MATH 595 **Hypergraph Container Method notes**

Friday, January 25, 2019

---

1 Lecture 5: The number of Sidon sets (1/25/2019)

A set $A \subseteq [n]$ is a *Sidon set* if there is no *Sidon 4-tuple*, i.e., (a, b, c, d) in A with $a+b = c+d$ and $\{a, b\} \cap \{c, d\} = \emptyset$. A major problem concerning Sidon sets is to find the largest cardinality of a Sidon set contained in $[n]$. A trivial upper bound, $|A| \leqslant 2\sqrt{n}$, can be given by observing that in a Sidon set A, the sums of two different numbers in A are all distinct, i.e. $\binom{|A|}{2} \leqslant 2n$. By the works of Erdős and Turán [6], Singer [10], Erdős [4], and Chowla [3], it is known that the maximum Sidon set is of size $(1 + o(1))\sqrt{n}$. This is also true for the Sidon sets in $\mathbb{Z}_n$.

1.1 A connection with C_4-free graphs

Due to Brown [1] and Erdős, Rényi, and Sós [5], it is well known that the maximum number of edges in a C_4-free graph is $(\frac{1}{2} + o(1))n^{3/2}$. The upper bound is relatively easy to obtain. However, it is difficult to construct n-vertex graphs without 4-cycles that have $(\frac{1}{2} + o(1))n^{3/2}$ edges. Next, we show a construction for the lower bound.

Construction 1.1 (The incidence graph of a finite projective plane, Reiman [8])**.** Let q be a prime power. It is known that there exists a finite projective plane with a point set $\mathcal{P}$ and a line set $\mathcal{L}$ such that the following hold.

- $|\mathcal{P}| = |\mathcal{L}| = q^2 + q + 1$;
- Each line contains exactly $q + 1$ points;
- Each point is contained in exactly $q + 1$ lines.

Let G be the graph with vertex set $\mathcal{P} \cup \mathcal{L}$ and edge set

$$E = \{(p, \ell) : p \in \mathcal{P},\ \ell \in \mathcal{L},\ p \text{ is contained in the line } \ell\}.$$

The graph G is a bipartite graph and also an optimal C_4-free graph. Why is G C_4-free? Suppose that G contains a 4-cycle $p_1\ell_1p_2\ell_2$. Then we would have two different points p_1, p_2 and two different lines ℓ_1, ℓ_2 such that $p_1, p_2 \in \ell_1, \ell_2$, which is impossible.

To construct such a projective plane, one can consider equivalence classes of the finite field $\mathbb{F}_q^3$; two elements (a,b,c) and (a',b',c') in $\mathbb{F}_q^3 \setminus \{(0,0,0)\}$ are equivalent if $(a,b,c) = \lambda(a',b',c')$ for some $\lambda \neq 0$. Let the point set $\mathcal{P}$ be the set of equivalence classes. There are $\frac{q^3-1}{q-1} = q^2+q+1$ such points. For every $(a,b,c) \in \mathcal{P}$, a straight line is defined as the set of all points (x,y,z) which satisfy the equation $ax+by+cz=0$. We let $\mathcal{L}$ be the set of all such lines.

To obtain a non-bipartite construction, one can consider the projective norm graph, which was used in [5]. Let G be a graph with vertex set $\mathcal{P}$, where $\mathcal{P}$ is the set of equivalence classes of $\mathbb{F}_q^3$ defined as above and $|\mathcal{P}| = q^2+q+1$. The equivalence class of (a,b,c) is connected by an edge to the class of (x,y,z) if (a,b,c) and (x,y,z) are in two different classes, and $ax+by+cz=0$. One can show that G is C_4-free with $e(G) = \frac{1}{2}q(q+1)^2$, and we omit the details of the proof here.

