k-fold Sidon sets

Javier Cilleruelo* Craig Timmons†

Submitted: Nov 4, 2013; Accepted: Sep 30, 2014; Published: Oct 9, 2014
Mathematics Subject Classifications: 05D99, 11B75

Abstract

Let $k \geqslant 1$ be an integer. A set $A \subset \mathbb{Z}$ is a *k-fold Sidon set* if A has only trivial solutions to each equation of the form $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 = 0$ where $0 \leqslant |c_i| \leqslant k$, and $c_1 + c_2 + c_3 + c_4 = 0$. We prove that for any integer $k \geqslant 1$, a k-fold Sidon set $A \subset [N]$ has at most $(N/k)^{1/2} + O((Nk)^{1/4})$ elements. Indeed we prove that given any k positive integers $c_1 < \cdots < c_k$, any set $A \subset [N]$ that contains only trivial solutions to $c_i(x_1 - x_2) = c_j(x_3 - x_4)$ for each $1 \leqslant i \leqslant j \leqslant k$, has at most $(N/k)^{1/2} + O((c_k^2 N/k)^{1/4})$ elements. On the other hand, for any $k \geqslant 2$ we can exhibit k positive integers $c_1, \dots, c_k$ and a set $A \subset [N]$ with $|A| \geqslant (\frac{1}{k} + o(1))N^{1/2}$, such that A has only trivial solutions to $c_i(x_1 - x_2) = c_j(x_3 - x_4)$ for each $1 \leqslant i \leqslant j \leqslant k$.

Keywords: Sidon sets, k-fold Sidon sets

1 Introduction

Let Γ be an abelian group. A set $A \subset \Gamma$ is a *Sidon* set if $a + b = c + d$ and $a, b, c, d \in A$ implies $\{a, b\} = \{c, d\}$. Sidon sets in $\mathbb{Z}$ and in the group $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$ have been studied extensively. Erdős and Turán [5] proved that a Sidon set $A \subset [N]$ has at most $N^{1/2} + O(N^{1/4})$ elements. Constructions of Singer [10], Bose and Chowla [2], and Ruzsa [9] show that this upper bound is asymptotically best possible. It is a prize problem of Erdős [4] to determine whether or not the error term is bounded. For more on Sidon sets we recommend O'Bryant's survey [8].

Let

$$c_1x_1 + \cdots + c_rx_r = 0 \tag{1}$$

be an integer equation where $c_i \in \mathbb{Z}\backslash\{0\}$, and $c_1 + \cdots + c_r = 0$. Call such an equation an *invariant equation*. A solution $(x_1, \dots, x_r) \in \mathbb{Z}^r$ to (1) is *trivial* if there is a partition of $\{1, \dots, r\}$ into nonempty sets $T_1, \dots, T_m$ such that for every $1 \leqslant i \leqslant m$, we have

*Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Madrid.

†Department of Mathematics and Statistics, California State University Sacramento. Partially supported by NSF Grant DMS-1101489 through Jacques Verstraëte.

$\sum_{j \in T_i} c_j = 0$, and $x_{j_1} = x_{j_2}$ whenever $j_1, j_2 \in T_i$. A natural extremal problem is to determine the maximum size of a set $A \subset [N]$ with only trivial solutions to (1). This problem was investigated in detail by Ruzsa [9]. One of the important open problems from [9] is the genus problem. Given an invariant equation $E : c_1 x_1 + \cdots + c_r x_r = 0$, the *genus* $g(E)$ is the largest integer m such that there is a partition of $\{1, \ldots, r\}$ into nonempty sets $T_1, \ldots, T_m$, such that $\sum_{j \in T_i} c_j = 0$ for $1 \leqslant i \leqslant m$. Ruzsa proved that if E is an invariant equation and $A \subset [N]$ has only trivial solutions to E, then $|A| \leqslant c_E N^{1/g(E)}$. Here c_E is a positive constant depending only on the equation E. Determining if there are sets $A \subset [N]$ with $|A| = N^{1/g(E) - o(1)}$ and having only trivial solutions to E is open for most equations. In particular, the genus problem is open for the equation $2x_1 + 2x_2 = 3x_3 + x_4$. This equation has genus 1 but the best known construction [9] gives a set $A \subset [N]$ with $|A| \geqslant cN^{1/2}$ where $c > 0$ is a positive constant. More generally, Ruzsa showed that for any four variable equation $E : c_1 x_1 + c_2 x_2 = c_3 x_3 + c_4 x_4$ with $c_1 + c_2 = c_3 + c_4$ and $c_i \in \mathbb{N}$, there is a set $A \subset [N]$ with only trivial solutions to E and $|A| \geqslant c_E N^{1/2 - o(1)}$. In this paper we consider special types of four variable invariant equations.

