The Probabilistic Method - Basic ideas

We draw materials mainly from [2, 4].

To show that some (combinatorial) object exists, one can envision working on some probability space which the object lives in, and show that the probability of such an existence is strictly positive.

We will often use the following notations:

- $\delta(G)$ - the minimum degree of a graph G
- $\Delta(G)$ - the maximum degree of a graph G
- $\deg(v)$ - the degree of a vertex $v \in V(G)$ of a graph G
- $\chi(v)$ - the *chromatic number* of a graph G
- $\chi_e(v)$ - the *chromatic index* of a graph G
- $[n] := \{1, \ldots, n\}$
- a *k-subset* is a subset of size k of some set
- 2^X - the superset of a set X
- $\binom{X}{k}$ - the set of all k-subsets of a set X
- a *hypergraph* is a pair $H = (V, E)$ where V is a finite set, and E is a collection of subsets of V. Naturally, members of V are called vertices, and E are called edges of the hypergraph H
- a *uniform hypergraph* is a hypergraph all of whose edges have the same size
- an *n-uniform hypergraph* is a hypergraph all of whose edges have size n. (Thus, a simple graph is a 2-uniform hypergraph.)
- S_n - the *symmetric group* on $[n]$, i.e. the set of all permutations on $[n]$ (or n symbols)

1 Ramsey numbers

The classical example to which Erdős applied the probabilistic method is the so-called *Ramsey numbers*. In the simplest form, let $R(a, b)$ be the smallest integer n such that in any 2-edge-coloring of K_n with RED and BLUE, there exists a RED K_a or a BLUE K_b. (You can also think along this line: what's the smallest number n so that in any set of n people there must be a mutually acquainted people, or b mutual strangers. Try it with $a = b = 3$.)

Proposition 1.1 (Erdős, 1947 [5]). *If $\binom{n}{k} 2^{1-\binom{k}{2}} < 1$, then $R(k, k) > n$. Consequently, $R(k, k) > \lfloor 2^{k/2} \rfloor$ for all $k \geq 3$.*

Proof. (Note that $R(k,k)$ is the minimum n such that a graph G on n vertices contains a K_k, or the complement $\bar{G}$ of G has a K_k.)

Consider K_n and a random 2-coloring on its edges, namely we color an edge BLUE with probability $1/2$, and RED with probability $1/2$. For any k-subset S of vertices, let E_S be the event that the induced subgraph on S is monochromatic. Then, Prob$[E_S] = 2^{1-\binom{k}{2}}$. Thus, the probability that *some* k-subset forms a monochromatic subgraph is at most $\binom{n}{k}2^{1-\binom{k}{2}}$. Consequently, when $\binom{n}{k}2^{1-\binom{k}{2}} < 1$ there exists some 2-coloring for which there is no monochromatic K_k. In other words, $K(k,k) > n$.

For $k \geq 3$, let $n = \lfloor 2^{k/2} \rfloor$. Then,

$$\binom{n}{k}2^{1-\binom{k}{2}} < \frac{n^k}{k!} \cdot \frac{2^{1+k/2}}{2^{k^2/2}} < \frac{2^{1+k/2}}{k!} \cdot \frac{n^k}{2^{k^2/2}} < 1.$$

□

Note:

- The previous argument can be made a perfectly fine and simple counting argument.
- In most results we shall see, however, the probability is essential. Straightforward counting normally is way too cumbersome or virtually impossible.
- One can give a randomized algorithm to find a 2-coloring with no monochromatic K_k based on the proof above. We have seen that the probability of having some monochromatic K_k is at most $\frac{2^{1+k/2}}{k!} < 1$. (In fact, it is $\ll 1$ when k is large.) Hence, after m trials of colorings - the probability of having no monochromatic K_k is $1 - \left(\frac{2^{1+k/2}}{k!}\right)^m$, which goes to 1 as m grows larger. We can control the error probability easily.

