J. Korean Math. Soc. **53** (2016), No. 3, pp. 503–517
http://dx.doi.org/10.4134/JKMS.j140275
pISSN: 0304-9914 / eISSN: 2234-3008

ON SIDON SETS IN A RANDOM SET OF VECTORS

Sang June Lee

Abstract. For positive integers d and n, let $[n]^d$ be the set of all vectors $(a_1, a_2, \dots, a_d)$, where a_i is an integer with $0 \le a_i \le n-1$. A subset S of $[n]^d$ is called a *Sidon set* if all sums of two (not necessarily distinct) vectors in S are distinct.

In this paper, we estimate two numbers related to the maximum size of Sidon sets in $[n]^d$. First, let $\mathcal{Z}_{n,d}$ be the number of all Sidon sets in $[n]^d$. We show that $\log(\mathcal{Z}_{n,d}) = \Theta(n^{d/2})$, where the constants of Θ depend only on d. Next, we estimate the maximum size of Sidon sets contained in a random set $[n]_p^d$, where $[n]_p^d$ denotes a random set obtained from $[n]^d$ by choosing each element independently with probability p.

1. Introduction

For positive integers d and n, let $[n]^d$ be the set of all vectors $(a_1, a_2, \dots, a_d)$, where a_i's are integers with $0 \le a_i \le n-1$. A subset S of $[n]^d$ is called a *Sidon set* if all sums of two (not necessarily distinct) vectors in S are distinct. A well-known problem on Sidon sets in $[n]^d$ is the determination of the maximum size $F([n]^d)$ of Sidon sets in $[n]^d$. For $d = 1$, Erdős and Turán [4] showed in 1941 that $F([n]) \le n^{1/2} + O(n^{1/4})$. Then, Lindström [8], in 1969, improved the bound to $F([n]) \le n^{1/2} + n^{1/4} + 1$. On the other hand, in 1944, Chowla [1] and Erdős [3] observed that a result of Singer [12] implies that $F([n]) \ge n^{1/2} - O(n^{5/16})$. Consequently, we know $F([n]) = n^{1/2}(1+o(1))$. For a general $d \ge 1$, Lindström [9] showed in 1972 that $F([n]^d) \le n^{d/2} + O(n^{d^2/(2d+2)})$. On the other hand, in 2010, Cilleruelo [2] proved that $F([n]^d) \ge F([n^d]) \ge n^{d/2} - O(n^{5d/16})$. Therefore,

$$F([n]^d) = n^{d/2}(1 + o(1)). \tag{1}$$

For more information, see the classical monograph of Halberstam and Roth [5] and a survey paper by O'Bryant [11].

Received May 7, 2014; Revised September 19, 2015.
2010 *Mathematics Subject Classification.* 11B75, 05A16.
Key words and phrases. Sidon set, Sidon sequence, vector.
The author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2013R1A1A1059913).

In this paper we consider two numbers related to the number $F([n]^d)$. The first one is the number $\mathcal{Z}_{n,d}$ of all Sidon sets contained in $[n]^d$. The second one is the maximum size of Sidon sets contained in a random subset of $[n]^d$ instead of $[n]^d$.

We first start with the problem of estimating $\mathcal{Z}_{n,d}$. Recalling that $F([n]^d) = n^{d/2}(1+o(1))$, one can easily see that

$$2^{F([n]^d)} \le \mathcal{Z}_{n,d} \le \sum_{k=1}^{F([n]^d)} \binom{n^d}{k} \le F([n]^d)\binom{n^d}{F([n]^d)}.$$

This implies the following.

Fact 1.

$$2^{n^{d/2}(1+o(1))} \le \mathcal{Z}_{n,d} \le n^{(d/2)n^{d/2}(1+o(1))}.$$

In this paper, we improve the above upper bound as follows.

Theorem 2. *For a positive integer d, there exists a positive constant $c = c(d)$ such that, for any sufficiently large $n = n(d)$,*

$$\mathcal{Z}_{n,d} \le 2^{cn^{d/2}}.$$

Note that this upper bound matches the lower bound in Fact 1 up to a multiplicative constant factor in the exponent. Our proof of Theorem 2 will be provided in Subsection 3.1. The case $d = 1$ of Theorem 2 was also proved in [7].

Next, we deal with the maximum size of Sidon sets contained in a random subset of $[n]^d$. Let $[n]_p^d$ be a random set obtained from $[n]^d$ by choosing each element independently with probability p. Let $F([n]_p^d)$ be the maximum size of Sidon sets in a random set $[n]_p^d$. Our result about $F([n]_p^d)$ is as follows.

Theorem 3. *For a positive integer d, let a be a constant with $-d < a \le 0$, and let $p = p(n) = n^a(1+o(1))$. Then, there exists a constant $b = b(a)$ such that, asymptotically almost surely (a.a.s.), that is, with probability tending to 1 as $n \to \infty$,*

$$F([n]_p^d) = n^{b+o(1)}. \tag{2}$$

Moreover,

$$b(a) = \begin{cases} a+d & \text{if } -d < a \le -2d/3, \\ d/3 & \text{if } -2d/3 \le a \le -d/3, \\ (a+d)/2 & \text{if } -d/3 \le a \le 0. \end{cases} \tag{3}$$

The graph of $b = b(a)$ is given in Figure 1. A refined version of Theorem 3 is stated in Theorems 7–10 in Subsection 2.2. Theorems 7–10 will be proved in Sections 4 and 5. The case $d = 1$ of Theorem 3 was also proved in [7].