Now let $A \subset [n]$ be a Sidon set. We define a bipartite graph G on the vertex set $[n] \cup [2n]$ such that for two vertices $i \in [n]$ and $j \in [2n]$, i is adjacent to j if and only if there exists a number $a \in A$ such that $i+a=j$. If A is of size $C\sqrt{n}$, then we have $e(G) = n \cdot |A| = Cn^{3/2}$. We claim that G is a C_4-free graph. Suppose that there exists a 4-cycle $i, i+a, j, j+d$, where $a,d \in A$. Since $(j, i+a)$ and $(i, j+d)$ are edges, we can find two numbers $b,c \in A$ such that $j+c = i+a$ and $i+b = j+d$. However, this also gives $a+d = b+c$, where $\{a,d\} \neq \{b,c\}$ because of $i \neq j$. Therefore, we find a Sidon 4-tuple (a,d,b,c) in A, which is a contradiction.

1.2 The number of Sidon sets

In 1990, Cameron and Erdős [2] proposed the problem of determining the number of Sidon sets in $[n]$. By the largest cardinality of a Sidon set, it is trivial to obtain the following bound:

$$2^{(1+o(1))\sqrt{n}} \leqslant \text{the number of Sidon sets } \leqslant \binom{n}{(1+o(1))\sqrt{n}} \leqslant 2^{\sqrt{n}\log n}.$$

It seems natural to think that the trivial lower bound is the best possible. However, surprisingly, Saxton and Thomason [9] showed that the lower bound is not tight.

Theorem 1.2 (Saxton-Thomason [9])**.** *The number of Sidon sets in* $[n]$ *is at least* $2^{1.16\sqrt{n}}$.

Proof. Assume that n is a multiple of 4. Let $A \subseteq [n/4]$ be the largest Sidon set in $\mathbb{Z}_{n/4}$, and $|A| = \left(\frac{1}{2}+o(1)\right)\sqrt{n}$. For every $a \in A$, we can choose u_a to be any one of $\{a, \frac{n}{4}+a, \frac{n}{2}+a, \frac{3}{4}n+a\}$, or nothing. Let $U = \{u_a : a \in A\}$. Clearly, the number of choices for U is $5^{\frac{1}{2}\sqrt{n}} \approx 2^{1.16\sqrt{n}}$. We claim that U is a Sidon set in $[n]$. Suppose that there is a Sidon 4-tuple

(a', b', c', d') in U such that $a' + b' = c' + d'$. Then we can find numbers $a, b, c, d \in A$ such that $a + b \equiv c + d \mod n/4$, which contradicts the fact that A is a Sidon set in $\mathbb{Z}_{n/4}$. □

The best result on the upper bound is given by Kohayakawa, Lee, Rödl and Samotij [7], using the graph container method.

Theorem 1.3 (Kohayakawa-Lee-Rödl-Samotij [7]). *The number of Sidon sets in $[n]$ is at most $2^{c\sqrt{n}}$, where c is a constant arbitrarily close to $\log_2(32e) \approx 6.442$ for sufficiently large enough n.*

We remark that Saxton and Thomason [9] obtained the upper bound $2^{(55+o(1))\sqrt{n}}$ by applying the hypergraph container method.

1.3 Supersaturation

For two sets $A, U \subseteq [n]$, define a multigraph $H^U(A)$ on vertex set A such that for every $a_1, a_2 \in A$ with $a_1 < a_2$, the multiplicity of the edge a_1a_2 in $H^U(A)$ is the number of ordered pairs (u_1, u_2) in U such that (a_1, u_1, u_2, a_2) is a Sidon 4-tuple.

Lemma 1.4. *Let $A, U \subseteq [n]$. If $|A| \cdot |U| \geqslant 6n$, then $e(H^U(A)) > \frac{|A|^2|U|^2}{12n}$.*

Proof. Let F be a simple bipartite graph defined on the set $A \cup [2n]$ satisfying that for every $a \in A$ and $m \in [2n]$, a is adjacent to m if and only if there is an element $u \in U$ such that $a + u = m$. Clearly, for every vertex $a \in A$, we have $d_F(a) = |U|$.