Let $k \geqslant 1$ be an integer. A set $A \subset \mathbb{Z}$ is a *k-fold Sidon* set if A has only trivial solutions to each equation of the form

$$c_1 x_1 + c_2 x_2 + c_3 x_3 + c_4 x_4 = 0$$

where $0 \leqslant |c_i| \leqslant k$, and $c_1 + c_2 + c_3 + c_4 = 0$. A 1-fold Sidon set is a Sidon set. A 2-fold Sidon set has only trivial solutions to each of the equations

$$x_1 + x_2 - x_3 - x_4 = 0, \qquad 2x_1 + x_2 - 2x_3 - x_4 = 0, \qquad 2x_1 - x_2 - x_3 = 0.$$

One can also define k-fold Sidon sets in $\mathbb{Z}_N$. We must add the condition that N is relatively prime to all integers in the set $\{1, 2, \ldots, k\}$. The reason for this is that if a coefficient $c_i \in \{1, 2, \ldots, k\}$ has a common factor with N, then in $\mathbb{Z}_N$ one could have $c_i(a_1 - a_2) = 0$ with $a_1 \neq a_2$. In this case, if $|A| \geqslant 3$, we can choose $a_3 \in A \backslash \{a_1, a_2\}$, and obtain the nontrivial solution $(x_1, x_2, x_3, x_4) = (a_1, a_2, a_3, a_3)$ to the equation $c_i(x_1 - x_2) + x_3 - x_4 = 0$.

Lazebnik and Verstraëte [6] were the first to define k-fold Sidon sets. They conjectured the following.

Conjecture 1 (Lazebnik, Verstraëte [6])**.** For any integer $k \geqslant 3$, there is a positive constant $c_k > 0$ such that for all integers $N \geqslant 1$, there is a k-fold Sidon set $A \subset [N]$ with $|A| \geqslant c_k N^{1/2}$.

This conjecture is still open. Lazebnik and Verstraëte proved that for infinitely many N, there is a 2-fold Sidon set $A \subset \mathbb{Z}_N$ with $|A| \geqslant \frac{1}{2} N^{1/2} - 3$. Axenovich [1] and Verstraëte (unpublished) observed that one can adapt Ruzsa's construction for four variable equations (Theorem 7.3, [9]) to construct k-fold Sidon sets $A \subset [N]$ or $A \subset \mathbb{Z}_N$ with $|A| \geqslant c_k N^{1/2} e^{-c_k \sqrt{\log N}}$ for any $k \geqslant 3$. An affirmative answer to Conjecture 1, even in the case when $k = 3$, would have applications to hypergraph Turán problems [6] and extremal graph theory [11].

Since any k-fold Sidon set is a Sidon set, the trivial upper bound $|A| \leqslant \sqrt{N-3/4}+1/2$ for a Sidon set $A \subset \mathbb{Z}_N$, and the Erdős-Turán bound $|A| \leqslant N^{1/2} + O(N^{1/4})$ for any Sidon set $A \subset [N]$, also hold for k-fold Sidon sets. We will obtain better upper bounds for k-fold Sidon sets. Instead of considering all the possible equations $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 = 0$ with $c_1 + c_2 + c_3 + c_4 = 0$, we will take advantage only of the equations of the form

$$c_1(x_1 - x_2) = c_2(x_3 - x_4).$$

For any $c_1, \ldots, c_k$ with $(c_i, N) = 1$, if $A \subset \mathbb{Z}_N$ contains only trivial solutions to $c_i(x_1 - x_2) = c_j(x_3 - x_4)$ for each $1 \leqslant i \leqslant j \leqslant k$, then

$$|A| \leqslant \sqrt{\frac{N-1}{k} + \frac{1}{4}} + \frac{1}{2}. \tag{2}$$

To see this, consider all elements of the form $c_i(x - y)$ where $1 \leqslant i \leqslant k$, and $x \neq y$ are elements of A. All of these elements are distinct and nonzero. Therefore, $k|A|(|A| - 1) \leqslant N - 1$ which is equivalent to (2).