Example 1.2. Prove that, if there is a real $p \in [0,1]$ such that

$$\binom{n}{a}p^{\binom{a}{2}} + \binom{n}{b}(1-p)^{\binom{b}{2}} < 1, \tag{1}$$

then the Ramsey number $R(a,b)$ satisfies $R(a,b) > n$. Use this to show

$$r(4,b) = \Omega\left(\frac{b^{3/2}}{(\ln b)^{3/2}}\right).$$

Solution. Randomly color each edge BLUE with probability p (and RED otherwise). The probability of having a BLUE K_a or a RED K_b is at most

$$\binom{n}{a}p^{\binom{a}{2}} + \binom{n}{b}(1-p)^{\binom{b}{2}} < 1.$$

Hence, $R(a,b) > n$.

To this end, note that

$$\binom{n}{a}p^{\binom{a}{2}} + \binom{n}{b}(1-p)^{\binom{b}{2}} < n^a p^{\binom{a}{2}}/a! + n^b e^{-\binom{b}{2}p}/b!.$$

Hence, as long as we maintain that

$$n^a p^{\binom{a}{2}}/a! \leq 1/2 \tag{2}$$

$$n^b e^{-\binom{b}{2}p}/b! \leq 1/2, \tag{3}$$

then 1 holds true. Put it another way, we want

$$p \leq \frac{(a!/2)^{1/\binom{a}{2}}}{n^{2/(a-1)}}, \tag{4}$$

$$p \geq \frac{\ln\left(b!/(2n^b)\right)}{\binom{b}{2}}. \tag{5}$$

Now, we can just pick an n as large as possible such that

$$\frac{\ln\left(b!/(2n^b)\right)}{\binom{b}{2}} \leq \frac{(a!/2)^{1/\binom{a}{2}}}{n^{2/(a-1)}}.$$

It is tedious yet easy to see that $n = \Theta\left((b/\ln b)^{3/2}\right)$ suffices for the case $a = 4$. □

2 Dominating set

Fact 2.1 (Linearity of expectation)**.** For any random variables $X_1, \ldots, X_k$, $\mathrm{E}[c_1X_1 + \cdots + c_kX_k] = c_1\mathrm{E}[X_1] + \cdots + c_k\mathrm{E}[X_k]$.

Fact 2.2. To minimize a function $f(x)$ doubly differentiable, where $f''(x) \geq 0$ (i.e. $f(x)$ is *convex*), we find x_0 such that $f'(x_0) = 0$. This x_0 is a minima.

Given a graph $G = (V, E)$, a subset $S \subseteq V$ is called a *dominating set* if every vertex of G is either in S or adjacent to some vertex in S.

Theorem 2.3. *Let $G = (V, E)$ be a graph on n vertices with $\delta(G) = \delta > 1$. Then, G has a dominating set of size at most $n\frac{1+\ln(\delta+1)}{\delta+1}$.*

Proof. Pick each vertex of G at random with probability p. Let X be the set of chosen vertices. Let Y be the subset of $V - X$ where no $y \in Y$ has a neighbor in X. Clearly $X \cup Y$ is a dominating set. We estimate the average size of $X \cup Y$. If the average size (according to p) of $X \cup Y$ is at most $n\frac{1+\ln(\delta+1)}{\delta+1}$, then there must exist a choice of X for which $|X \cup Y| \leq n\frac{1+\ln(\delta+1)}{\delta+1}$.

For any $v \in V$,

$$\text{Prob}[v \in Y] = \text{Prob}[v \text{ and its neighbors were not picked}] = (1-p)^{1+\deg(v)} \leq (1-p)^{1+\delta}.$$

Hence,

$$\mathrm{E}[|Y|] = \sum_v \text{Prob}[v \in Y] \leq n(1-p)^{1+\delta}.$$

Consequently,

$$\mathrm{E}[|X| + |Y|] \leq np + n(1-p)^{1+\delta}.$$

The right hand side is minimized at $p_0 = 1 - (1+\delta)^{1/\delta}$. Thus, we can prove a slightly stronger result: there is a dominating set of size at most $np_0 + n(1-p_0)^{1+\delta}$. This bound, however, is not "clean."

