The Probabilistic Method

Topics on Randomized Computation

Spring Semester

Co.Re.Lab.-N.T.U.A.

Overview

In the first part we will see simple methods (basically through examples)

1. The counting method
2. The first moment method
3. The deletion method
4. The second moment method
5. Derandomization with conditional probabilities

The second part is THE part(y):

1. General Lovasz Local Lemma
2. Other (usual and helpful) forms of LLL
3. Constructive proof of LLL

Counting Expanders

We will relay on $\Pr(Q(x)) > 0 \Rightarrow \exists x Q(x)$

Definition: An *(n,d,a,c) OR-concentrator* is a bipartite multigraph *G(L,R,E)* such that:

- Each vertex in *L* has degree at most *d*
- For any $S \subseteq L : |S| \leq a \cdot n \rightarrow |N(S)| \geq c|S|$

Theorem: There is an integer n_0 such that for all $n > n_0$ there is an *(n,18,1/3,2) OR-concentrator*.

We will choose a random graph from a suitable probabilistic space and we will show that it has positive probability of being an *(n,18,1/3,2) OR-concentrator*.

Counting Expanders

Proof: Our random bipartite graph will have

- Vertex set $V = L \cup R$
- Each $v \in L$ "chooses" *d* times a neighbor (in *R*) uniformly (multiple edges become one edge).

Let E_s be the event that a subset with *s* vertices of *L* has fewer than *cs* neighbors.

We will bound $\Pr[E_s]$ and then sum up for all the values $s \leq an$ to get a bound on the probability of failure

Fix an $S \subseteq L$ of size *s* and a $T \subseteq R$ of size *cs*.

Counting Expanders

- There are $\binom{n}{s}$ ways of choosing *S*
- There are $\binom{n}{cs}$ ways of choosing *T*
- The probability that *T* contains all neighbors of *S* is $\leq \left(\frac{cs}{n}\right)^{ds}$

Thus $\Pr[E_S] \leq \binom{n}{s}\binom{n}{cs}\left(\frac{cs}{n}\right)^{ds} \leq \left(\frac{ne}{s}\right)^{s}\left(\frac{ne}{cs}\right)^{cs}\left(\frac{cs}{n}\right)^{ds} \leq \left[\left(\frac{s}{n}\right)^{d-c-1} e^{c+1}c^{d-c}\right]^{s}$

Simplifying for a=1/3, c=2, d=18 and using $s \leq an$ we get

$$\Pr[E_S] \leq \left[\left(\frac{s}{n}\right)^{d-c-1} e^{c+1}c^{d-c}\right]^{s} \leq \left[\left(\frac{1}{3}\right)^{d-c-1} e^{c+1}c^{d-c}\right]^{s} \leq \left[\left(\frac{c}{3}\right)^{d} (3e)^{c+1}\right]^{s} \leq \left[\left(\frac{2}{3}\right)^{18} (3e)^{3}\right]^{s}$$

Summing up we get $\Pr[failure] \leq \sum_{S} \Pr[E_S] < 1$

The First Moment Method

1. At first we design a "thought experiment" in which a random process plays a role
2. We analyze the random experiment and draw a conclusion using *the first moment principle*:

$$E[X] \le t \Rightarrow \Pr(X \le t) > 0$$

Example 1

Theorem:

For any undirected graph *G(V,E)* with *n* vertices and *m* edges there is a partition of the vertex set into two sets *A, B* such that

$$|\{\{u,v\}\in E \mid u\in A \wedge v\in B\}| \geq \frac{m}{2}$$

Proof:

- Assign each vertex independently and equiprobably in either A or B.
- *Let* $X_{\{u,v\}}=1$ when *{u,v} has endpoints in different sets and* $X_{\{u,v\}}=0$ otherwise: $\Pr[X_{\{u,v\}}=1]=1/2 \Rightarrow E[X_{\{u,v\}}]=1/2$
- By linearity of expectations:

$$E[|\,separated \quad edges\,|]=\sum_{\{u,v\}\in E} E[X_{\{u,v\}}]=m/2$$

Example 2

Theorem:

For any set of *m* clauses there is a truth assignment that satisfies at least *m/2* clauses. (a clause is $(x_1 \vee \neg x_2 \vee x_3 \vee \ldots \vee x_k)$)

Proof:

- Independently set each variable *TRUE* or *FALSE*
- For each clause let $Z_i=1$ if the *i-th* clause is satisfied and $Z_i=0$ otherwise
- If the *i-th* clause has *k* literals: $\Pr(Z_i = 1) = 1 - 2^{-k}$
- For every clause: $E[Z_i] \geq 1/2$
- The expected number of satisfied clauses is

$$E[\sum_{i=1}^{m} Z_i] = \sum_{i=1}^{m} E[Z_i] \geq \frac{m}{2}$$

Example 3

Theorem:

Any instance of *k-Sat* with $<2^k$ clauses is satisfiable

Proof:

- Independently set each variable *TRUE* or *FALSE*
- For each clause let $Z_i=0$ if the *i-th* clause is satisfied and $Z_i=1$ otherwise: $\Pr(Z_i = 1) = 2^{-k}$
- For every clause: $E[Z_i] = 2^{-k}$
- The expected number of unsatisfied clauses is

$$E[\sum_{i=1}^{m} Z_i] = \sum_{i=1}^{m} E[Z_i] = m2^{-k} < 1$$

The Deletion Method

(“sample and modify” method)

We want to prove that a combinatorial object *F* exist

1. At first we show that there exist an F' very “close” to *F*.
2. Then we change F' to *F* and show that the probability of existence remains positive

Turan's Theorem*

Theorem: Let $G(V,E)$ be a graph. If $|V|=n$ and $|E|=nk/2$ then $a(G) \geq n/2k$

Proof: Using probabilistic arguments we will prove the existence of a subset that has many more vertices than edges

Deleting vertices corresponding to these edges we get an independent set.

Let S be a subset of V containing each vertex with probability p (to be fixed later). We have $E[|S|]=np$

Let G' be the subgraph induced by S.

For every $e \in E$ define $Y_e=1$ if $e \in E(G')$ and $Y_e=0$ otherwise. Then:

$$E[Y_e] = p^2$$

Turan's Theorem*

Let *Y=|E(G')|* the number of edges in the induced subgraph. Then:

$$E[Y] = E[\sum_{e \in E} Y_e] = \sum_{e \in E} E[Y_e] = \frac{nk}{2} p^2$$

Deletion time: We drop all edges (by deleting vertices) from *G'* and we get an independent set *S**. We have:

$$E[|S^*|] \geq E[|S| - Y] = E[|S|] - E[Y] = np - \frac{nk}{2} p^2$$

We fix *p* to maximize this expression. It's a parabola, which attains its maximum at *p=1/k* and so

$$E[|S^*|] \geq \frac{n}{2k}$$

Erdos's Theorem

Definitions:

1. The chromatic number, *x(G)*, of a graph *G* is the minimum number of colors needed to color the vertices of *G* such that adjacent vertices have different colors.
2. By *a(G)* we denote the cardinality of a maximum independent set of *G*.
3. The girth, *g(G)*, of a graph *G* is the length of a shortest cycle in *G*

Theorem: For any naturals *k*, *l* there exist a graph *G* such that: $x(G) \geq k$ and $g(G) \geq l$.

We will find a graph that has

- Small *a(G)*
- Not many "bad" cycles of length <*l* (that will be destroyed!)

In the end we'll use that $|V(G)| \leq x(G)a(G)$ and "force" *x(G)* to get big

Erdos's Theorem

Proof: We choose a random graph G_{np} (n vertices and each edge chosen independently with probability p).

- Small p gives large independent sets and thus small chromatic number
- Large p gives small cycles.

Let $p=n^{\theta-1}$ and we'll fix θ later

Let $(b_1,\dots,b_c)$ an ordered sequence of vertices. The probability of b_1 - b_2 -…- b_c - b_1 being a cycle is p^c. Let $Y_B=1$ when this happens and $Y_B=0$ otherwise

For a subset $B'=\{b_1,\dots,b_c\}$ of V there are $c!$ ways to form cyclic ordered sequences with the vertices of B'. There are $\binom{n}{c}$ ways of choosing B.

Let X_c be the number of cycles of length c in G. Combining we get:

$$E[X_c] = E\left[\frac{1}{2c}\sum_{B\subseteq\{V\}^C} Y_B\right] = \binom{n}{c}\frac{(c-1)!}{2}p^c$$

Erdos's Theorem

Let X be the number of cycles of length no greater than *l*:

$$E[X]=E[\sum_{c=3}^{l}X_c]=\sum_{i=3}^{l}\binom{n}{i}\frac{(i-1)!}{2}p^i=\sum_{i=3}^{l}\frac{n!}{(n-i)!2i}p^i\le\sum_{i=3}^{l}n^i\frac{1}{2i}(n^{\theta-1})^i\le\sum_{i=3}^{l}\frac{n^{\theta i}}{2i}$$