Let $\mathcal{P}$ be the set of paths of length 2 (or 3-paths) in F with endpoints in A. Then we have

$$|\mathcal{P}| = \sum_{m\in[2n]} \binom{d_F(m)}{2} \geqslant 2n \binom{\frac{\sum_{m\in[2n]} d_F(m)}{2n}}{2} = 2n \binom{\frac{|A|\cdot|U|}{2n}}{2} > \frac{|A|^2|U|^2}{6n}.$$

A path $P = \{xyz\} \in \mathcal{P}$ is called *trivial* if $x + z = y$; otherwise, P is *nontrivial*. Note that P is trivial if and only if both x and z belong to $A \cap U$. Thus, the number of trivial paths in $\mathcal{P}$ is exactly $\binom{|A\cap U|}{2}$. Let $\mathcal{P}'$ be the set of nontrivial paths in $\mathcal{P}$. Every 3-path in $\mathcal{P}'$ corresponds to an edge in $H^U(A)$ and vice versa. Therefore, we obtain

$$e(H^U(A)) = |\mathcal{P}'| = |\mathcal{P}| - \binom{|A \cap U|}{2} > \frac{|A|^2|U|^2}{6n} - \frac{|A| \cdot |U|}{2} \geqslant \frac{|A|^2|U|^2}{12n},$$

where the first inequality is given by $|A \cap U| \leqslant \min\{|A|, |U|\} \leqslant \sqrt{|A| \cdot |U|}$ and the second inequality follows from the assumption $|A| \cdot |U| \geqslant 6n$. □

1.4 Proof of Theorem 1.3

Proposition 1.5. *Let $U \subseteq [n]$ be a Sidon set, and $A \subseteq [n] - U$. Then $H^U(A)$ is a simple graph.*

Proof. Suppose that a_1a_2 has multiplicity at least 2. There there exist $u_1, u_2, u_3, u_4 \in U$ such that $a_1 + u_1 = a_2 + u_2$ and $a_1 + u_3 = a_2 + u_4$. Then we obtain $u_1 + u_4 = u_2 + u_3$, which contradicts the fact that U is a Sidon set. □

Proposition 1.6. *Let $U \subseteq [n]$ be a Sidon set, and $I \subseteq [n] - U$ such that $U \cup I$ is also a Sidon set. Then I is an independent set in $H^U(A)$.*

Proof. Otherwise, there exist $a_1, a_2 \in I$ and $u_1, u_2 \in U$ such that $a_1 + u_1 = a_2 + u_2$, which contradicts the fact that $U \cup I$ is a Sidon set. □

Let U be a Sidon set of size $\frac{\sqrt{n}}{\log n}$. The reason to choose this size is that later in the counting process, we need to make sure that the number of choices for U is at most $2^{O(\sqrt{n})}$. Then by Proposition 1.6, it suffices to count the number of independent sets in $H^U([n]-U)$.

First, let us try to apply the standard one phase graph container method. Fix an arbitrary set $I \subseteq A$ such that $U \cup I$ is a Sidon set. We start with $A = [n] - U$ and $T = \emptyset$. In each iteration, we take a vertex v of maximum degree in $H^U(A)$. If $v \in I$, then we let $T = T \cup \{v\}$, and $A = A - \{v\} - N(v)$. Otherwise, let $T = T$, and $A = A - \{v\}$. We stop the algorithm when A is small enough, i.e. $A = O(\sqrt{n})$.

Note that this method works only if $H^U(A)$ has many edges. By the supersaturation, i.e. Lemma 1.4, we would require $|A||U| \geqslant 6n$, that is, $|A| \geqslant \sqrt{n}\log n$. Therefore, the size of A cannot reach $O(\sqrt{n})$. Moreover, it turns out that we can prove $|T| \leqslant \frac{\sqrt{n}}{\log n}$ is true only when $|A| \geqslant \sqrt{n}\log^3 n$. This is because that when A is small, the maximum degree of $H^U(A)$ also becomes small, and then we need add more vertices in T to shrink the set A. The standard one phase graph container method fails to work.