A cleaner bound can be obtained by noticing that

$$np + n(1-p)^{1+\delta} \leq np + ne^{-p(1+\delta)}.$$

The right hand side is minimized at $p_1 = \frac{\ln(1+\delta)}{(1+\delta)}$, yielding the bound stated in the theorem. □

3 Extremal set theory

A hypergraph $H = (V, E)$ has *property* B if it is two-colorable, i.e. there exists a two-coloring of the vertices so that no edge is monochromatic. Obviously the fewer the number of edges, the more likely for H to have property B. Let $m(n)$ be the least number of edges so that an n-uniform hypergraph does not have property B. We want to find a lower bound for $m(n)$.

Theorem 3.1 (Erdős, 1963 [6])**.** *Every n-uniform hyper graph with $< 2^{n-1}$ edges has a property B. Hence, $m(n) \geq 2^{n-1}$.*

Proof. To prove the existence of a certain type of coloring, we generate random colorings and show the probability of the existence of the "type" is positive.

Color each vertex of $H = (V, E)$ with two colors at random (probability $1/2$ for each color). The probability that some $e \in E$ is monochromatic is $2/2^n$. Hence, the probability that at least one edge in E is monochromatic is at most $|E|/2^{n-1} < 1$. Consequently, there exists a good coloring. □

Exercise 1. Suppose $n \geq 4$ and let H be an n-uniform hypergraph with at most $4^{n-1}/3^n$ edges. Prove that there is a vertex coloring of H by 4 colors so that in every edge, all four colors are presented.

The following very well-known result is called the Erdős-Ko-Rado theorem [7]. We present a proof by Kantona [8].

Theorem 3.2 (Erdős-Ko-Rado)**.** *Let $n \geq 2k$ be positive integers. Let $\mathcal{F}$ be a family of k-subsets of $[n]$ for which $A, B \in \mathcal{F}$ implies $A \cap B \neq \emptyset$. Then,*

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

A direct counting proof of Erdős-Ko-Rado theorem. Consider a permutation $\pi \in S_n$. Put $\pi(1), \ldots, \pi(n)$ on a cycle in the clock-wise order. Call the cycle C_π. A member $A \in \mathcal{F}$ is said to be *consecutive* on C_π if all elements of A occur consecutively on the cycle. It is easy to see that there are at most k members of $\mathcal{F}$ which are consecutive on C_π for a fixed π. Also, there are only $(n-1)!$ different cycles, not $n!$ (why?). Let $\mathcal{C}$ be the set of all such cycles. Then,

$$\sum_{C \in \mathcal{C}} |\{A \in \mathcal{F} \mid A \text{ consecutive on } C\}| \leq k \cdot (n-1)!$$

Moreover,

$$\sum_{C \in \mathcal{C}} |\{A \in \mathcal{F} \mid A \text{ consecutive on } C\}| = \sum_{A \in \mathcal{F}} |\{C \in \mathcal{C} \mid A \text{ consecutive on } C\}| = |\mathcal{F}| k!(n-k)!.$$

Hence, $|F| \leq \binom{n-1}{k-1}$ as desired. □

A probabilistic proof of Erdős-Ko-Rado theorem. Consider $\pi \in S_n$. For each $i \in [n]$, the probability that $A_i^\pi = \{\pi(i), \ldots, \pi(i+k-1)\}$ (taken circularly) is a member of $\mathcal{F}$ is at most k/n, because, as in the previous proof, there can be at most k member of $\mathcal{F}$ that are consecutive on C_π.

