The Probabilistic Method

C. Y. Ku

June 6, 2003

1 Introduction

(1) Founder: Paul Erdős.

(2) To prove existence of a combinatorial structure with certain probabilities:

  (i) construct appropriate probabilty space,

  (ii) show a randomly chosen element in this space has the desired properties with *positive* probabilities.

(3) Isn't this just a counting proof in disguise? (theorectically yes, but in practise, the method is essential. It's hopeless to replace some of our proofs by counting arguments.)

2 Some background

Let $X_1, \ldots, X_m$ be random variables (they are just functions on a given sample space). Suppose that $X = c_1 X_1 + \cdots + c_m X_m$ for some constants c_i, then

$$\begin{aligned} \mathrm{E}[X] &= c_1\,\mathrm{E}[X_1] + \cdots + c_m\,\mathrm{E}[X_m], && (1) \\ \mathrm{Var}[X] &= \sum_{i=1}^{m} \mathrm{Var}[X_i] + \sum_{i \neq j} \mathrm{Cov}[X_i, X_j] && (2) \end{aligned}$$

where $\mathrm{Cov}[YZ] = \mathrm{E}[YZ] - \mathrm{E}[Y]\,\mathrm{E}[Z]$. But if X_i and X_j are mutually independent for all $i \neq j$, then the second summand in (2) is 0. Also if X is a random variable and $Y = aX$, we have

$$\begin{aligned} \mathrm{Var}[X] &= \sum_a (a-\mu)^2 \Pr[X = a] && (3) \\ \mathrm{Var}[Y] &= a^2\,\mathrm{Var}[X]. && (4) \end{aligned}$$

3 Method 1: The Second Moment

The second moment method is a method which uses the following inequality due to Chebyschev:

Theorem 1 (Chebyschev's Inequality) *For any positive* λ*,*

$$\Pr[|X - \mu| \geq \lambda\sigma] \leq \frac{1}{\lambda^2}.$$

Apparently this is an effective tool in number theory. We shall give a simple example below.

Let $f(n)$ be the largest integer k for which there is a set $\{x_1, \ldots, x_k\} \subseteq \{1, \ldots, n\}$ such that the sums $\sum_{i \in S} x_i$, S is a subset of $\{1, \ldots, k\}$, are all distinct.

Theorem 2

$$f(n) \leq \log_2 n + \frac{1}{2} \log_2 \log_2 n + O(1).$$

Proof Fix $\{x_1, \ldots, x_k\}$. Let $\epsilon_1, \ldots, \epsilon_k \in \{0, 1\}$ be random variable such that for each i,

$$\Pr[\epsilon_i = 0] = \Pr[\epsilon_i = 1] = \frac{1}{2}.$$

a	0	1
$\Pr[\epsilon_i = a]$	$\frac{1}{2}$	$\frac{1}{2}$

Now let $X = x_1\epsilon_1 + \cdots + x_k\epsilon_k$. We can think of X as a random sum. We first do some calculations. By applying equations (1)-(4):

$$
\begin{aligned}
\mathrm{E}[\epsilon_i] &= \sum_a a \cdot \Pr[\epsilon_i = a], \\
&= 0 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2}; \\
\mathrm{E}[X] &= x_1 \,\mathrm{E}[\epsilon_1] + \cdots + x_k \,\mathrm{E}[\epsilon_k], \\
\mathrm{E}[X] &= \frac{x_1 + \cdots + x_k}{2}; \qquad (5) \\
\mathrm{Var}[\epsilon_i] &= \sum_a (a-\mu)^2 \cdot \Pr[\epsilon_i = a], \\
&= (0 - \frac{1}{2})^2 \cdot \frac{1}{2} + (1 - \frac{1}{2})^2 \cdot \frac{1}{2}; \\
&= \frac{1}{4} \\
\mathrm{Var}[X] &= \sum_{i=1}^{k} \mathrm{Var}[x_i \epsilon_i], \\
&= \sum_{i=1}^{k} x_i^2 \,\mathrm{Var}[\epsilon_i], \\
&= \frac{x_1^2 + \cdots + x_k^2}{4}, \\
&\leq \frac{n^2 k}{4}. \qquad (6)
\end{aligned}
$$

