Probabilistic method

The **probabilistic method** is a nonconstructive method, primarily used in combinatorics and pioneered by Paul Erdős, for proving the existence of a prescribed kind of mathematical object. It works by showing that if one randomly chooses objects from a specified class, the probability that the result is of the prescribed kind is more than zero. Although the proof uses probability, the final conclusion is determined for *certain*, without any possible error.

This method has now been applied to other areas of mathematics such as number theory, linear algebra, and real analysis, as well as in computer science (e.g. randomized rounding), and information theory.

Contents

1 **Introduction**

2 **Two examples due to Erdős**
- 2.1 First example
- 2.2 Second example

3 **See also**

4 **References**

5 **Footnotes**

Introduction

If every object in a collection of objects fails to have a certain property, then the probability that a random object chosen from the collection has that property is zero.

Similarly, showing that the probability is (strictly) less than 1 can be used to prove the existence of an object that does *not* satisfy the prescribed properties.

Another way to use the probabilistic method is by calculating the expected value of some random variable. If it can be shown that the random variable can take on a value less than the expected value, this proves that the random variable can also take on some value greater than the expected value.

Common tools used in the probabilistic method include Markov's inequality, the Chernoff bound, and the Lovász local lemma.

Two examples due to Erdős

Although others before him proved theorems via the probabilistic method (for example, Szele's 1943 result that there exist tournaments containing a large number of Hamiltonian cycles), many of the most well known proofs using this method are due to Erdős. Indeed, the Alon-Spencer textbook on the subject has his picture on the cover to highlight the method's association with Erdős. The first example below describes one such result from 1947 that gives a proof of a lower bound for the Ramsey number $R(r, r)$.

First example

Suppose we have a complete graph on n vertices. We wish to show (for small enough values of n) that it is possible to color the edges of the graph in two colors (say red and blue) so that there is no complete subgraph on r vertices which is monochromatic (every edge colored the same color).

To do so, we color the graph randomly. Color each edge independently with probability $1/2$ of being red and $1/2$ of being blue. We calculate the expected number of monochromatic subgraphs on r vertices as follows:

For any set S of r vertices from our graph, define the variable $X(S)$ to be 1 if every edge amongst the r vertices is the same color, and 0 otherwise. Note that the number of monochromatic r-subgraphs is the sum of $X(S)$ over all possible subsets. For any S, the expected value of $X(S)$ is simply the probability that all of the

$$\binom{r}{2}$$

edges in S are the same color,

$$2 \cdot 2^{-\binom{r}{2}}$$

(the factor of 2 comes because there are two possible colors).

This holds true for any of the $C(n, r)$ possible subsets we could have chosen, so we have that the sum of $E[X(S)]$ over all S is

$$\binom{n}{r} 2^{1-\binom{r}{2}}.$$

The sum of an expectation is the expectation of the sum (*regardless* of whether the variables are independent), so the expectation of the sum (the expected number of monochromatic r-subgraphs) is

$$\binom{n}{r} 2^{1-\binom{r}{2}}.$$

Consider what happens if this value is less than 1. The number of monochromatic r-subgraphs in our random coloring will always be an integer, so at least one coloring must have less than the expected value. But the only integer that satisfies this criterion is 0. Thus if

$$\binom{n}{r} < 2^{\binom{r}{2}-1},$$

(which holds, for example, for n=5 and r=4) then some coloring fits our desired criterion.[1]

By definition of the Ramsey number, this implies that $R(r, r)$ must be bigger than n. In particular, $R(r, r)$ must grow at least exponentially with r.

A peculiarity of this argument is that it is entirely nonconstructive. Even though it proves (for example) that almost every coloring of the complete graph on $(1.1)^r$ vertices contains no monochromatic r-subgraph, it gives no explicit example of such a coloring. The problem of finding such a coloring has been open for more than 50 years.

Second example

A 1959 paper of Erdős (see reference cited below) addressed the following problem in graph theory: given positive integers g and k, does there exist a graph G containing only cycles of length at least g, such that the chromatic number of G is at least k?

It can be shown that such a graph exists for any g and k, and the proof is reasonably simple. Let n be very large and consider a random graph G on n vertices, where every edge in G exists with probability $p = n^{1/g-1}$. We show that with positive probability, a graph satisfies the following two properties:

Property 1. G contains at most $n/2$ cycles of length less than g.

