Annals of Discrete Mathematics 28 (1985) 1-5

WELCOMING ADDRESS

PAUL ERDÖS

Mathematical Institute of the Hungarian Academy of Sciences, H-1053 Budapest, Hungary

It gives me great pleasure to give this welcoming address to the first Poznań meeting on random graphs. Perhaps the audience will forgive a very old man to give a few historical reminiscences how I came to apply probability methods in combinatorial analysis. I must do this while my mind and memory are still more or less intact. I do not intend to give a history of the probability method but will restrict myself almost entirely to my own contributions.

I will start with Ramsey's theorem. Denote by $r(u,v)$ the smallest integer for which every graph of $r(u,v)$ vertices either contains a complete graph of u vertices or an independent set of v vertices. The well known proof of Szekeres gives

$$r(u,v) \leqslant \binom{u+v-2}{u-1} \text{ and in particular } r(n,n) \leqslant \binom{2n-2}{n-1}. \tag{1}$$

No non-trivial lower bounds were known. In 1946 (after many failures) it occurred to me to try non-constructive methods i.e. consider all possible graphs on m labelled vertices (there are clearly $2^{\binom{m}{2}}$ such graphs), a very simple computation shows that if

$$m < cn2^{\frac{n}{2}}$$

then the number of graphs on m vertices which contain a $K(n)$ (i.e. a complete graph of n vertices) or an independent set of n vertices is $o(2^{\binom{m}{2}})$. This of course implies

$$r(n,n) > cn2^{\frac{n}{2}}. \tag{2}$$

By using a lemma of Lovász, Spencer improved the values of the constant in (2), but as far as I know

$$\lim \frac{r(n, n)}{n 2^{\frac{n}{2}}} = \infty \tag{3}$$

is still open. I offered (and offer) 100 dollars for the proof of the existence of $\lim r(n, n)^{\frac{1}{n}}$ and 500 dollars for the determination of the value of this limit (this latter offer probably violates the minimum wage act). The limit if it exists (it surely does) is between $2^{1/2}$ and 4.

My next success with the probability method was to give a good lower bound for $r(3, n)$. I was always sure that $r(3, n) = o(n^2)$ and $\frac{r(3, n)}{n} \to \infty$ but for many years I could get nowhere. In November 1956 in the bus travelling from the Dowkers (Yael and Hugh) to University College London I realized that by a construction in n-dimensional geometry I can show that $r(3, n) > n^{1+c}$. By a fairly complicated application of the probability method (later simplified by Spencer) I showed that

$$r(3, n) > \frac{cn^2}{(\log n)^2}. \tag{4}$$

A few years later (1966) Graver and Yackel showed

$$r(3, n) < \frac{cn^2}{\log n} \log\log n. \tag{5}$$

I offered 50 dollars for $r(3, n) = o(n^2)$. They also used the probability method. Recently Ajtai, Komlós and Szemerédi proved by a new method (which has many other applications and is also probabilistic in nature) that

$$r(3, n) < \frac{cn^2}{\log n}. \tag{6}$$

An asymptotic formula for $r(3, n)$ is nowhere in sight at the moment.

I was (and am) sure that $r(4, n) > n^{3-\varepsilon}$ and more generally $r(k, n) > n^{k-\varepsilon}$ for every fixed k, and was very disappointed that the probability method gives only a much weaker result. Several other mathematicians tried without success this natural and attractive conjecture. I offer 250 dollars for a proof or disproof of $r(4, n) > n^{3-\varepsilon}$, the difficulties are perhaps not only technical in nature.

Very few Ramsey numbers are known, $r(4,4)=18$ was proved by Greenwood and Gleason in 1955. $r(3,n)$ is known for all $n \leqslant 9$ except $n=8$. I sometimes make the following joke in my lectures: Suppose an evil spirit would tell us, "Unless you tell me the value of $r(5,5)$ I will exterminate the human race." Our best strategy would perhaps be to get all the computers and computer scientists to work on it. If he would ask for $r(6,6)$ our best bet would perhaps be to try to destroy him before he destroys us (unfortunately we are very good at destroying [especially ourselves]). If we could be so smart as to be able to compute these numbers without computers, we would not have to pay any attention to the evil spirit and could tell him "just try and see what will happen to you."

For the sake of historical accuracy I have to add that in fact several years before the work on $r(3,n)$ I proved by probabilistic methods for every k and l there is a graph of chromatic number k and girth l. Lovász and later Nešetřil and Rödl obtained a constructive proof of this result. As far as I know there is no constructive proof for the following result of mine (which follows quite easily from the probabilistic method): For every k there is an ε_k so that for every $n > n_0(\varepsilon, k)$ there is a $\mathcal{G}(n)$ i.e. a graph of n vertices of girth $>k$ for which the largest independent (or stable) set is $<n^{1-\varepsilon}$ (and therefore of course its chromatic number is $>n^{\varepsilon}$).

