COMPSCI 690RA: Randomized Algorithms and Probabilistic Data Analysis

Prof. Cameron Musco

University of Massachusetts Amherst. Spring 2022.

Lecture 12 (Final Lecture!)

Logistics

- The final exam is this Friday 5/6 at 10:30am in this room.
- I will hold extended office hours today from 2-4pm and tomorrow from 4-6pm.
- I will accept final project submissions up until Sunday 5/8 at 11:59pm.
- Please complete your SRTI for the class when you get a chance!

Summary

Last Week: Finish up Markov Chains Unit.

- Mixing time analysis via coupling.
- Example applications to shuffling and random walks on the hypercube.
- Markov Chain Monte Carlo (MCMC) methods.
- Example of reductions from counting to sampling (e.g., for counting independent sets).

Summary

Last Week: Finish up Markov Chains Unit.

- Mixing time analysis via coupling.
- Example applications to shuffling and random walks on the hypercube.
- Markov Chain Monte Carlo (MCMC) methods.
- Example of reductions from counting to sampling (e.g., for counting independent sets).

Today: The Probabilistic Method (not on the exam)

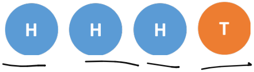
- From probabilistic proofs to algorithms via the method of conditional expectations.
- The Lovasz local lemma for events with 'bounded' correlation.
- Entropic proof of the algorithmic LLL.

First...a detour

The St. Petersburg Paradox

Consider the following game: you keep flipping a fair coin, until it hits tails. You win \$$2^{k+1}$, where k is the number of heads you see.

$2^4 = 16$



$2^1 = 2$

T

The St. Petersburg Paradox

Consider the following game: you keep flipping a fair coin, until it hits tails. You win $\$2^{k+1}$, where k is the number of heads you see.

Let X be the amount of money you win. What is $\mathbb{E}[X]$?

$$\frac{1}{2}\cdot 2 + \frac{1}{4}\cdot 4 + \frac{1}{8}\cdot 8 = 1 + 1 + \dots 1 = \infty$$

The St. Petersburg Paradox

Consider the following game: you keep flipping a fair coin, until it hits tails. You win $\$2^{k+1}$, where k is the number of heads you see.

1 + 1 + 1 + 1

Let X be the amount of money you win. What is $\mathbb{E}[X]$? $= \infty$

How much money would you pay to play this game? Why?

\$2

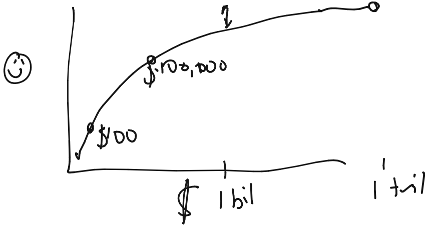
\$20

- don't care about low prob events
- finite amount of money

Expected Utility Theory

One Solution to the Paradox: The expected value of the game is not $\mathbb{E}[X]$, but $\mathbb{E}[U(X)]$ where U is some utility function.

$U(\cdot)$ determines how much actual value you derive from a given amount of money. We expect generally that U is concave – diminishing marginal utility.



Maximizing Expected Log Winnings

$:2$

What is $\mathbb{E}[U(X)] = \mathbb{E}[\log_2(X)]$ for our game?

$$\frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{8} \cdot 3 + \cdots$$

$$\left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} \cdots\right) + \left(\frac{1}{4} + \frac{1}{8} + \cdots\right) + \left(\frac{1}{8} + \frac{1}{16} + \cdots\right)$$

$$1 + \frac{1}{2} + \frac{1}{4}$$

$$= 2$$

A More ‘Realistic’ Scenario

You are given \$25 and are allowed to play the following game repeatedly: You have a biased coin that hits heads 60% of the time. You can wager \$$w$ on if the coin hits heads or tails. If you are correct, you win \$$w$, and if you are incorrect, you lose \$$w$.

How should you determine the size of your bets?

you can play for 1 hour

\$25

1/2 your money.

$\mathbb{E}x_i$

$\mathbb{E}[\log(x_i)]$

You are given \$25 and are allowed to play the following game repeatedly: You have a biased coin that hits heads 60% of the time. You can wager \$$w$ on if the coin hits heads or tails. If you are correct, you win \$$w$, and if you are incorrect, you lose \$$w$.

How should you determine the size of your bets?

$$\mathbb{E}[\log(X_{i+1})|X_i] = .6 \cdot \overset{X_{i+1}}{\log(X_i + w)} + .4 \cdot \overset{X_{i+1}}{\log(X_i - w)}.$$

A More 'Realistic' Scenario

You are given \$25 and are allowed to play the following game repeatedly: You have a biased coin that hits heads 60% of the time. You can wager $\$w$ on if the coin hits heads or tails. If you are correct, you win $\$w$, and if you are incorrect, you lose $\$w$.

