THREE FAMOUS THEOREMS ON FINITE SETS

DANIEL MULCAHY

1. Introduction

There are several results on combinatorics of subsets of a finite set $N = \{1, 2, \ldots, n\}$ that have been very historically significant and inspired the development of new areas of mathematics. We present three of these theorems following [1] and the talk by Aiden Mathieu: the theorems of Sperner and Erdős-Ko-Rado and Hall's "Marriage theorem"

2. Sperner's Theorem

This question was proposed and solved by Emanuel Sperner in 1928, but the argument we present is by David Lubell. Let $N = \{1, 2, \ldots, n\}$

Definition 1. *An* antichain *in N is a family of subsets $\mathcal{F}$ of N such that no subset in $\mathcal{F}$ is contained in another.*

We may ask what is the size of the largest antichain?

The family $\mathcal{F}_k$ consisting of subsets of order k is an antichain of size $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, and the largest of these is $\binom{n}{\lfloor n/2 \rfloor}$. Sperner's theorem tells us that there is none larger.

Theorem 1 (Sperner)**.** *For any antichain $\mathcal{F}$,*

$$|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$$

Proof. Consider chains of subsets $\varnothing = C_0 \subset C_1 \subset \cdots \subset C_n = N$. Each C_{i+1} must contain one more element than C_i, i.e. such a chain consists of adding each element of N one by one, so the number of such chains is $n!$, the number of permutations of N. Let $A \subset N$ of size k. The number of chains containing A is the number of ways to form a chain $\varnothing = C_0 \subset C_1 \subset \cdots \subset C_k = A$ multiplied by the number of ways to form $A = C_k \subset C_{k+1} \subset \cdots \subset C_n = N$, which is $k!(n-k)!$. Let $\mathcal{F}$ be an antichain; then no two elements of $\mathcal{F}$ can appear in the same chain. Thus if $m_k = |\{A \in \mathcal{F} \mid |A| = k\}|$, the total number of chains containing sets in $\mathcal{F}$ is

$$\sum_{k=0}^{n} m_k k!(n-k)! \leq n!$$

$$\sum_{k=0}^{n} \frac{m_k}{\binom{n}{k}} \leq 1$$

$$\min_k \left\{ \frac{1}{\binom{n}{k}} \right\} \sum_{k=0}^{n} m_k \leq 1$$

$$\frac{1}{\max_k \left\{ \binom{n}{k} \right\}} |\mathcal{F}| \leq 1$$

$$\frac{1}{\binom{n}{\lfloor n/2 \rfloor}} |\mathcal{F}| \leq 1$$

$$|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$$

□

3. Erdős-Ko-Rado Theorem

This result was found in 1938 by Paul Erdős, Chao Ko and Richard Rado, but this proof is due to Gyula Katona.

Definition 2. *A family $\mathcal{F}$ of subsets of N is called an* intersecting family *if $A \cap B \neq \varnothing$ $\forall A, B \in \mathcal{F}$. An intersecting family consisting of sets of size k is called an* intersecting k-family*.*

The largest intersecting family is of size 2^{n-1}, e.g. the family of all subsets that contain 1. This is maximal as for any $A \subset N,\ A \cap (N \setminus A) = \varnothing$ so no intersecting family can contain more than half of the 2^n subsets of N. If $k > \frac{n}{2}$ then any two subsets of size k intersect. Otherwise by taking all sets of size k that contain 1, we obtain an intersecting k-family of size $\binom{n-1}{k-1}$

Theorem 2 (Erdős-Ko-Rado). *For any intersecting k-family $\mathcal{F}$, $|\mathcal{F}| \leq \binom{n-1}{k-1}$ if $n \geq 2k$.*

Proof. Consider a circle divided into n edges by n points. An arc of length k consists of k consecutive edges joining $k+1$ points.

