Lecture 4 - The Probabilistic Method

Jan Bouda

FI MU

March 27, 2012

Part I

The Asymptotic Notation

The Asymptotic Notation: Big-O

In many applications of computer science we have to compare two functions to decide which one grows faster with the input, or whether they are approximately the same.

Definition

Let $f(x)$ and $g(x)$ be two functions defined on some subset of the real numbers. We say that

$$f(x) \in O(g(x))$$

if and only if there exists a positive real number M and a real number x_0 such that

$$|f(x)| \leq M|g(x)| \text{ for all } x > x_0.$$

The big-O establishes that $f(x)$ does not grow faster that $g(x)$ (up to a constant multiplication).

The Asymptotic Notation: Little-o

Definition

Let $f(x)$ and $g(x)$ be two functions defined on some subset of the real numbers. We say that

$$f(x) \in o(g(x))$$

(read as "$f(x)$ is little-o of $g(x)$") if for every (small) positive constant ε there exists a constant N such that

$$|f(n)| \leq \varepsilon |g(n)| \qquad \text{for all } n \geq N \ .$$

Intuitively, it means that g(x) grows much faster than f(x), or similarly, the growth of f(x) is nothing compared to that of g(x).

The Asymptotic Notation: Little-o

Note the difference between definition for the big-O notation, and the definition of little-o: while the former has to be true for at least one constant M the latter must hold for every positive constant ε, however small.

If $g(x)$ is nonzero, or at least becomes nonzero beyond a certain point, the relation $f(x) \in o(g(x))$ is equivalent to

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

The Asymptotic Notation: Big Omega

Definition

Let $f(x)$ and $g(x)$ be two functions defined on some subset of the real numbers. We say that

$$f(x) \in \Omega(g(x))$$

if $f(x)$ is bounded below by $g(x)$ (up to constant factor) asymptotically, i.e. $\exists k > 0$ and $\exists n_0$ s.t.

$$\forall n > n_0 \; g(n)k \leq f(n)$$

The Asymptotic Notation: Big Theta

Definition

Let $f(x)$ and $g(x)$ be two functions defined on some subset of the real numbers. We say that

$$f(x) \in \Theta(g(x))$$

if $f(x)$ is bounded both above and below by $g(x)$ asymptotically, i.e. $\exists k_1 > 0, \exists k_2 > 0$ and $\exists n_0$ s.t.

$$\forall n > n_0 \; g(n)k_1 \leq f(n) \leq g(n)k_2$$

The Asymptotic Notation: Small Omega

Definition

Let $f(x)$ and $g(x)$ be two functions defined on some subset of the real numbers. We say that

$$f(x) \in \omega(g(x))$$

if $f(x)$ dominates $g(x)$ asymptotically, i.e. $\forall k > 0$ there $\exists n_0$ s.t.

$$\forall n > n_0 \; g(n)k \leq f(n)$$

The Asymptotic Notation

Definition

Let $f(x)$ and $g(x)$ be two functions defined on some subset of the real numbers. We say that

$$f(x) \sim g(x)$$

if $f(x)$ is of the order of $g(x)$, i.e.

$$\forall \varepsilon > 0 \; \exists n_0 \; \forall n > n_0 \; \left| \frac{f(n)}{g(n)} - 1 \right| < \varepsilon$$

Part II

Basic Counting Argument

Probabilistic method

- The probabilistic method is a way of proving existence of objects with certain properties.
- The basic technique is to construct a probabilistic space of objects (and a way to sample a random object). The next step is to show that our desired object will be sampled with nonzero probability, i.e. it exists.
- This construction often samples he object with high probability establishing thus a randomized algorithm to construct it.
- The proof of existence as well as randomized algorithms can sometimes be derandomized.

Basic Counting Argument

- To prove existence of an object with certain properties, we first construct a suitable probability space and then show that the desired object is sampled with nonzero probability.

We want to find a edge-coloring of a graph using two colors so that there no large cliques with all edges of the same color.