The short counting argument used to obtain (2) does not work in $\mathbb{Z}$. Using a more sophisticated argument, we can show that a bound similar to (2) does hold in $\mathbb{Z}$.

Theorem 2. *Let $k \geqslant 1$ be an integer and $1 \leqslant c_1 < c_2 < \cdots < c_k$ be a set of k distinct integers. If $A \subset [N]$ is a set with only trivial solutions to $c_i(x_1 - x_2) = c_j(x_3 - x_4)$ for each $1 \leqslant i \leqslant j \leqslant k$, then*

$$|A| \leqslant \left(\frac{N}{k}\right)^{1/2} + O\left(\left(\frac{c_k^2 N}{k}\right)^{1/4}\right).$$

Taking $c_j = j$ for $1 \leqslant j \leqslant k$, we have the following corollary.

Corollary 3. *If $k \geqslant 1$ is an integer and $A \subset [N]$ is a k-fold Sidon set, then*

$$|A| \leqslant \left(\frac{N}{k}\right)^{1/2} + O((kN)^{1/4}).$$

In Theorem 2 and Corollary 3, the Landau symbols are with respect to N. That is, we view k, $c_1, \ldots, c_k$ as being fixed, and N tending to infinity.

It is natural to ask if we can improve Corollary 3 if we make full use of the assumption that A is a k-fold Sidon set. For example, the bound $|A| \leqslant (N/3)^{1/2} + O(N^{1/4})$ holds under the assumption that $A \subset [N]$ has only trivial solutions to $c_1(x_1 - x_2) = c_2(x_3 - x_4)$ for each $1 \leqslant c_1 \leqslant c_2 \leqslant 3$. A 3-fold Sidon set additionally has only trivial solutions to $2x_1 + 2x_2 = 3x_3 + x_4$. Our argument does not capture this property. It is not known if this additional assumption would improve the upper bound $|A| \leqslant (N/3)^{1/2} + O(N^{1/4})$.

The method used by Lazebnik and Verstraëte to construct 2-fold Sidon sets is rather robust. Using this method, we prove the following theorem.

Theorem 4. *There exist k distinct integers $c_1, \ldots, c_k$ and infinitely many N, such that there is a set $A \subset \mathbb{Z}_N$ with*

$$|A| \geqslant \frac{N^{1/2}}{k}(1 - o(1))$$

and having only trivial solutions to $c_i(x_1 - x_2) = c_j(x_3 - x_4)$ for each $1 \leqslant i \leqslant j \leqslant k$.

The next section contains the proof of Theorem 2. Section 3 contains the proof of Theorem 4.

2 Proof of Theorem 2

For finite sets $B, C \subset \mathbb{Z}$, define

$$r_{B+C}(x) = |\{(b, c) : b + c = x, b \in B, c \in C\}|$$

and

$$r_{B-C}(x) = |\{(b, c) : b - c = x, b \in B, c \in C\}|.$$

The following useful lemma has appeared in the literature (see [3] or [9]).

Lemma 5. *For any finite sets $B, C \subset \mathbb{Z}$,*

$$\frac{(|B||C|)^2}{|B + C|} \leqslant |B||C| + \sum_{x \neq 0} r_{B-B}(x) r_{C-C}(x). \tag{3}$$

Proof. Observe $\sum_{x \in B+C} r_{B+C}(x)$ counts every ordered pair $(b, c) \in B \times C$ exactly once so that $|B||C| = \sum_{x \in B+C} r_{B+C}(x)$. By the Cauchy-Schwarz inequality,

$$\frac{(|B||C|)^2}{|B + C|} = \frac{\left(\sum_{x \in B+C} r_{B+C}(x)\right)^2}{|B + C|} \leqslant \sum_x r_{B+C}^2(x). \tag{4}$$