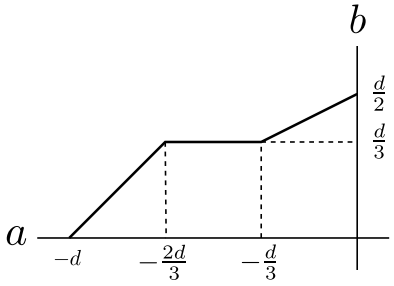

FIGURE 1. The graph of $b = b(a)$ in Theorem 3

1.1. Remark and notation

From now on, let d be a fixed positive integer. Constants in O, Ω, and Θ may depend on d. We write $f = o(g)$ if f/g goes to 0 as $n \to \infty$. We also write $f \ll g$ if $f/g = o(1)$.

2. Main results

2.1. The number of Sidon sets of a given size

We will obtain an upper bound on the number of Sidon sets in $[n]^d$ of a given size. For a positive integer t, let $\mathcal{Z}_{n,d}(t)$ be the number of Sidon sets in $[n]^d$ of size t. Observe that the following result applies when $t = \Omega\left(n^{d/3}(\log n)^{1/3}\right)$.

Theorem 4. *Let d be a positive integer. For a sufficiently large integer $n = n(d)$, the following holds: If t is a positive integer with $t \geq 2s_0$, where $s_0 = (d2^{d+1}n^d \log n)^{1/3}$, then*

$$\mathcal{Z}_{n,d}(t) \leq n^{2(d+1)s_0} \left(\frac{e2^{d+5}n^d}{t^2}\right)^t.$$

Our proof of Theorem 4 will be given in Subsection 3.2. Theorem 4 will be used in order to prove Theorem 2 (see Subsection 3.1 for its proof) and the upper bounds in Theorems 9 and 10 (see Section 4 for its proof).

The next theorem provides an upper bound on the number $\mathcal{Z}_{n,d}(t)$ for $t = \Omega(n^{d/3})$. Observe that the range of t here is a bit wider than the range of t in Theorem 4.

Theorem 5. *Let γ and ω be real numbers and let n, s^* and t be positive integers satisfying that*

$$0 < \gamma < s^*/2^{d+1}, \quad s^* = (2^{(d+1)}n^d \log \gamma)^{1/3}, \tag{4}$$

$$\omega \geq 4, \qquad \text{and} \qquad t = \omega s^*. \tag{5}$$

Then

$$\mathcal{Z}_{n,d}(t) \le \left(\frac{4en^d}{t\gamma^{1-2/\omega}}\right)^t.$$

Remark 6. For $d = 1$, a version of Theorem 5 was given in Lemma 3.3 in [7], but we improve the previous one as follows:

(1) We have a better upper bound on $\mathcal{Z}_{n,1}(t)$ by removing the multiplicative factor ω in the base in Lemma 3.3 of [7].
(2) We remove the variable σ used in Lemma 3.3 of [7].

Our proof of Theorem 5 will be given in Subsection 3.3. Theorem 5 will be applied to our proof of the upper bound in Theorem 8. (See Section 4 for the proof.)

2.2. The maximum size of Sidon sets in a random set $[n]_p^d$

Recall that $[n]_p^d$ is a random set obtained from $[n]^d$ by choosing each element independently with probability p. Also, recall that $F\left([n]_p^d\right)$ denotes the maximum size of Sidon sets in a random set $[n]_p^d$. We state our results on the upper and lower bounds of $F\left([n]_p^d\right)$ in Theorems 7–10 in full. Recall that $f \ll g$ if $f/g = o(1)$.

Theorem 7. *The following holds a.a.s.*:
If $n^{-d} \ll p \ll n^{-2d/3}$, then

$$F\left([n]_p^d\right) = (1+o(1))\, n^d p. \tag{6}$$

If $n^{-d} \ll p \le 2n^{-2d/3}$, then

$$(1/3+o(1))\, n^d p \le F\left([n]_p^d\right) \le (1+o(1))\, n^d p. \tag{7}$$

Theorem 8. *Let $\varepsilon < d/3$. If $2n^{-2d/3} \le p \le n^{-d/3-\varepsilon}$, then there exist a positive absolute constant c_1 and a positive constant $c_2 = c_2(d)$ such that a.a.s.*

$$c_1 n^{d/3} \left(\log(n^{2d}p^3)\right)^{1/3} \le F\left([n]_p^d\right) \le c_2 n^{d/3} \left(\log(n^{2d}p^3)\right)^{1/3}.$$

Theorem 9. *Let $\varepsilon < d/3$. If $n^{-d/3-\varepsilon} \le p \le n^{-d/3} (\log n)^{8/3}$, then there exist a positive absolute constant c_3 and a positive constant $c_4 = c_4(d)$ such that a.a.s.*

$$c_3 n^{d/3} (\log n)^{1/3} \le F\left([n]_p^d\right) \le c_4 n^{d/3} (\log n)^{4/3}.$$

Theorem 10. *If $n^{-d/3} (\log n)^{8/3} \le p \le 1$, then there exist a positive absolute constant c_5 and a positive constant $c_6 = c_6(d)$ such that a.a.s.*

$$c_5 n^{d/2} p^{1/2} \le F\left([n]_p^d\right) \le c_6 n^{d/2} p^{1/2}.$$

2.3. Organization

In Section 3, we prove Theorem 2 and Theorems 4 and 5. Our proof of the upper bounds in Theorems 7–10 will be provided in Section 4. In Section 5, we prove the lower bounds in Theorems 7–10.

3. The number of Sidon sets in $[n]^d$ of a given size

3.1. The number of Sidon sets

Now we show Theorem 2 by using Theorem 4.