Monochromatic k-cliques

Theorem

For any $n, k \in \mathbb{N}$ such that $\binom{n}{2}2^{-\binom{k}{2}+1} < 1$ it is possible to color edges of K_n (complete graph on n vertices) with two colors so that it has no monochromatic K_k subgraph.

Proof.

- The sample space consists of all $2^{\binom{n}{2}}$ possible colorings of K_n.
- Assume each of the colorings is chosen with the uniform probability, i.e. $2^{-\binom{n}{2}}$.
- We randomly construct the coloring in the way that to each edge we independently assign one of the colors with probability $1/2$.

Monochromatic k-cliques

Proof.

Fix an arbitrary ordering on the k-cliques of K_n, and let A_i $(i = 1, \ldots, \binom{n}{k})$ be the event that the i-th clique is monochromatic. Note that once the first edge of the clique is (randomly) colored, all remaining edges must be given the same color.

$$P(A_i) = 2^{-\binom{k}{2}+1}.$$

We get the bound

$$P\left(\bigcup_{i=1}^{\binom{n}{k}} A_i\right) \leq \sum_{i=1}^{\binom{n}{k}} P(A_i) = \binom{n}{k} 2^{-\binom{k}{2}+1} < 1$$

using the assumption of the theorem.

Monochromatic k-cliques

Proof.

We have

$$P\left(\bigcap_{i=1}^{\binom{n}{k}} \overline{A_i}\right) = 1 - P\left(\bigcup_{i=1}^{\binom{n}{k}} A_i\right) > 0$$

Since the probability of choosing a coloring with no monochromatic k-clique is strictly greater than zero, there must exists such coloring. □

Monochromatic k-cliques: Example

As a particular instance consider 2-coloring K_{1000} so that there is no monochromatic K_{20} clique. We will use the following observation to bound the probability: for $n \leq 2^{k/2}$ and $k \geq 3$

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

Observing that $1000 \leq 2^1 0 = 2^{k/2}$ we see that there is such coloring.

Monochromatic k-cliques: Algorithm

- The key question is: How many samples we have to generate before we obtain the desired result?
- Assuming we obtain the desired sample with probability p, this is the geometric probability distribution with the expected value $1/p$.
- $1/p$ must be polynomial in the input parameters.

Considering a Monte Carlo algorithm, it is incorrect with probability $1 - p$. For the class of inputs satisfying $n \leq 2^{k/2}$ the probability is bounded by $\frac{2^{k/2+1}}{k!}$, hence the error is in $o(1)$.

Monochromatic k-cliques: Algorithm

- We can turn the previous Monte Carlo algorithm into a Las Vegas, if be bound the k so that it does grow with n.
- For the probability of success p, it takes on average $1/p$ rounds of computation to find the result.
- Each round takes $\binom{n}{2} \leq n^2/2$ steps to generate the coloring, and at most $k\binom{n}{k} \leq n^{k+1}$ steps to verify that all cliques are monochromatic.
- Provided p does not drop faster than polynomially, and k does not grow with n, we have an efficient algorithm.

Part III

The Expectation Argument

The Expectation Argument

- Sometimes easier way to prove an existence of an object is to use the expectation argument.
- The main idea behind is that in a discrete probability space, random variable must with nonzero probability assume at least one value not greater than its expectation and one value not smaller than its expectation.
- If the average price for a cinema ticket is 160 CZK, there must be at least one ticket for at most 160 CZK, and at least one ticket for at least 160 CZK.

The Expectation Argument

Theorem

Suppose we have a discrete random variable X such that $E(X) = \mu$. Then $P(X \geq \mu) > 0$ and $P(X \leq \mu) > 0$.

Proof.

If $P(X \geq \mu) = 0$ we have that

$$\mu = \sum_{x} xP(X = x) = \sum_{x<\mu} xP(X = x) < \sum_{x<\mu} \mu P(X = x) = \mu$$

giving a contradiction. Similarly for $P(X \leq \mu) = 0$. □

Finding a Large Cut

We use the expectation argument to show that in each graph there exists a cut with at least $1/2$ of the edges of the graph.

