COMPSCI 614: Randomized Algorithms with Applications to Data Science

Prof. Cameron Musco
University of Massachusetts Amherst. Spring 2024.
Lecture 24 (Final Lecture!)

Logistics

- Optional Problem Set 5 due 5/13 at 11:59pm.
- Final exam will be **Tuesday 5/14, 10:30-12:30pm in the classroom**. See Piazza post for info on study materials.
- I will hold additional final review office hours **Monday 5/13 from 3-4:30pm**.
- Final project due the last day of finals: Friday 5/17 – if you have questions as you come into the last couple of weeks of the project feel free to reach out.
- Please fill our SRTIs when you get a chance!

Summary

Last Time: Convex relaxation and randomized rounding.

- High level idea of convex relaxation for approximating NP-hard problems.
- Deterministic rounding for vertex cover. Randomized rounding for set cover.
- SDP relaxation and hyperplane rounding for max-cut (Goemans-Williamson algorithm)

$\{-1, 1\} \to x \in \mathbb{R}^d$, $\|x\|_2 = 1$

Summary

Last Time: Convex relaxation and randomized rounding.

- High level idea of convex relaxation for approximating NP-hard problems.
- Deterministic rounding for vertex cover. Randomized rounding for set cover.
- SDP relaxation and hyperplane rounding for max-cut (Goemans-Williamson algorithm)

Today: The Probabilistic Method (not on the exam)

- From probabilistic proofs to algorithms via the method of conditional expectations.
- The Lovasz local lemma for events with 'bounded' correlation.

The Probabilistic Method

The Basic Idea: Suppose we want to prove that a combinatorial object satisfying a certain property exists. Then it suffices to exhibit a random process that produces such an object with probability > 0.

The Basic Idea: Suppose we want to prove that a combinatorial object satisfying a certain property exists. Then it suffices to exhibit a random process that produces such an object with probability > 0.

We have already seen examples of this – e.g. the JL Lemma and Newman's Theorem reducing private coin communication complexity to public coin communication complexity (Problem Set 2).

$\forall$ sets $x_1 \ldots x_n \in \mathbb{R}^d$, $\exists\ \Pi \in \mathbb{R}^{m \times d}$ w/ $m = O\left(\frac{\log n}{\varepsilon^2}\right)$

s.t. $\|x_i\| \approx (1 \pm \varepsilon) \|\Pi x_i\|$

The Probabilistic Method

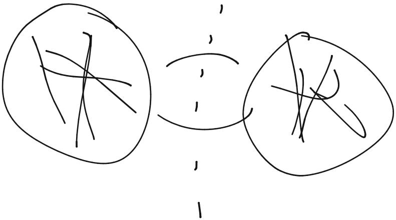
The Basic Idea: Suppose we want to prove that a combinatorial object satisfying a certain property exists. Then it suffices to exhibit a random process that produces such an object with probability > 0.

We have already seen examples of this – e.g. the JL Lemma and Newman's Theorem reducing private coin communication complexity to public coin communication complexity (Problem Set 2).

A common tool: For a random variable with $\mathbb{E}[X = \mu]$, $\Pr[X \geq \mu] > 0$ and $\Pr[X \leq \mu] > 0$.

Example 1: Max-Cut

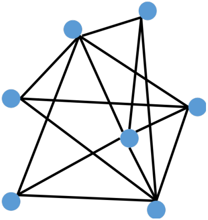
Prove that for any graph with m edges, there exists a cut containing at least $m/2$ edges.



Example 1: Max-Cut

Prove that for any graph with m edges, there exists a cut containing at least $m/2$ edges.

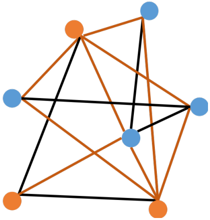
Consider a random partition of the nodes (each node is included independently in each half with probability 1/2). Let X be the size of the corresponding cut.



Example 1: Max-Cut

Prove that for any graph with m edges, there exists a cut containing at least $m/2$ edges.

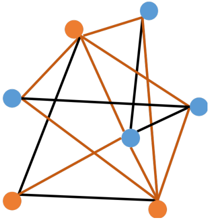
Consider a random partition of the nodes (each node is included independently in each half with probability 1/2). Let X be the size of the corresponding cut.



Example 1: Max-Cut

Prove that for any graph with m edges, there exists a cut containing at least $m/2$ edges.