By Markov's inequality: $\Pr(X\ge n/2)\le\frac{E[X]}{n/2}\le\frac{2}{n}\sum_{i=3}^{l}\frac{n^{\theta i}}{2i}=\sum_{i=3}^{l}\frac{n^{\theta i-1}}{i}<(l-2)n^{\theta l-1}$

Fixing $\theta<1/l$ we get: $\Pr_{n\to\infty}(X\ge n/2)=0$

Let *Y* be the number of independent sets of size *y* (to be fixed later) in *G*. By Markov's inequality:

$$\Pr(a(G)\ge y)=\Pr(Y\ge 1)\le E[Y]=\binom{n}{y}(1-p)^{y(y-1)/2}<n^y(e^{-p})^{y(y-1)/2}$$

Now let $y=\frac{3}{p}\ln n$. We get: $\Pr(a(G)\ge y)\le(ne^{-p(y-1)/2})^y\le(ne^{\frac{-3\ln n}{2}+\frac{p}{2}})^y=\left(\frac{1}{\sqrt{n}}e^{\frac{p}{2}}\right)^y$

So $\Pr_{n\to\infty}(a(G)\ge y)=0$

Erdos's Theorem

By taking *n* large enough we manage both events

- $a(G) \geq y$ and
- $X \geq n/2$,

to have probability <1/2.

So there is a G such that: $a(G) < y$ and $X < n/2$

Deletion time: We remove one vertex from each of the at most n/2 "bad" cycles. Thus we get a G' with $g(G) \geq l$, more than n/2 vertices and $a(G') \leq a(G)$

Putting it all together: $x(G') \geq \frac{|V(G')|}{a(G')} \geq \frac{|V(G)|/2}{a(G)} \geq \frac{n/2}{\frac{3}{p}\ln n} = \frac{n^{\theta}}{6\ln n} \geq k$ for large enough n.

G' is our Graph.

The Second Moment Method

- Method based on Chebysev's inequality:

$$\Pr(|X - E[X]| \geq t) \leq \frac{\mathrm{var}[X]}{t^2}$$

reaching conclusions using concentration results

- Useful tool for determining the threshold function of an event *A*:
  - Below threshold, *Pr(A)* tends to 0
  - Above it, *Pr(A)* tends to 1

Distinct sums

Let $A = \{a_1, a_2, \ldots, a_k\}$. Define $S(I) = \{s(I) : I \subseteq A\}$, where *s(I)* is the sum of the elements of *I*.

Question: How large can a subset of *{1,…,n}* with distinct sums be?

One of size $k = \lfloor \log n \rfloor + 1$ is $A = \{2^{i-1} \mid i = 1, \ldots, k\}$.

On the other hand every sum is at most *kn* and so

$$2^k \leq kn \Rightarrow k \leq \log n + \log\log n + O(1)$$

Theorem: if $A \subset \{1, \ldots, n\}$ has distinct sums then

$$|A| \leq \log n + \tfrac{1}{2}\log\log n + O(1)$$

Distinct sums

Proof: To get an A "close" to the upper bound we need

- S(A) "close" to {1,…,kn}
- The sums of the subsets of A to be spread evenly.

Using Chebysev's inequality we'll prove that most of the sums are around the middle.

Picking at random a sum from *S(A)* is equivalent to picking a random subset *I* of *A* and then computing its sum.

Let $A = \{a_1, \ldots, a_k\}$ and $X_i = 1 \Leftrightarrow a_i \in I$. Let *X=s(I).* We have

$$E[X] = \sum_{i=1}^{k} a_i E[X_i] = \frac{1}{2} \sum_{i=1}^{k} a_i$$

Distinct sums

Var(X): $E[X^2]=E[(\sum_{i=1}^{k} a_i X_i)^2]=E[(\sum_{i=1}^{k} a_i^{\,2} X_i^{\,2} + 2\sum_{1\le i<j\le k} a_i a_j X_i X_j]=$

$$\underbrace{\begin{aligned}&\sum_{i=1}^{k} a_i^{\,2} E[X_i^{\,2}] + 2\sum_{1\le i<j\le k} a_i a_j E[X_i X_j] = \frac{1}{2}\sum_{i=1}^{k} a_i^{\,2} + \frac{1}{2}\sum_{1\le i<j\le k} a_i a_j\\ &E[X]^2 = \frac{1}{4}\sum_{i=1}^{k} a_i^{\,2} + \frac{1}{2}\sum_{1\le i<j\le k} a_i a_j\end{aligned}}$$

$$\Rightarrow \mathrm{var}[X] = E[X^2] - E[X]^2 = \frac{1}{4}\sum_{i=1}^{t} a_i^{\,2} < \frac{n^2 k}{4}$$

