An upper bound on the size of Sidon sets

[*]József Balogh, [†]Zoltán Füredi, [‡]Souktik Roy

Abstract. A classical combinatorial number theory problem is to determine the maximum size of a Sidon set of $\{1, 2, \ldots, n\}$, where a subset of integers is *Sidon* if all its pairwise sums are different. For this entry point into the subject, combining two elementary proofs, we decrease the gap between the upper and lower bounds by 0.2% for infinitely many values of n. We show that the maximum size of a Sidon set of $\{1, 2, \ldots, n\}$ is at most $\sqrt{n} + 0.998n^{1/4}$ for n sufficiently large.

1. AN ABBREVIATED HISTORY: In 1932 S. Sidon asked a question of a fellow student P. Erdős. Their advisor was L. Fejér, an outstanding mathematician (cf. Fejér kernel) working on summability of infinite series, who had a number of outstanding students who contributed to mathematical analysis including M. Fekete 1909 [Fekete's Lemma, see [**9**]], G. Pólya 1912, John von Neumann 1926, P. Erdős 1934, P. Turán 1935, and V. T. Sós 1957. Studying the L_p-norm of certain Fourier series, Sidon [**18**] proposed the following problem, which we present here in contemporary wording.

A set of numbers A is a *Sidon set*, or alternately a B_2*-set*, if $a + b = c + d$, $a, b, c, d \in A$ imply $\{a, b\} = \{c, d\}$, i.e., all pairwise sums are distinct. Note that here do not require that all numbers are different, i.e., $1 + 3 = 2 + 2$ is not allowed either.

Let $S(n)$ denote the maximum size a Sidon set $A \subset \{1, 2, \ldots, n\} =: [n]$ can have. As each pair of elements of A has a different sum, and the number of possibilities is $2n - 1$, we have $\binom{|A|+1}{2} \leq 2n - 1$, implying $S(n) \leq 2\sqrt{n}$. The sequence of powers of 2, i.e., $1, 2, 4, 8, \ldots$ is an infinite Sidon set showing $S(n) > \log_2 n$. It is rather difficult to construct large Sidon sets, but Sidon found one showing $S(n) > n^{1/4}$. Erdős immediately observed that the greedy algorithm gives $S(n) \geq n^{1/3}$ as follows. If $A \subset [n]$ and $n > |A|^3$ then one can always find an $x \in [n]$ such that x cannot be written as $x = a + b - c$, $a, b, c \in A$. Then $A \cup \{x\}$ is a Sidon set as well. In 1941, Erdős and Turán [**7**] observed that a result of Singer [**19**] implies that $S(n) > \sqrt{n}$ infinitely many times. Erdős and Turán [**7**] also proved, but did not state in that form, which was done much later by Cilleruelo [**4**], that

$$S(n) < n^{1/2} + n^{1/4} + \frac{1}{2}. \tag{1.1}$$

Lindström [**13**] in 1969 gave a different proof for $S(n) < n^{1/2} + n^{1/4} + 1$.

The study of Sidon sets became a classic topic of additive number theory; see e.g., the survey by O'Bryant [**3**]. The notion can be extended in a natural way to (finite)

[*] Department of Mathematical Sciences, University of Illinois at Urbana-Champaign, IL, USA. e-mail: jobal@illinois.edu. Research supported by NSF RTG Grant DMS-1937241, NSF Grant DMS-1764123 and Arnold O. Beckman Research Award (UIUC) Campus Research Board 18132, the Langan Scholar Fund (UIUC) and the Simons Fellowship.

[†] Alfréd Rényi Institute of Mathematics, Budapest, Hungary. and Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL, USA. e-mail: z-furedi@illinois.edu. Research was supported in part by NKFIH grant KH130371 and NKFI–133819.

[‡] Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL, USA. e-mail: souktik2@illinois.edu.

groups and fields of characteristic zero see, e.g., Cilleruelo [**5**]. Many authors apply deep tools, although Ben Green [**11**] notes that some approaches via Fourier analysis have the same spirit as the one in Erdős-Turán [**7**].

The upper bound in (1.1) has remained the same since 1941. Erdős [**6**] offered $500 for a proof or disproof that for every $\varepsilon > 0$ the equality $S(n) < \sqrt{n} + o(n^{\varepsilon})$ holds.