Consider a random partition of the nodes (each node is included independently in each half with probability 1/2). Let X be the size of the corresponding cut.



We have $\mathbb{E}[X] = \sum_{e \in E} \mathbb{E}\, I_e = \sum_{e \in E} \frac{1}{2} = \frac{m}{2}$

Example 1: Max-Cut

Prove that for any graph with m edges, there exists a cut containing at least $m/2$ edges.

Consider a random partition of the nodes (each node is included independently in each half with probability 1/2). Let X be the size of the corresponding cut.

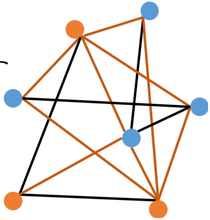
$e=(u,v)$

$I_e = 1$ if e in cut

$\quad\;\; 0$ o.w

$I_e = 1$ if u, v have different colors

$\Pr(I_e=1) = \frac{1}{2}$



We have $\mathbb{E}[\mathsf{X}] =$

Therefore, $\Pr[\mathsf{X} \geq m/2] > 0$. So every graph with m edges has a cut containing at least $m/2$ edges.

Example 2: 3-SAT

Prove that for any 3-SAT formula, there is some assignment of the variables such that at least 7/8 of the clauses are true.

Example 2: 3-SAT

Prove that for any 3-SAT formula, there is some assignment of the variables such that at least 7/8 of the clauses are true.

Consider a random assignment of the variables. And let X be the number of satisfied clauses.

only 1/8 chance to not be satisfied

$$(x_1 \vee \bar{x}_2 \vee x_4) \wedge (x_2 \vee \bar{x}_4 \vee x_3) \wedge (x_2 \vee x_3 \vee x_4) \wedge \ldots$$

What is $\mathbb{E}[X]$? $= \sum_{i=1}^{m} I_i = \sum_{i=1}^{m} 7/8 = 7/8 \cdot m$

Example 2: 3-SAT

Prove that for any 3-SAT formula, there is some assignment of the variables such that at least 7/8 of the clauses are true.

Consider a random assignment of the variables. And let X be the number of satisfied clauses.

$$(x_1 \vee \bar{x}_2 \vee x_4) \wedge (x_2 \vee \bar{x}_4 \vee x_3) \wedge (x_2 \vee x_3 \vee x_4) \wedge \ldots$$

What is $\mathbb{E}[X]$?

So, $\Pr[X \geq 7/8m] > 0$. So there is an assignment satisfying at least 7/8 of the clauses in every 3-SAT formula.

From Existence to Efficient Algorithms

Simple Max-Cut Approximation: A randomly sampled partition cuts $m/2$ edges in expectation. But how many partitions do we need to sample before finding a cut of size at least $m/2$ with good probability?

From Existence to Efficient Algorithms

Simple Max-Cut Approximation: A randomly sampled partition cuts $m/2$ edges in expectation. But how many partitions do we need to sample before finding a cut of size at least $m/2$ with good probability?

Let p be the probability of finding a cut of size $\geq m/2$. Then:

$$\mathbb{E}[X] = \frac{m}{2} \leq (1-p) \cdot \left(\frac{m}{2} - 1\right) + p \cdot m$$

From Existence to Efficient Algorithms

Simple Max-Cut Approximation: A randomly sampled partition cuts $m/2$ edges in expectation. But how many partitions do we need to sample before finding a cut of size at least $m/2$ with good probability?

Let p be the probability of finding a cut of size $\geq m/2$. Then:

$$\mathbb{E}[X] = \frac{m}{2} \leq (1-p) \cdot \left(\frac{m}{2} - 1\right) + p \cdot m$$
$$\implies \frac{1}{\frac{m}{2}+1} \leq p.$$

From Existence to Efficient Algorithms

Simple Max-Cut Approximation: A randomly sampled partition cuts $m/2$ edges in expectation. But how many partitions do we need to sample before finding a cut of size at least $m/2$ with good probability?

Let p be the probability of finding a cut of size $\geq m/2$. Then:

$$\mathbb{E}[X] = \frac{m}{2} \leq (1-p) \cdot \left(\frac{m}{2} - 1\right) + p \cdot m$$
$$\implies \frac{1}{\frac{m}{2}+1} \leq p.$$

How many attempts do we need to take to find a large cut with probability at least $1-\delta$? $O\left(\frac{1}{p}\log(1/\delta)\right)$

$O\left(m \log(1/\delta)\right)$

From Existence to Efficient Algorithms

Simple Max-Cut Approximation: A randomly sampled partition cuts $m/2$ edges in expectation. But how many partitions do we need to sample before finding a cut of size at least $m/2$ with good probability?