By Chebysev’s inequality

$$\Pr(|X - E[X]| \ge 2\sqrt{\mathrm{var}[X]}) \le \frac{\mathrm{var}[X]}{\left(2\sqrt{\mathrm{var}[X]}\right)^2} \Rightarrow \Pr(|X - E[X]| \ge n\sqrt{k}) \le \frac{1}{4}$$

Thus at least ¾ of the sums are inside an interval of length $2n\sqrt{k}$

Therefore $\frac{3}{4}2^k \le 2n\sqrt{k} \Rightarrow k \le \log n + \frac{1}{2}\log\log n + O(1)$

Threshold for Clique

Theorem: Let $G_{n,p}$ a graph and *K* the number of cliques with *4* vertices.

- If $p=o(n^{-2/3})$ then $\Pr_{n\to\infty}(K\geq 1)=0$
- If $p=\omega(n^{-2/3})$ then $\Pr_{n\to\infty}(K\geq 1)=1$

Proof: Let $\{C_1,\ldots,C_t\}$ be the enumeration of the $\binom{n}{4}$ *4-tuples*, and $X_i=1$ when C_i induces a *4-clique* and $X_i=0$ otherwise.

- In the first case $K=\sum_{i=1}^{t}X_i$, so $E[K]=\binom{n}{4}p^6\approx\frac{n^4p^6}{24}$ and

$$\Pr_{n\to\infty}(K\geq 1)\leq \underset{n\to\infty}{E}[K]\approx\lim_{n\to\infty}\frac{n^4p^6}{24}\overset{p=o(n^{-2/3})}{=}0$$

- Unfortunately in the second case we get

$$\Pr_{n\to\infty}(K\geq 1)\leq \underset{n\to\infty}{E}[K]\approx\lim_{n\to\infty}\frac{n^4p^6}{24}\overset{p=\omega(n^{-2/3})}{=}\infty$$

Chebysev's inequality proves useful. After bounding *Var*[*K*] we can use the fact:

$$\Pr(K=0)\leq\Pr(|K-E[K]|\geq E[K])\leq\frac{Var[K]}{(E[K])^2}$$

Threshold for Clique

To compute *Var[K]=E[K²]-E[K]²*

- *E[K]²*: $E[K]^2 = (\sum_{i=1}^{t} E[X_i])^2 = \sum_{i=1}^{t} E[X_i]^2 + \sum_{i \neq j} E[X_i]E[X_j]$
- *E[K²]*: $E[K^2] = E[(\sum_{i=1}^{t} X_i)^2] = \sum_{i=1}^{t} E[X_i^2] + \sum_{i \neq j} E[X_i X_j]$

1. If $|C_i \cap C_j| \leq 1$ then $E[X_i X_j] = E[X_i]E[X_j]$
2. If $|C_i \cap C_j| = 2$ then $E[X_i X_j] = p \cdot p^5 \cdot p^5 = p^{11}$. We count $\binom{n}{4}\binom{4}{2}\binom{n-4}{2}$ such instances.
3. If $|C_i \cap C_j| = 3$ then $E[X_i X_j] = p^3 \cdot p^3 \cdot p^3 = p^9$. We count $\binom{n}{4}\binom{4}{3}\binom{n-4}{1}$ such instances.

Thus

$$Var[K] = \sum_{i=1}^{t} E[X_i^2] - \sum_{i=1}^{t} E[X_i]^2 + \sum_{i \neq j} E[X_i X_j] - \sum_{i \neq j} E[X_i]E[X_j] \Rightarrow$$

$$Var[K] \leq \binom{n}{4} p^6 + \binom{n}{4}\binom{4}{2}\binom{n-4}{2} p^{11} + \binom{n}{4}\binom{4}{3}\binom{n-4}{1} p^9 \overset{p=\omega(n^{-2/3})}{=} o(n^8 p^{12}) = o(E[X]^2)$$

Finally:

$$\lim_{n \to \infty} \Pr(K = 0) \leq \lim_{n \to \infty} \frac{Var[K]}{(E[K])^2} = 0$$

Derandomizing

F boolean formula in *CNF* with variables $x_1,\dots,x_n$.

Set x_i= *True* or *False* equiprobably and let *X* denote the number of unsatisfied clauses.