The aim of this paper, the main result: We improve the current best upper bound by $\Theta(n^{1/4})$.

Theorem 1. *There exists a constant $\gamma \geq 0.002$ and a number n_0 such that for every $n > n_0$*

$$S(n) < n^{1/2} + n^{1/4}(1 - \gamma).$$

In Section 2, we recall Lindström's argument [**13**] and point out how introducing a slack term in a critical inequality can imply possible improvements downstream. In Section 3, we present a different proof, a generalized version of an argument of Ruzsa [**17**]. We put his proof into a different framework and we explain, how introducing a slack term in a critical inequality there as well can lead to a possible improvement. In Section 4, we put the two proof methods together and leverage conditions on these slack terms to get Theorem 1. In fact, we show that a very dense Sidon set must have large discrepancy on some initial segment of $[n]$, for related results see Cilleruelo [**5**], Erdős and Freud [**8**].

Our second aim is to have a self-contained introduction to Sidon sets, so we include Bose's construction, a lower bound $S(n) \geq \sqrt{n+1}$ for infinitely many values of n.

Overall, we do not think that our work deserves 0.2% of Erdős' prize money, i.e., $1, but we want to emphasize here the wonderful unity of mathematics by showing the many remarkable connections Sidon's problem has not only to Fourier analysis but also to abstract algebra and coding and graph theory as well.

2. LINDSTRÖM'S UPPER BOUND:

In this Section we explain Lindström's [**13**] proof. Recall that A is a Sidon set if all pairwise sums of its elements are distinct, except $a + b = b + a$.

Proof. Let the elements of A be $a_1 < \ldots < a_k$. Given $i < j$, call $j - i$ the *order* of the difference $a_j - a_i$. We sum all differences of order at most ℓ, where ℓ will be chosen later to be around $n^{1/4}$. There are $(k-1) + (k-2) + \ldots + (k-\ell) = \ell(k - \frac{\ell+1}{2})$ such differences. By the Sidon property these differences are all distinct. We obtain the lower bound

$$\frac{1}{2}\ell^2\left(k - \frac{\ell+1}{2}\right)^2 < 1 + 2 + \ldots + \ell\left(k - \frac{\ell+1}{2}\right) \leq \sum_{1 \leq i < j \leq k,\, j \leq i+\ell} (a_j - a_i). \tag{2.1}$$

To simplify the sum on the right hand side, observe that for every $1 \leq i \leq r$, with $t := \lfloor (n-i)/r \rfloor$

$$(a_{r+i} - a_i) + (a_{2r+i} - a_{r+i}) + \ldots + (a_{tr+i} - a_{(t-1)r+i}) = a_{tr+i} - a_i \leq n - 1.$$

Using this, due to cancellation, we have that the sum of all differences of order r is at most $r \cdot n$. Hence, the sum of differences of order at most ℓ is at most $\binom{\ell+1}{2}n$.

Comparing with the right hand side of (2.1), we obtain

$$\frac{1}{2}\ell^2\left(k-\frac{\ell+1}{2}\right)^2 < \sum_{1\le i<j\le k,\, j\le i+\ell}(a_j-a_i) < \frac{1}{2}\ell(\ell+1)n. \tag{2.2}$$

Rearranging, we have $k-\frac{\ell+1}{2} < \sqrt{n(\ell+1)/\ell}$ which, using $\sqrt{1+x}\le 1+x/2$, leads to

$$k < \sqrt{n}+\frac{\sqrt{n}}{2\ell}+\frac{\ell}{2}+\frac{1}{2}.$$

Substituting $\ell := \lfloor n^{1/4}\rfloor$ yields $k < n^{1/2}+n^{1/4}+1$. ■

A Possible Improvement, Slackness: If the set of differences $\{(a_j-a_i) : 1\le i< j\le k,\, j\le i+\ell\}$ contains large values, then one can obtain a better inequality in (2.1), which would improve the upper bound on k. We formalize this idea by defining the non-negative slack term $C = C(A,\ell)$ as follows:

$$C = C(A,\ell) := \left(\sum_{1\le i<j\le k,\, j\le i+\ell}(a_j-a_i)\right) - \sum_{1\le i\le \ell(k-(\ell+1)/2)} i. \tag{2.3}$$