Proof of Theorem 2. We have that

$$\mathcal{Z}_{n,d} = \sum_{t=1}^{n^d} \mathcal{Z}_{n,d}(t) = \sum_{t=1}^{F([n]^d)} \mathcal{Z}_{n,d}(t),$$

where the second equality holds since $F([n]^d)$ is the maximum size of Sidon sets in $[n]^d$. Since $F([n]^d) = n^{d/2}(1+o(1))$, we have that

$$\mathcal{Z}_{n,d} = \sum_{t=1}^{n^{d/3}\log n} \mathcal{Z}_{n,d}(t) + \sum_{t=n^{d/3}\log n+1}^{F([n]^d)} \mathcal{Z}_{n,d}(t). \tag{8}$$

The first sum of (8) is estimated by

$$\begin{aligned}\sum_{t=1}^{n^{d/3}\log n} \mathcal{Z}_{n,d}(t) &\le \sum_{t=1}^{n^{d/3}\log n} \binom{n^d}{t} \le n^{d/3}\log n \cdot \left(\frac{en^d}{n^{d/3}\log n}\right)^{n^{d/3}\log n} \\ &\le n^{(2d/3)n^{d/3}\log n(1+o(1))} \le 2^{c_1 n^{d/3}(\log n)^2},\end{aligned}$$

where $c_1 = c_1(d)$ is a positive constant depending only on d. Next, it follows from Theorem 4 that the second sum of (8) is estimated by

$$\begin{aligned}\sum_{t=n^{d/3}\log n+1}^{F([n]^d)} \mathcal{Z}_{n,d}(t) &\le F([n]^d)\cdot n^{c_2 n^{d/3}(\log n)^{1/3}} \left(\frac{c_3 n^d}{(F([n]^d))^2}\right)^{F([n]^d)} \\ &\le 2^{c_4 n^{d/2}},\end{aligned}$$

where c_2, c_3, and c_4 are positive constants depending only on d. Therefore, in view of identity (8), the above estimates of the first and second sums of (8) imply Theorem 2. □

3.2. The number of Sidon sets of a larger size

Recall that $\mathcal{Z}_{n,d}(t)$ is the number of Sidon sets in $[n]^d$ of size t. Now we show Theorem 4 which gives an upper bound on $\mathcal{Z}_{n,d}(t)$ for $t = \Omega\left(n^{d/3}(\log n)^{1/3}\right)$. Our proof uses the following strategy from [7]. Let s be an integer with $s < t$, and let S be a seed Sidon set in $[n]^d$ of size s. For such a Sidon set S, we estimate the number of extensions of S to larger Sidon sets S^* of size t containing S. Then, by summing over all Sidon sets S of size s, we will obtain an upper bound on $\mathcal{Z}_{n,d}(t)$. In order to bound the number of extensions, we define the following graph.

Definition 11. For a Sidon set S in $[n]^d$, let G_S be the graph on $V = [n]^d \setminus S$ in which $\{v_1, v_2\}$ is an edge of G_S if and only if there exist some $b_1, b_2 \in S$ such that $v_1 + b_1 = v_2 + b_2$.

Observe that if S^* is a Sidon set in $[n]^d$ of size t containing S, then the set $S^* \setminus S$ is an independent set in G_S of size $t - s$. Hence, the number of extensions of S to larger Sidon sets S^* of size t is bounded above by the number of independent sets in G_S of size $t - s$.

In order to bound the number of independent sets in G_S of a given size, we will use the following result from [7].

Lemma 12 (Lemma 3.1 of [7])**.** *For positive integers N and R and a positive real number β, let G be a graph on N vertices such that for every vertex set U with $|U| \geq R$, the number $e(U)$ of edges in the subgraph of G induced on U satisfies*

$$e(U) \geq \beta \binom{|U|}{2}. \tag{9}$$

If q is a positive integer satisfying

$$q \geq \beta^{-1} \log(N/R), \tag{10}$$

then, for all positive integers r, the number of independent sets in G of size $q + r$ is at most

$$\binom{N}{q}\binom{R}{r}. \tag{11}$$

Next we show that the graph G_S with a Sidon set S satisfies condition (9) with suitable R and β.

Lemma 13. *For a Sidon set S in $[n]^d$ of size s, the graph G_S on $N := n^d - s$ vertices satisfies the following: For every vertex set U with*

$$|U| \geq \frac{2^{d+1} n^d}{s}, \tag{12}$$

the number $e(U)$ of edges in the subgraph of G_S induced on U satisfies

$$e(U) \geq \frac{s^2}{2^{d+1} n^d} \binom{|U|}{2}. \tag{13}$$

Proof. Let U be an arbitrary vertex set of G_S with $|U| \geq (2^{d+1}/s)n^d$. We define an auxiliary bipartite graph B with disjoint vertex classes $[2n]^d$ and U in which a vertex $w \in [2n]^d$ is adjacent to a vertex $u \in U$ if and only if there exists $b \in S$ such that $w = u + b$. Observe that distinct vertices u_1 and u_2 in U have a common neighbor $w \in [2n]^d$ if and only if $\{u_1, u_2\}$ is an edge of the subgraph $G_S[U]$ of G_S induced on U. Hence, we infer that $e(U) \leq \sum_{w \in [2n]^d} \binom{d_B(w)}{2}$, where $d_B(w)$ denotes the degree of w in B.