Suppose that $E[X]<1$ (e.g. *k-Sat* instance with less than 2^k clauses), so there is a truth assignment that satisfies the formula

Derandomize..:

- Set x_1 = *True* simplify *F* and compute $E[X|\ x_1=True]$.
- Set x_1 = *False* simplify *F* and compute $E[X|\ x_1=False]$.

<u>It is $E[X|\ x_1=True]<1$ or $E[X|\ x_1=False]<1$</u>.

Keep a value of x_1 that keeps $E[X|\ x_1]<1$.

Repeat for all variables and you get $E[X|\ x_1,\dots,\ x_n]<1$.

The values for $x_1,\dots,\ x_n$ is the satisfying truth assignment

Conditional Probabilities

Generalizing the previous technique we get the "method of conditional probabilities".

In general it is something like this:

- X is a random variable determined by a sequence of random trials $T_1, \ldots, T_n$.
- We want to find a set of outcomes such that $X \leq E[X]$
- There must be a $t_1 : E[X \mid T_1 = t_1] \leq E[X]$. We find it.
- We repeat to find the outcome

$$t_i : E[X \mid T_1 = t_1, \ldots, T_{i-1} = t_{i-1}, T_i = t_i] \leq E[X \mid T_1 = t_1, \ldots, T_{i-1} = t_{i-1}] \leq E[X]$$

- At the end we get $E[X \mid T_1 = t_1, \ldots, T_n = t_n] \leq E[X]$. But there is no randomness left thus we have determined a desired set of outcomes for which $X \leq E[X]$

In order to succed we need

1. "Small" number of trials
2. The computations for determining t_i can be carried out efficiently

Max-cut

Theorem: For any undirected graph *G(V,E)* with *n* vertices and *m* edges there is a partition of the vertex set into two sets *A, B* such that

$$|\{\{u,v\}\in E \mid u\in A \wedge v\in B\}| \geq \frac{m}{2}$$

Let C(A,B) denote the number of edges between A, B. We have $E[C(A,B)] \geq \frac{m}{2}$ when vertices equiprobably go either to A or B.

- To begin with: v_1 goes to *A* (or *B*) and we get $E[C(A,B) \mid v_1] \geq E[C(A,B)]$
- For the intermediate steps when the k first nodes are in some set then
  - We can compute the cut that these vertices "give" in the final cut
  - Each of the edges that are "incomplete" have ½ probability to be in the cut
- So $E[C(A,B) \mid v_1,\ldots,v_k,v_{k+1}\in A]$ and $E[C(A,B) \mid v_1,\ldots,v_k,v_{k+1}\in B]$ can be computed efficiently. We keep the big one.

We'll do *n* steps to fully determine *A, B*. Each step needs polynomial time

The Lovasz Local Lemma

Let $A_1,\ldots,A_n$ be some "bad" events and for all *i*: $\Pr(A_i) < \frac{1}{2}$

If A_i are pairwise independent then we could assert that none of these will happen with probability

$$\Pr\left(\overline{A_1}\cap\ldots\cap\overline{A_n}\right)=\underbrace{\Pr\left(\overline{A_1}\right)\cdot\Pr\left(\overline{A_2}\mid\overline{A_1}\right)\cdot\ldots\cdot\Pr\left(\overline{A_n}\mid\overline{A_1}\cap\ldots\cap\overline{A_{n-1}}\right)}_{\left(1-\Pr\left(A_1\right)\right)\cdot\left(1-\Pr\left(A_2\mid\overline{A_1}\right)\right)\cdot\ldots\cdot\left(1-\Pr\left(A_n\mid\overline{A_1}\cap\ldots\cap\overline{A_{n-1}}\right)\right)}=\Pr\left(\overline{A_1}\right)\cdot\ldots\cdot\Pr\left(\overline{A_n}\right)>0$$

The Lovasz Local Lemma states that if each event is dependent to "few" other events then there is a probability that none of this will happen.

Definition: Dependency graph of events $A_1,\ldots,A_n$ is a digraph G in which

- For every A_i there is a vertex corresponding to it
- A_i is independent to all other A_j's such that (A_i,A_j) is not an edge of *G*

Theorem: Let *G(V,E)* be a dependency graph of the events $A_1,\ldots,A_n$. Then

$$\left[\forall i\exists x_i : \Pr(A_i)\le x_i\prod_{(i,j)\in E}(1-x_j)\right]\Rightarrow\Pr\left(\bigcap_{i=1}^{n}\overline{A_i}\right)\ge\prod_{i=1}^{n}(1-x_i)$$

Lovasz Local Lemma Proof

Let $S \subseteq \{1,\ldots,n\}$. By induction on *k=|S|* we will show that for any S and $i \notin S$: $\Pr(A_i \mid \bigcap_{j\in S} \overline{A_j}) \le x_i$

For *k=0* the result follows from $\forall i \exists x_i : \Pr(A_i) \le x_i \prod_{(i,j)\in E} (1-x_j)$

For the inductive step we want to compute $\Pr(A_i \mid \bigcap_{j\in S} \overline{A_j}) \le x_i$. Separate *S* to $S_1 = \{ j \in S : (i,j) \in E \}$ and $S_2 = S \setminus S_1$.