Let p be the probability of finding a cut of size $\geq m/2$. Then:

$$\mathbb{E}[X] = \frac{m}{2} \leq (1-p)\cdot\left(\frac{m}{2}-1\right) + p\cdot m$$
$$\implies \frac{1}{\frac{m}{2}+1} \leq p.$$

How many attempts do we need to take to find a large cut with probability at least $1-\delta$? $O(m \cdot \log(1/\delta))$

Method of Conditional Expectations

We can also derandomize this algorithm in a very simple way.

Let $x_1, x_2, \ldots \in \{0, 1\}$ indicate if the vertices are included on one side of the random partition.

Method of Conditional Expectations

We can also derandomize this algorithm in a very simple way.

Let $x_1, x_2, \ldots \in \{0, 1\}$ indicate if the vertices are included on one side of the random partition.

Consider determining these random variables sequentially.

$$\frac{m}{2} = \mathbb{E}[X] = \frac{1}{2}\mathbb{E}[X | x_1 = 1] + \frac{1}{2}\mathbb{E}[X | x_1 = 0].$$

Method of Conditional Expectations

We can also derandomize this algorithm in a very simple way.

Let $x_1, x_2, \ldots \in \{0, 1\}$ indicate if the vertices are included on one side of the random partition.

Consider determining these randsom variables sequentially.

$$\frac{m}{2} = \mathbb{E}[X] = \frac{1}{2}\mathbb{E}[X|x_1 = 1] + \frac{1}{2}\mathbb{E}[X|x_1 = 0].$$

Set $x_1 = v_1$ such that $\mathbb{E}[X|x_1 = v_1] \geq \frac{m}{2}$ Then we have:

$$\frac{m}{2} \leq \mathbb{E}[X|x_1 = v_1] = \frac{1}{2}\mathbb{E}[X|x_1 = v_1, x_2 = 1] + \frac{1}{2}\mathbb{E}[X|x_1 = v_1, x_2 = 0]$$

Method of Conditional Expectations

We can also derandomize this algorithm in a very simple way.

Let $\mathsf{x}_1, \mathsf{x}_2, \ldots \in \{0, 1\}$ indicate if the vertices are included on one side of the random partition.

Consider determining these randsom variables sequentially.

$$\frac{m}{2} = \mathbb{E}[\mathsf{X}] = \frac{1}{2}\mathbb{E}[\mathsf{X}|\mathsf{x}_1 = 1] + \frac{1}{2}\mathbb{E}[\mathsf{X}|\mathsf{x}_1 = 0].$$

Set $\mathsf{x}_1 = v_1$ such that $\mathbb{E}[\mathsf{X}|\mathsf{x}_1 = v_1] \geq \frac{m}{2}$ Then we have:

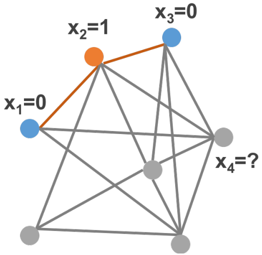
$$\frac{m}{2} \leq \mathbb{E}[\mathsf{X}|\mathsf{x}_1 = v_1] = \frac{1}{2}\mathbb{E}[\mathsf{X}|\mathsf{x}_1 = v_1, \mathsf{x}_2 = 1] + \frac{1}{2}\mathbb{E}[\mathsf{X}|\mathsf{x}_1 = v_1, \mathsf{x}_2 = 0]$$

Set $\mathsf{x}_2 = v_2$ such that $\mathbb{E}[\mathsf{X}|\mathsf{x}_1 = v_1, \mathsf{x}_2 = v_2] \geq \frac{m}{2}$. And so on...

$$\mathbb{E}[X | x_1 = v_1 \ldots x_n = v_n] \geq \frac{m}{2}$$

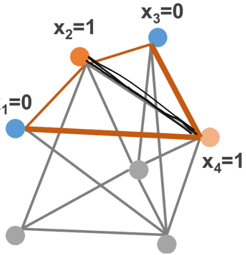
Conditional Expectations for Cuts

How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?



Conditional Expectations for Cuts

How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?

