Three famous theorems on finite sets

Chapter 30

In this chapter we are concerned with a basic theme of combinatorics: properties and sizes of special families $\mathcal{F}$ of subsets of a finite set $N = \{1, 2, \dots, n\}$. We start with two results which are classics in the field: the theorems of Sperner and of Erdős–Ko–Rado. These two results have in common that they were reproved many times and that each of them initiated a new field of combinatorial set theory. For both theorems, induction seems to be the natural method, but the arguments we are going to discuss are quite different and truly inspired.

Emanuel Sperner

In 1928 Emanuel Sperner asked and answered the following question: Suppose we are given the set $N = \{1, 2, \dots, n\}$. Call a family $\mathcal{F}$ of subsets of N an *antichain* if no set of $\mathcal{F}$ contains another set of the family $\mathcal{F}$. What is the size of a largest antichain? Clearly, the family $\mathcal{F}_k$ of all k-sets satisfies the antichain property with $|\mathcal{F}_k| = \binom{n}{k}$. Looking at the maximum of the binomial coefficients (see page 14) we conclude that there is an antichain of size $\binom{n}{\lfloor n/2 \rfloor} = \max_k \binom{n}{k}$. Sperner's theorem now asserts that there are no larger ones.

Theorem 1. *The size of a largest antichain of an n-set is $\binom{n}{\lfloor n/2 \rfloor}$.*

■ **Proof.** Of the many proofs the following one, due to David Lubell, is probably the shortest and most elegant. Let $\mathcal{F}$ be an arbitrary antichain. Then we have to show $|\mathcal{F}| \le \binom{n}{\lfloor n/2 \rfloor}$. The key to the proof is that we consider *chains* of subsets $\varnothing = C_0 \subseteq C_1 \subseteq C_2 \subseteq \cdots \subset C_n = N$, where $|C_i| = i$ for $i = 0, \dots, n$. How many chains are there? Clearly, we obtain a chain by adding one by one the elements of N, so there are just as many chains as there are permutations of N, namely $n!$. Next, for a set $A \in \mathcal{F}$ we ask how many of these chains contain A. Again this is easy. To get from $\varnothing$ to A we have to add the elements of A one by one, and then to pass from A to N we have to add the remaining elements. Thus if A contains k elements, then by considering all these pairs of chains linked together we see that there are precisely $k!(n-k)!$ such chains. Note that no chain can pass through two different sets A and B of $\mathcal{F}$, since $\mathcal{F}$ is an antichain.

To complete the proof, let m_k be the number of k-sets in $\mathcal{F}$. Thus $|\mathcal{F}| = \sum_{k=0}^{n} m_k$. Then it follows from our discussion that the number of chains passing through some member of $\mathcal{F}$ is

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

and this expression cannot exceed the number $n!$ of *all* chains. Hence

M. Aigner, G. M. Ziegler, *Proofs from THE BOOK*, https://doi.org/10.1007/978-3-662-57265-8_30

we conclude

$$\sum_{k=0}^{n} m_k \frac{k!(n-k)!}{n!} \;\leq\; 1, \qquad \text{or} \qquad \sum_{k=0}^{n} \frac{m_k}{\binom{n}{k}} \;\leq\; 1.$$

Replacing the denominators by the largest binomial coefficient, we therefore obtain

$$\frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \sum_{k=0}^{n} m_k \;\leq\; 1, \qquad \text{that is,} \qquad |\mathcal{F}| \;=\; \sum_{k=0}^{n} m_k \;\leq\; \binom{n}{\lfloor n/2 \rfloor},$$

and the proof is complete. □

Check that the family of all $\frac{n}{2}$-sets for even n respectively the two families of all $\frac{n-1}{2}$-sets and of all $\frac{n+1}{2}$-sets, when n is odd, are indeed the *only* antichains that achieve the maximum size!

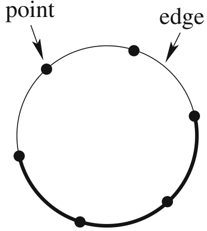
Our second result is of an entirely different nature. Again we consider the set $N = \{1, \dots, n\}$. Call a family $\mathcal{F}$ of subsets an *intersecting family* if any two sets in $\mathcal{F}$ have at least one element in common. It is almost immediate that the size of a largest intersecting family is 2^{n-1}. If $A \in \mathcal{F}$, then the complement $A^c = N \backslash A$ has empty intersection with A and accordingly cannot be in $\mathcal{F}$. Hence we conclude that an intersecting family contains at most half the number 2^n of all subsets, that is, $|\mathcal{F}| \leq 2^{n-1}$. On the other hand, if we consider the family of all sets containing a fixed element, say the family $\mathcal{F}_1$ of all sets containing 1, then clearly $|\mathcal{F}_1| = 2^{n-1}$, and the problem is settled.