Now we claim that

$$e(U) = \sum_{w \in [2n]^d} \binom{d_B(w)}{2}. \tag{14}$$

In order to prove (14), we need to show that B contains no 4-cycle, i.e., that two distinct vertices in U do not have two distinct common neighbors in $[2n]^d$. Towards contradiction, suppose that there is a 4-cycle in B, that is, both u_1 and u_2 ($u_1 \neq u_2$) in U are adjacent to both w_1 and w_2 ($w_1 \neq w_2$) in $[2n]^d$. From the definition of B, there exist some $b_{11}, b_{12}, b_{21}, b_{22} \in S$ such that $w_1 = u_1 + b_{11}$, $w_1 = u_2 + b_{12}$, $w_2 = u_1 + b_{21}$ and $w_2 = u_2 + b_{22}$. Thus, $u_1 + b_{11} = u_2 + b_{12}$ and $u_1 + b_{21} = u_2 + b_{22}$, and hence, we have that $b_{11} - b_{21} = b_{12} - b_{22}$, that is, $b_{11} + b_{22} = b_{12} + b_{21}$. Since S is a Sidon set, we infer that $\{b_{11}, b_{22}\} = \{b_{12}, b_{21}\}$. However, by the assumptions $u_1 \neq u_2$ and $w_1 \neq w_2$, we have that $b_{11} \neq b_{12}$ and $b_{11} \neq b_{21}$, which contradicts to $\{b_{11}, b_{22}\} = \{b_{12}, b_{21}\}$. Therefore, there is no 4-cycle in B, and hence, identity (14) holds.

It follows from (14) that

$$e(U) = \sum_{w \in [2n]^d} \binom{d_B(w)}{2} \geq (2n)^d \binom{\frac{1}{(2n)^d} \sum_{w \in [2n]^d} d_B(w)}{2},$$

where the inequality follows from the convexity of $\binom{x}{2}$. Since B is a bipartite graph in which $d_B(u) = s$ for all $u \in U$, we have that

$$\begin{aligned} e(U) &\geq (2n)^d \binom{\frac{1}{(2n)^d} \sum_{u \in U} d_B(u)}{2} = (2n)^d \binom{s|U|/(2n)^d}{2} \\ &= (2n)^d \cdot \frac{1}{2} \frac{s|U|}{(2n)^d} \left(\frac{s|U|}{(2n)^d} - 1 \right). \end{aligned}$$

Under the assumption (12), that is, $1 \leq \frac{1}{2} \frac{s|U|}{(2n)^d}$, we infer that

$$e(U) \geq \frac{s|U|}{2} \cdot \frac{1}{2} \frac{s|U|}{(2n)^d} = \frac{s^2}{2^{d+1} n^d} \frac{|U|^2}{2} \geq \frac{s^2}{2^{d+1} n^d} \binom{|U|}{2}.$$

This completes the proof of Lemma 13. □

Now we are ready to bound the number of Sidon sets of a larger size by applying Lemmas 12 and 13 as follows.

Lemma 14. *Let n, s, and q be positive integers satisfying*

$$s^2 q \geq d 2^{d+1} n^d \log n. \tag{15}$$

Then, for any integer $r \geq 0$, we have

$$\mathcal{Z}_{n,d}(s + q + r) \leq \mathcal{Z}_{n,d}(s) \binom{n^d}{q} \binom{2^{d+1} n^d / s}{r}. \tag{16}$$

Proof. Fix S as an arbitrary Sidon set in $[n]^d$ of size s. We first consider the number of Sidon sets S^* of size $s+q+r$ containing S. Recall that if S^* is a Sidon set of size $s+k$ containing S, then the set $S^* \setminus S$ is an independent set in G_S of size k. Hence, in order to bound the number of Sidon sets of size $s+q+r$ containing S, we are going to estimate the number of independent sets of size $q+r$ in G_S. To this end, we will apply Lemma 12 to the graph G_S.

We first check conditions (9) and (10) of Lemma 12. First, Lemma 13 implies that (9) holds with $R = (2^{d+1}/s)n^d$ and $\beta = s^2/(2^{d+1}n^d)$. Next, condition (10) follows from inequality (15) because

$$q \geq \frac{d2^{d+1}n^d \log n}{s^2} = \frac{2^{d+1}n^d \log(n^d)}{s^2} \geq \beta^{-1} \log\left(\frac{N}{R}\right).$$

Thus, Lemma 12 with $G = G_S$, $N \leq n^d$ and $R = (2^{d+1}/s)n^d$ gives that for any integer $r \geq 0$, the number of independent sets in G_S of size $q+r$ is at most $\binom{n^d}{q}\binom{2^{d+1}n^d/s}{r}$. Consequently, the number of Sidon sets of size $s+q+r$ containing S is at most $\binom{n^d}{q}\binom{2^{d+1}n^d/s}{r}$. By summing over all Sidon sets S of size s, we infer that the number of all Sidon sets of size $s+q+r$ is at most $\mathcal{Z}_{n,d}(s)\binom{n^d}{q}\binom{2^{d+1}n^d/s}{r}$, which completes the proof of Lemma 14. □

Now we show Theorem 4 by applying Lemma 14 iteratively.

Proof of Theorem 4. Since $F([n]^d) = n^{d/2}(1+o(1))$, we infer that $\mathcal{Z}_{n,d}(t) = 0$ if $t > 1.1n^{d/2}$ for a sufficiently large $n = n(d)$, depending only on d. Hence, let t be an integer satisfying

$$2s_0 \leq t \leq 1.1n^{d/2}, \tag{17}$$

where $s_0 = (d2^{d+1}n^d \log n)^{1/3}$. Let K be the largest integer satisfying $t2^{-K} \geq s_0$. We define three sequences s_k, q_k, and r_k as follows: Set $s_1 = t2^{-K}$ and $q_1 = s_0$. For $1 \leq k \leq K+1$,

$$s_{k+1} = 2s_k, \quad q_{k+1} = q_k/4, \quad \text{and} \quad r_k = s_{k+1} - s_k - q_k. \tag{18}$$