By definition: $$\Pr(A_i \mid \bigcap_{j\in S} \overline{A_j}) = \frac{\Pr\left(A_i \cap \bigcap_{j\in S_1} \overline{A_j} \mid \bigcap_{j\in S_2} \overline{A_j}\right)}{\Pr\left(\bigcap_{j\in S_1} \overline{A_j} \mid \bigcap_{j\in S_2} \overline{A_j}\right)}$$

Numerator: $\Pr\left(A_i \cap \bigcap_{j\in S_1} \overline{A_j} \mid \bigcap_{j\in S_2} \overline{A_j}\right) \le \Pr\left(A_i \mid \bigcap_{j\in S_2} \overline{A_j}\right) = \Pr\left(A_i\right) \le x_i \prod_{(i,j)\in E} (1-x_j)$

Denominator: $\Pr\left(\bigcap_{j\in S_1} \overline{A_j} \mid \bigcap_{j\in S_2} \overline{A_j}\right) \ge \prod_{j\in S_1} (1-x_j) \ge \prod_{(i,j)\in E} (1-x_j)$

To complete the proof:
$$\Pr\left(\bigcap_{i=1}^{n} \overline{A_i}\right) = (1-\Pr(A_1))(1-\Pr(A_2 \mid \overline{A_1}))\ldots(1-\Pr(A_n \mid \bigcap_{i=1}^{n-1} \overline{A_i})) \ge \prod_{i=1}^{n} (1-x_i)$$

Other forms of LLL

- The basic form: If
  1. $\forall i : \Pr(A_i) \leq p < 1$
  2. For all *i*: A_i is mutually independent of all but at most *d* of the other events
  3. $4pd < 1$ (or $ep(d+1) < 1$)

Then with positive probability none of the events will occur

- The Asymmetric form: If for all *i*:
  1. A_i is mutually independent of $A \setminus (D_i \cup A_i)$ for some D_i
  2. $\Pr(A_i) \leq 1/8$
  3. $\sum_{A_j \in D_i} \Pr(A_i) \leq 1/4$

Then with positive probability none of the events will occur

- The weighted form: If
  1. A_i is mutually independent of $A \setminus (D_i \cup A_i)$ for some D_i
  2. There are $t_1, \ldots, t_n$ and $p : 0 \leq p < 1/8$ such that for all *i*:
     - $\Pr(A_i) \leq p^{t_i}$
     - $\sum_{A_j \in D_i} (2p)^{t_j} \leq t_i/4$

Then with positive probability none of the events will occur

Some Proofs

- The general (compact!) form

$$\left[\forall i \exists x_i : \Pr(A_i) \le x_i \prod_{(i,j)\in E} (1-x_j)\right] \Rightarrow \Pr\left(\bigcap_{i=1}^{n} \overline{A_i}\right) \ge \prod_{i=1}^{n} (1-x_i)$$

- For the Weighted LLL set $x_i = (2p)^{t_i} \overset{p<\frac{1}{8}}{\Rightarrow} x_i < (1/4)^{t_i} \overset{t_i>0}{\Rightarrow} (1-x_i) \ge e^{-1.2x_i}$

$$x_i \prod_{A_j\in D_i} (1-x_j) \ge x_i \prod_{A_j\in D_i} e^{-1.2x_j} \ge 2^{t_i}\Pr(A_i)\cdot e^{-1.2\sum_{A_j\in D}(2p)^{t_i}} \ge 2^{t_i}\Pr(A_i)\cdot e^{0.6} > \Pr(A_i)$$

- For the Asymmetric LLL set $x_i = 2\Pr(A_i) \Rightarrow x_i \le 1/4 \Rightarrow (1-x_i) \ge e^{-1.2x_i}$
This way:

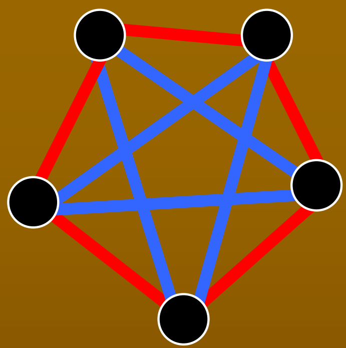
$$x_i \prod_{A_j\in D_i} (1-x_j) \ge x_i \prod_{A_j\in D_i} e^{-1.2x_j} \ge 2\Pr(A_i)\cdot e^{-1.2\sum_{A_j\in D}2\Pr(A_j)} \ge 2\Pr(A_i)\cdot e^{0.6} > \Pr(A_i)$$

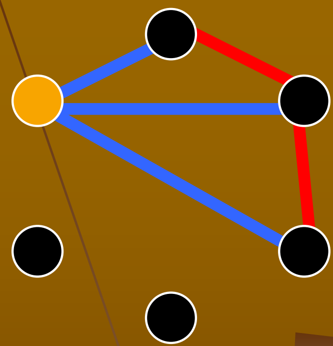
- For the Basic LLL we can assume* d>1 and then $\Pr(A_i) \le 1/8$ and $\sum_{A_j\in D_i}\Pr(A_i) \le pd = (1/4)4pd < 1/4$

Ramsey numbers

Definition: *R(k,l)* is the minimal n such that if the edges of the complete graph on *n* vertices, K_n, are colored *Red* or *Blue*, then there is (as a subgraph) a K_k with all edges *Red* or a K_l with all edges *Blue*.

For example R(3,3)>5. In particular R(3,3)=6





Using the basic form of the Lovasz Local Lemma we will get a lower bound for R(k,k).

Theorem: $$R(k,k) > n \approx \frac{k}{e} 2^{(k+1)/2}(1+O(1))$$

Ramsey numbers

Proof: Color the edges of K_n uniformly at random.

For every $S \subset V, |S| = k$ let A_S be the event that *S* induces a *monochromatic k-clique*. It is

$$\Pr(A_S) = \left(\frac{1}{2}\right)^{\binom{k}{2}-1} = p$$

Let G be a dependency graph of the events A_S. The events A_S, $A_{S'}$, are dependent only if *S* and *S′* share at least one edge. Thus

$$d = \Delta(G) \le \binom{k}{2}\binom{n-2}{k-2}$$

By Lovasz Local Lemma if *4pd<1* then there is positive probability that no monochromatic K_k exists.

$$4pd < 1 \Leftrightarrow 4 \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}-1} \cdot \binom{k}{2}\binom{n-2}{k-2} < 1$$

The maximal *n* for which the above holds is our lower bound.

Coloring Hypergraphs

A hypergraph *H=(V,E)* is a generalization of a graph where *E* is $E \subseteq 2^V$. *H* is:

- *k-uniform* if each edge contains exactly *k* vertices and
- *K-regular* if every vertex participates in exactly *k* edges

Let *H* be a hypergraph. Graph *H* has *property B* if there exist a *2-coloring* of the *vertices* such that none of the edges is monochromatic

Theorem: Let *H* be a *k-uniform*, *k-regular* hypergraph. Then for all *k>8*, *H* has *property B* .

Coloring Hypergraphs

Proof: Color the vertices uniformly at random and let A_f be the event that edge *f* is monochromatic.

- *H* is *k-uniform*. Thus for all *f*: $\Pr(A_f) = \left(\frac{1}{2}\right)^{k-1} = p$

- *H* is *k-regular*, so each edge intersects with at most *k(k-1)* other edges and thus: $d \leq k(k+1)$

Getting it all together:

$$\forall k > 8 : ep(d+1) \leq e\left(\frac{1}{2}\right)^{k-1}\left(k(k+1)+1\right) < 1$$

So using Lovasz Local Lemma:

$$\Pr\left(\bigcap_f \overline{A_f}\right) > 0$$

Edge-disjoint Paths

Assume we have a network and *n* pairs of users who wish to communicate via *edge-disjoint* paths.

Each pair of users, *i*, has a collection F_i of *m* possible paths from which it chooses his path.

If the possible paths do not share too many edges then there is a set of edge-disjoint paths that does the work.

Theorem: If any path in F_i shares edges with no more than *k* paths in F_j ($\forall j \neq i$) and $8nk/m \leq 1$ then there are *n* disjoint paths connecting the *n* pairs

Edge-disjoint Paths

Proof: Each pair chooses equiprobably one path from his *m* possible paths

Let $E_{i,j}$ denote the event that the paths of *i* and *j* share a common edge. It is $p = \Pr(E_{i,j}) \leq k/m$

Event $E_{i,j}$ could be depended only to events $E_{i,t}$ or $E_{j,t}$. So $d<2n$.