How should you determine the size of your bets?

$$\mathbb{E}[\log(X_{i+1})|X_i] = .6 \cdot \log(X_i + w) + .4 \cdot \log(X_i - w).$$

Write $w = r \cdot X_i$. Then:

$$\mathbb{E}[\log(X_{i+1})|X_i] = .6 \cdot \log(X_i \cdot (1 + r)) + .4 \cdot \log(X_i \cdot (1 - r))$$

A More 'Realistic' Scenario

You are given \$25 and are allowed to play the following game repeatedly: You have a biased coin that hits heads 60% of the time. You can wager $\$w$ on if the coin hits heads or tails. If you are correct, you win $\$w$, and if you are incorrect, you lose $\$w$.

How should you determine the size of your bets?

$\lim_{n \to \infty} \frac{1}{n} \log\left(\frac{X_n}{X_{n+1}}\right)$

$$\mathbb{E}[\log(X_{i+1})|X_i] = .6 \cdot \log(X_i + w) + .4 \cdot \log(X_i - w).$$

Write $w = r \cdot X_i$. Then:

$$\begin{aligned}\mathbb{E}[\log(X_{i+1})|X_i] &= .6 \cdot \log(X_i \cdot (1 + r)) + .4 \cdot \log(X_i \cdot (1 - r)) \\ &= \log(X_i) + .6 \log(1 + r) + .4 \log(1 - r).\end{aligned}$$

10 vs 2 vs 1

$\log(5)$

$\log(2)$

A More ‘Realistic’ Scenario

You are given \$25 and are allowed to play the following game repeatedly: You have a biased coin that hits heads 60% of the time. You can wager $\$w$ on if the coin hits heads or tails. If you are correct, you win $\$w$, and if you are incorrect, you lose $\$w$.

How should you determine the size of your bets?

$$\mathbb{E}[\log(X_{i+1})|X_i] = .6 \cdot \log(X_i + w) + .4 \cdot \log(X_i - w).$$

Write $w = r \cdot X_i$. Then:

$$\begin{aligned} \mathbb{E}[\log(X_{i+1})|X_i] &= .6 \cdot \log(X_i \cdot (1 + r)) + .4 \cdot \log(X_i \cdot (1 - r)) \\ &= \log(X_i) + .6 \log(1 + r) + .4 \log(1 - r). \end{aligned}$$

To maximize $.6 \log(1 + r) + .4 \log(1 - r)$, set its derivative to 0:

A More 'Realistic' Scenario

You are given \$25 and are allowed to play the following game repeatedly: You have a biased coin that hits heads 60% of the time. You can wager $\$w$ on if the coin hits heads or tails. If you are correct, you win $\$w$, and if you are incorrect, you lose $\$w$.

How should you determine the size of your bets?

$$\mathbb{E}[\log(X_{i+1})|X_i] = .6 \cdot \log(X_i + w) + .4 \cdot \log(X_i - w).$$

Write $w = r \cdot X_i$. Then:

$$\begin{aligned}\mathbb{E}[\log(X_{i+1})|X_i] &= .6 \cdot \log(X_i \cdot (1+r)) + .4 \cdot \log(X_i \cdot (1-r)) \\ &= \log(X_i) + .6 \log(1+r) + .4 \log(1-r).\end{aligned}$$

To maximize $.6 \log(1+r) + .4 \log(1-r)$, set its derivative to 0:

$$0 = \frac{.6}{1+r} - \frac{.4}{1-r}.$$

$$\frac{.4}{(1-r)} = \frac{.6}{1+r}$$

$$.4 + .4r = .6 - .6r$$

$$r = .6 - .4 = .2$$

A More 'Realistic' Scenario

You are given \$25 and are allowed to play the following game repeatedly: You have a biased coin that hits heads 60% of the time. You can wager \$$w$ on if the coin hits heads or tails. If you are correct, you win \$$w$, and if you are incorrect, you lose \$$w$.

How should you determine the size of your bets?

$$\mathbb{E}[\log(X_{i+1})|X_i] = .6 \cdot \log(X_i + w) + .4 \cdot \log(X_i - w).$$

Write $w = r \cdot X_i$. Then:

$$\begin{aligned}\mathbb{E}[\log(X_{i+1})|X_i] &= .6 \cdot \log(X_i \cdot (1 + r)) + .4 \cdot \log(X_i \cdot (1 - r)) \\ &= \log(X_i) + .6 \log(1 + r) + .4 \log(1 - r).\end{aligned}$$

To maximize $.6 \log(1 + r) + .4 \log(1 - r)$, set its derivative to 0:

$$0 = \frac{.6}{1 + r} - \frac{.4}{1 - r}.$$

Optimal $r = 0.2$. I.e., you should bet 20% of your money each time.

