm \lfloor n/2 \rfloor\}\}$. Thus, $\binom{|S|}{2} \leqslant \lfloor n/2 \rfloor$.

This bound is actually achieved for $n = p^2 + p + 1$ when p is prime (see Theorem 2(iii)).

(ii) Now suppose that $\|S^*\|_\infty = 3$, and consider the pairs of distinct elements of S. Any solution to (3) must have $\{s_1, s_2\} \cap \{s_3, s_4\} \neq \emptyset$ since $\|S^*\|_\infty < 4$, and each of the $|S|$ possible intersections can occur only once. Therefore, after deleting one pair for each element of S, we get a set of $\binom{|S|}{2} - |S|$ pairs which is mapped 1-1 by $\{s_1, s_2\} \mapsto \{\pm(s_1 - s_2)\}$ into $\{\{\pm 1\}, \{\pm 2\}, \ldots, \{\pm\lfloor n/2 \rfloor\}\}$. This proves Theorem 1 for $g = 3$.

(iii) Now suppose that $\|S^*\|_\infty = 4$, where $S \subseteq \mathbb{Z}_n$. The obvious map from

$$X := \{((s_1, s_2), (s_3, s_4)) \colon s_1 - s_2 \equiv s_3 - s_4, s_1 \notin \{s_2, s_3\}\}$$

to

$$Y := \{((s_1, s_4), (s_3, s_2)) \colon s_1 + s_4 \equiv s_3 + s_2, \{s_1, s_4\} \not\equiv \{s_2, s_3\}\}$$

is easily seen to be 1-1 (but not necessarily onto): $|X| \leqslant |Y|$. We have

$$\begin{aligned}|X| &= \sum_{\substack{k \neq 0 \\ k \in \mathbb{Z}_n}} \left(S \circ S(k)^2 - S \circ S(k)\right) \geqslant \frac{1}{n-1} \left(\sum_{\substack{k \neq 0 \\ k \in \mathbb{Z}_n}} S \circ S(k) \right)^2 - \sum_{\substack{k \neq 0 \\ k \in \mathbb{Z}_n}} S \circ S(k) \\ &= \frac{(|S|^2 - |S|)^2}{n-1} - |S|^2 + |S|,\end{aligned}$$

$$|Y| = |(S * S)^{-1}(3)|\,4 + |(S * S)^{-1}(4)|\,8 \leqslant 4|S| + 8\frac{|S|^2 - |S|}{4} = 2|S|^2 + 2|S|.$$

Comparing the lower bound on $|X|$ with the upper bound on $|Y|$ yields $|S| \leqslant \sqrt{3n} + 7/6$.

(iv) and (v). There are $|S|^2$ pairs of elements from $S \subseteq \mathbb{Z}_n$, and there are just n possible values for the sum of two elements. If $\|S^*\|_\infty \leqslant g$ then each possible value is realized at most g times. Thus $|S|^2 \leqslant gn$. The only way a sum can occur an odd number of times is if it is twice an element of S, so for odd g, $|S|^2 \leqslant (g-1)n + |S|$. $\square$

3.2. Theorem 2

The first three parts of Theorem 2 are all proved in a similar manner, which we outline here. For disjoint sets $S_1, \ldots, S_k$, with $S = \cup S_i$, we have

$$S * S = (S_1 + \cdots + S_k) * (S_1 + \cdots + S_k) = \sum_{i,j=1}^{k} S_i * S_j$$

and since $S_i * S_j$ is nonnegative,

$$\|S * S\|_\infty \leqslant \sum_{i,j=1}^{k} \|S_i * S_j\|_\infty \leqslant k^2 \max_{1 \leqslant i,j \leqslant k} \|S_i * S_j\|_\infty.$$

To prove (i), we need to show that the sets $\mathtt{Ruzsa}(p, \theta, i)$ $(1 \leqslant i < p)$ are disjoint (hence $\mathtt{Ruzsa}(p, \theta, \mathcal{K})$ has cardinality $|\mathcal{K}|(p-1)$), and that

$$\|\mathtt{Ruzsa}(p, \theta, i) * \mathtt{Ruzsa}(p, \theta, j)\|_\infty \leqslant 2.$$

Specifically, we use unique factorization in $\mathbb{F}_p[x]$ to show that there are not 3 distinct pairs

$$(a_{r_m,i}, a_{v_m,j}) \in \mathtt{Ruzsa}(p,\theta,i) \times \mathtt{Ruzsa}(p,\theta,j)$$

with the same sum.

