Lecture 14: The probabilistic method and the Erdős-Rényi random graph · 1MA020

Vilhelm Agdur[1]

[1] vilhelm.agdur@math.uu.se

28 November 2023

> We introduce a new tool to the course, the probabilistic method, and use it to prove some new results. We also introduce the Erdős-Rényi random graph, which is interesting in its own right as well as being a tool in the probabilistic method.

The minimum bisection problem

Suppose we are given a graph G, which is too large to fit on a single computer – so we wish to distribute the computation we want to do on the graph between two machines. We imagine the computation we want to do is in some sense possible to do "locally" – so if the graph had two equally sized connected components, the two computers wouldn't have to talk to each other at all.

Of course, most graphs do not split up that nicely, but we can still try to divide it into two equally sized parts that have as few edges between them as possible. How well can we do this?

Proposition 1. *For any graph $G = (V, E)$ on $n \in 2\mathbb{N}$ vertices with maximum degree $\Delta < \frac{n}{2}$, there exists a partition $A \coprod B$ of V, such that $|A| = |B| = \frac{n}{2}$, and*

$$e(A, B) \leq \frac{|E|}{2},$$

where $e(A, B)$ is the number of edges between A and B.

Proof. Let G^c be the complement graph of G – that is, G^c has the same vertices as G, and there is an edge $x \sim y$ in G^c if and only if $x \sim y$ is not an edge of G.

Since we assumed $\Delta < \frac{n}{2}$, it is clear that the *minimum* degree of G^c is at least $\frac{n}{2}$, and so by Dirac's theorem[2] there exists a Hamilton cycle in G^c. Picking every second edge of this Hamilton cycle, we get a perfect matching M on G^c.

[2] Which we proved earlier in the course.

Now, we apply the probabilistic method, picking a random partition $A \coprod B$ of V: For each edge of M, we randomly place one of its endpoints in A and one in B, independently between different edges. We can then compute that

$$\mathbb{E}\left[|e(A, B)|\right] = \mathbb{E}\left[\sum_{x \sim y \in E} \mathbb{1}_{\{x \sim y \in E(A,B)\}}\right]$$

$$= \sum_{x \sim y \in E} \mathbb{P}\left(x \text{ and } y \text{ are in different sets}\right).$$

Now, whenever x and y are not connected by an edge in M, their assignment to A or B is independent, and so the probability that they are in different sets is precisely $\frac{1}{2}$. However, we picked our matching M so that it is a perfect matching on G^c – in particular this means that $M \cap E = \varnothing$, and so all of the probabilities that we are summing must in fact be $\frac{1}{2}$ by our previous argument.

So the sum is just a sum of $|E|$ many $\frac{1}{2}$'s, and so what we have seen is that $\mathbb{E}\left[|e(A, B)|\right] = \frac{|E|}{2}$. Now, we know that the expectation is never greater than every specific outcome, so there must exist some choice of A and B with no more than $\frac{|E|}{2}$ edges between them, and we have shown the proposition. $\qquad\square$

The Erdős-Rényi graph

As we saw in the previous exercise session, the simplest and most common random graph model is the Erdős-Rényi graph, where all edges appear independently with the same probability. Let us restate the definition here, for completeness.

Definition 2. For any integer $n \in \mathbb{N}$ and any probability $p \in [0, 1]$, the *Erdős-Rényi graph* $G(n, p)$ is a random graph on n vertices,[3] where each of the $\binom{n}{2}$ potential edges is present independently at random with probability p.

Proposition 3. *Let $\hat{G} = (V, E)$ be a labelled graph on n vertices, and $G = G(n, p)$ be an Erdős-Rényi graph on the same number of vertices. The probability that $G = \hat{G}$ is precisely*

$$\mathbb{P}\left(G = \hat{G}\right) = p^{|E|}(1 - p)^{\binom{n}{2} - |E|},$$

and so in particular if $p = \frac{1}{2}$, the Erdős-Rényi graph is in fact a uniformly random graph.

We proved two things about the Erdős-Rényi graph during the exercises, but let us restate those results and their proofs here.

Lemma 4. *If $G = G(n, p)$ is an Erdős-Rényi graph, the probability that it has an independent set of size at least k is bounded by*

$$\mathbb{P}\left(\alpha(G) \geq k\right) \leq \binom{n}{k}(1 - p)^{\binom{k}{2}}.$$

Proof. There are a total of $\binom{n}{k}$ subsets of $[n]$ of size k, so for each such set $X \in \binom{[n]}{k}$, let A_X be the event that X is an independent set in G.