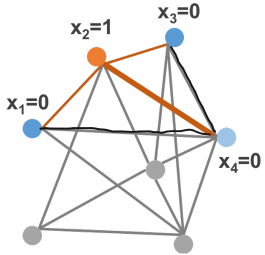


2+

$\mathbb{E}[X|x_1 = 0, \ldots, x_4 = 1] = \frac{1}{2} \cdot 10 + 2 = 7$

Conditional Expectations for Cuts

How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?



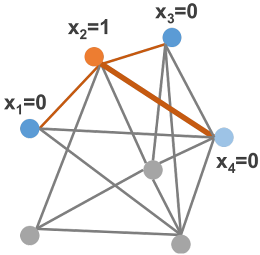
2+

$\mathbb{E}[X|x_1 = 0, \ldots, x_4 = 0] = \frac{1}{2} \cdot 10 + 1 = 6$

unassigned edges

Conditional Expectations for Cuts

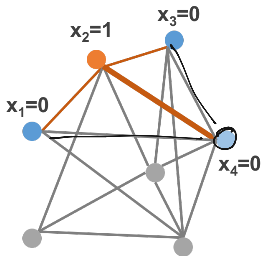
How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?

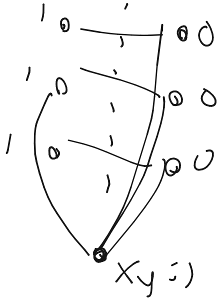


Natural greedy approach: add vertex i to the side of the cut to which it has fewest edges.

Conditional Expectations for Cuts

How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?



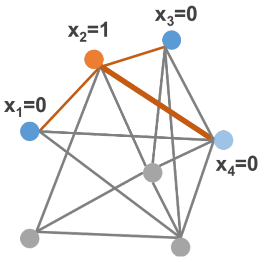


Natural greedy approach: add vertex i to the side of the cut to which it has fewest edges.

Yields a 1/2 approximation algorithm for max-cut.

Conditional Expectations for Cuts

How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?

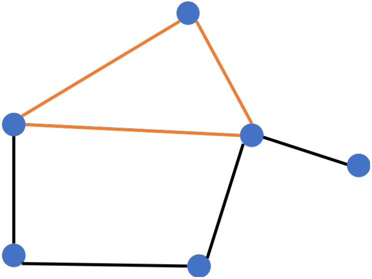


Natural greedy approach: add vertex i to the side of the cut to which it has fewest edges.

Yields a 1/2 approximation algorithm for max-cut. Recall that 16/17 is the best possible assuming $P \neq NP$, and .878 is the best known (Goemans, Williamson) from last lecture, and optimal under unique games conjecture

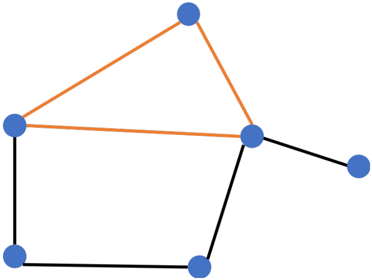
Large Girth Graphs

The girth of a graph is the length of its shortest cycle.



Large Girth Graphs

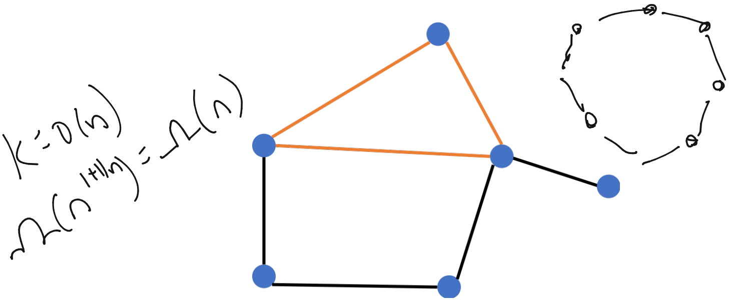
The girth of a graph is the length of its shortest cycle.



Natural Question: How large can the girth be for a graph with m edges?

Large Girth Graphs

The girth of a graph is the length of its shortest cycle.

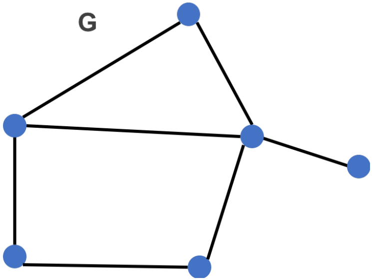


Natural Question: How large can the girth be for a graph with m edges?

Erdös Girth Conjecture: For any $k \geq 1$, there exists a graph with $m = \Omega(n^{1+1/k})$ edges and girth $2k+1$.