The proofs of (ii) and (iii) follow the same outline, but use unique factorization in $\mathbb{F}_q[x]$ and $\mathbb{F}_{q^2}[x]$, respectively.

Proof. (i) For the entirety of the proof, we work with fixed p and θ. It is therefore convenient to introduce the notation $R_k = \mathtt{Ruzsa}(p,\theta,k)$. We need to show that $R_i \cap R_j = \emptyset$ for $1 \leqslant i < j < p$, and that $\|R_i * R_j\|_\infty \leqslant 2$ (including the possibility $i = j$).

Suppose that $a_{m_1,i} = a_{m_2,j} \in R_i \cap R_j$, with $m_1, m_2 \in [1, p)$. We have $m_1 \equiv a_{m_1,i} = a_{m_2,j} \equiv m_2 \pmod{p-1}$, so $m_1 = m_2$. Reducing the equation $a_{m_1,i} = a_{m_2,j}$ modulo p, we find $i\theta^{m_1} \equiv j\theta^{m_2} = j\theta^{m_1} \pmod p$, so $i = j$. Thus for $i \neq j$, the sets R_i, R_j are disjoint.

Now suppose, by way of contradiction, that there are three pairs $(a_{r_m,i}, a_{v_m,j}) \in R_i \times R_j$ satisfying $a_{r_m,i} + a_{v_m,j} \equiv k \pmod{p^2 - p}$. Each pair gives rise to a factorization modulo p of

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

Factorization modulo p is unique, so it must be that two of the three pairs are congruent modulo p, say

$$a_{r_1,i} \equiv a_{r_2,i} \pmod p. \tag{4}$$

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

$$a_{r_1,i} \equiv a_{r_2,i} \pmod{p-1}. \tag{5}$$

Eqs. (4) and (5), together with

$$a_{r_1,i} + a_{v_1,j} \equiv k \equiv a_{r_2,i} + a_{v_2,j} \pmod{p^2 - p}$$

imply that the first two pairs are identical, and so there are *not* three such pairs. Thus, for each $k \in \mathbb{Z}_n$, we have shown that $R_i * R_j(k) \leqslant 2$.

(ii) For $k \in \mathbb{F}_q$, let $B_k = \mathtt{Bose}(q,\theta,k)$. We need to show that $|B_i| = q$, that $B_i \cap B_j = \emptyset$ for distinct $i, j \in \mathbb{F}_q \setminus \{0\}$, and that $\|B_i * B_j\|_\infty \leqslant 2$ (including the possibility that $i = j$).

Since $\{\theta, 1\}$ is a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, we can for each $s' \in [q^2 - 1]$ write $\theta^{s'}$ as a linear combination of θ and 1. We define s (unprimed) to be the coefficient of 1, i.e.,

$$\theta^{s'} = i\theta + s$$

for some i. In this proof, primed variables are integers between 1 and $q^2 - 1$, and unprimed variables are elements of $\mathbb{F}_q$. Note also that $a' = b'$ implies $a = b$, whereas $a = b$ does not imply $a' = b'$.

Since θ generates the multiplicative group, for $i \neq 0$ each $s \in \mathbb{F}_q$ has a corresponding s', so that $|B_i| = q$. Moreover, we know that $i\theta + s_1 = j\theta + s_2$ implies that $i = j$ and $s_1 = s_2$. In particular, if $i \neq j$, then $B_i \cap B_j = \emptyset$. Thus $|\mathtt{Bose}(q,\theta,\mathcal{K})| = |\mathcal{K}|q$.