Proof. Let X be the number cycles of length less than g. Number of cycles of length i in the complete graph on n vertices is

$$\frac{n!}{2 \cdot i \cdot (n-i)!} \leq \frac{n^i}{2}$$

and each of them is present in G with probability p^i. Hence by Markov's inequality we have

$$\Pr\left(X > \tfrac{n}{2}\right) \leq \frac{2}{n}E[X] \leq \frac{1}{n}\sum_{i=3}^{g-1} p^i n^i = \frac{1}{n}\sum_{i=3}^{g-1} n^{\frac{i}{g}} \leq \frac{g}{n} n^{\frac{g-1}{g}} = g n^{-\frac{1}{g}} = o(1).$$

Thus for sufficiently large n, property 1 holds with a probability of more than $1/2$.

Property 2. G contains no independent set of size $\lceil \frac{n}{2k} \rceil$.

Proof. Let Y be the size of the largest independent set in G. Clearly, we have

$$\Pr(Y \geq y) \leq \binom{n}{y}(1-p)^{\frac{y(y-1)}{2}} \leq n^y e^{-\frac{py(y-1)}{2}} = e^{-\frac{y}{2}\cdot(py - 2\ln n - p)} = o(1),$$

when

$y = \left\lceil \frac{n}{2k} \right\rceil$. Thus, for sufficiently large n, property 2 holds with a probability of more than $1/2$.

For sufficiently large n, the probability that a graph from the distribution has both properties is positive, as the events for these properties cannot be disjoint (if they were, their probabilities would sum up to more than 1).

Here comes the trick: since G has these two properties, we can remove at most $n/2$ vertices from G to obtain a new graph G' on $n' \geq n/2$ vertices that contains only cycles of length at least g. We can see that this new graph has no independent set of size $\lceil \frac{n'}{k} \rceil$. G' can only be partitioned into at least k independent sets, and, hence, has chromatic number at least k.

This result gives a hint as to why the computation of the chromatic number of a graph is so difficult: even when there are no local reasons (such as small cycles) for a graph to require many colors the chromatic number can still be arbitrarily large.

See also

- Interactive proof system
- Method of conditional probabilities
- Probabilistic proofs of non-probabilistic theorems
- Random graph

References

- Alon, Noga; Spencer, Joel H. (2000). *The probabilistic method* (2ed). New York: Wiley-Interscience. ISBN 0-471-37046-0.
- Erdős, P. (1959). "Graph theory and probability" (http://www.math-inst.hu/~p_erdos/1959-06.pdf) (PDF). *Canad. J. Math*. **11** (0): 34–38. MR 0102081 (https://www.ams.org/mathscinet-getitem?mr=0102081). doi:10.4153/CJM-1959-003-9 (https://doi.org/10.4153%2FCJM-1959-003-9).
- Erdős, P. (1961). "Graph theory and probability, II" (http://www.math-inst.hu/~p_erdos/1961-06.pdf) (PDF). *Canad. J. Math*. **13** (0): 346–352. MR 0120168 (https://www.ams.org/mathscinet-getitem?mr=0120168). doi:10.4153/CJM-1961-029-9 (https://doi.org/10.4153%2FCJM-1961-029-9).

- J. Matoušek, J. Vondrak. The Probabilistic Method (http://wayback.archive.org/web/20120205002452/http://kam.mff.cuni.cz/~matousek/prob-ln-2pp.ps.gz). Lecture notes.
- Alon, N and Krivelevich, M (2006). Extremal and Probabilistic Combinatorics (http://www.math.tau.ac.il/~nogaa/PDFS/epc7.pdf)

Footnotes

1. The same fact can be proved without probability, using a simple counting argument:
   - The total number of *r*-subgraphs is $\binom{n}{r}$.
   - Each *r*-subgraphs has $\binom{r}{2}$ edges and thus can be colored in $2^{\binom{r}{2}}$ different ways.
   - Of these colorings, only 2 colorings are 'bad' for that subgraph (the colorings in which all vertices are red or all vertices are blue).
   - Hence, the total number of colorings that are bad for *all* subgraphs is at most $2\binom{n}{r}$.
   - Hence, if $2^{\binom{r}{2}} > 2\binom{n}{r}$, there must be at least one coloring which is not 'bad' for any subgraph.