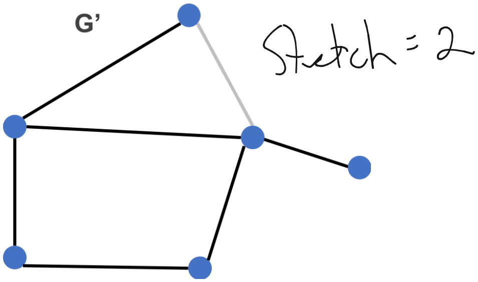
Relevance to Spanners

A spanner is a subgraph that approximately preserves shortest path distances. We say G' is a spanner for G with stretch t if for all u, v $d_{G'}(u, v) \leq t \cdot d_G(u, v)$.



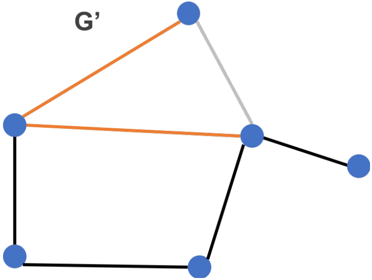
Relevance to Spanners

A spanner is a subgraph that approximately preserves shortest path distances. We say G' is a spanner for G with stretch t if for all u, v $d_{G'}(u, v) \leq t \cdot d_G(u, v)$.



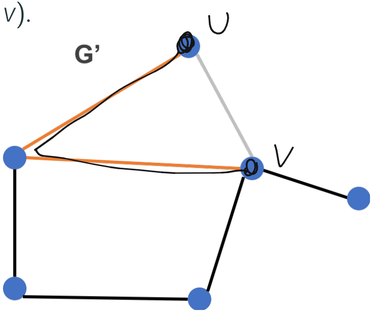
Relevance to Spanners

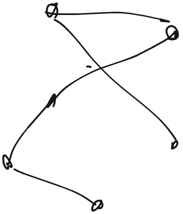
A spanner is a subgraph that approximately preserves shortest path distances. We say G' is a spanner for G with stretch t if for all u, v $d_{G'}(u, v) \leq t \cdot d_G(u, v)$.



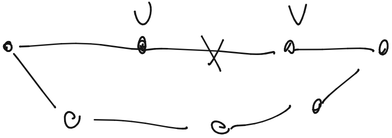
Relevance to Spanners

A spanner is a subgraph that approximately preserves shortest path distances. We say G' is a spanner for G with stretch t if for all u, v $d_{G'}(u,v) \leq t \cdot d_G(u,v)$.



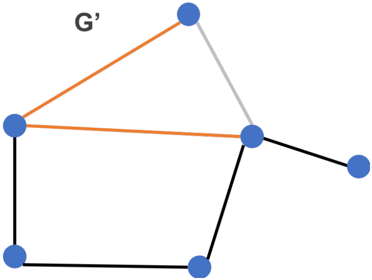


Even when G' excludes a single edge, $t \geq girth(G) - 1$.



Relevance to Spanners

A spanner is a subgraph that approximately preserves shortest path distances. We say G' is a spanner for G with stretch t if for all u, v $d_{G'}(u, v) \leq t \cdot d_G(u, v)$.



Even when G' excludes a single edge, $t \geq girth(G) - 1$.

Erdös Girth Conjecture $\implies$ there are no generic spanner constructions with $o(n^{1+1/k})$ edges and stretch $\leq 2k - 1$.

!?

Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

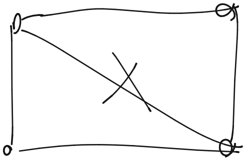
Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

$$\mathbb{E}[\text{edges}] = n^2 \cdot p = n^2 \cdot n^{1/k-1} = n^{1+1/k}$$



Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

$n^{1+1/k}$

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[X - Y] = \Omega(n^{1+1/k})$.

Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[X - Y] = \Omega(n^{1+1/k})$.

$$\mathbb{E}[X] =$$

Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[X - Y] = \Omega(n^{1+1/k})$.

$$\mathbb{E}[X] = \frac{n(n-1)}{2} \cdot p$$

Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[X - Y] = \Omega(n^{1+1/k})$.

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

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[X - Y] = \Omega(n^{1+1/k})$.