But now let us ask the following question: How large can an intersecting family $\mathcal{F}$ be if all sets in $\mathcal{F}$ have the same size, say k ? Let us call such families *intersecting k-families*. To avoid trivialities, we assume $n \geq 2k$ since otherwise any two k-sets intersect, and there is nothing to prove. Taking up the above idea, we certainly obtain such a family $\mathcal{F}_1$ by considering all k-sets containing a fixed element, say 1. Clearly, we obtain all sets in $\mathcal{F}_1$ by adding to 1 all $(k-1)$-subsets of $\{2, 3, \dots, n\}$, hence $|\mathcal{F}_1| = \binom{n-1}{k-1}$. Can we do better? No — and this is the theorem of Erdős–Ko–Rado.

Theorem 2. *The largest size of an intersecting k-family in an n-set is $\binom{n-1}{k-1}$ when $n \geq 2k$.*

Paul Erdős, Chao Ko and Richard Rado found this result in 1938, but it was not published until 23 years later. Since then multitudes of proofs and variants have been given, but the following argument due to Gyula Katona is particularly elegant.

■ **Proof.** The key to the proof is the following simple lemma, which at first sight seems to be totally unrelated to our problem. Consider a circle C divided by n points into n edges. Let an *arc* of length k consist of $k+1$ consecutive points and the k edges between them.



A circle C for $n = 6$. The bold edges depict an arc of length 3.

Lemma. *Let $n \geq 2k$, and suppose we are given t distinct arcs $A_1, \dots, A_t$ of length k, such that any two arcs have an edge in common. Then $t \leq k$.*

To prove the lemma, note first that any point of C is the endpoint of at most one arc. Indeed, if A_i, A_j had a common endpoint v, then they would have to start in different direction (since they are distinct). But then they cannot have an edge in common as $n \geq 2k$. Let us fix A_1. Since any A_i $(i \geq 2)$ has an edge in common with A_1, one of the endpoints of A_i is an inner point of A_1. Since these endpoints must be distinct as we have just seen, and since A_1 contains $k-1$ inner points, we conclude that there can be at most $k-1$ further arcs, and thus at most k arcs altogether. $\square$

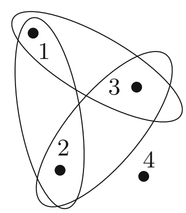
Now we proceed with the proof of the Erdős–Ko–Rado theorem. Let $\mathcal{F}$ be an intersecting k-family. Consider a circle C with n points and n edges as above. We take any cyclic permutation $\pi = (a_1, a_2, \dots, a_n)$ and write the numbers a_i clockwise next to the edges of C. Let us count the number of sets $A \in \mathcal{F}$ which appear as k *consecutive* numbers on C. Since $\mathcal{F}$ is an intersecting family we see by our lemma that we get at most k such sets. Since this holds for any cyclic permutation, and since there are $(n-1)!$ cyclic permutations, we produce in this way at most

$$k(n-1)!$$

sets of $\mathcal{F}$ which appear as consecutive elements of some cyclic permutation. How often do we count a fixed set $A \in \mathcal{F}$? Easy enough: A appears in π if the k elements of A appear consecutively in some order. Hence we have $k!$ possibilities to write A consecutively, and $(n-k)!$ ways to order the remaining elements. So we conclude that a fixed set A appears in precisely $k!(n-k)!$ cyclic permutations, and hence that

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

Again we may ask whether the families containing a fixed element are the only intersecting k-families of maximal size. This is certainly not true for $n = 2k$. For example, for $n = 4$ and $k = 2$ the family $\{1,2\}, \{1,3\}, \{2,3\}$ also has size $\binom{3}{1} = 3$. More generally, for $n = 2k$ we get the largest intersecting k-families, of size $\frac{1}{2}\binom{n}{k} = \binom{n-1}{k-1}$, by arbitrarily including one out of every pair of sets formed by a k-set A and its complement $N \backslash A$. But for $n > 2k$ the special families containing a fixed element are indeed the only ones. The reader is invited to try his hand at the proof.



An intersecting family for $n = 4$, $k = 2$

Finally, we turn to the third result which is arguably the most important basic theorem in finite set theory, the "marriage theorem" of Philip Hall proved in 1935. It opened the door to what is today called matching theory, with a wide variety of applications, some of which we shall see as we go along.

Consider a finite set X and a collection $A_1, \dots, A_n$ of subsets of X (which need not be distinct). Let us call a sequence $x_1, \dots, x_n$ a *system of distinct representatives* of $\{A_1, \dots, A_n\}$ if the x_i are distinct elements of X, and if $x_i \in A_i$ for all i. Of course, such a system, abbreviated SDR, need not exist, for example when one of the sets A_i is empty. The content of the theorem of Hall is the precise condition under which an SDR exists.