The sum $\sum_x r_{B+C}^2(x)$ counts 4-tuples (b, b', c, c') with $b, b' \in B$, $c, c' \in C$, and $b + c = b' + c'$. The equation $b + c = b' + c'$ is equivalent to $b - b' = c' - c$ and so

$$\sum_x r_{B+C}^2(x) = \sum_x r_{B-B}(x) r_{C-C}(x). \tag{5}$$

Combining (4) and (5), we have

$$\frac{(|B||C|)^2}{|B + C|} \leqslant \sum_x r_{B-B}(x) r_{C-C}(x) = |B||C| + \sum_{x \neq 0} r_{B-B}(x) r_{C-C}(x)$$

which proves (3). □

Before giving the proof of Theorem 2 we take a moment to describe some of ideas of the proof. Suppose $A \subset [N]$ is a set satisfying the hypothesis of Theorem 2. If $c_rA := \{c_ra : a \in A\}$, then the k-fold Sidon property implies that

$$\sum_{r=1}^{k} r_{c_rA-c_rA}(y) \leqslant 1 \tag{6}$$

for any $y \neq 0$. One may then apply Lemma 5 to c_rA and the interval $C = \{0, 1, \dots, m-1\}$ for each $1 \leqslant r \leqslant k$. An obstacle in this approach is the expression $|c_rA + C|$ that appears in the denominator on the left hand side of (3). Since $c_rA + C \subset \{1, 2, \dots, c_rN + m - 1\}$, we have $|c_rA + C| \leqslant c_rN + m$ but this upper bound that is too large for our approach. Instead of c_rA, we will consider the sets $B_{r,i} := \{x : c_rx + i \in A\}$, $0 \leqslant i \leqslant c_r - 1$. We will show that an analogue of (6) holds for the $B_{r,i}$'s which, although not difficult, is one of the most important parts of the proof. Additionally, we have that $|B_{r,i} + C| \leqslant N/c_r + m$ and this is what leads to a more effective application of Lemma 5.

Proof of Theorem 2. Let $1 \leqslant c_1 < c_2 < \cdots < c_k$ be k distinct integers. Let $A \subset [N]$ be a set with only trivial solutions to $c_i(x_1 - x_2) = c_j(x_3 - x_4)$ for each $1 \leqslant i \leqslant j \leqslant k$. Let

$$B_{r,i} = \{x : c_rx + i \in A\}$$

for $1 \leqslant r \leqslant k$ and $0 \leqslant i \leqslant c_r - 1$. Therefore,

$$|A| = \sum_{i=0}^{c_r-1} |\{a \in A : \ a \equiv i \pmod{c_r}\}| = \sum_{i=0}^{c_r-1} |B_{r,i}|$$

so by the Cauchy-Schwarz inequality,

$$|A|^2 = \left(\sum_{i=0}^{c_r-1} |B_{r,i}|\right)^2 \leqslant c_r \sum_{i=0}^{c_r-1} |B_{r,i}|^2. \tag{7}$$

For any $y \neq 0$,

$$\sum_{r=1}^{k} \sum_{i=0}^{c_r-1} r_{B_{r,i}-B_{r,i}}(y) \leqslant 1. \tag{8}$$

To see this, suppose

$$y = x_1 - x_2 = x_3 - x_4 \tag{9}$$

where $x_1, x_2 \in B_{r,i}$ and $x_3, x_4 \in B_{r',i'}$ for some $1 \leqslant r, r' \leqslant k$, $1 \leqslant i \leqslant c_r - 1$, and $1 \leqslant i' \leqslant c_{r'} - 1$. There are elements $a_1, a_2, a_3, a_4 \in A$ such that

$$c_rx_1 + i = a_1, \quad c_rx_2 + i = a_2, \quad c_{r'}x_3 + i' = a_3, \quad \text{and} \quad c_{r'}x_4 + i' = a_4.$$

Then (9) implies

$$\frac{1}{c_r}(a_1 - i) - \frac{1}{c_r}(a_2 - i) = \frac{1}{c_{r'}}(a_3 - i') - \frac{1}{c_{r'}}(a_4 - i'),$$

thus $c_{r'}(a_1 - a_2) = c_r(a_3 - a_4)$. Since $y \neq 0$, we have $a_1 \neq a_2$ and $a_3 \neq a_4$ and then we would have a non trivial solution to the equation $c_{r'}(x_1 - x_2) = c_r(x_3 - x_4)$.