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

$$\mathbb{E}[Y] =$$

Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

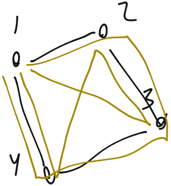
For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[\mathrm{X} - \mathrm{Y}] = \Omega(n^{1+1/k})$.

$$\mathbb{E}[\mathrm{X}] = \frac{n(n-1)}{2} \cdot p = \frac{1}{2} \cdot \left(1 - \frac{1}{n}\right) \cdot n^{1+1/k}.$$

$$\mathbb{E}[\mathrm{Y}] = \sum_{i=3}^{k} \binom{n}{i} \cdot \frac{(i-1)!}{2} \cdot p^i$$



$$\mathbb{E}[Y] = \sum_{i=3}^{k} \sum_{\text{cycles of length } i} \Pr(\text{cycle in graph})$$

Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[X - Y] = \Omega(n^{1+1/k})$.

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

$$\mathbb{E}[Y] = \sum_{i=3}^{k} \binom{n}{i} \cdot \frac{(i-1)!}{2} \cdot p^i \leq \sum_{i=3}^{k} n^i p^i$$

$$\frac{n(n-1)\cdots(n-i)}{i!}$$

Large Girth Graphs via Probabilistic Method

Theorem (Weaker Version of Girth Conjecture)

For any fixed $k \geq 3$, there exists a graph with n nodes, $\Omega(n^{1+1/k})$ edges, and girth $k+1$.

Sample and Modify Approach: Let G be an Erdös-Renyi random graph, where each edge is included independently with probability $p = n^{1/k-1}$. Remove one edge from every cycle in G with length $\leq k$, to get a graph with girth $k+1$.

Let X be the number of edges in the graph and Y be the number of cycles of length $\leq k$. Suffices to show $\mathbb{E}[\mathrm{X} - \mathrm{Y}] = \Omega(n^{1+1/k})$.

$$\mathbb{E}[\mathrm{X}] = \frac{n(n-1)}{2} \cdot p = \frac{1}{2} \cdot \left(1 - \frac{1}{n}\right) \cdot n^{1+1/k}.$$

$\leq n$

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

$n^{i+i/k-i}$

Large Girth Graphs via Probabilistic Method

So far: An Erdös-Renyi random graph with $p = n^{1/k-1}$ has expected number of edges (X) and cycles of length $\leq k-1$ (Y) bounded by:

$$\mathbb{E}[X] = \frac{1}{2} \cdot \left(1 - \frac{1}{n}\right) \cdot n^{1+1/k}$$

$$\mathbb{E}[Y] < k \cdot n.$$

So far: An Erdös-Renyi random graph with $p = n^{1/k-1}$ has expected number of edges (X) and cycles of length $\leq k-1$ (Y) bounded by:

$$\mathbb{E}[X] = \frac{1}{2} \cdot \left(1 - \frac{1}{n}\right) \cdot n^{1+1/k}$$
$$\mathbb{E}[Y] < k \cdot n.$$

When k is fixed and n is sufficiently large, $k \cdot n \ll n^{1+1/k}$. Thus,

$$\mathbb{E}[X - Y] = \Omega(\mathbb{E}[X]) = \Omega(n^{1+1/k}),$$

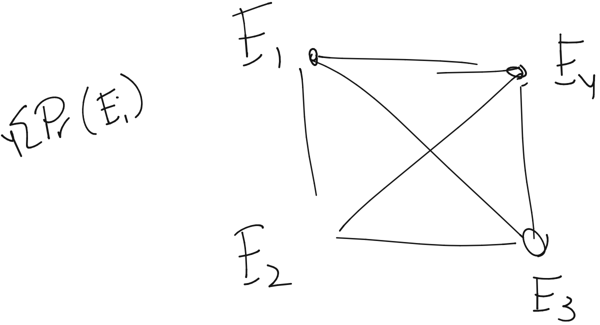
proving the theorem.

Lovasz Local Lemma

Probabilities of Correlated Events

Suppose we want to sample a random object that avoids n 'bad events' $E_1, \ldots, E_n$.

E.g., we want to sample a random assignment for variables that satisfies a a k-SAT formula with n clauses. E_i is the event that clause i is not satisfied.



Probabilities of Correlated Events

Suppose we want to sample a random object that avoids n 'bad events' $E_1, \ldots, E_n$.

E.g., we want to sample a random assignment for variables that satisfies a a k-SAT formula with n clauses. E_i is the event that clause i is not satisfied.

If the E_i are independent, and $\Pr[E_i] < 1$ for all i then:

$$\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] = \prod_{i=1}^{n}(1 - E_i) > 0.$$

Probabilities of Correlated Events

Suppose we want to sample a random object that avoids n 'bad events' $E_1, \ldots, E_n$.