We now fix i and j in $\mathbb{F}_p \setminus \{0\}$ (not necessarily distinct), and show that $B_i * B_j(k) \leqslant 2$ for $k \in \mathbb{Z}_{q^2-1}$. Define $c_1, c_2 \in \mathbb{F}_p$ by $(ij)^{-1}\theta^{k'} - \theta^2 = c_1\theta + c_2$, and consider pairs $(r', v') \in B_i \times B_j$ with $r' + v' \equiv k' \pmod{q^2-1}$. We have

$$\begin{aligned} c_1\theta + c_2 &= (ij)^{-1}\theta^{k'} - \theta^2 = (ij)^{-1}\theta^{r'+v'} - \theta^2 = (ij)^{-1}\theta^{r'}\theta^{v'} - \theta^2 \\ &= (ij)^{-1}(i\theta + r)(j\theta + v) - \theta^2 = (i^{-1}r + j^{-1}v)\theta + i^{-1}rj^{-1}v. \end{aligned}$$

This means that $(a, b) = (i^{-1}r, j^{-1}v)$ is a solution to $x^2 - c_1x + c_2 = (x - a)(x - b)$. By unique factorization over finite fields, there are at most two such pairs. Thus, $B_i * B_j(k) \leqslant 2$ and so $\|B_i * B_j\|_\infty \leqslant 2$.

(iii) We first note that θ^a and θ^b (for any integers a, b) are linearly dependent over $\mathbb{F}_q$ if and only if their ratio is in $\mathbb{F}_q$. Since $\mathbb{F}_q^\times$ is a subgroup of $\mathbb{F}_{q^3}^\times$, we see that $\mathbb{F}_q = \{\theta^{x(q^2+q+1)}: x \in \mathbb{Z}\}$. Thus, we have the following linear dependence criterion: θ^a and θ^b are linearly dependent if and only if $a \equiv b \pmod{q^2+q+1}$.

Since $\{\theta^2, \theta, 1\}$ is a basis for $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$, we can for each $s' \in [q^3 - 1]$ write $\theta^{s'}$ as a linear combination of θ^2, θ and 1. We define s (unprimed) to be the coefficient of 1, i.e.,

$$\theta^{s'} = k_2\theta^2 + k_1\theta + s$$

for some k_1, k_2. In this proof, primed variables are integers between 1 and $q^3 - 1$, and unprimed variables are elements of $\mathbb{F}_q$. Note, as above, that $a' = b'$ implies $a = b$, whereas $a = b$ does not imply $a' = b'$. We also define $\bar{s}$ to be the congruence class of the integer s' modulo $q^2 + q + 1$.

For $\vec{k} = \langle k_1, k_2\rangle \in \mathbb{F}_q^2$ define

$$T(\vec{k}) := \{s' \in [q^3 - 1] : \theta^{s'} = s + k_1\theta + k_2\theta^2, \quad s \in \mathbb{F}_q\}$$

which also reiterates the connection between primed variables (such as $s' \in [q^3 - 1]$) and unprimed variables (such as $s \in \mathbb{F}_q$). Define $S(\vec{k})$ to be the set of congruence classes modulo $q^2 + q + 1$ that intersect $T(\vec{k})$; as noted above, we denote the congruence class $s' \bmod q^2 + q + 1$ as $\bar{s}$. Let $\mathcal{K} = \{\vec{k}_1, \vec{k}_2, \ldots\} \subseteq \mathbb{F}_q \times \mathbb{F}_q$ be a set that does not contain two pairs with one being a multiple of the other. Let $S_1 := \{0\} \cup S(\vec{k}_1)$, and for $i > 1$ let $S_i := S(\vec{k}_i)$.

We need to show that $|S_1| = q + 1$, for $i > 1$ that $|S_i| = q$, and for distinct i and j, the sets S_i and S_j are disjoint. This will imply that

$$\texttt{Singer}(q, \theta, \mathcal{K}) = \bigcup_{i=1}^{|\mathcal{K}|} S_i$$

has cardinality $|\mathcal{K}|q + 1$. All of these are immediate consequences of the fact that each element of $\mathbb{F}_{q^3}$ has a unique representation as an $\mathbb{F}_q$-linear combination of θ^2, θ, and 1.