Note that for $1 \leq k \leq K$,

$$s_k^2 q_k = s_1^2 q_1 \geq s_0^3 = d2^{d+1}n^d \log n,$$

equivalently, condition (15) holds with $s = s_k$ and $q = q_k$. Thus, Lemma 14 with $s = s_k$, $q = q_k$, and $r = r_k$ gives that for $1 \leq k \leq K$,

$$\mathcal{Z}_{n,d}(s_{k+1}) = \mathcal{Z}_{n,d}(s_k + q_k + r_k) \leq \mathcal{Z}_{n,d}(s_k)\binom{n^d}{q_k}\binom{2^{d+1}n^d/s_k}{r_k}.$$

Consequently,

$$\mathcal{Z}_{n,d}(t) = \mathcal{Z}_{n,d}(s_{K+1}) \leq \binom{n}{s_1} \cdot \prod_{k=1}^{K}\binom{n^d}{q_k} \cdot \prod_{k=1}^{K}\binom{2^{d+1}n^d/s_k}{r_k}. \tag{19}$$

Now we estimate three parts of the right-hand side of (19) separately. The first part is estimated by

$$\binom{n}{s_1} \le \binom{n}{2s_0} \le n^{2s_0}. \tag{20}$$

Next, for the second part of (19), we have that

$$\begin{aligned} \prod_{k=1}^{K} \binom{n^d}{q_k} &\le \prod_{k=1}^{K} (n^d)^{q_k} = (n^d)^{\sum_{k=1}^{K} q_k} \overset{(18)}{=} (n^d)^{q_1 \sum_{k=1}^{K} 4^{-k+1}} \\ &\le (n^d)^{4q_1/3} \le n^{2ds_0}, \end{aligned} \tag{21}$$

where the second inequality follows from $\sum_{k=1}^{K} 4^{-k+1} \le \sum_{k=1}^{\infty} 4^{-k+1} = 4/3$. For the last part of (19), we first have that

$$\prod_{k=1}^{K} \binom{2^{d+1}n^d/s_k}{r_k} \le \prod_{k=1}^{K} \binom{2^{d+1}n^d/s_k}{r_k + q_k}$$

since

$$\frac{r_k + q_k}{2^{d+1}n^d/s_k} \le \frac{s_{k+1} - s_k}{2^{d+1}n^d/s_k} = \frac{s_k}{2^{d+1}n^d/s_k} = \frac{s_k^2}{2^{d+1}n^d} \le \frac{s_0^2}{2^{d+1}n^d} \le \frac{t^2}{2^{d+1}n^d} \overset{(17)}{\le} \frac{1}{2}.$$

We further have that

$$\begin{aligned} \prod_{k=1}^{K} \binom{2^{d+1}n^d/s_k}{r_k} &\le \prod_{k=1}^{K} \binom{2^{d+1}n^d/s_k}{s_{k+1} - s_k} = \prod_{k=1}^{K} \binom{2^{d+1}n^d/s_k}{s_k} \\ &\le \prod_{k=1}^{K} \left(\frac{e2^{d+1}n^d}{s_k^2} \right)^{s_k} = \prod_{k=1}^{K} \left(\frac{e2^{d+1}n^d}{s_{K-k+1}^2} \right)^{s_{K-k+1}} \\ &\overset{(18)}{=} \prod_{k=1}^{K} \left(\frac{e2^{d+1}2^{2k}n^d}{t^2} \right)^{t2^{-k}} \\ &= \left(\frac{e2^{d+1}n^d}{t^2} \right)^{t\sum_{k=1}^{K} 2^{-k}} 2^{2t\sum_{k=1}^{K} k2^{-k}} \\ &\le \left(\frac{e2^{d+1}n^d}{t^2} \right)^{t} 2^{4t} = \left(\frac{e2^{d+5}n^d}{t^2} \right)^{t}. \end{aligned} \tag{22}$$

In view of (19), combining (20)–(22) yields that

$$\mathcal{Z}_{n,d}(t) \le n^{2(d+1)s_0} \left(\frac{e2^{d+5}n^d}{t^2} \right)^{t}$$

for $2s_0 \le t \le 1.1n^{d/2}$, which completes our proof of Theorem 4. □

3.3. The number of Sidon sets of a smaller size

Now we show Theorem 5 which gives an upper bound on $\mathcal{Z}_{n,d}(t)$ for $t = \Omega(n^{d/3})$. Our proof of Theorem 5 is similar to the proof of Lemma 14, and hence, we only give a sketch. By weakening condition (12) of Lemma 13 into $|U| \geq n^d/\gamma$, where $1/\gamma \geq 2^{d+1}/s$, we clearly have the following corollary of Lemma 13. (We omit the proof.)

Corollary 15. *Let γ be an arbitrary real number with $0 < \gamma \leq s/2^{d+1}$. For a Sidon set S in $[n]^d$ of size s, the graph G_S on $N := n^d - s$ vertices satisfies the following: For every vertex set U with $|U| \geq n^d/\gamma$, the number $e(U)$ of edges in the subgraph of G_S induced on U satisfies*

$$e(U) \geq \frac{s^2}{2^{d+1}n^d}\binom{|U|}{2}. \tag{23}$$

Combining Lemma 12 and Corollary 15 implies Theorem 5 as follows.

Proof of Theorem 5. Before applying Lemma 12 with $G = G_S$, we first check conditions (9) and (10) in Lemma 12 with $G = G_S$. First, by Corollary 15, the graph G_S satisfies (9) with $R = n^d/\gamma$ and $\beta = s^2/(2^{d+1}n^d)$. Next, condition (10) holds by setting $s = q = s^*$ where $s^* = \left(2^{(d+1)}n^d \log\gamma\right)^{1/3}$.