Let $C = \{0, 1, \ldots, m-1\}$. For any $1 \leqslant r \leqslant k$ and $0 \leqslant i \leqslant c_r - 1$, the set $B_{r,i} + C$ is contained in the interval $\{0, 1, \ldots, \lfloor N/c_r \rfloor + m - 1\}$. This gives the trivial estimate $|B_{r,i} + C| \leqslant N/c_r + m$. By Lemma 5 applied to $B_{r,i}$ and C,

$$\frac{|B_{r,i}|^2 m^2}{N/c_r + m} \leqslant |B_{r,i}|m + \sum_{y \neq 0} r_{B_{r,i} - B_{r,i}}(y) r_{C-C}(y).$$

We sum this inequality over all $1 \leqslant r \leqslant k$ and $0 \leqslant i \leqslant c_r - 1$ to get

$$\begin{aligned} m^2 \sum_{r=1}^{k} \frac{1}{N/c_r + m} \sum_{i=0}^{c_r - 1} |B_{r,i}|^2 &\leqslant \sum_{r=1}^{k} \sum_{i=0}^{c_r-1} |B_{r,i}|m \\ &+ \sum_{y \neq 0} \sum_{r=1}^{k} \sum_{i=0}^{c_r-1} r_{B_{r,i} - B_{r,i}}(y) r_{C-C}(y) \\ &\leqslant k|A|m + \sum_{y \neq 0} r_{C-C}(y) \\ &\leqslant m(k|A| + m). \end{aligned}$$

From (7) and the previous inequality, we deduce that

$$m^2 |A|^2 \sum_{r=1}^{k} \frac{1}{N + c_r m} \leqslant m(k|A| + m). \tag{10}$$

The left hand side of (10) is at least $\frac{|A|^2 k m^2}{N + c_k m}$. Therefore, $\frac{|A|^2 k m}{N + c_k m} \leqslant k|A| + m$, and so

$$|A|^2 k m \leqslant (N + c_k m)(m + k|A|).$$

We complete the square and use the inequality $(x+y)^2 \leqslant 2x^2 + 2y^2$ to obtain

$$\begin{aligned} \left(|A| - \left(\frac{N}{2m} + \frac{c_k}{2}\right)\right)^2 &\leqslant \frac{N}{k} + \frac{c_k m}{k} + \left(\frac{N}{2m} + \frac{c_k}{2}\right)^2 \\ &\leqslant \frac{N}{k} + \frac{c_k m}{k} + \frac{N^2}{2m^2} + \frac{c_k^2}{2} \\ &= \frac{N}{k}\left(1 + \frac{c_k m}{N} + \frac{Nk}{2m^2} + \frac{k c_k^2}{2N}\right). \end{aligned}$$

Taking square roots and using the inequality $\sqrt{1+x} \leqslant 1 + x$ for $x \geqslant 0$, we solve for $|A|$ to get

$$\begin{aligned} |A| &\leqslant \left(\frac{N}{k}\right)^{1/2} \left(1 + \frac{c_k m}{N} + \frac{Nk}{2m^2} + \frac{k c_k^2}{2N}\right) + \frac{N}{2m} + \frac{c_k}{2} \\ &= \left(\frac{N}{k}\right)^{1/2} + \frac{c_k m}{k^{1/2} N^{1/2}} + \frac{N^{3/2} k^{1/2}}{2m^2} + \frac{k^{1/2} c_k^2}{2N^{1/2}} + \frac{N}{2m} + \frac{c_k}{2}. \end{aligned}$$

Take $m = \lceil (N^{3/4}k^{1/4})/c_k^{1/2} \rceil$ to get $|A| \leqslant \left(\frac{N}{k}\right)^{1/2} + O((c_k^2 N/k)^{1/4})$. This completes the proof of Theorem 2.

□

3 Proof of Theorem 4

Let $k \geqslant 2$ be an integer. Let p be a prime, and let $M \geqslant 1$ be a large integer. Let r be any prime with $r > Mk$. Let $i \geqslant 1$ be an integer, and set $t = r^i$ and $q = p^t$.