Theorem

Given an undirected graph $G = (V, E)$ with n vertices and m edges, there is a partition of V into two disjoint sets A, B such that at least $m/2$ edges connect a vertex in A to a vertex in B, i.e. the cut value is at least $m/2$.

Proof.

Construct A and B by randomly and independently assigning each vertex either to A or to B. Let $e_1, \ldots, e_m$ be an arbitrary enumeration of edges in G. For $i = 1, \ldots, m$ we define

$$X_i = \begin{cases} 1 & \text{if edge } i \text{ connects } A \text{ to } B \\ 0 & \text{otherwise.} \end{cases}$$

Finding a Large Cut

Proof.

The probability that a particular edge connect A and B is $1/2$. Hence,

$$E(X_i) = \frac{1}{2}.$$

Let $C(A,B)$ denotes the number of edges in the cut defined by A and B. Then

$$E(C(A,B)) = E\left(\sum_{i=1}^{m} X_i\right) = \sum_{i=1}^{m} E(X_i) = \frac{m}{2}.$$

Since the expecttaion of $C(A,B)$ is $m/2$, there must be partition A, B with at least $m/2$ edges connecting the sets, i.e. there is a cut of size $m/2$. □

Finding a Large Cut: Algorithm

We want to design a Las Vegas algorithm. To verify that it is efficient, we need an estimate of the success probability in the aforementioned sampling. Let

$$p = P(C(A,B) \geq \frac{m}{2}).$$

Using that $C(A,B) \leq m$ we get

$$\begin{aligned}\frac{m}{2} =& E(C(A,B)) \\ =& \sum_{i\leq m/2-1} iP(C(A,B)=i) + \sum_{i\geq m/2} iP(C(A,B)=i) \\ \leq& (1-p)\left(\frac{m}{2}-1\right) + pm,\end{aligned}$$

what gives

$$p \geq \frac{1}{m/2+1}.$$

The expected number of samplings is at most $m/2+1$. Each sampling takes $O(n)$ steps. To verify whether the cut size is at least $m/2$ is done by counting the number of edges crossing the cut in $O(m) \leq O(n^2)$.

MAX-SAT

The goal of the MAX-SAT problem is to satisfy (i.e. find a truth assignment of variables such that the clause is true) as many clauses as possible, given a formula in the conjunctive normal form, e.g.

$$(x_1 \vee \neg x_2 \vee \neg x_3) \wedge (\neg x_1 \vee \neg x_3) \wedge (x_1 \vee x_2 \vee x_4).$$

We assume that no clause contains a variable and its complement, since such a clause is always satisfied.

Theorem

Given a set of m clauses, let k_i be the number of literals in the ith clause, for $i = 1, \ldots, m$. Let $k = \min_{i=1}^{m} k_i$. Then there is a truth assignment that satisfies at least

$$\sum_{i=1}^{m} (1 - 2^{-k_i}) \geq m(1 - 2^{-k})$$

clauses.

MAX-SAT

Proof.

Assign to each variable independently and uniformly either *True* or *False*. The probability that ith clause (with k_i literals) is satisfied is $(1 - 2^{-k_i})$. Let $X_i = 1$ if the ith clause is satisfied, and 0 otherwise. The number of satisfied clauses is $X = \sum_{i=1}^{m} X_i$ and the expected value of satisfied clauses is

$$E(X) = \sum_{i=1}^{m} E(X_i) = \sum_{i=1}^{m} (1 - 2^{-k_i}) \geq m(1 - 2^{-k})$$

and there must be an assignment that satisfies at least as many clauses. □

Part IV

Derandomization Using Conditional Expectations

Derandomization Using Conditional Expectations

Our next goal is to derandomize the algorithm for finding cut of size $m/2$.