E.g., we want to sample a random assignment for variables that satisfies a a k-SAT formula with n clauses. E_i is the event that clause i is not satisfied.

If the E_i are independent, and $\Pr[E_i] < 1$ for all i then:

$$\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] = \prod_{i=1}^{n}(1 - E_i) > 0.$$

What if the events are not independent?

Probabilities of Correlated Events

Suppose we want to sample a random object that avoids n ‘bad events’ $E_1, \ldots, E_n$.

E.g., we want to sample a random assignment for variables that satisfies a a k-SAT formula with n clauses. E_i is the event that clause i is not satisfied.

If the E_i are independent, and $\Pr[E_i] < 1$ for all i then:

$$\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] = \prod_{i=1}^{n}(1 - E_i) > 0.$$

What if the events are not independent?

If $\sum_{i=1}^{n} \Pr[E_i] < 1$ then by a union bound,

$$\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] \geq 1 - \sum_{i=1}^{n} E_i > 0.$$

Probabilities of Correlated Events

Suppose we want to sample a random object that avoids n 'bad events' $E_1, \ldots, E_n$.

E.g., we want to sample a random assignment for variables that satisfies a a k-SAT formula with n clauses. E_i is the event that clause i is not satisfied.

If the E_i are independent, and $\Pr[E_i] < 1$ for all i then:

$$\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] = \prod_{i=1}^{n} (1 - E_i) > 0.$$

What if the events are not independent?

If $\sum_{i=1}^{n} \Pr[E_i] < 1$ then by a union bound,

$$\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] \geq 1 - \sum_{i=1}^{n} E_i > 0.$$

As n gets large, the union bound gets very weak – each event has to occur with probability $< 1/n$ on average.

Bounded Correlation

Consider events $E_1, \ldots, E_n$ where E_i is independent of any $j \notin \Gamma(i)$ (the neighborhood of i in the dependency graph)

Bounded Correlation

Consider events $E_1, \ldots, E_n$ where E_i is independent of any $j \notin \Gamma(i)$ (the neighborhood of i in the dependency graph)

E.g., consider randomly assigning variables in a k-SAT formula with n clauses, and let E_i be the event that clause i is unsatisfied.

$$(x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_2 \vee \bar{x}_4 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6) \wedge (\neg x_4 \vee x_6 \vee x_7) \ldots$$

Bounded Correlation

Consider events $E_1, \ldots, E_n$ where E_i is independent of any $j \notin \Gamma(i)$ (the neighborhood of i in the dependency graph)

E.g., consider randomly assigning variables in a k-SAT formula with n clauses, and let E_i be the event that clause i is unsatisfied.

$$(x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_2 \vee \bar{x}_4 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6) \wedge (\neg x_4 \vee x_6 \vee x_7) \ldots$$

Theorem (Lovasz Local Lemma)

Suppose for a set of events $E_1, E_2, \ldots, E_n$, $\Pr[E_i] \leq p$ for all i, and that each E_i is dependent on at most d other events E_j (i.e., $|\Gamma(i)| \leq d$, then if $4dp \leq 1$:

$$\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] > (1-2p)^n > 0.$$

In the worse case, $d = n-1$ and this is similar to the union bound. But it can be much stronger.

LLL Application: k-SAT

Theorem

If no variable in a k-SAT formula appears in more than $\frac{2^k}{4k}$ clauses, then the formula is satisfiable.

LLL Application: k-SAT

Theorem

If no variable in a k-SAT formula appears in more than $\frac{2^k}{4k}$ clauses, then the formula is satisfiable.

Let E_i be the event that clause i is unsatisfied by a random assignment.

LLL Application: k-SAT

Theorem

If no variable in a k-SAT formula appears in more than $\frac{2^k}{4k}$ clauses, then the formula is satisfiable.

Let E_i be the event that clause i is unsatisfied by a random assignment. $\Pr[E_i] \leq$

LLL Application: k-SAT

Theorem

If no variable in a k-SAT formula appears in more than $\frac{2^k}{4k}$ clauses, then the formula is satisfiable.

Let E_i be the event that clause i is unsatisfied by a random assignment. $\Pr[E_i] \leq \frac{1}{2^k} = p$.

LLL Application: k-SAT

Theorem

If no variable in a k-SAT formula appears in more than $\frac{2^k}{4k}$ clauses, then the formula is satisfiable.