Now Lemma 12 with $G = G_S$ and $s = q = s^*$ implies that, for $t \geq 4s^*$,

$$\begin{aligned}
\mathcal{Z}_{n,d}(t) &\leq \mathcal{Z}_{n,d}(s^*)\binom{n^d}{s^*}\binom{n^d/\gamma}{t-2s^*} \leq \binom{n^d}{s^*}\binom{n^d}{s^*}\binom{n^d/\gamma}{t-2s^*} \\
&\leq \left(\frac{en^d}{s^*}\right)^{2s^*}\left(\frac{en^d}{\gamma(t-2s^*)}\right)^{t-2s^*} = \left(\frac{en^d}{s^*}\right)^{t}\left(\frac{1}{\gamma(\omega-2)}\right)^{t-2s^*} \\
&= \left(\frac{e\omega n^d}{t}\right)^{t}\left(\frac{1}{\gamma(\omega-2)}\right)^{t(1-2/\omega)} = \left(\frac{e\omega n^d}{t[\gamma(\omega-2)]^{1-2/\omega}}\right)^{t} \\
&= \left(C_\omega \frac{n^d}{t\gamma^{1-2/\omega}}\right)^{t}, \qquad (24)
\end{aligned}$$

where $C_\omega = e\omega/(\omega-2)^{1-2/\omega}$. We also have that

$$C_\omega = \frac{e\omega}{(\omega-2)^{1-2/\omega}} \leq \frac{e\omega}{(\omega/2)^{1-2/\omega}} = e2^{1-2/\omega}\omega^{2/\omega} \leq 2e\omega^{2/\omega} \leq 2e4^{1/2} = 4e, \tag{25}$$

where the first inequality follows from the assumption $\omega \geq 4$, and the last inequality follows from the fact that $f(x) = x^{2/x}$ is a decreasing function for $x \geq 4$. Combining (24) and (25) completes our proof of Theorem 5. □

4. Upper bounds on $F([n]_p)$

In this section we prove the upper bounds in Theorems 7–10. We first provide our proof of the upper bound in Theorem 7. In the proof, we will use the following version of Chernoff's bound.

Lemma 16 (Chernoff's bound, Corollary 4.6 in [10])**.** *Let X_i be independent random variables such that* $\Pr[X_i = 1] = p_i$ *and* $\Pr[X_i = 0] = 1 - p_i$*, and let* $X = \sum_{i=1}^{n} X_i$*. For* $0 < \lambda < 1$*,*

$$\Pr\Big[|X - \mathbb{E}(X)| \geq \lambda \mathbb{E}(X)\Big] \leq 2\exp\Big(-\frac{\lambda^2}{3}\mathbb{E}(X)\Big).$$

Proof of the upper bound in Theorem 7. We clearly have that $F\left([n]_p^d\right) \leq \left|[n]_p^d\right|$. Hence, in order to show the upper bound in Theorem 7, it suffices to show that a.a.s.

$$X := \left|[n]_p^d\right| \leq n^d p(1 + o(1)). \tag{26}$$

By the definition of $[n]_p^d$, we have that the expectation $\mathbb{E}(X)$ is $n^d p$. Then, Lemma 16 implies that a.a.s. $X = n^d p(1 + o(1))$ provided that $p \gg n^{-d}$. It gives (26), and hence, it completes our proof of the upper bound in Theorem 7. □

Next, we prove the upper bound in Theorem 8 using Theorem 5 as follows.

Proof of the upper bound in Theorem 8. For the upper bound, it suffices to show that there exists a positive constant $c = c(d)$ such that

$$\Pr\Big[[n]_p^d \text{ contains a Sidon set of size } cn^{d/3}\left(\log(n^{2d}p^3)\right)^{1/3}\Big] \to 0 \quad \text{as } n \to \infty. \tag{27}$$

The first moment method gives that the probability that $[n]_p^d$ contains a Sidon set of size t is at most $p^t \mathcal{Z}_{n,d}(t)$. We will use Theorem 5 in order to bound $\mathcal{Z}_{n,d}(t)$. Now we define suitable numbers γ, ω, and t satisfying both (4) and (5) in Theorem 5. For a positive constant $\delta \leq d/9$, we consider two cases separately: the first case is when $2n^{-2d/3} \leq p \leq n^{-2d/3+\delta}$ and the second case is for the remaining range of p, that is, $n^{-2d/3+\delta} \leq p \leq n^{-d/3-\varepsilon}$.

- **Case 1:** This case is when $2n^{-2d/3} \leq p \leq n^{-2d/3+\delta}$. Let $\gamma = n^{2d}p^3$. Under the assumption $2n^{-2d/3} \leq p \leq n^{-2d/3+\delta}$, we have that $8 \leq \gamma \leq n^{3\delta} \leq n^{d/3}$, and hence, the second inequality of (4) holds. Let $t = Cn^{d/3}\left(\log(n^{2d}p^3)\right)^{1/3}$, where $C = C(d)$ is a sufficiently large positive constant depending only on d. Then, the inequality of (5) holds.