We will show that for any i, j (not necessarily distinct) there are not three pairs $(\bar{r}_m, \bar{v}_m) \in S_i \times S_j$ with the same sum modulo $q^2 + q + 1$.

Suppose that $\vec{k}_i = \langle k_1, k_2 \rangle$ and $\vec{k}_j = \langle \ell_1, \ell_2 \rangle$. Set $K(r, z) := r + k_1 z + k_2 z^2$ and $L(v, z) = v + \ell_1 z + \ell_2 z^2$. Since

$$\bar{r}_1 + \bar{v}_1 = \bar{r}_2 + \bar{v}_2 = \bar{r}_3 + \bar{v}_3,$$

there are constants $c_2, c_3 \in \mathbb{F}_q$ such that $\theta^{r'_1+v'_1} = c_2 \theta^{r'_2+v'_2} = c_3 \theta^{r'_3+v'_3}$, and since $\theta^{r'+v'} = \theta^{r'} \theta^{v'} = K(r, \theta) L(v, \theta)$, the polynomials

$$\begin{aligned} f_2(z) &:= c_2 K(r_2, z) L(v_2, z) - K(r_1, z) L(v_1, z), \\ f_3(z) &:= c_3 K(r_3, z) L(v_3, z) - K(r_1, z) L(v_1, z) \end{aligned}$$

both have θ as a root (we are assuming for the moment that none of $\bar{v}_m, \bar{r}_m$ are $\bar{0}$).

If $c_2 = 1$, then $f_2(z)$ is a quadratic with the cubic θ as a root: consequently $f_2(z) = 0$ identically. This gives three equations in the unknowns $r_1, v_1, r_2, v_2, k_1, k_2, \ell_1, \ell_2$. These equations with the assumption that $\langle k_1, k_2 \rangle$ is not a multiple of $\langle \ell_1, \ell_2 \rangle$, imply that $r_1 = r_2$ and $v_1 = v_2$. Thus $\theta^{r'_1} = \theta^{r'_2}$, and so $r'_1 = r'_2$, and so $(r'_1, v'_1) = (r'_2, v'_2)$, contrary to our assumption of distinctness. Similarly $c_3 \neq 1$ and $c_2 \neq c_3$.

Now

$$g(z) := (c_3 - 1) f_2(z) - (c_2 - 1) f_3(z)$$

is a quadratic with θ as a root. Setting its coefficients equal to 0 gives 3 equations:

$$\begin{aligned} 0 &= c_2(r_1 v_1 - r_2 v_2) + c_3(r_3 v_3 - r_1 v_1) + c_2 c_3 (r_2 v_2 - r_3 v_3), \\ 0 &= c_2(\ell_1(r_1 - r_2) + k_1(v_1 - v_2)) + c_3(\ell_1(r_3 - r_1) + k_1(v_3 - v_1)) \\ &\quad + c_2 c_3 (\ell_1(r_2 - r_3) + k_1(v_2 - v_3)), \\ 0 &= c_2(\ell_2(r_1 - r_2) + k_2(v_1 - v_2)) + c_3(\ell_2(r_3 - r_1) + k_2(v_3 - v_1)) \\ &\quad + c_2 c_3 (\ell_2(r_2 - r_3) + k_2(v_2 - v_3)). \end{aligned}$$

When combined with our knowledge that c_2, c_3 are not 0, 1, or equal, and $\langle k_1, k_2 \rangle$ not a multiple of $\langle \ell_1, \ell_2 \rangle$, this implies that the pairs $(\bar{r}_m, \bar{v}_m)$ are not distinct.