Let E_i be the event that clause i is unsatisfied by a random assignment. $\Pr[E_i] \leq \frac{1}{2^k} = p$.

$|\Gamma(i)| \leq$

LLL Application: k-SAT

Theorem

If no variable in a k-SAT formula appears in more than $\frac{2^k}{4k}$ clauses, then the formula is satisfiable.

Let E_i be the event that clause i is unsatisfied by a random assignment. $\Pr[E_i] \leq \frac{1}{2^k} = p$.

$|\Gamma(i)| \leq k \cdot \frac{2^k}{4k} = \frac{2^k}{4} = d$

LLL Application: k-SAT

Theorem

If no variable in a k-SAT formula appears in more than $\frac{2^k}{4k}$ clauses, then the formula is satisfiable.

Let E_i be the event that clause i is unsatisfied by a random assignment. $\Pr[E_i] \leq \frac{1}{2^k} = p$.

$|\Gamma(i)| \leq k \cdot \frac{2^k}{4k} = \frac{2^k}{4} = d$

So $4dp = 4 \cdot \frac{1}{2^k} \cdot \frac{2^k}{4} \leq 1$, and thus $\Pr\left[\neg \bigcup_{i=1}^{n} E_i\right] > 0$. I.e., a random assignment satisfies the formula with non-zero probability.

Algorithmic LLL

Important Question: Given an Lovasz Local Lemma based proof of the existence, can we convert it into an efficient algorithm?

Moser and Tardos [2010] prove that a very natural algorithm can be used to do this.

Let $E_1, \ldots, E_n$ be events determined by a set of independent random variables $V = \{v_1, \ldots, v_m\}$. Let $v(E_i)$ be the set of variables that E_i depends on.

Resampling Algorithm:

1. Assign $v_1, \ldots, v_m$ random values.
2. While there is some E_i that occurs, reassign random values to all varables in $v(E_i)$.
3. Halt when an assignment is found such that no E_i occurs.

Algorithmic LLL

Theorem (Algorithmic Lovasz Local Lemma)

Consider a set of events $E_1, E_2, \ldots, E_n$ *determined by a finite set of random variables* V*. If for all* i, $\Pr[E_i] \leq p$ *and* $|\Gamma(i)| \leq d$*, and if* $ep(d+1) \leq 1$*, then* RESAMPLING *finds an assignment of the variables in* V *such that no event* E_i *occurs. Further, the algorithm makes* $O(\frac{n}{d})$ *iterations in expectation.*

Algorithmic LLL

Theorem (Algorithmic Lovasz Local Lemma)

Consider a set of events $E_1, E_2, \ldots, E_n$ determined by a finite set of random variables V. If for all i, $\Pr[E_i] \le p$ and $|\Gamma(i)| \le d$, and if $ep(d+1) \le 1$, then Resampling *finds an assignment of the variables in V such that no event E_i occurs. Further, the algorithm makes $O(\frac{n}{d})$ iterations in expectation.*

Application to k-SAT: Consider a k-SAT formula where no variable appears in more than $\frac{2^k}{5k}$ clauses. Let E_i be the event that clause i is unsatisfied by a random assignment

$$\Pr[E_i] \le \frac{1}{2^k} = p \quad \text{and} \quad |\Gamma(i) \le k \cdot \frac{2^k}{5k} = \frac{2^k}{5} = d.$$

Theorem (Algorithmic Lovasz Local Lemma)

Consider a set of events $E_1, E_2, \ldots, E_n$ determined by a finite set of random variables V. If for all i, $\Pr[E_i] \leq p$ and $|\Gamma(i)| \leq d$, and if $ep(d+1) \leq 1$, then Resampling *finds an assignment of the variables in V such that no event E_i occurs. Further, the algorithm makes $O(\frac{n}{d})$ iterations in expectation.*

Application to k-SAT: Consider a k-SAT formula where no variable appears in more than $\frac{2^k}{5k}$ clauses. Let E_i be the event that clause i is unsatisfied by a random assignment

$$\Pr[E_i] \leq \frac{1}{2^k} = p \quad \text{and} \quad |\Gamma(i) \leq k \cdot \frac{2^k}{5k} = \frac{2^k}{5} = d.$$

Have $ep(d+1) \leq \frac{e}{5} + \frac{e}{2^k} \leq 1$ as long as $k \geq 3$, so the theorem applies, giving a polynomial time algorithm for this variant of k-SAT.

Thanks for a great semester!