We can add C, or any lower bound for it, to the left hand side of (2.2) to obtain

$$k-\frac{\ell+1}{2} < \sqrt{\left(1+\frac{1}{\ell}-\frac{2C}{\ell^2 n}\right)n}.$$

Using $\sqrt{1+x}\le 1+x/2$, we conclude

$$k < \sqrt{n}+\frac{\sqrt{n}}{2\ell}-\frac{C}{\ell^2\sqrt{n}}+\frac{\ell}{2}+\frac{1}{2}.$$

An important feature of this inequality is that it is stable in the following sense. If we use a somewhat smaller ℓ, then the upper bound on k changes only a little bit. We shall substitute $\ell = (1-\alpha)n^{1/4}$ with some $0\le\alpha<1$, and use it as follows:

$$k < n^{1/2}+n^{1/4}-\frac{2C/n-n^{1/4}\alpha^2(1-\alpha)}{2(1-\alpha)^2}+\frac{1}{2}. \tag{2.4}$$

If we knew $C=\Omega(n^{5/4})$ and α was sufficiently small, then Theorem 1 would follow.

3. SAME BOUND VIA SET SYSTEMS

An inequality from coding theory: The following theorem is usually attributed to Johnson [**12**], who used it to establish upper bounds for error-correcting codes. It was rediscovered several times, e.g., Bassalygo [**2**]. In hypergraph language (as in Lovász's exercise book [**15**]), it is a statement about the size of the ground set of a set system with restricted intersection sizes.

Theorem 2. *Let $\mathcal{A}$ be a family of k-sets $A_1,\dots,A_m$ such that the intersection $A_i\cap A_j$ of any distinct pair has cardinality at most t. Then $v := |\cup A_i| \ge \frac{k^2m}{tm+k-t}$.*

Proof. Let d_x be the number of sets A_i containing the vertex x. Given A_i, we have $\sum_j |A_i \cap A_j| \le (m-1)t + k$. This leads to the following chain of inequalities:

$$tm(m-1) + mk \ge \sum_i \left(\sum_j |A_i \cap A_j| \right) = \sum d_x^2 \ge \frac{(\sum d_x)^2}{v} = \frac{k^2 m^2}{v}. \quad (3.1)$$

■

A second combinatorial proof: Here we give a second proof of (1.1). The proof is a generalized version of an argument of Ruzsa [**17**], which is slightly different from the original proof of Erdős and Turán [**7**]. In our proof we are going to use Johnson's inequality, Theorem 2, directly. It is an interesting phenomenon that the two different proofs give exactly the same bound.

Proof. Set $k := |A|$, m a positive integer, and $A_i := A + (i-1)$ for $i = 1, \dots, m$. Note that $\cup A_i \subseteq [n+m-1]$. The crucial observation is that $|A_i \cap A_j| \le 1$ for $i \ne j$. Indeed, if there are two distinct elements $x, y \in A_i \cap A_j$ for some $i < j$ then there would exist elements $a, b, c, d \in A$ with $a + i = x = b + j$ and $c + i = y = d + j$, which would give us $a + d = b + c$. Since A is a Sidon set, this forces $\{a, d\} = \{b, c\}$ hence $x = y$, and Theorem 2 is applicable with $t = 1$, $v \le n + m - 1$, and we get

$$(n + m - 1)(m + k - 1) \ge k^2 m.$$

Suppose $k \ge n^{1/2} + n^{1/4}$ and define $m := \lceil n^{3/4} \rceil$. Then $(n + m - 1)/k < \sqrt{n}$, so we obtain $\sqrt{n}(m + k - 1) > km$. This leads to

$$k < \sqrt{n} \frac{m-1}{m - \sqrt{n}} \le n^{1/2} \frac{n^{3/4} - 1}{n^{3/4} - n^{1/2}} = n^{1/2} + n^{1/4} + 1.$$

This is Lindström's bound. A more careful calculation, what we omit, yields (1.1). ■

A possible improvement using variance: Consider the family $\mathcal{A}$ in Theorem 2. One can naturally have the idea that the lower bound in (3.1) can be improved if one knows that the variance of the degree sequence $\{d_x\}$ is large, as the relation $\sum d_x^2 \ge (\sum d_x)^2 / v$ could be improved if the values are not equal to each other. We will utilize the fact that for our shifted set system, the degrees in an appropriate initial segment (and similarly in an end segment) are necessarily much smaller than the average, i.e., the degree sequence cannot be totally smooth.