Now suppose that $\bar{r}_1 = 0$, $\bar{v}_1 \neq 0$, and set

$$\begin{aligned} f_2(z) &:= c_2 K(r_2, z) L(v_2, z) - L(v_1, z), \\ f_3(z) &:= c_3 K(r_3, z) L(v_3, z) - L(v_1, z). \end{aligned}$$

We have $f_2(\theta) = f_3(\theta) = 0$, and in particular

$$g(z) := c_3 f_2(z) - c_2 f_3(z)$$

is a quadratic with θ as a root. Setting the coefficients of $g(z)$ equal to 0 yields equations which, as before, with our assumptions about $c_2, c_3, k_1, k_2, \ell_1, \ell_2$, imply that the three pairs $(\bar{r}_m, \bar{v}_m)$ are not distinct. The case $\bar{r}_1 = \bar{v}_1 = 0$ is handled similarly. The case $\bar{r}_1 = \bar{v}_2 = 0$ is eliminated for distinct i, j by the disjointness of S_i and S_j, and for $i = j$ by the distinctness assumption on the three pairs.

Thus there are not such $(\bar{r}_m, \bar{v}_m)$ $(1 \leqslant m \leqslant 3)$, whether none of these six variables are 0, one of them is 0, or two of them are 0.

(iv) Consider $m_i, n_i \in M'$ and $s_i, t_i \in S'$ with

$$(m_1 + ys_1) + (n_1 + yt_1) \equiv \cdots \equiv (m_{gh+1} + ys_{gf+1}) \\ +(n_{gf+1} + yt_{gf+1}) \pmod{xy}. \tag{6}$$

We need to show that $m_i = m_j$, $s_i = s_j$, $n_i = n_j$, and $t_i = t_j$, for some distinct i, j. Reducing Eq. (6) modulo y, we see that $m_1 + n_1 \equiv m_2 + n_2 \equiv \cdots \equiv m_{gf+1} + n_{gf+1} \pmod{y}$. Since $\|M^*\|_\infty \leqslant f$, we can reorder the m_i, n_i, s_i, t_i so that $m_1 = m_2 = \cdots = m_{g+1}$ and $n_1 = n_2 = \cdots = n_{g+1}$. Reducing Eq. (6) modulo x we arrive at

$$ys_1 + yt_1 \equiv ys_2 + yt_2 \equiv \cdots \equiv ys_{g+1} + yt_{g+1} \pmod{x}$$

whence, since $\gcd(x, y) = 1$,

$$s_1 + t_1 \equiv s_2 + t_2 \equiv \cdots \equiv s_{g+1} + t_{g+1} \pmod{x}.$$

The $s_i \bmod x$ and $t_i \bmod x$ are from S, and $\|S^*\|_\infty \leqslant g$, so that for some distinct i, j, $s_i = s_j$ and $t_i = t_j$.

(v) Let $M \subseteq \mathbb{Z}_y$ have cardinality $C(f, y)$ and $\|M^*\|_\infty \leqslant f$. Set $M' = \{m \in [y]: m \bmod y \in M\}$. Let $S' \subseteq [0, r)$ have cardinality $R(g, r)$ and $\|(S')^*\|_\infty \leqslant g$. Set (with $x > 2r$) $S := \{s \bmod x: s \in S'\} \subseteq \mathbb{Z}_x$. By the construction in (iv) of this theorem $M + yS \subseteq \mathbb{Z}_{xy}$ has

$$\|(M + yS)^*\|_\infty \leqslant gf.$$

Since $M' + yS' \subseteq [y + yr]$ and $M' + yS' \equiv M + yS \pmod{xy}$, if $xy > 2(y + yr)$ then $\|(M' + yS')^*\|_\infty = \|(M + yS)^*\|_\infty \leqslant gf$.

We can shift M modulo y without affecting $|M|$ or $\|M^*\|_\infty$. Since there clearly must be two consecutive elements of M with difference at least $\lceil y/C(f, y)\rceil$, we may assume that $M' \subseteq [y - \lceil y/C(f, y)\rceil + 1]$. Thus,

$$M' + yS' \subseteq [y - \lceil y/C(f, y)\rceil + 1 + y(r-1)] = [yr + 1 - \lceil y/C(f, y)\rceil]$$

and

$$|M' + yS'| = |M||S'| = C(f, y)R(g, r).$$

This proves (v).