- The technique of the algorithm is to assign randomly and independently each vertex to set A or B.
- Imagine we do this deterministically, in an arbitrary order on vertices $v_1, \dots, v_n$, with x_i being the set to which we assigned v_i.
- Suppose that we have placed the first k vertices deterministically, and we want to place the rest randomly.
- We calculate the expected value of such a cut given the location of the first k vertices, i.e.

$$E(C(A,B)|x_1,\dots,x_k).$$

Derandomization Using Conditional Expectations

We want to find a method to place the $(k+1)$st vertex so that the expectation does not decrease, i.e.

$$E(C(A,B)|x_1,\ldots,x_k) \leq E(C(A,B)|x_1,\ldots,x_{k+1}).$$

It follows that

$$m/2 \leq E(C(A,B)) \leq E(C(A,B)|x_1,\ldots,x_n).$$

Derandomization Using Conditional Expectations

We design and prove the algorithm by induction. The base case is easy, since it does not matter where we place the first vertex

$$E(C(A,B)|x_1) = E(C(A,B)).$$

In the induction step we have to find an algorithm that satisfies

$$E(C(A,B)|x_1,\dots,x_k) \leq E(C(A,B)|x_1,\dots,x_{k+1}).$$

Assume we choose the next vertex randomly, as in the original randomized algorithm. Let Y_{k+1} be the random variable representing the set where v_{k+1} is placed. Then

$$\begin{aligned} E(C(A,B)|x_1,\dots,x_k) =& \frac{1}{2}E(C(A,B)|x_1,\dots,x_k,Y_{k+1}=A) \\ &+\frac{1}{2}E(C(A,B)|x_1,\dots,x_k,Y_{k+1}=B). \end{aligned}$$

Derandomization Using Conditional Expectations

We see that

$$\max\left\{E(C(A,B)|x_1,\ldots,x_k,Y_{k+1}=A),E(C(A,B)|x_1,\ldots,x_k,Y_{k+1}=B)\right\} \geq E(C(A,B)|x_1,\ldots,x_k).$$

To design the algorithm, it remains to calculate the conditional expectations

$$E(C(A,B)|x_1,\ldots,x_k,Y_{k+1}=A)$$
$$E(C(A,B)|x_1,\ldots,x_k,Y_{k+1}=B)$$

and then place the vertex into the set giving the higher conditional expectation.

Derandomization Using Conditional Expectations

Having fixed the placement of the first $(k+1)$ vertices, we can calculate the expectation as follows

1. We calculate the number of edges connecting the $(k+1)$ vectors that connect A and B. We can calculate this in time linear in m.
2. Each of the remaining edges has the probability $1/2$ to connect A and B. We can calculate this in time linear in m as well.

In fact, it satisfies to decide whether v_{k+1} has more neighbors already assigned to A or B and place it accordingly.

Derandomization Using Conditional Expectations: The Algorithm

1. Fix an arbitrary order of edges.
2. Place the first vertex arbitrarily to A or B.
3. For each successive vertex, determine whether it has more neighbors in A (and place it to B) or in B (and place it to A).

Part V

Sample and Modify

Derandomization Using Conditional Expectations

In the previous part of the lecture we demonstrated how to construct random structures directly.

Here we present a two-stage procedure to construct the desired object

1. First we sample an object, that does not have yet the desired properties, but that can be (easily) modified to have them.
2. We modify the sampled object so that we obtain the desired object.

Independent Sets

An independent set in a graph is a set of vertices with no edges connecting them. Finding the largest independent set is an NP-hard problem. We will bound the size of the largest independent set.

Theorem

Let $G = (V, E)$ be a graph on n vertices with m edges. The G has an independent set with at least $n^2/(4m)$ vertices.

Proof.

Let $d = 2m/n$ be the average degree of the vertices in G. Consider the following algorithm:

1. Delete each vertex of G (together with its incident edges) independently with probability $1 - 1/d$.
2. For each remaining edge, remove it and one of its adjacent vertices.

Independent Sets

Proof.

The remaining vertices clearly form an independent set, since all edges have been removed.