Define the non-negative *defect* term $K(\mathcal{A})$ as the difference, where $d_{ave} = \sum d_x / v$,

$$K(\mathcal{A}) := \sum d_x^2 - \frac{(\sum d_x)^2}{v} \quad = \sum_x (d_{ave} - d_x)^2.$$

We also call $K(\mathcal{A})$ or any lower bound K of it a "*gain*". Instead of (3.1) one obtains

$$tm(m-1) + mk \ge \frac{k^2 m^2}{v} + K. \quad (3.2)$$

Using $t = 1$ and $v \leq n + m - 1$ we obtain

$$m + k - 1 > \frac{k^2 m}{n + m} + \frac{K}{m}.$$

This rearranges to

$$\left(k - \frac{n+m}{2m}\right)^2 < (n+m)\left(1 + \frac{m+n}{4m^2} - \frac{1}{m} - \frac{K}{m^2}\right) < (n+m)\left(1 - \frac{4K - n}{4m^2}\right).$$

Define $m := \lfloor n^{3/4} \rfloor$, and suppose that $K < 2n^{3/2}$, as otherwise one could easily obtain much stronger results. Using $\sqrt{1+x} \leq 1 + x/2$, we have

$$k < \frac{n+m}{2m} + \sqrt{n} \cdot \sqrt{1 + \frac{m}{n} - \frac{4K-n}{4m^2} - \frac{4K-n}{4mn}} \leq n^{1/2} + n^{1/4} - \frac{K}{2n} + 2. \tag{3.3}$$

We shall use later that if $K > 2\gamma n^{5/4} + 4n$, then (3.3) implies Theorem 1.

Recall the following corollary of the Cauchy-Schwarz inequality about the variance of numbers.

Lemma 3. Let $(y_1, \ldots, y_v)$ be a sequence of real numbers with average d. For a subset $X \subseteq [v]$ the average of the elements of $\{d_x : x \in X\}$ is denoted by d_X. Then $\sum (d - y_i)^2 \geq |X|(d - d_X)^2$.

Proof. We have

$$\sum_{i \in [v]} (d - y_i)^2 \geq \sum_{x \in X} (d - y_x)^2 = |X|(d - d_X)^2 - |X| d_X^2 + \sum_{x \in X} y_x^2.$$

■

4. PUTTING THE TWO METHODS TOGETHER: PROOF OF THEOREM 1

Proof of Theorem 1. The proof is a combination of the proofs in the previous two sections. The first proof provides a better bound, unless all the differences $a_i - a_j$ are "small" when i and j are close to each other, and the second proof gives a better bound, unless all the degrees are "close" to each other. We prove that both cannot happen at the same time, which implies our result.

Recall that $A = \{a_1, a_2, \ldots, a_k\} \subset [n]$ is a Sidon set, $a_1 < \ldots < a_k$, $m = \lfloor n^{3/4} \rfloor$ is a positive integer, and $\mathcal{A}$ is the family $\{A_i : A_i := A + (i-1)$ for $i = 1, \ldots, m\}$ with degree sequence $\{d_1, \ldots, d_{n+m-1}\}$. We may suppose that $n^{1/2} + \frac{1}{2} n^{1/4} < k < n^{1/2} + n^{1/4} + 1/2$, hence the average degree $d := \frac{km}{n+m-1} = n^{1/4} + O(1)$.

In this section we fix a "small" $\alpha > 0$ and a "smaller" β, and an ε to get a positive γ satisfying (4.1). E.g., one can choose $\alpha = 0.137$, $\beta = 0.037$, $\varepsilon = 0.235$ and any γ with $0.00204 \geq \gamma > 0.002$, then these values satisfy

$$\min\left\{\varepsilon^2 \beta, \frac{2(1 - \alpha - 2\varepsilon)^2(\alpha - 2\beta) - \alpha^2(1-\alpha)}{2(1-\alpha)^2}\right\} > \gamma. \tag{4.1}$$

We also define $s = \lfloor \beta n^{3/4} \rfloor$, $r_1 = |A \cap [s]|$, $r_2 = |A \cap [n+1-s, n]|$, $r = r_1 + r_2$, $R_1 := |A \cap [m-s]|$, $R_2 := |A \cap [n+1-m+s, n]|$, $R = R_1 + R_2$, and $\ell =$