Lemma 1. *Suppose we have t different arcs $A_1, \dots, A_t$ of length k, where $n \geq 2k$, such that any two arcs have an edge in common. Then $t \leq k$.*

Proof. No two arcs may share an endpoint: if they did they would have to start in different directions as they are distinct, but then they could not share an edge as $n \geq 2k$. Each $A_2, \dots, A_t$ overlaps with A_1 and must therefore have a distinct endpoint at one of the $k-1$ points inside A_1, meaning there are at most $k-1$ of them.

$$\therefore t \leq k$$

□

Up to rotation there are $(n-1)!$ ways of writing the numbers 1 to n on the edges of an n-edged circle. For a chosen such circle, there are by the lemma at most k sets $A \in \mathcal{F}$ that appear as arcs on the circle; thus there are at most $k(n-1)!$ ways of representing elements of $\mathcal{F}$ on any such circle. Given $A \in F$, there are $k!(n-k)!$ possible ways to represent A on such a circle: $k!$ ways to order the elements of A consecutively and $(n-k)!$ for the rest. Therefore

$$|\mathcal{F}| \leq \frac{k(n-1)!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \binom{n-1}{k-1}$$

□

4. Marriage Theorem

Proven by Philip Hall in 1935, this very important theorem led to the field of matching theory.

Definition 3. *Let $A_1, \dots, A_n$ be subsets of a finite set X. A* system of distinct representatives *(SDR) of $\{A_1, \dots, A_n\}$ is a sequence of dictinct $x_1, \dots, x_n$ such that $x_i \in A_i \forall i$.*

This was referred to as the marriage theorem as, if we have n girls and a set X of boys, and the i'th girl is romantically interested in a set A_i, a system of distinct representatives provide each girl a distinct boy x_i to marry.

Clearly if an SDR exists then the union of any m distinct A_i must contain at least the m distinct elements x_i. It turns out that this condition is sufficient.

Theorem 3. *If the union of any m distinct A_i contains at least m elements ($1 \leq m \leq n$), then an SDR exists*

Proof. Induction on n: $n = 1$ trivial. Let $n > 1$. We call a collection of l sets A_i ($1 \leq l \leq n$) whose union contains exactly l elements a *critical family*. Suppose no critical family exists. Let x_n be some element of A_n and $\tilde{A}_i = A_i \setminus \{x_n\}$ for $1 \leq i \leq n-1$. For any m sets $A_{i_1}, \dots A_{i_m}$ with $i_k < n$ we know $A_{i_1} \cup \dots A_{i_m}$ contains at least $m+1$ elements, so $\tilde{A}_{i_1} \cup \dots \tilde{A}_{i_m}$ contains at least m elements, so by induction $\tilde{A}_1, \dots \tilde{A}_{n-1}$ has an SDR $x_1, \dots, x_{n-1}$ and thus $x_1, \dots, x_{n-1}, x_n$ is an SDR for $A_1, \dots, A_n$.

Suppose alternatively that a critical family exists, assume wlog it is $A_1, \dots A_l$. Then $\{A_1, \dots A_l\}$ as subsets of $X' = \bigcup_{i=1}^{l} A_i$ satisfy the condition of the theorem so has an SDR $x_1, \dots, x_l$. For any m of $A_{l+1}, \dots, A_n$ their combined union with X' must contain at least $l+m$ elements. Therefore if $\tilde{A}_i = A_i \setminus X'$ for $l+1 \leq i \leq n$ we have that the union of any m $\tilde{A}_i$ contains at least m elements, so these have an SDR $x_{l+1}, \dots, x_n$ disjoint from X' (which is also an SDR for $\{A_{l+1}, \dots, A_n\}$. Thus $x_1, \dots, x_n$ is an SDR for $\{A_1, \dots, A_n\}$ □

References

[1] Martin Aigner and Günter M. Ziegler. *Proofs from The Book.* Springer-Verlag, Berlin, fifth edition, 2014. Including illustrations by Karl H. Hofmann.