This is an example of the sample and modify technique. We first sample the vertices, and then we modify the remaining graph.

Let X be the number of vertices that survive the first step of the algorithm. Since the graph has n vertices and each of them survives with probability $1/d$, we have

$$E(X) = \frac{n}{d}.$$

Let Y be the number of edges that survive the first step. There are $nd/2$ edges in the graph, and each survives if and only if both adjacent vertices survive. Thus

$$E(Y) = \frac{nd}{2}\left(\frac{1}{d}\right)^2 = \frac{n}{2d}.$$

Independent Sets

Proof.

The second step removes all edges and at most Y vertices. Thus, the size of the final set is at least $X - Y$ with the expectation

$$E(X - Y) = \frac{n}{d} - \frac{n}{2d} = \frac{n}{2d}.$$

The expected size of the independent set is $n/(2d) = n^2/(4m)$. □

Graphs with Large Girth

The girth of a graph is the length of its smallest circle. Counterintuitively, we will show that there exists dense graphs with relatively large girth.

Theorem

For any integer $k \geq 3$ there is a graph with n node, at least $\frac{1}{4}n^{1+1/k}$ edges, and a girth at least k.

Proof.

We first sample a p-random graph with $p = n^{1/k-1}$. Let X be the number of edges in G. Then

$$E(X) = p\binom{n}{2} = \frac{1}{2}\left(1 - \frac{1}{n}\right)n^{1/k+1}.$$

Let Y be the number of cycles in the graph of length at most $(k-1)$. Any concrete cycle of length i $(3 \geq i \leq k-1)$ occurs with probability p^i.

Graphs with Large Girth

Proof.

There are $\binom{n}{i}\frac{(i-1)!}{2}$ possible cycles of length i: i vertices, all possible orders, reversing a particular order gives the same cycle.
Hence,

$$E(Y) = \sum_{i=3}^{k-1} \binom{n}{i} \frac{(i-1)!}{2} p^i \leq \sum_{i=3}^{k-1} n^i p^i = \sum_{i=3}^{k-1} n^{i/k} < kn^{(k-1)/k}.$$

We modify the original randomly chosen graph by removing one edge from each cycle of length up to $(k-1)$. The modified graph has girth at least k.

Graphs with Large Girth

Proof.

When n is sufficiently large, the expected number of edges in the final graph is

$$E(X-Y) \geq \frac{1}{2}\left(1-\frac{1}{n}\right) n^{1/k+1} - kn^{(k-1)/k} \geq \frac{1}{4}n^{1/k+1}.$$

Hence, there exists a graph with so many edges and girth at least k. □

Part VI

The Second Moment Method

The Second Moment Method

This method usually uses a derivation of the Chebyshev inequality:

Theorem

If X is a non-negative integer-valued random variable, then

$$P(X = 0) \leq \frac{Var(X)}{(E(X))^2}.$$

Proof.

$$P(X = 0) \leq P(|X - E(X)| \geq E(X)) \leq \frac{Var(X)}{(E(X))^2}.$$

□

Threshold behavior in Random Graphs

We will use the method to prove a certain threshold property in a p-random graph.

In general,there is a threshold function f such that

- when p is less than f, then almost no graph has the property
- when p is larger than f, then almost all graphs have the property.

Theorem

Let G be a p-random graph with n vertices and $p = f(n)$ and $f(n) = o(n^{-2/3})$. Then for any $\epsilon > 0$ and for sufficiently large n, then the probability that a random graph has a clique of size 4 or more is less than ϵ. Similarly, if $f(n) \in \omega(n^{-2/3})$, then for sufficiently large n the probability that a random graph does not have a clique with 4 or more vertices is less than ϵ.

Threshold behavior in Random Graphs

Before proving the theorem, we need to establish the following lemma

Lemma

Let Y_i $(i = 1, \dots, m)$ be a random variable with outputs 0 and 1, and let $Y = \sum_{i=1}^{m} Y_i$. Then

$$Var(Y) \leq E(Y) + \sum_{1 \leq i,j \leq m; i \neq j} Cov(Y_i, Y_j).$$

Proof of the lemma.