"A mass wedding"

Before giving the result let us state the human interpretation which gave it the folklore name *marriage theorem*: Consider a set $\{1, \dots, n\}$ of girls and a set X of boys. Whenever $x \in A_i$, then girl i and boy x are inclined to get married, thus A_i is just the set of possible matches of girl i. An SDR represents then a mass-wedding where every girl marries a boy she likes.

Back to sets, here is the statement of the result.

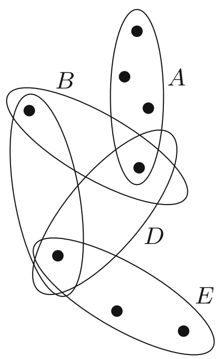
Theorem 3. *Let $A_1, \dots, A_n$ be a collection of subsets of a finite set X. Then there exists a system of distinct representatives if and only if the union of any m sets A_i contains at least m elements, for $1 \leq m \leq n$.*

The condition is clearly necessary: If m sets A_i contain between them fewer than m elements, then these m sets can certainly not be represented by distinct elements. The surprising fact (resulting in the universal applicability) is that this obvious condition is also sufficient. Hall's original proof was rather complicated, and subsequently many different proofs were given, of which the following one (due to Easterfield and rediscovered by Halmos and Vaughan) may be the most natural.

■ **Proof.** We use induction on n. For $n = 1$ there is nothing to prove. Let $n > 1$, and suppose $\{A_1, \dots, A_n\}$ satisfies the condition of the theorem which we abbreviate by (H). Call a collection of ℓ sets A_i with $1 \leq \ell < n$ a *critical family* if its union has cardinality ℓ. Now we distinguish two cases.

Case 1: There is no critical family.

Choose any element $x \in A_n$. Delete x from X and consider the collection $A'_1, \dots, A'_{n-1}$ with $A'_i = A_i \backslash \{x\}$. Since there is no critical family, we find that the union of any m sets A'_i contains at least m elements. Hence by induction on n there exists an SDR $x_1, \dots, x_{n-1}$ of $\{A'_1, \dots, A'_{n-1}\}$, and together with $x_n = x$, this gives an SDR for the original collection.



$\{B, C, D\}$ is a critical family

Case 2: There exists a critical family.

After renumbering the sets we may assume that $\{A_1, \dots, A_\ell\}$ is a critical family. Then $\bigcup_{i=1}^{\ell} A_i = \widetilde{X}$ with $|\widetilde{X}| = \ell$. Since $\ell < n$, we infer the existence of an SDR for $A_1, \dots, A_\ell$ by induction, that is, there is a numbering $x_1, \dots, x_\ell$ of $\widetilde{X}$ such that $x_i \in A_i$ for all $i \leq \ell$.

Consider now the remaining collection $A_{\ell+1}, \dots, A_n$, and take any m of these sets. Since the union of $A_1, \dots, A_\ell$ and these m sets contains at least $\ell + m$ elements by condition (H), we infer that the m sets contain at least m elements outside $\widetilde{X}$. In other words, condition (H) is satisfied for the family

$$A_{\ell+1} \backslash \widetilde{X}, \; \dots \; , A_n \backslash \widetilde{X}.$$

Induction now gives an SDR for $A_{\ell+1}, \dots, A_n$ that avoids $\widetilde{X}$. Combining it with $x_1, \dots, x_\ell$ we obtain an SDR for all sets A_i. This completes the proof. □

As we mentioned, Hall's theorem was the beginning of the now vast field of matching theory [6]. Of the many variants and ramifications let us state one particularly appealing result which the reader is invited to prove for himself:

> *Suppose the sets $A_1, \dots, A_n$ all have size $k \geq 1$ and suppose further that no element is contained in more than k sets. Then there exist k SDR's such that for any i the k representatives of A_i are distinct and thus together form the set A_i.*

A beautiful result which should open new horizons on marriage possibilities.

References

[1] T. E. EASTERFIELD: *A combinatorial algorithm,* J. London Math. Soc. **21** (1946), 219-226.

[2] P. ERDŐS, C. KO & R. RADO: *Intersection theorems for systems of finite sets,* Quart. J. Math. (Oxford), Ser. (2) **12** (1961), 313-320.

[3] P. HALL: *On representatives of subsets,* J. London Math. Soc. **10** (1935), 26-30.

[4] P. R. HALMOS & H. E. VAUGHAN: *The marriage problem,* Amer. J. Math. **72** (1950), 214-215.

[5] G. KATONA: *A simple proof of the Erdős–Ko–Rado theorem,* J. Combinatorial Theory, Ser. B **13** (1972), 183-184.

[6] L. LOVÁSZ & M. D. PLUMMER: *Matching Theory,* Akadémiai Kiadó, Budapest 1986.

[7] D. LUBELL: *A short proof of Sperner's theorem,* J. Combinatorial Theory **1** (1966), 299.

[8] E. SPERNER: *Ein Satz über Untermengen einer endlichen Menge,* Math. Zeitschrift **27** (1928), 544-548.