$\lfloor(1-\alpha)n^{1/4}\rfloor$. Recall that $K = K(\mathcal{A}) := \sum d_x^2 - (\sum d_x)^2/(n+m-1)$. In the course of the proof we distinguish three cases: $r \le 2(1-\varepsilon)n^{1/4}$, and $R \ge 2(1+\varepsilon)n^{1/4}$, and $2(1-\varepsilon)n^{1/4} < r \le R < 2(1+\varepsilon)n^{1/4}$. ■

The density of the initial segments of A: The first main idea is to have a closer look at the variance of the degree sequence of $\mathcal{A}$.

In the claim below, we handle the case when A contains only few small numbers (i.e., $|A \cap [s]|$ is “small”) or only few large numbers. In this case, the degrees in the end segments will be lower than the average degree, and Lemma 3 will be applicable.

Claim 4. If $r \le 2(1-\varepsilon)n^{1/4}$ then $K \ge 2\varepsilon^2\beta n^{5/4} + O(n)$.

Proof. Let $d_X = (\sum_{x\in X} d_x)/|X|$ be the average of the degrees for the elements of a set $X \subset [n+m-1]$. By the definition of the defect $K = K(\mathcal{A})$ and by Lemma 3 we have $K = \sum_x (d-d_x)^2 \ge |X|(d-d_X)^2$. For $X = [s] \cup [n+m-s, n+m-1]$ we have

$$d_X \;=\; \frac{1}{|X|}\sum_{i\in X} d_i \;=\; \frac{1}{2s}\sum_{1\le j\le s}\left(|A\cap[j]| + |A\cap[n+1-j,n]|\right)$$

$$\le \frac{1}{2}|A\cap([s]\cup[n+1-s,n])| \;=\; \frac{r}{2} \;\le\; (1-\varepsilon)n^{1/4}.$$

Using $d - \frac{r}{2} \ge \varepsilon n^{1/4} + O(1)$, $|X| = 2s$, and $s = \beta n^{3/4} + O(1)$, the inequality $K \ge |X|(d-d_X)^2$ yields the required lower bound. ■

In the claim below we consider the case when A contains too many small numbers (i.e., $|A\cap[m-s]|$ is “too large”) or too many large numbers. (Note that we consider the interval $[m-s]$ which is small compared to $[n+m-1]$ but larger than $[s]$ from Claim 4). In this case, the degrees in these end segments will be larger than the average degree, and Lemma 3 will be applicable.

Claim 5. If $R \ge 2(1+\varepsilon)n^{1/4}$ then $K \ge 2\varepsilon^2\beta n^{5/4} + O(n)$.

Proof. Set $X = [m-s+1,m] \cup [n, n+s-1]$. Every $x \in [m-s+1,m]$ gets covered $|A\cap[m-s]| = R_1$ times just by the translates of $A\cap[m-s]$. Similarly, every $x \in [n,n+s-1]$ gets covered at least $|A\cap[n+1-m+s,n]| = R_2$ times. Hence, $|d_X - d| \ge \frac{R}{2} - d \ge \varepsilon n^{1/4}$, and using $|X| = 2s$ and $s = \beta n^{3/4} + O(1)$, the application of Lemma 3 completes the proof. ■

Large gaps in A: If Claims 4 and 5 are not applicable to A, then there is an interval of size about $n^{3/4}$, which contains very few elements of A. This means that A contains many pairs of numbers, whose indices are close to each other, but their difference is large.

The segment $[s+1,m-s]$ contains $R_1 - r_1$ members of A, similarly $[n+1-m+s, n-s]$ contains $R_2 - r_2$ of them, which adds up to $R-r$. After having Claims 4 and 5, we may assume that $2(1-\varepsilon)n^{1/4} < r \le R < 2(1+\varepsilon)n^{1/4}$, hence $A\cap([s+1,m-s]\cup[n+1-m+s,n-s])$ has fewer than $R - r < 4\varepsilon n^{1/4}$ elements. Using these assumptions, we shall slightly modify the proof of (1.1) by defining $\ell = \lfloor(1-\alpha)n^{1/4}\rfloor$.