The reader might feel that the part of the argument concerning the largest gap in M is more trouble than it is worth. We include this for two reasons. First, Erdős [10, Problem C9] offered \$500 for an answer to the question, "Is $R(2, n) = \sqrt{n} + O(1)$?" This question would be answered in the negative if one could show, for example, that $\texttt{Bose}(p, \theta, 1)$ contains a gap that is not $O(p)$, as seems likely from the experiments of Zhang [20] and Lindström [13]. Second, there is some literature (e.g., [7,17]) concerning the possible size of the largest gap in a maximal Sidon set contained in $\{1, \ldots, n\}$. In short, we include this argument because there is some reason to believe that this is a significant source of the error term in at least one case, and because there is some reason to believe that improvement is possible.

(vi) The set

$$S := \left[0, \left\lfloor \frac{g}{3} \right\rfloor\right) \cup \left\{g - \left\lfloor \frac{g}{3} \right\rfloor + 2\left[0, \left\lfloor \frac{g}{6} \right\rfloor\right)\right\} \cup \left[g, g + \left\lfloor \frac{g}{3} \right\rfloor\right) \cup \left(2g - \left\lfloor \frac{g}{3} \right\rfloor, 3g - \left\lfloor \frac{g}{3} \right\rfloor\right]$$

has cardinality $g + 2\lfloor g/3 \rfloor + \lfloor g/6 \rfloor$, is contained in $[0, 3g - \lfloor g/3 \rfloor]$, and has

$$\|S^*\|_\infty = g + 2\left\lfloor \frac{g}{3} \right\rfloor + \left\lfloor \frac{g}{6} \right\rfloor.$$

We remark that this family of examples was motivated by the finite sequence

$$S = (1, 0, \tfrac{1}{2}, 1, 0, 1, 1, 1),$$

which has the property that its autocorrelations

$$S * S = (1, 0, 1, 2, \tfrac{1}{4}, 3, 3, 3, 3, 3, 3, 2, 3, 2, 1)$$

are small relative to the sum of its entries. In other words, the ratio of the ℓ^∞-norm of $S * S$ to the ℓ^1-norm of S itself is small. If we could find a finite sequence of rational numbers for which the corresponding ratio were smaller, it could possibly be converted into a family of examples that would improve the lower bound for $\underline{\rho}(2g)$ in Theorem 4 for large g. □

3.3. Theorems 3 and 4

Our plan is to employ the inequality of Theorem 2(v) when y is large, $f = 2$, and $x \approx \frac{8}{3}g$. In other words, we need nontrivial lower bounds for $C(2, y)$ for $y \to \infty$ and for $R(g, x)$ for values of x that are not much larger than g. The first need is filled by Theorem 2(i), (ii) or (iii), while the second need is filled by Theorem 2(vi).

For any positive integers x and $m \leqslant \sqrt{n/x}$, the monotonicity of R in the second variable gives $R(2g, n) \geqslant R(2g, x(m^2 - 1)) \geqslant R(g, x)C(2, m^2 - 1)$ by Theorem 2(v). If we choose m to be the largest prime not exceeding $\sqrt{n/x}$ (so that $m \gtrsim \sqrt{n/x}$ by the Prime Number Theorem), Then Theorem 2(ii) gives $R(2g, n) \geqslant R(g, x) \cdot m \gtrsim R(g, x)\sqrt{n/x}$ for any fixed positive integer g, and hence

$$\sigma(2g) = \liminf_{n\to\infty} \frac{R(2g, n)}{\sqrt{gn}} \geqslant \liminf_{n\to\infty} \frac{R(g, x)\sqrt{n/x}}{\sqrt{gn}} = \frac{R(g, x)}{\sqrt{gx}}.$$

The problem now is to choose x so as to make $R(g, x)/\sqrt{gx}$ as large as we can manage for each g. For $g = 2, 3, \ldots, 11$, we use Table 2 to choose $x = 7, 5, 31, 9, 20, 15, 30, 24, 33$, and 25, respectively (see Table 4 for witnesses to the values claimed for $R(g, x)$). This yields Theorem 3.