Moreover, Prob$[A_i^\pi \in \mathcal{F}] = |\mathcal{F}|/\binom{n}{k}$. Hence, $|\mathcal{F}| \leq \binom{n}{k} k/n = \binom{n-1}{k-1}$. □

Exercise 2 (Sperner Lemma, 1928 [9])**.** The maximum size of a family of subsets of $[v]$ none of whose member is contained in another is $\binom{v}{\lfloor v/2 \rfloor}$.

The following theorem implies Sperner's Lemma, although no one noticed it until Tuza (1984, [10]).

Theorem 3.3 (Bollobás, 1965 [3])**.** *Let $\mathcal{X} = \{X_1, \ldots, X_m\}$, and $\mathcal{Y} = \{Y_1, \ldots, Y_m\}$ be two set systems of $[n]$ such that*

(i) $X_i \cap Y_i = \emptyset, \forall i$.

(ii) $X_i \cap Y_j \neq \emptyset, \forall i \neq j$.

Then,

$$\sum_{i=1}^{m} \frac{1}{\binom{|X_i|+|Y_i|}{|X_i|}} \leq 1. \tag{6}$$

Proof. Let $x_i = |X_i|$, and $y_j = |Y_j|$. Consider a random $\pi \in S_n$. Let E_i be the event that elements of X_i come before elements of Y_i in π. Then,

$$\text{Prob}[E_i] = \frac{\binom{n}{x_i+y_i} x_i! y_i! (n - x_i - y_i)!}{n!} = \frac{1}{\binom{x_i+y_i}{x_i}}.$$

It's easy to see that the events E_i are mutually exclusive. The theorem follows easily. □

Corollary 3.4. *If $x_i = x$, $y_i = x$, for all $i = 1, \ldots, m$ in the previous theorem, then $m \leq \binom{x+y}{x}$.*

Exercise 3. Prove that Bollóbas' Theorem implies Sperner's Lemma.

Exercise 4. Let $\mathcal{F} = \{(A_i, B_i), 1 \leq i \leq m\}$ be a family of pairs of subsets of the set of integers such that $|A_i| = a$, $|B_i| = b$, for all i, $A_i \cap B_i = \emptyset$, and $(A_i \cap B_j) \cup (A_j \cap B_i) \neq \emptyset$ for all $i \neq j$. Show that

$$m \leq \frac{(a+b)^{a+b}}{a^a b^b}. \tag{7}$$

4 Coding Theory

Note that the following theorems hold for q-ary codes, also. We only stated the binary versions for clarity of presentation.

Theorem 4.1 (Kraft inequality)**.** *Let $\mathcal{C}$ be a finite collection of finite binary strings such that no string is a prefix of another. Let n_i be the number of strings of length i in $\mathcal{C}$. Then,*

$$\sum_i \frac{n_i}{2^i} \leq 1.$$

Proof. Let m be the length of longest string in the collection. Flip a fair coin m times to generate a binary string s of length m. No two strings in $\mathcal{C}$ can both be prefixes of s at the same time. For a particular *codeword* $w \in \mathcal{C}$ (i.e. a string in $\mathcal{C}$) of length i, the probability that s has w as a prefix is $1/2^i$. These possibilities are mutually exclusive for all codewords w, hence the total probability is ≤ 1, namely

$$\sum_i \frac{n_i}{2^i} \leq 1,$$

as desired. □

Kraft showed that the converse is also true, i.e. given the numbers n_i satisfying the inequality, then there exists a prefix-free code with n_i codewords of length i.

McMillan later discovered that the inequality is also the necessary condition for a code to be *uniquely decipherable*, which is the content of the following theorem. (Sufficiency, again, follows from Kraft's result.)