It is $4dp < \frac{8nk}{m} < 1$. So using LLL we get: $\Pr\left(\bigcap_{i\neq j} \overline{E_{i,j}}\right) > 0$

Expanders

Definition: A graph *G(V,E)* is called *β-expander* if

$$\forall S \subset V \left[|S| \le \tfrac{1}{2}|V| \rightarrow E(S,\bar{S}) \ge \beta |S| \right]$$

We will show that if we have a *β-expander G(V,E)*, we can partition *E* to E_1, E_2, so that both $G_1(V,E_1)$ and $G_2(V,E_2)$ are nearly a *(β/2)-expander.*

Theorem: Let $\varepsilon>0$, $r\geq 3$ and *β* sufficiently large in terms of *ε, r*. If *G* is an *r-regular β-expander* then there is a partition $E(G) = E_1 \cup E_2$ such that each E_i induces a $\beta(\frac{1}{2}-\varepsilon)$-expander.

Proof: We will (as usual) place each edge equiprobably to one of the two sets. We will "define" what is "bad" and use the <u>weighted</u> version of LLL.

Expanders

For each $S \subset V$ (connected) of size $|S| \le \frac{1}{2}|V|$, let A_S be the event that *S* "fails":

$$\left[E_1(S,\bar{S}) < \beta(\tfrac{1}{2}-\varepsilon)|S|\right] \vee \left[E_2(S,\bar{S}) < \beta(\tfrac{1}{2}-\varepsilon)|S|\right]$$

It is:

$$\Pr\left[E_i(S,\bar{S}) < \beta(\tfrac{1}{2}-\varepsilon)|S|\right] = \Pr\left[\beta\tfrac{1}{2}|S| - E_i(S,\bar{S}) > \varepsilon\beta|S|\right]$$

It is like throwing *β|S|* coins and $|E_1| \geqslant |heads| = |E'_1|$, $|E_2| \geqslant |tails| = |E'_2|$.

1. $\Pr\left[\beta\tfrac{1}{2}|S| - E_i(S,\bar{S}) > \varepsilon\beta|S|\right] \le \Pr\left[\beta\tfrac{1}{2}|S| - E'_i(S,\bar{S}) > \varepsilon\beta|S|\right]$
2. $\Pr\left[\beta\tfrac{1}{2}|S| - E'_2(S,\bar{S}) > \varepsilon\beta|S|\right] \underset{E'_1(S,\bar{S})+E'_2(S,\bar{S})=\beta|S|}{=} \Pr\left[E'_1(S,\bar{S}) - \beta\tfrac{1}{2}|S| > \varepsilon\beta|S|\right]$

So:

$$\Pr[A_S] \le \sum_{i=1,2} \Pr\left[\beta\tfrac{1}{2}|S| - E_1(S,\bar{S}) > \varepsilon\beta|S|\right] \underset{1,2}{\le} \Pr\left[\left|\beta\tfrac{1}{2}|S| - E'_i(S,\bar{S})\right| > \varepsilon\beta|S|\right]$$

Using Chernoff Bound:

$$\Pr[A_S] \le \Pr\left[\left|\tfrac{1}{2}\beta|S| - E'_i(S,\bar{S})\right| > \varepsilon\beta|S|\right] \le 2e^{-\frac{\varepsilon^2\beta^2|S|^2}{3n\frac{1}{2}}} \underset{\frac{1}{\beta}=\frac{|S|}{n}}{\le} 2e^{-\frac{2}{3}\varepsilon^2\beta|S|} = p^{|S|}$$

Expanders

G is *r-regular*. It is known… that in this case every vertex lies in at most $\binom{rt}{t} < \left(\frac{ert}{t}\right)^t = (er)^t$ connected subsets of size t.

A_s is dependent to at most $(er)^t |S|$ other events $A_{s'}$ for which $|S'|=t$

We have

- $\Pr[A_S] \le 2e^{-\frac{2}{3}\varepsilon^2\beta|S|} = p^{|S|}$
- $\sum_{A_{S'}\in D_S} (2p)^{t_{S'}} \le |S|\cdot\sum_{t=1}^{n/2}(2p)^t(er)^t = |S|\sum_{t=1}^{n/2}\left(2re^{1-\frac{2}{3}\varepsilon^2\beta}\right)^t < \frac{|S|}{4}$

as long as $2re^{1-\frac{2}{3}\varepsilon^2\beta} < 1/5$ (for $\beta > \frac{3\log(10er)}{2\varepsilon^2}$)

The weighted version of LLL does the work