We will prove that for $c_j = p^{j-1}$ for $j = 1, \dots k$ there exists a set $A \subset \mathbb{Z}_{q^2-1}$ with $|A| \geqslant \frac{q}{k}\left(1 - \frac{1}{M}\right) - (p^4 - 1)(M - 1)$ and having only trivial solutions to

$$x_1 - x_2 = p^{j-1}(x_3 - x_4)$$

for $1 \leqslant j \leqslant k$. This proves Theorem 4 because as i tends to infinity, the term $\frac{q}{k}\left(1 - \frac{1}{M}\right)$ is the dominant term. M can be taken as large as we want, and $(p^4 - 1)(M - 1)$ is constant with respect to i.

Let θ be a generator of the cyclic group $\mathbb{F}_{q^2}^*$. Bose and Chowla [2] proved that the set

$$C(q, \theta) = \{a \in \mathbb{Z}_{q^2-1} : \theta^a - \theta \in \mathbb{F}_q\}$$

is a Sidon set in $\mathbb{Z}_{q^2-1}$. Lindström [7] proved

$$B(q, \theta) = \{b \in \mathbb{Z}_{q^2-1} : \theta^b + \theta^{qb} = 1\}$$

is a translate of $C(q, \theta)$ and is therefore a Sidon set.

Lemma 6. *The map $x \mapsto px$ is an injection from $\mathbb{Z}_{q^2-1}$ to $\mathbb{Z}_{q^2-1}$ that maps $B(q, \theta)$ to $B(q, \theta)$.*

Proof. The map $x \mapsto px$ is 1-to-1 since p is relatively prime to $q^2 - 1$. If $b \in B(q, \theta)$, then

$$1 = (\theta^b + \theta^{qb})^p = \theta^{pb} + \theta^{q(pb)}$$

so $pb \in B(q, \theta)$. □

Let $\pi : B(q, \theta) \to B(q, \theta)$ be the permutation $\pi(b) = pb$. As in [6], we use the cycles of π to define A. Let $\sigma = (b_1, \dots, b_m)$ be a cycle of π. If $m < k$, then remove all elements of σ from $B(q, \theta)$. If $m \geqslant k$, then remove all b_j in σ for which j is not divisible by k. Do this for each cycle of π. Let A be the resulting subset of $B(q, \theta)$.

Lemma 7. *For each $c \in \{1, p, p^2, \dots, p^{k-1}\}$, A has only trivial solutions to*

$$x_1 - x_2 = c(x_3 - x_4).$$

Proof. Suppose $a_1, a_2, a_3, a_4 \in A$ and $a_1 - a_2 = p^j(a_3 - a_4)$ for some $0 \leqslant j \leqslant k-1$. By Lemma 6, there are elements $b_3, b_4 \in B(q,\theta)$ such that $p^j a_3 = b_3$ and $p^j a_4 = b_4$. This gives $a_1 - a_2 = b_3 - b_4$. Since $B(q,\theta)$ is a Sidon set, either $a_1 = a_2$, $b_3 = b_4$ or $a_1 = b_3$, $a_2 = b_4$.

If $a_1 = a_2$ and $b_3 = b_4$, then $a_3 = a_4$ and the solution (a_1, a_2, a_3, a_4) is trivial. Suppose $a_1 = b_3$ and $a_2 = b_4$. This implies $b_3 \in A$, so both $p^j a_3$ and a_3 are in A. This contradicts the way in which A was constructed. □

Lemma 8. $|A| \geqslant \frac{q}{k}\left(1 - \frac{1}{M}\right) - (p^4-1)(M-1)$.

Proof. In order to obtain a lower bound on $|A|$, we need to estimate the number of cycles of π that are short. For instance, if all cycles of π have length less than k, then $|A| = 0$. For a cycle σ of π with length $mk \geqslant Mk$, we delete at most $m(k-1)$ elements from $B(q,\theta)$ and keep at least $m-1$ elements.