For any sequence of random variables $Y_1, \dots, Y_m$

$$Var\left(\sum_{i=1}^{m} Y_i\right) = \sum_{i=1}^{m} Var(Y_i) + \sum_{1 \leq i,j \leq m; i \neq j} Cov(Y_i, Y_j).$$

Threshold behavior in Random Graphs

Proof of the lemma.

When Y_i attains only values 0 or 1, $E(Y_i^2) = E(Y_i)$ and

$$Var(Y_i) = E(Y_i^2) - (E(Y_i))^2 \leq E(Y_i),$$

what completes the proof. □

Threshold behavior in Random Graphs

Now we can prove the theorem.

Proof of the theorem.

We consider first $p = f(n) \in o(n^{-2/3})$. Let $C_1, \ldots, C_{\binom{n}{4}}$ be any enumeration of 4 vertex subsets in G. Let

$$X_i = \begin{cases} 1 & \text{if } C_i \text{ is a 4-clique,} \\ 0 & \text{otherwise.} \end{cases}$$

Let

$$X = \sum_{i=1}^{\binom{n}{4}} X_i,$$

to get

$$E(X) = \binom{n}{4} p^6.$$

Threshold behavior in Random Graphs

Proof of the theorem.

We have $E(X) = o(1)$, i.e. $E(X) < \epsilon$ for sufficiently large n. Recall that X is a non-negative integer random variable to get using the Markov inequality

$$P(X \geq 1) \leq E(X) < \epsilon,$$

what completes this part of the proof.

Let us consider the case when $p = f(n) \in \omega(n^{-2/3})$. In this case $E(X) \to \infty$ as n grows. However, this is not a sufficient evidence that with a high probability a random graph has a clique of size 4 or more (why :-)?)! On the other hand, it suffices to show that $Var(X) \in o((E(X))^2)$ and use the second moment method.

Threshold behavior in Random Graphs

Proof of the theorem.

We want to calculate

$$Var(X) = Var\left(\sum_{i=1}^{\binom{n}{4}}\right).$$

To use the lemma we introduced before this proof, we need to calculate the covariances of X_i, X_j.

- If $C_i \cap C_j = \emptyset$, then X_i and X_j are independent and the covariance is 0. The same holds if $|C_i \cap C_j| = 1$.

Threshold behavior in Random Graphs

Proof of the theorem.

- If $|C_i \cap C_j| = 2$, the corresponding cliques share exactly one edge. For both cliques to appear in the graph, all corresponding 11 edges must appear in the graph. Hence,

$$E(X_i X_j) - E(X_i)E(X_j) \leq E(X_i X_j) \leq p^{11}$$

The are $\binom{n}{6}$ ways to choose the 6 vertices defining the two cliques, and $\binom{6}{2,2,2}$ ways to split them into C_i and C_j.

Threshold behavior in Random Graphs

Proof of the theorem.

- If $|C_i \cap C_j| = 3$, the corresponding cliques share exactly three edges. For both cliques to appear in the graph, all corresponding 9 edges must appear in the graph. Hence,

$$E(X_iX_j) - E(X_i)E(X_j) \leq E(X_iX_j) \leq p^9$$

The are $\binom{n}{5}$ ways to choose the 6 vertices defining the two cliques, and $\binom{5}{3,1,1}$ ways to split them into C_i and C_j.

Threshold behavior in Random Graphs

Proof of the theorem.

To conclude the proof, recall that $E(X) = \binom{n}{4}p^6$ and $p = f(n) \in \omega(n^{-2/3})$. Therefore,

$$\begin{aligned} Var(X) \leq& \binom{n}{4}p^6 + \binom{n}{6}\binom{6}{2,2,2}p^{11} + \binom{n}{5}\binom{5}{3,1,1}p^9 = o(n^8p^{12}) \\ =& o((E(X))^2), \end{aligned}$$

since

$$(E(X))^2 = \left(\binom{n}{4}p^6\right)^2 = \Theta(n^8p^{12}).$$

Finally, we can apply the method of second moments to get that $P(X = 0) \in o(1)$. □

Part VII

The Conditional Expectation Inequality

The Conditional Expectation Inequality

Imposing the additional restriction that the random variables attain only values 0 or 1, we get a method easier to apply than the second moment method.