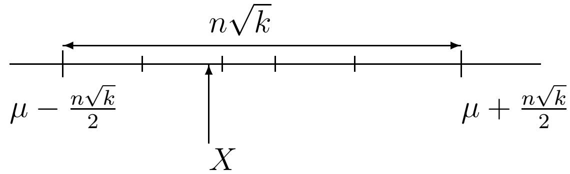
giving,

$$\sigma \leq \frac{n\sqrt{k}}{2}.$$

By Chebyschev's Ineqality, we have,

$$
\begin{aligned}
\Pr[|X - \mu| \geq \lambda\sigma] &\leq \frac{1}{\lambda^2}, \\
\Pr[|X - \mu| \geq \lambda\frac{n\sqrt{k}}{2}] &\leq \frac{1}{\lambda^2}. \qquad (7)
\end{aligned}
$$

Observe that the random sum X could only achieve a particular value in one unique way (by our definition of a set with distinct sums). It follows that the probability for X taking values between $\mu - \frac{n\sqrt{k}}{2}$ and $\mu + \frac{n\sqrt{k}}{2}$ is either 0 or 2^{-k}.



From (7), we deduce that

$$1 - \frac{1}{\lambda^2} \leq 2^{-k} n\sqrt{k}.$$

Solving for k yields the result. ■

4 Method 2: Lovász Local Lemma

Theorem 3 (Lovász Local Lemma) *Let $A_1, \ldots, A_n$ be events in arbitrary probability space such that for each i, the event A_i is mutually independent of all the other events but at most d. Suppose that for all i, $\Pr(A_i) \leq p$. If*

$$ep(d+1) = 1, \tag{8}$$

then,

$$\Pr(\bigwedge_{i=1}^{n} \overline{A}_i) > 0.$$

We give an example using the local lemma to give a lower bound of the *Ramsey number*. Let $R(k,k)$ denote the smallest integer n such that for any 2-colouring (colour the edges with red and blue) of the complete graph K_n, there is a monochromatic K_k.

Theorem 4 *If $e(\binom{k}{2}\binom{n}{k-2} + 1)2^{1-\binom{k}{2}} < 1$, then $R(k,k) > n$.*

We first see that $R(k,k) > n$ if and only if there exists a 2-colouring of K_n for which there is no red and blue K_k. We want to show the existence of such a colouring by using the local lemma. Pick a random 2-colouring of K_n (colour each edge independently and equally likely to be red or blue).

Let T to be the family of all k-subsets of $\{1, \ldots, n\}$. Then for $S \in T$, we define

$$A_S = \text{the event that the induced subgraph on } S \text{ is monochromatic.}$$

It follows that $\Pr(A_S) = 2 \times \frac{1}{2^{\binom{k}{2}}} = 2^{1-\binom{k}{2}}$. Also now the required colouring exists if and only if $\Pr(\bigwedge_T \overline{A}_S) > 0$.

But given A_S, we observe that the event $A_{S'}$ is dependent on A_S if and only if the corresponding induced subgraphs share at least one common edge, that is, $|S \cap S'| \geq 2$. Hence every A_S is mutually independent of all other events but at most $\binom{k}{2}\binom{n}{k-2}$, though we note that this bound is quite crude as we allow many repetitions (and even illegal configurations by choosing the same vertices more than once!); but who cares!

Taking $d = \binom{k}{2}\binom{n}{k-2}$, $p = 2^{1-\binom{k}{2}}$, the result follows immediately from the local lemma. Splendid. ■

References

[1] N. Alon, J. H. Spencer, and Paul Erdős. *The Probabilistic Method*. John Wiley and Sons, Inc, 1991.