Clearly, A_X happens whenever none of the $\binom{k}{2}$ possible edges inside X are present, which happens with probability $(1 - p)^{\binom{k}{2}}$. So

we can calculate, using a union bound, that

$$
\begin{aligned}
\mathbb{P}\left(\alpha(G) \geq k\right) = \mathbb{P}\left(\bigcup_{X \in \binom{[n]}{k}} A_X\right) \\
\leq \sum_{X \in \binom{[n]}{k}} \mathbb{P}\left(A_X\right) \\
= \sum_{X \in \binom{[n]}{k}} (1-p)^{\binom{k}{2}} = \binom{n}{k}(1-p)^{\binom{k}{2}}
\end{aligned}
$$

where we used in the last equality that we had $\binom{n}{k}$ summands, giving the lemma. □

Proposition 5. *For any $p \in (0,1)$, if $G_n = G(n,p)$ is an Erdős-Rényi graph for each n, it holds that*

$$
\mathbb{P}\left(\mathrm{diam}(G_n) = 2\right) \to 1 \quad as \quad n \to \infty.
$$

It is somewhat cumbersome to explicitly write out the sequence of random graphs and the limit every time we want to say something about an asymptotic property of the Erdős-Rényi graph, so we will generally use the following way of phrasing such results instead:

Proposition 6. *For each fixed $p \in (0,1)$, it holds that $\mathrm{diam}(G(n,p)) = 2$ with high probability.*[4]

Proof. The only graphs with diameter one are the complete graphs, and it is easy to see[5] that the Erdős-Rényi graph is not complete w.h.p. for any $p < 1$. So all we need to do is to show that $\mathrm{diam}\, G(n,p) \leq 2$ w.h.p.

So, for any pair of two distinct vertices i and j, let B_{ij} be the event that there is no edge between i and j and they additionally have no common neighbour. We call such a pair of vertices a *bad* pair – it is clear that a graph has diameter at most two precisely when it has no bad pairs.

Now we can compute, using the fact that edges appear independently, that

$$
\begin{aligned}
\mathbb{P}\left(B_{ij}\right) = \mathbb{P}\left((i \sim j \notin E) \wedge \left(\bigwedge_{k \in [n] \setminus \{i,j\}} (i \sim k \notin E) \vee (k \sim j \notin E)\right)\right) \\
= (1-p) \prod_{k \in [n] \setminus \{i,j\}} \mathbb{P}\left((i \sim k \notin E) \vee (k \sim j \notin E)\right) \\
= (1-p) \prod_{k \in [n] \setminus \{i,j\}} (1-p^2) = (1-p)(1-p^2)^{n-2},
\end{aligned}
$$

[4] We also synonymously say that a property holds "asymptotically almost surely" – these two phrases are then abbreviated to "w.h.p." or "a.a.s." when convenient. In both cases, what we mean is that the property holds with probability tending to one as we increase the number of vertices of the graph.

[5]

Exercise 1. See this.

and so letting X be the number of bad pairs, we compute using linearity of expectation that

$$
\begin{aligned}
\mathbb{E}\left[X\right] &= \mathbb{E}\left[\sum_{\{i,j\}\in\binom{[n]}{2}} \mathbb{1}_{\left\{B_{ij}\right\}}\right] \\
&= \sum_{\{i,j\}\in\binom{[n]}{2}} \mathbb{P}\left(B_{ij}\right) \\
&= \binom{n}{2}(1-p)(1-p^2)^{n-2}
\end{aligned}
$$

which we easily see goes to zero for fixed $p \in (0,1)$ as $n \to \infty$.

The result now follows by following the recipe for the first-moment method, applying Markov's inequality to see that we also have $\mathbb{P}\left(X > 0\right) \to 0$ as $n \to \infty$. □

Girth and chromatic number

Already when we first introduced the chromatic number, we mentioned the obvious fact that a large clique forces a graph to have high chromatic number. One might be led by this to believe that being very sparse, without any cliques, would mean you have low chromatic number. This unfortunately turns out to be not at all true, in a pretty strong sense.

Definition 7. The *girth* of a graph G is the length of the shortest cycle in the graph.

So the notion of girth generalizes the notion of being triangle-free, which is just having girth greater than three. Of course any triangle-free graph also contains no larger cliques, so this is indeed a strong notion of having no cliques.

Theorem 8 (Erdős, 1959). *For all positive integers k there exists a graph G of girth and chromatic number at least k.*

The proof of this uses the probabilistic method, and proceeds by considering a random graph from a suitably chosen distribution, and showing that the probability that it has girth and chromatic number at least k is greater than 0. We postpone the proof of this until a later lecture, when we will have developed our probabilistic toolbox a bit more.

Exercises