Theorem 4.2 (Kraft-McMillan inequality)**.** *Let $\mathcal{C}$ be a finite collection of finite binary strings such that no two distinct concatenations of two finite sequences of codewords result in the same binary sequence. Let n_i be the number of strings of n_i in $\mathcal{C}$. Then,*

$$\sum_i \frac{n_i}{2^i} \leq 1.$$

A typical proof. Let m be the largest string length. A trivial combinatorial reasoning shows that

$$\left(\sum_{i=1}^{m} \frac{n_i}{2^i}\right)^k \leq mk, \tag{8}$$

for all integers k. Since $(mk)^{1/k} \to 1$ as $k \to \infty$, the desired inequality follows.

One can show (8) with a somewhat messy probabilistic argument. □

5 Number Theory

Exercise 5 (Legendre Theorem)**.** For any prime p, the power of p in the factorization of $n!$ is $\sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.

Exercise 6 (Erdős)**.** Let $q = 2m + 1$ be an odd prime. Show that

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq 2^{2m},$$

where the product goes over all primes p. Use this fact to prove by induction that

$$\prod_{p\leq x} \leq 4^{x-1}, \text{ for all real } x \geq 2.$$

Again, the product is taken over primes p.

Joseph Bertrand conjectured that, for every integer $n \geq 1$, there is a prime p such that $n < p \leq 2n$. This is known as the *Bertrand's postulate*, which is also referred to as the *Chebyshev theorem* because Chebyshev proved it in 1850. The genius Ramanujan gave a simpler proof. In 1932, Paul Erdős published his first paper which gave a proof of the theorem. This proof does not appear to be probabilistic, but it contains all spirit of a probabilistic proof: the pigeonhole principle and a counting argument. A yet simpler proof from Erdős is presented below and is taken from the superb text [1].

Theorem 5.1. *For every integer $n \geq 1$, there is a prime p such that $n < p \leq 2n$.*

Proof. Suppose the postulate is false, then $\binom{2n}{n}$ has only prime factors at most n. In fact, it is easy to see that $\binom{2n}{n}$ has no prime factor p such that $2n/3 < p \leq n$. Consequently, we can write

$$\binom{2n}{n} = \prod_{p\leq 2n/3} p^{e_p},$$

where the product goes over all primes p, and e_p is the exponent of p in this factorization.

The following fact can be shown from Legendre theorem.

Fact 5.2. in the factorization of $\binom{2n}{n}$, $p^{e_p} \leq 2n$ for any prime p. Hence, $e_p \leq 1$ for any prime $p > \sqrt{2n}$.

Combining the fact and Exercise 6, we have

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} p^{e_p} \cdot \prod_{\sqrt{2n} < p \leq 2n/3} p \leq (2n)^{\sqrt{2n}} \cdot 4^{2n/3}.$$

This cannot happen for $n \geq 4000$ (simple calculus would confirm it). For $n \leq 4000$, the following sequence of primes, where the next is not more than twice the previous, proves the postulate:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001.$$

□

References

[1] M. AIGNER AND G. M. ZIEGLER, *Proofs from The Book*, Springer-Verlag, Berlin, second ed., 2001. Including illustrations by Karl H. Hofmann.

[2] N. ALON AND J. H. SPENCER, *The probabilistic method*, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley-Interscience [John Wiley & Sons], New York, second ed., 2000. With an appendix on the life and work of Paul Erdős.

[3] B. BOLLOBÁS, *On generalized graphs*, Acta Math. Acad. Sci. Hungar, 16 (1965), pp. 447–452.

[4] B. BOLLOBÁS, *Random graphs*, vol. 73 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, second ed., 2001.

[5] P. ERDÖS, *Some remarks on the theory of graphs*, Bull. Amer. Math. Soc., 53 (1947), pp. 292–294.

[6] P. ERDŐS, *On a combinatorial problem*, Nordisk Mat. Tidskr., 11 (1963), pp. 5–10, 40.

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

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

[9] E. SPERNER, *Ein satz uber untermengen einer endlichen Menge*, Math. Z., 27 (1928), pp. 544–548.

[10] Z. TUZA, *Helly-type hypergraphs and Sperner families*, European J. Combin., 5 (1984), pp. 185–187.