Proof of Theorem 1.3 [7]. First, we shall apply a multi-phase graph container method to get the certificates. Fix a Sidon set I. Let U be an arbitrary subset of I of size $\frac{\sqrt{n}}{\log n}$.

Phase I. We start with $A = [n] - U$ and $T = \emptyset$. We shall apply the graph container algorithm on the graph $H^U(A)$ in the range $|A| \geqslant 6\sqrt{n}\log^3 n$.

To be more precise, in each iteration, we take a vertex $v \in A$ of maximum degree in $H^U(A)$. If $v \in I$, then we let $T = T \cup \{v\}$, and $A = A - \{v\} - N(v)$. Otherwise, let $T = T$, and $A = A - \{v\}$. We stop the algorithm when the size of A reaches $6\sqrt{n}\log^3 n$.

In the end of Phase I, let $T_{\rm I} := T$, and $A_{\rm I} := A$. By Lemma 1.4 and $|A| \geqslant 6\sqrt{n}\log^3 n$, in each iteration, we obtain that the average degree of $H^U(A)$ is

$$d(H^U(A)) = \frac{2e(H^U(A))}{|A|} \geqslant \frac{|A||U|^2}{6n} \geqslant |U|\log^2 n.$$

Therefore, we have $|T_{\rm I}| \leqslant \frac{n}{|U|\log^2 n} = \frac{\sqrt{n}}{\log n}$.

Phase II. We start with $A = A_{\rm I}$ and $T = \emptyset$. We shall apply the graph container algorithm on the graph $H^U(A)$ in the range $6\sqrt{n}\log^3 n > |A| \geqslant 6\sqrt{n}\log n$.

In the end of Phase II, let $T_{\rm II} := T$, and $A_{\rm II} := A$. Note that in this phase, we still keep $|A||U| \geqslant 6n$, and then $d(H^U(A)) \geqslant \frac{|A||U|^2}{6n} \geqslant |U|$. Therefore, $|T_{\rm II}| \leqslant \frac{6\sqrt{n}\log^3 n}{|U|} = 6\log^4 n$.

Phase III$_j$, for $1 \leqslant j \leqslant \log\log n$. For $j = 1$, we start with $A = A_{\rm II}$ and $T = \emptyset$; for $j \geqslant 2$, we start with $A = A_{j-1}$ and $T = \emptyset$. Let U_j be an arbitrary subset of $A \cap I$ of size $2^j\frac{\sqrt{n}}{\log n}$. We shall apply the graph container algorithm on the graph $H^{U_j}(A)$ in the range $\frac{6\sqrt{n}\log n}{2^{j-1}} > |A| \geqslant \frac{6\sqrt{n}\log n}{2^j}$.

In the end of Phase III$_j$, let $T_j := T$, and $A_j := A$. Note that in this phase, we still keep $|A||U_j| \geqslant 6n$, and similarly, we have $|T_j| \leqslant \frac{6\sqrt{n}\log n}{2^{j-1}}/2^j\frac{\sqrt{n}}{\log n} \leqslant 3\log^2 n$.

From the multi-phase graph container algorithm, for each Sidon set I, we build a certificate $\{U, U_1, \ldots, U_{\log\log n}\}\bigcup\{T_{\rm I}, T_{\rm II}, T_1, \ldots, T_{\log\log n}\}$, which uniquely determines a set sequence $\{A_{\rm I}, A_{\rm II}, A_1, \ldots, A_{\log\log n}\}$. Let $C = A_{\log\log n}$. Then the following conditions are satisfied:

- $U = \frac{\sqrt{n}}{\log n}$;
- $U_j = 2^j\frac{\sqrt{n}}{\log n}$ and $U_j \subseteq A_{j-1}$;
- $T_{\rm I} \subseteq [n]$, $|T_{\rm II}| \leqslant \log^4 n$, and $|T_j| \leqslant 3\log^2 n$ for all $j \geqslant 1$;
- $I \subseteq C\bigcup T_{\rm I}\bigcup T_{\rm II}\bigcup_{j=1}^{\log\log n} T_j$, and $|C| = O(\sqrt{n})$.