  With the choice of γ and t, Theorem 5 implies that

$$\Pr\Big[[n]_p^d \text{ contains a Sidon set of size } t\Big] \leq p^t \mathcal{Z}_{n,d}(t) \leq \left(\frac{4en^d p}{t\gamma^{1-2/\omega}}\right)^t. \tag{28}$$

  The base in the right-hand side of (28) is

$$\begin{aligned}\frac{4en^d p}{t\gamma^{1-2/\omega}} &\leq \frac{4en^d p}{Cn^{d/3}(n^{2d}p^3)^{0.99}} \leq (n^{2d}p^3)^{1/3-0.99} \\ &\leq 8^{1/3-0.99} \leq 0.5,\end{aligned} \tag{29}$$

where the first inequality holds because of $t \geq Cn^{d/3}$, and the second inequality holds since $C \geq 4e$. Combining (28) and (29) yields that

$$\Pr\left[[n]_p^d \text{ contains a Sidon set of size } t\right] \leq 0.5^t \to 0 \quad \text{as } n \to \infty,$$

which gives (27).

- **Case 2:** This case is when $n^{-2d/3+\delta} \leq p \leq n^{-d/3-\varepsilon}$. Let $\gamma = n^{d/3}$. Then

$$s^* = c_0 n^{d/3} \left(\log(n^{d/3})\right)^{1/3} = c_0' n^{d/3} (\log n)^{1/3}$$

with positive constants $c_0 = c_0(d)$ and $c_0' = c_0'(d)$, and hence, the second inequality of (4) holds. Let

$$t = Cn^{d/3} \left(\log(n^{2d} p^3)\right)^{1/3} = C' n^{d/3} (\log n)^{1/3},$$

where $C = C(d)$ and $C' = C'(d, \delta)$ are sufficiently large positive constants. Then, the inequality of (5) holds.

With the choice of γ and t, Theorem 5 implies (28). The base in the right-hand side of (28) is

$$\frac{4en^d p}{t\gamma^{1-2/\omega}} \leq \frac{4en^d \cdot n^{-d/3-\varepsilon}}{C' n^{d/3} (\log n)^{1/3} n^{(d/3)(1-\varepsilon')}},$$

where $\varepsilon' = \varepsilon'(d)$ is a positive constant such that ε' goes to 0 as $C \to \infty$. We have that

$$\frac{4en^d p}{t\gamma^{1-2/\omega}} \leq \frac{n^{2d/3-\varepsilon}}{n^{2d/3-d\varepsilon'/3} \log n} \leq 0.5, \tag{30}$$

where the first and second inequalities follow from a choice of a sufficiently large $C = C(d)$. Therefore, inequalities (28) and (30) yield (27).

Therefore, the analysis in **Case 1** and **Case 2** implies (27), which completes our proof of the upper bound in Theorem 8. □

Next we show the upper bounds in Theorems 9 and 10. First, we claim that the upper bound in Theorem 9 follows from the upper bound in Theorem 10. Indeed, by monotonicity, the upper bound in Theorem 10 with $p = n^{-d/3} (\log n)^{8/3}$ gives the upper bound in Theorem 9. Therefore, it only remains to show the upper bound in Theorem 10. We show it by using Theorem 4 as follows.

Proof of the upper bound in Theorem 10. Let $q(t)$ be the probability that there exists a Sidon set in $[n]_p^d$ of size t. In order to show the upper bound in Theorem 10, it suffices to prove that there exists a positive constant $C = C(d)$ such that if $t = Cn^{d/2} p^{1/2}$, then $q(t) = o(1)$.

The first moment method gives that $q(t) \le p^t \mathcal{Z}_{n,d}(t)$. Since $t = Cn^{d/2}p^{1/2} \ge Cn^{d/3}(\log n)^{4/3}$, Theorem 4 implies that

$$q(t) \le n^{2(d+1)s_0} \left(\frac{e2^{d+5}n^d p}{t^2} \right)^t,$$

where $s_0 = cn^{d/3}(\log n)^{1/3}$ with a positive constant $c = c(d)$. From the choice $t = Cn^{d/2}p^{1/2}$, we have that

$$q(t) \le n^{c'n^{d/3}(\log n)^{1/3}} \left(\frac{e2^{d+5}}{C^2} \right)^t \le n^{c'n^{d/3}(\log n)^{1/3}} \left(\frac{1}{2} \right)^t,$$

where $c' = c'(d)$ is a positive constant. It is equivalent to the inequality

$$\log q(t) \le c'n^{d/3}(\log n)^{4/3} + t \log (1/2)\,. \tag{31}$$

Since $t = Cn^{d/2}p^{1/2} \ge Cn^{d/3}(\log n)^{4/3}$ with a sufficiently large constant $C = C(d)$, we infer that $\log q(t) \le -2 \log n$, that is, $q(t) \le n^{-2} = o(1)$. This completes our proof of the upper bound in Theorem 10. □

5. Lower bounds on $F([n]_p)$

We are going to show the lower bounds in Theorems 7–10. To this end, we first introduce a result from [6, 7] about lower bounds on the maximum size $F([n]_p)$ of Sidon sets in a random set $[n]_p = [n]_p^1$. Then, we define a bijection φ_d from $[n^d]$ to $[n]^d$, which was given by Cilleruelo [2], such that a Sidon set in $[n^d]$ is mapped to a Sidon set in $[n]^d$. Using the bijection φ_d, the lower bounds on $F([n^d]_p)$ in [7] will be converted to the lower bounds on $F([n]_p^d)$ in Theorems 7–10.

We first introduce the lower bounds on $F([n]_p)$ which were proved in Theorems 2.3–2.7 of [7].

Lemma 17 ([7])**.** *There exist positive absolute constants c_1 and c_2 such that the following holds a.a.s.*:

(a) $F([n]_p) \ge (1 + o(1))np$ *if* $n^{-1} \ll p \ll n^{-2/3}$,
(b) $F([n]_p) \ge (1/3 + o(1))\, np$ *if* $n^{-1} \ll p \le 2n^{-2/3}$,
(c) $F([n]_p) \ge c_1 n^{1/3} \Big(\log(n^2p^3) \Big)^{1/3}$ *if* $2n^{-2/3} \le p \le n^{-1/3}(\log n)^{2/3}$,
(d) $F([n]_p) \ge c_2 \sqrt{np}$ *if* $n^{-1/3}(\log n)^{2/3} \le p \le 1$.