We estimate the number of cycles of length at most $Mk-1$. Let $\sigma = (b, pb, \dots, p^{e-1}b)$ be a cycle of π of length e where $e \leqslant Mk-1$. The integer e is the smallest positive integer such that $p^e b \equiv b (\text{mod } q^2-1)$. This is the same as saying that the order of p in the multiplicative group of units $\mathbb{Z}_n^*$ is e where $n = \frac{q^2-1}{\gcd(b, q^2-1)}$. Since

$$p^{4t} - 1 = (p^{2t}-1)(p^{2t}+1) = (q^2-1)(p^{2t}+1)$$

we have $p^{4t} \equiv 1 (\text{mod } q^2-1)$, so e must divide $4t = 4r^i$. Since r is prime and $r \geqslant Mk$, e cannot divide r, so e must divide 4. To count the number of cycles of π with length at most $Mk-1$, it is enough to count the elements $x \in \mathbb{Z}_{q^2-1} \backslash \{0\}$ such that $p^4 x \equiv x (\text{mod } q^2-1)$. This follows from the fact that if $e \in \{1,2\}$ and $p^e x \equiv x (\text{mod } q^2-1)$, then $p^4 x \equiv x (\text{mod } q^2-1)$. The number of solutions to this congruence is $\gcd(p^4-1, q^2-1) \leqslant p^4-1$. Therefore, there are at most p^4-1 cycles of π of length at most $Mk-1$. For a cycle of length at least Mk, the proportion of elements of the cycle that are put into A is at least $\frac{M-1}{Mk}$ (the function $f(x) = \frac{x-1}{xk}$ is increasing provided $k > 0$). Since $|B(q,\theta)| = q$,

$$|A| \geqslant \left(q - (p^4-1)Mk\right)\left(\frac{M-1}{Mk}\right) = \frac{q}{k}\left(1 - \frac{1}{M}\right) - (p^4-1)(M-1).$$

□

Theorem 4 follows from Lemmas 7 and 8.

4 Concluding Remarks

The most important open problem concerning k-fold Sidon sets is an answer to Conjecture 1. The case $k = 3$ is particularly interesting. A 3-fold Sidon set $A \subset [N]$ with $|A| \geqslant cN^{1/2}$ is known to imply the existence of a graph with $c_1 N$ vertices, $c_2 N^{3/2}$ edges, and every edge is in exactly one cycle of length four [11].

Another problem is to determine the maximum size of a 2-fold Sidon set in $\mathbb{Z}_N$ or $[N]$. Let $S_k(N)$ be the maximum size of a k-fold Sidon set in $\mathbb{Z}_N$. For any integer $t \geqslant 1$, there are 2-fold Sidon sets $A \subset \mathbb{Z}_N$, $N = 2^{2^{t+1}} + 2^{2^t} + 1$, with $|A| \geqslant \frac{1}{2}N^{1/2} - 3$ (see [6]). Theorem 2 gives an upper bound of $(N/2)^{1/2} + O(N^{1/4})$ so

$$\frac{1}{2} \leqslant \limsup_{N\to\infty} \frac{S_2(N)}{N^{1/2}} \leqslant \frac{1}{2^{1/2}}.$$

It would be interesting to determine the above limit. In the case of Sidon sets, we have $\limsup_{N\to\infty} \frac{S_1(N)}{N^{1/2}} = 1$ by [5] and [10].

References

[1] M. Axenovich, personal communication.

[2] R. C. Bose, S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962/1963), 141-147.

[3] J. Cilleruelo, *Sidon sets in* $\mathbb{N}^d$, J. Combin. Theory, Series A **117** (2010) 857-871.

[4] P. Erdős, *A survey of problems in combinatorial number theory*, Annals of Discrete Mathematics **6** (1980), 89-115.

[5] P. Erdős, P. Turán, *On a problem of Sidon in additive number theory, and on some related results*, Journal of the London Mathematical Society, 16 (1941).

[6] F. Lazebnik, J. Verstraëte, *On hypergraphs of girth five*, Electronic J. of Combinatorics, **10**, (2003), #R25.

[7] B. Lindström, *A translate of Bose-Chowla B_2-sets*, Studia Sc. Math. Hungar., **36**, (2000), 331-333.

[8] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electronic J. of Combinatorics **DS 11** (2004).

[9] I. Ruzsa, *Solving a linear equation in a set of integers I*, Acta Arith. **65** 3 (1993), 259-282.

[10] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. 43 (1938), 377-385.

[11] C. Timmons, J. Verstraëte, *A counterexample to sparse removal*, submitted. arXiv:1312.2994.