Note that the third condition indicates that the number of choices for $\{T_{\rm I}, T_{\rm II}, T_1, \ldots, T_{\log\log n}\}$ is $2^{O(\sqrt{n})}$.

Claim 1.7.

$$\prod_{j=1}^{\log\log n}\binom{\frac{6\sqrt{n}\log n}{2^{j-1}}}{2^j\frac{\sqrt{n}}{\log n}} = 2^{O(\sqrt{n})}.$$

Proof. Let $x = \frac{6\sqrt{n}\log n}{2^{\log\log n-1}} = 12\sqrt{n}$. Then the left side is equal to

$$\begin{aligned}\prod_{i=0}^{\log\log n-1}\binom{2^i x}{\frac{12n}{2^i x}} &\leqslant \prod_{i=0}^{\log\log n-1}\left(\frac{e\cdot x^2 2^{2i}}{12n}\right)^{\frac{12n}{2^i x}} = \prod_{i=0}^{\log\log n-1}(12e2^{2i})^{\frac{\sqrt{n}}{2^i}}\\ &\leqslant \prod_{i=0}^{\log\log n-1} 2^{\left[(\log(12e)+2i)2^{-i}\right]\sqrt{n}} \leqslant 2^{\left[\sum_{i=0}^{\infty}(\log(12e)+2i)2^{-i}\right]\sqrt{n}}\\ &= 2^{(2\log(12e)+4)\sqrt{n}},\end{aligned}$$

where the first inequality follows from the Stirling's formula. □

Therefore, the number of Sidon sets is at most

$$2^{|C|}2^{O(\sqrt{n})}\binom{n}{\frac{\sqrt{n}}{\log n}}\prod_{j=1}^{\log\log n}\binom{|A_{j-1}|}{2^j\frac{\sqrt{n}}{\log n}} = 2^{O(\sqrt{n})}\prod_{j=1}^{\log\log n}\binom{\frac{6\sqrt{n}\log n}{2^{j-1}}}{2^j\frac{\sqrt{n}}{\log n}} = 2^{O(\sqrt{n})}.$$

□

References

[1] W. G. Brown. *On the non-existence of a type of regular graphs of girth 5.* Canadian Journal of Mathematics 19 (1967): 644–648.

[2] P. J. Cameron and P. Erdős. *On the number of sets of integers with various properties.* Number theory (Banff, AB, 1988), 61–79. (1990)

[3] 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. 1, 1.2, 7.2.

[4] P. Erdős. *On a Problem of Sidon in Additive Number Theory and on Some Related Problems Addendum.* Journal of the London Mathematical Society 19, no. 76 Part 4 (1944): 208–208.

[5] P. Erdős, A. Rényi, and Vera T. Sós. *On a problem of graph theory.* Publ. Math. Inst. Hungar. Acad. Sci 7 (1962): 215–235.

[6] P. Erdős, P. Turán. *On a problem of Sidon in additive number theory, and on some related problems.* Journal of the London Mathematical Society 1, no. 4 (1941): 212–215.

[7] Y. Kohayakawa, S. J. Lee, V. Rödl, 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, no. 1 (2015): 1–25.

[8] I. Reiman. *Uber ein Problem von K. Zarankiewicz*. Acta Mathematica Hungarica 9.3–4 (1958): 269–273.

[9] D. Saxton and A.G. Thomason, *Hypergraph Containers*. Inventiones Mathematicae, 201 (2015), 925–992.

[10] J. Singer. *A theorem in finite projective geometry and some applications to number theory.* Transactions of the American Mathematical Society 43, no. 3 (1938): 377–385.