Let $\varphi_d : [n^d] \to [n]^d$ be the bijection defined by $\varphi_d(a) = (a_0, \dots, a_{d-1})$ where

$$a = a_0 + a_1 n + a_2 n^2 + \cdots + a_{d-1} n^{d-1}.$$

Cilleruelo [2] showed the following property of the bijection φ_d.

Property 18. If A is a Sidon set in $[n^d]$, then $\varphi_d(A)$ is a Sidon set in $[n]^d$.

For a proof of Property 18, see Theorem 5 and its proof in [2].

Now we are ready to show the following lower bounds on $F\left([n]_p^d\right)$ which easily imply the lower bounds in Theorems 7–10.

Lemma 19. *There exist positive absolute constants c_1 and c_2 such that the following holds a.a.s.*:

(a) $F\left([n]_p^d\right) \geq (1+o(1))n^d p$ *if* $n^{-d} \ll p \ll n^{-2d/3}$

(b) $F\left([n]_p^d\right) \geq (1/3+o(1))\, n^d p$ *if* $n^{-d} \ll p \leq 2n^{-2d/3}$

(c) $F\left([n]_p^d\right) \geq c_1 n^{d/3}\Big(\log(n^{2d}p^3)\Big)^{1/3}$ *if* $2n^{-2d/3} \leq p \leq d^{2/3}n^{-d/3}\,(\log n)^{2/3}$

(d) $F\left([n]_p^d\right) \geq c_2 n^{d/2}p^{1/2}$ *if* $d^{2/3}n^{-d/3}\,(\log n)^{2/3} \leq p \leq 1$.

Proof. Recall the bijection φ_d introduced just before Property 18. By the bijection φ_d, a random set $[n^d]_p$ is mapped to $\varphi_d\left([n^d]_p\right)$. Since $\varphi_d\left([n^d]_p\right)$ is stochastically identical to $[n]_p^d$, we have that $[n^d]_p$ is stochastically identical to $[n]_p^d$. Property 18 implies that if $A \subset [n^d]_p$ is a Sidon set, then $\varphi_d(A) \subset \varphi_d([n^d]_p) = [n]_p^d$ is a Sidon set. Hence we infer that

$$F([n^d]_p) \leq F\left([n]_p^d\right). \tag{32}$$

Therefore, in order to obtain a lower bound on $F\left([n]_p^d\right)$, one can use a lower bound on $F([n^d]_p)$. By Lemma 17 with n^d instead of n, we obtain the following lower bounds on $F([n^d]_p)$: There exist absolute constants c_1 and c_2 such that the following holds a.a.s.:

(a) $F([n^d]_p) \geq (1+o(1))n^d p$ if $n^{-d} \ll p \ll n^{-2d/3}$.

(b) $F([n^d]_p) \geq (1/3+o(1))\, n^d p$ if $n^{-d} \ll p \leq 2n^{-2d/3}$.

(c) $F([n^d]_p) \geq c_1 n^{d/3}\Big(\log(n^{2d}p^3)\Big)^{1/3}$ if $2n^{-2d/3} \leq p \leq n^{-d/3}\left(\log(n^d)\right)^{2/3}$.

(d) $F([n^d]_p) \geq c_2\sqrt{n^d p}$ if $n^{-d/3}\left(\log(n^d)\right)^{2/3} \leq p \leq 1$.

Combining inequality (32) and the above (a)–(d) implies Lemma 19. □

Acknowledgement. The author thanks Mark Siggers for helpful comments and corrections, Domingos Dellamonica Jr. for discussion yielding the improvement in Theorem 5, and the referee for valuable comments.

References

[1] S. Chowla, *Solution of a problem of Erdős and Turán in additive-number theory*, Proc. Nat. Acad. Sci. India. Sect. A. **14** (1944), 1–2.

[2] J. Cilleruelo, *Sidon sets in $\mathbb{N}^d$*, J. Combin. Theory Ser. A **117** (2010), no. 7, 857–871.

[3] P. Erdős, *On a problem of Sidon in additive number theory and on some related problems. Addendum*, J. Lond. Math. Soc. **19** (1944), 208.

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

[5] H. Halberstam and K. F. Roth, *Sequences*, Second ed., Springer-Verlag, New York, 1983.

[6] Y. Kohayakawa, S. Lee, and V. Rödl, *The maximum size of a Sidon set contained in a sparse random set of integers*, Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, 159–171, SIAM, Philadelphia, PA, 2011.

[7] Y. Kohayakawa, S. J. Lee, V. Rödl, and W. Samotij, *The number of Sidon sets and the maximum size of Sidon sets contained in a sparse random set of integers*, Random Structures Algorithms **46** (2015), no. 1, 1–25.

[8] B. Lindström, *An inequality for B_2-sequences*, J. Combin. Theory **6** (1969), 211–212.

[9] ———, *On B_2-sequences of vectors*, J. Number Theory **4** (1972), 261–265.
[10] M. Mitzenmacher and E. Upfal, *Probability and Computing*, Cambridge University Press, Cambridge, 2005.
[11] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electron. J. Combin. (2004), Dynamic surveys 11, 39 pp.
[12] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), no. 3, 377–385.

Sang June Lee
Department of Mathematics
Duksung Women's University
Seoul 01369, Korea
E-mail address: sanglee242@duksung.ac.kr, sjlee242@gmail.com