We note that Habsieger and Plagne [11] have proven that $R(2, x)/\sqrt{2x}$ is actually maximized at $x = 7$. For $g > 2$, we have chosen x based solely on the computations reported in Table 2. For general g, it appears that $R(g, x)/\sqrt{gx}$ is actually maximized at a fairly small value of x, suggesting that this construction suffers from "edge effects" and is not best possible.

Table 4
Important values of $R(g, x)$ and witnesses

g	x	$R(g,x)$	Witness	$R(g,x)/\sqrt{gx}$
2	7	4	{1, 2, 5, 7}	$\sqrt{8/7} \approx 1.069$
3	5	4	{1, 2, 3, 5}	$\sqrt{16/15} \approx 1.033$
4	31	12	{1, 2, 4, 10, 11, 12, 14, 19, 25, 26, 30, 31}	$\sqrt{36/31} \approx 1.078$
5	9	7	{1, 2, 3, 4, 5, 7, 9}	$\sqrt{49/45} \approx 1.043$
6	20	12	{1, 2, 3, 4, 5, 6, 9, 10, 13, 15, 19, 20}	$\sqrt{6/5} \approx 1.095$
7	15	11	{1, 2, 3, 7, 8, 9, 10, 11, 12, 13, 15}	$\sqrt{121/105} \approx 1.073$
8	30	17	{1, 2, 5, 7, 8, 9, 11, 12, 13, 14, 16, 18, 26, 27, 28, 29, 30}	$\sqrt{289/240} \approx 1.097$
9	24	16	{1, 2, 3, 4, 5, 6, 7, 8, 9, 13, 14, 15, 17, 22, 23, 24}	$\sqrt{32/27} \approx 1.089$
10	33	20	{1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 13, 15, 20, 21, 22, 23, 30, 31, 32, 33}	$\sqrt{40/33} \approx 1.101$
11	25	18	{1, 2, 3, 4, 5, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 25}	$\sqrt{324/275} \approx 1.085$

The first assertion of Theorem 4 is the immediate consequence of the obvious $R(2g+1, n) \geqslant R(g, n)$. To prove the lower bound on $\sigma(2g)$, we set $x = 3g - \lfloor g/3 \rfloor + 1$ and appeal to Theorem 2(vi).

We remark that the above proof gives the more refined result

$$R(2g, n) \geqslant \frac{11}{8\sqrt{3}} \sqrt{2gn}\Big(1 + O\Big(g^{-1} + \Big(\frac{n}{g}\Big)^{(\alpha-1)/2}\Big)\Big)$$

as $\frac{n}{g}$ and g both go to infinity, where $\alpha < 1$ is any number such that for sufficiently large y, there is always a prime between $y - y^{\alpha}$ and y. For instance, we can take $\alpha = 0.525$ by Baker et al. [1]. This clarification implies the final assertion of the theorem for even g, and the obvious inequality $R(2g+1, n) \geqslant R(2g, n)$ implies the final assertion for odd g as well.

4. Significant open problems

It seems highly likely that

$$\lim_{n\to\infty} \frac{R(g,n)}{\sqrt{n}}$$

is well-defined for each g, but this is known only for $g = 2$ and 3. It also seems likely that

$$\lim_{n\to\infty} \frac{R(2g,n)}{R(2g+1,n)} = 1.$$

The evidence so far is consistent with the conjecture $\lim_{g\to\infty} \sigma(g) = \sqrt{2}$.

One truly outstanding problem is to construct sets $S \subseteq \mathbb{Z}$ with $\|S^*\|_\infty = 4$ that are not the union of two Sidon sets. In fact, all known constructions of sets with $\|S^*\|_\infty \leqslant g$ are not native, but are built up by combining Sidon sets. It seems doubtful that this type of construction can be asymptotically densest possible. The asymptotic growth of $R(4, n)$, or even of $C(4, n)$, is a major target.