Theorem

Let $X = \sum_{i=1}^{n} X_i$, where each X_i attains only values 0 and 1. Then

$$P(X > 0) \geq \sum_{i=1}^{n} \frac{P(X_i = 1)}{E(X|X_i = 1)}.$$

Notice that X_I do not have to be independent.

Proof.

Let $Y = 1/X$ if $X > 0$, and $Y = 0$ otherwise. Then

$$P(X > 0) = E(XY).$$

The Conditional Expectation Inequality

Proof.

However,

$$\begin{aligned}
E(XY) &= E\left(\sum_{i=1}^{n} X_i Y\right) = \sum_{i=1}^{n} E(X_i Y) \\
&= \sum_{i=1}^{n} \big(E(X_i Y | X_i = 1) P(X_i = 1) + E(X_i Y | X_i = 0) P(X_i = 0)\big) \\
&= \sum_{i=1}^{n} E(Y | X_i = 1) P(X_i = 1) = \sum_{i=1}^{n} E(1/X | X_i = 1) P(X_i = 1) \\
&\overset{\text{Jensen's inequality}}{\geq} \sum_{i=1}^{n} \frac{P(X_i = 1)}{E(X | X_i = 1)}.
\end{aligned}$$

□

Threshold behavior in Random Graphs

- We can use the previous theorem to get a more simple analysis of the 4-clique problem.
- We will show that if $p = f(n) = \omega(n^{-2/3})$, then for arbitrary $\epsilon > 0$ there exists a sufficiently large n such that the probability of a p-random graph to not have a clique of sice 4 or more is less than ϵ.

Let $X = \sum_{i=1}^{\binom{n}{4}} X_i$, where X_i is 1 if the corresponding four vertex subset is a clique, and 0 otherwise. For each particular X_j we have $P(X_j = 1) = p^6$. We use the linearity of expectation

$$E(X|X_j = 1) = E\left(\sum_{i=1}^{\binom{n}{4}} X_i \middle| X_j = 1\right) = \sum_{i=1}^{\binom{n}{4}} E(X_i|X_j = 1).$$

The Conditional Expectation Inequality

Observe that

$$E(X_i|X_j = 1) = P(X_i = 1|X_j = 1).$$

- There are $\binom{n-4}{4}$ sets of vertices C_i that do not intersect a particular C_j. Each corresponding $X_i = 1$ with probability p^6.
- $X_i = 1$ with probability p^6 for all $4\binom{n-4}{3}$ sets C_i that have one vertex in common with C_j.
- 2 vertices: $P(X_i = 1) = p^5$, there are $\binom{4}{2}\binom{n-4}{2}$ such sets.
- 3 vertices: $P(X_i = 1) = p^3$, there are $\binom{4}{3}\binom{n-4}{1}$ such sets.

The Conditional Expectation Inequality

We have

$$\begin{aligned} E(X|X_j = 1) &= \sum_{i=1}^{\binom{n}{4}} E(X_i|X_j = 1) \\ &= 1 + \binom{n-4}{4} p^6 + 4\binom{n-4}{3} p^6 + 6\binom{n-4}{2} p^5 + 4\binom{n-4}{1} p^3 \end{aligned}$$

We use the last theorem to get

$$P(X > 0) \geq \frac{\binom{n}{4} p^6}{1 + \binom{n-4}{4} p^6 + 4\binom{n-4}{3} p^6 + 6\binom{n-4}{2} p^5 + 4\binom{n-4}{1} p^3},$$

which approaches 1 as n grows large.

Part VIII

The Lovasz Local Lemma

The Conditional Expectation Inequality