The second idea of the proof is that with ℓ defined as above we can find many differences $a_j - a_i$ of small order which are significantly larger than $k\ell$, hence we give a lower bound for $C(A, \ell)$, which was defined in (2.3). This provides the right hand side bound in (4.1).

Claim 6. If $2(1-\varepsilon)n^{1/4} < r \le R < 2(1+\varepsilon)n^{1/4}$ and ℓ, k, and m are defined as above, then

$$C(A, \ell) > (1-\alpha-2\varepsilon)^2(\alpha-2\beta)n^{5/4} + O(n).$$

Proof. Consider the pairs (a_i, a_j) with $a_i \le s < m - s < a_j$ and $j \le i + \ell$. Each such pair appears in the definition of $C(A, \ell)$ and each of such difference $a_j - a_i$ is at least $m - 2s$, which exceeds $\ell(k - (\ell+1)/2)$, as $\alpha > 2\beta$. Each such pair adds a gain of at least $m - 2s - (\ell(k - (\ell+1)/2)) \ge (\alpha - 2\beta)n^{3/4} + O(n^{1/2})$ toward C in (2.3).

Given a_i with $1 \le i \le r_1$ we choose j as $R_1 < j \le \ell + i$; there are $\ell - R_1 + i$ possibilities, whenever this last quantity is positive. Altogether we have at least $1 + 2 + \ldots + (\ell - R_1 + r_1) > (\ell - R_1 + r_1)^2/2$ such pairs.

Similarly, pairs (a_i, a_j) with $a_i < n + 1 - m + s < n + 1 - s \le a_j$ and $j \le i + \ell$ give us more than $(\ell - R_2 + r_2)^2/2$ such pairs.

Since $R_1 - R_2 - r_1 - r_2 = R - r \le 4\varepsilon n^{1/4}$, the total number of pairs is at least $(2\ell - R + r)^2/4 > (1-\alpha-2\varepsilon)^2 n^{1/4} + O(1)$, and we get the lower bound for the total gain as stated. ■

Completing the proof of Theorem 1: The constraints in the above three claims cover all possibilities for A. In the cases covered by Claims 4 and 4 we have a large defect $K(\mathcal{A})$ so inequalities (4.1) and (3.3) establish the required upper bound for k. In the case covered by Claim 4 the large slackness term C in the inequality (2.4) completes the proof of Theorem 1.

Remark: Note that one could optimize somewhat better the parameters α, β, etc., but we did not see the point of computing more digits of the optimal values. Much more refining should be possible by exploring the structure of a Sidon set more thoroughly; i.e., giving further conditions on the number of elements in some intervals. For example, when $a \in A$ is close to s, then one can improve the bounds from Claim 4, as such a will not contribute much to the degrees of vertices in X. From the other side, when $a \in A$ is close to 1, then a will participate in larger gaps, and one can improve Claim 6. The computation is rather delicate, and it seems to improve the bound on γ to 0.00342. It is likely that it could be improved a bit further, with an additional analysis of the structure of A.

There is a discussion of the structure of dense Sidon sets in the blog of Gowers [**10**], though probably there is no connection toward our proof. It seems that further ideas are needed to get rid of the $n^{1/4}$ term in its entirety.

5. SIDON SETS AND EXTREMAL GRAPH THEORY: A classical problem of Zarankiewicz [**20**] is to determine the maximum number of edges of bipartite C_4-free graphs, with class sizes n. Reiman [**16**] constructed extremal graphs using finite geometries. One can construct large such graphs using Sidon sets as follows. Let $A \subset [n]$ be a Sidon set, X, Y be two copies of $[n]$. Let $G(A, n)$ be the bipartite graph with vertex set $X \cup Y$, with xy being an edge when $x \in X, y \in Y$ and $y - x \in A$. As A is a Sidon set, $G(A, n)$ is a C_4-free graph.

6. THE LOWER BOUND CONSTRUCTION FROM FINITE FIELDS: For completeness we recall a classical construction that in case where q is a power of a prime one has

$$S(q^2-1) \geq q. \tag{6.1}$$

For these values of n we have $S(n) \geq \sqrt{n+1}$. Since the set of primes is sufficiently "dense" among the integers, see [**1**], one can conclude the lower bound $S(n) = \sqrt{n} + O(n^{21/40})$.