As a computational observation, the set $S = B_{\langle 1,0\rangle} \cup B_{\langle 1,1\rangle} \cup B_{\langle 1,2\rangle}$, where

$$B_{\langle k_1,k_2\rangle} := \{a' \in [q^3 - 1]\colon \theta^{a'} - k_2\theta^2 - k_1\theta \in \mathbb{F}_q\}$$

and θ generates the multiplicative group of $\mathbb{F}_{q^3}$, has the property that

$$S * S * S(k) = \left|\left\{(s_1, s_2, s_3)\colon s_i \in S, \sum s_i = k\right\}\right| \leqslant 81,$$

even when the sums are considered modulo $q^3 - 1$. As such, it seems likely that the generalizations of Bose's and Singer's constructions given in this paper generalize further to give sets whose h-fold sums repeat a bounded number of times. Proving this, however, will require a more efficient handling of systems of equations than is presented in the current paper.

We direct our readers to the survey and annotated bibliography [15] for the current status of these and other open problems related to Sidon sets.

Acknowledgments

The authors thank Heini Halberstam for thoughtful readings of this manuscript and numerous helpful suggestions. G. Martin was supported in part by grants from the Natural Sciences and Engineering Research Council. K. O'Bryant was supported by an NSF-VIGRE fellowship and by NSF grant DMS-0202460.

References

[1] R.C. Baker, G. Harman, J. Pintz, The difference between consecutive primes. II, Proc. London Math. Soc. 3 (83) (2001) 532–562 MR 1851081.
[2] R.C. Bose, An affine analogue of Singer's theorem, J. Indian Math. Soc. (N.S.) 6 (1942) 1–15 MR 0006735.
[3] R.C. Bose, S. Chowla, Theorems in the additive theory of numbers, Comment. Math. Helv. 37 (1962/1963) 141–147 MR 0144877.
[5] J. Cilleruelo, I.Z. Ruzsa, C. Trujillo, Upper and lower bounds for finite $B_h[g]$ sequences, J. Number Theory 97 (2002) 26–34 MR 1939134.
[6] P. Erdős, On a problem of Sidon in additive number theory and on some related problems, Addendum, J. London Math. Soc. 19 (1944) 208 MR 0014111.
[7] P. Erdős, A. Sárközy, V.T. Sós, On sum sets of Sidon sets II, Israel J. Math. 90 (1995) 221–233 MR 1336324.
[8] P. Erdős, P. Turán, On a problem of Sidon in additive number theory, and on some related problems, J. London Math. Soc. 16 (1941) 212–215 MR 0006197.
[9] B. Green, The number of squares and $B_h[g]$ sets, Acta Arith. 100 (2001) 365–390 MR 1862059.
[10] R.K. Guy, Unsolved problems in number theory, Problem Books in Mathematics, Springer, New York, 1994 ISBN 0-387-94289-0, MR 1299330.
[11] L. Habsieger, A. Plagne, Ensembles $B_2[2]$: l'étau se resserre, Integers 2 (2002) (Paper A2) 20 (electronic), MR 1896147 (French).
[12] M.N. Kolountzakis, The density of $B_h[g]$ sequences and the minimum of dense cosine sums, J. Number Theory 56 (1996) 4–11 MR 1370193.
[13] B. Lindström, Finding finite B_2-sequences faster, Math. Comput. 67 (1998) 1173–1178 MR 1484901.
[14] G. Martin, K. O'Bryant, Upper bounds for generalized Sidon sets, arXiv:math.NT/0210041.
[15] K. O'Bryant, A complete annotated bibliography of work related to sidon sequences, Electron. J. Combin. Dynamic Survey 11 (2004) 39 (electronic).

[16] I.Z. Ruzsa, Solving a linear equation in a set of integers I, Acta Arith. 65 (1993) 259–282 MR 1254961.
[17] I.Z. Ruzsa, Sumsets of Sidon sets, Acta Arith. 77 (1996) 353–359 MR 1414515.
[18] S. Sidon, Ein Satz über trigonometrische polynome und seine anwendung in der theorie der Fourier–Reihen, Math. Ann. 106 (1932) 536–539.
[19] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938) 377–385 MR 1501951.
[20] Zhen Xiang Zhang, Finding finite B_2-sequences with larger $m - a_m^{1/2}$, Math. Comput. 63 (1994) 403–414 MR 1223235.