Let me now tell you two "spectacular" (?) successes which I had with the probability method. In 1962 Professor Schütte at a meeting in Oberwolfach asked me the following question: Is it true that for every k there is a tournament for which every set of k players is beaten by one of the other players? Denote by n_k (if it exists) the smallest number of players in such a tournament. Schütte observed that $n_1=3$, $n_2=7$, but he did not know if n_3 exists. In the language of graph theory a tournament is a directed complete graph. Schütte's problem asks for a directed complete graph in which for every set of k vertices $x_1, \ldots, x_k$ there is a y so that all the edges are directed from y to x_i, $i=1,2,\ldots,k$.

At first I was baffled by this problem but then while I was resting for a few minutes after lunch it occurred to me to try the probability method and to direct the edges at random. Sure enough I proved without much trouble that for every $n > ck^2 2^k$ there is such a tournament on n players. In other words $n_k < ck^2 2^k$. $n_k \geqslant 2^{k+1}-1$ is easy and a few years later Esther and George Szekeres proved $n_k > ck2^k$ and they also showed $n_3=19$. An asymptotic formula for n_k is nowhere in sight at the moment and the value of n_4 is also unknown.

The following interesting problem remains open. Is it true that for every $n > n_k$ there is a tournament on n players in which every set of k players is beaten by another player. I was never able to get anywhere with this simple and attractive problem. Perhaps I overlook a simple argument but perhaps this problem can not be attacked by the probability method.

My second triumph occurred at dinner at St John's College in the summer of 1971. Professor Mordell who invited me told me, "I know you are willing and eager to talk Mathematics at any time, sit down next to my young colleague, he is working in functional analysis and he has a combinatorial problem whose positive solution would be useful for his work." The problem stated as follows: Let there be given an n by n matrix all whose entries are 0 or 1. Assume that the number of 0's is $>cn^2$ where $0<c<1$ is a constant independent of n. Is it then true that there is a rectangle of u columns and v rows which consists entirely of 0-s and for which $\frac{u\cdot v}{n}\to\infty$. Here I could give the answer before I finished my soup. The answer is negative and in fact for almost all such (0, 1) matrices

$$\max u\cdot v=(1+o(1))\max_r rc^r n. \tag{7}$$

(7) follows quite easily by the probability method. The unhappy ending is that the negative answer was of no use for the problem of my colleague.

As a triumph I could also mention our disproof with Fajtlowicz (in this case he suggested the probabilistic approach) of a well known conjecture of Hajós. Here Catlin earlier disproved the conjecture by a simple example, the point of our disproof was that we disproved the conjecture in a very strong form.

As you will see from the lectures which will follow our subject is definitely alive and there are many successes but also unsolved problems.

To finish this address I just make two remarks. As far as I know this method was perhaps first used in combinatorial analysis in a paper by Szekeres and Turán written nearly 50 years ago. They estimate the maximum possible value of an n by n determinant all whose entries are 0 or 1, and Szele in a paper written more than 40 years ago estimates the maximum number of possible directed hamiltonian cycles of a directed complete graph. Finally, mainly due to considerations of space I did not discuss our papers with Rényi on evolution of random graphs a subject which is certainly alive, Rényi always wanted to apply these ideas to physics (change of state) and perhaps to traffic engineering i.e. when a superhighway at a certain traffic density suddenly turns into a giant parking lot, these phenomena may be related to the appearance of the giant component if the number of edges is $>\frac{n}{2}(1+\varepsilon)$. Rényi's untimely death prevented his investigating these questions, perhaps this work will be taken up by others in the future.

I would just like to mention one problem due to Shamir which is very attractive and which Rényi and I unfortunately missed: Let there be given a set of $3n$ vertices and m triples chosen at random. How large must m be that with probability tending to 1 the m triples should contain n disjoint triples, then of course these n triples will form a cover. Shamir proved that $m<n^{3/2}$ suffices for this but perhaps

$n^{1+\varepsilon}$ or even $cn \log n$ triples could suffice. Rényi and I solved the case of graphs instead of triples and there $(\frac{1}{2}+\varepsilon)n \log n$ suffices.

Most of the results I referred to in this note can be found in Erdös-Spencer probabilistic methods in combinatorica analysis or in my book *The Art of Counting*, see also the book of Moon on tournaments. B. Bollobás is writing a book on random graphs which I hope will appear soon.

Perhaps I should end by remarking that the probability used here is rather elementary, in fact, when I lectured 35 years ago at the University of Illinois on $r(n, n) > cn\, 2^{n/2}$ Doob remarked, "This is very nice but it is more like counting than probability." I think Doob was right, but perhaps the later applications are a little more sophisticated.

G. Szekeres and P. Turán, An extremal problem in the theory of determinants, Math. és Természettudományi Értesitö (1937) 796–806. This was a publication of the Hungarian Academy of Sciences, the paper is in Hungarian.

T. Szele, Combinatorial investigations concerning the complete graph, Mat. Fiz. Lapok 50 (1943) 223–256 (in Hungarian).