Recall a few definitions from introductory abstract algebra. Let p be a power of a prime, $\mathbb{F}_p = (\mathbb{F}_p, +, \cdot)$ the finite field of size p, $\mathbb{F}_p^* = \mathbb{F} \setminus \{0\}$. We have $x^{p-1} = x^0 = 1$ for every element $x \in \mathbb{F}^*$. There are elements g such that $\mathbb{F}^* = \{g, g^2, \dots, g^{p-1}\}$, these are called *primitive* elements of $\mathbb{F}$. In fact, there are $\varphi(p-1)$ of them, where φ is Euler's totient function. Then $(\mathbb{F}^*, \cdot)$ is a cyclic group $\mathbb{Z}_{p-1}$.

To show (6.1) we define $p := q^2$ and take a primitive element g of $\mathbb{F}_{q^2}$. The Bose–Chowla Sidon set $A_q \subset [q^2-1]$ is defined as

$$A_q := \{a : 1 \leq a \leq q^2-1,\ g^a - g = f \text{ for some } f \in \mathbb{F}_q\}.$$

This A_q is a q-element Sidon set in $\mathbb{Z}_{q^2-1}$, i.e., the numbers $\{a - a' : a, a' \in A, a \neq a'\}$ are all distinct $\mod (q^2-1)$. The properties of the set A_q can be found in many places, e.g., in Chapter 27 of the excellent textbook of van Lint and Wilson [**14**].

Acknowledgements: We thank Bernard Lidicky for assisting in the optimization of formulae. We also thank the referees for their useful comments.

REFERENCES

1. Baker, R.C., Harman, G., Pintz, J. The difference between consecutive primes. II. Proc. London Math. Soc. (3) 83 (2001), 532–562.
2. Bassalygo, L.A. New upper bounds for error-correcting codes. (Russian) Problemy Peredači Informacii 1 (1965), vyp. 4, 41–44.
3. O'Bryant, K. A complete annotated bibliography of work related to Sidon sequences. Electron. J. Combin. Dynamic Survey 11 (2004), 39 (electronic).
4. Cilleruelo, J. Sidon sets in $\mathbb{N}^d$. J. Combin. Theory Ser. A 117 (2010), 857–871.
5. Cilleruelo, J. Combinatorial problems in finite fields and Sidon sets. Combinatorica 32 (2012), 497–511.
6. Erdős, P. Some problems in number theory, combinatorics and combinatorial geometry. Math. Pannon. 5 (1994), 261–269.
7. Erdős, P., Turán, P. On a problem of Sidon in additive number theory, and on some related problems. J. London Math. Soc. 16 (1941), 212–215.
8. Erdős, P., Freud, R. On sums of a Sidon-sequence. J. Number Theory 38 (1991), 196–205.
9. Füredi, Z., Ruzsa, I. Z. Nearly subadditive sequences, Acta Math. Hungar. 161 (2020), 401–411.
10. Gowers, T. What are dense Sidon subsets of $\{1, 2, \dots, n\}$ like? https://gowers.wordpress.com/2012/07/13/what-are-dense-sidon-subsets-of-12-n-like/.
11. Green, B. The number of squares and $B_h[g]$ sets. Acta Arith. 100 (2001), 365–390.
12. Johnson, S.M. A new upper bound for error-correcting codes. IRE Trans. IT-8 (1962), 203–207.
13. Lindström, B. An inequality for B_2-sequences. J. Combinatorial Theory 6 (1969), 211–212.
14. van Lint, J.H., Wilson, R.M. A course in combinatorics. Second edition. Cambridge University Press, Cambridge, 2001. xiv+602 pp.
15. Lovász, L. Combinatorial problems and exercises. Second edition. North-Holland Publishing Co., Amsterdam, 1993. 635 pp. (Exercise 13.13).
16. Reiman, I. Über ein Problem von K. Zarankiewicz, Acta Math. Acad. Sci. Hungar. (1958), 269–273.
17. Ruzsa, I.Z. Solving a linear equation in a set of integers. I. Acta Arith. 65 (1993), 259–282.
18. Sidon, S. Ein Satz über trigonometrische polynome und seine anwendung in der theorie der Fourier-Reihen, Math. Ann. 106 (1932), 536–539.
19. Singer, J. A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. 43 (1938), 377–385.
20. Zarankiewicz, K. Problem 101, Colloq. Math. 2 (1951), 301.