The prior analysis is a special case of the Kelly criterion.

$$r = p - \frac{q}{b}.$$

Lots of interesting topics here, closely related to Markov chains and Martingales.

$.4 - .6 = -.2$

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.

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

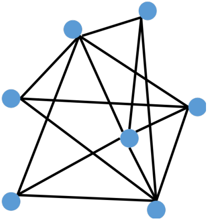
Example 1: Max-Cut

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.

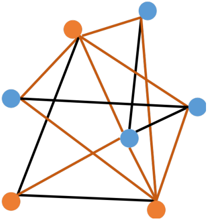
Consider a random partition of the nodes (each node is included independently in each half with probability 1/2). Let X be the size of the corresponding cut.



Example 1: Max-Cut

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

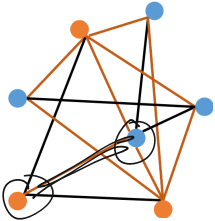
Consider a random partition of the nodes (each node is included independently in each half with probability 1/2). Let X be the size of the corresponding cut.



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 $\mathbb{E}[X] =$ $\frac{m}{2}$

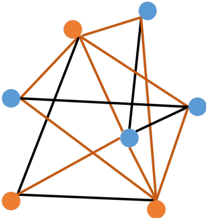
$$\mathbb{E}\, X_{u,v} = \frac{1}{2}$$

$$\mathbb{E}\, X = \sum_{(u,v)} \mathbb{E} X_{u,v} = m \cdot \frac{1}{2} = \frac{m}{2}$$

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.



We have $\mathbb{E}[X] = \frac{m}{2}$

Therefore, $\Pr[X \geq m/2] > 0$. 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.

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

1 1 0

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.

$$\overset{\{0,1\}}{(x_1} \vee \bar{x}_2 \vee x_4) \wedge \overset{\{0,1\}}{(x_2} \vee \bar{x}_4 \vee x_3) \wedge (x_2 \vee x_3 \vee x_4) \wedge \ldots$$

$\underline{x_1} = 0$, $\bar{x}_2 = 1$, $x_4 = 0$

$\mathbb{E} X_i = \Pr(\text{clause } i \text{ is sat.})$
$= 7/8$

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

$$\mathbb{E}[X] = \sum_{i=1}^{m} \mathbb{E} X_i$$

$$= \frac{7}{8} \cdot m$$

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 $\mathbb{E}[X]$? $\underline{7/8\ m}$

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

$\leq m$

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?

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

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:

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

$$\Omega\left(\frac{1}{m}\right) \qquad \implies \frac{1}{\frac{m}{2}+1} \leq p.$$

$$\cancel{\frac{m}{2}} \leq \cancel{\frac{m}{2}} - 1 - \frac{pm}{2} + p + pm$$

$$1 \leq p \cdot \left(\frac{m}{2} + 1\right)$$

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:

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

How many attempts do we need to take to find a large cut with probability at least $1 - \delta$?

$$O(\underbrace{m \log(1/\delta)}_{})$$

$$\left(1 - \frac{1}{m}\right)^{m \log(1/\delta)} \approx \underline{\delta}$$

From Existence to Efficient Algorithms

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.

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

Set $x_1 = \overset{\{0,1\}}{v_1}$ 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 $x_1, x_2, \ldots \in \{0,1\}$ indicate if the vertices are included on one side of the random partition.

Consider determining these randsom variables sequentially.

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

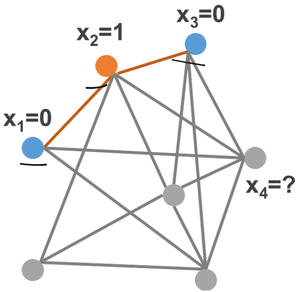
Set $x_1 = v_1$ such that $\mathbb{E}[X|x_1 = v_1] \geq \frac{m}{2}$ Then we have:

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

Set $x_2 = v_2$ such that $\mathbb{E}[X|x_1 = v_1, x_2 = v_2] \geq \frac{m}{2}$. And so on...

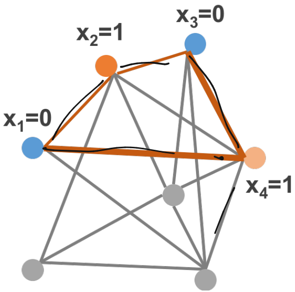
Conditional Expectations for Cuts

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



Conditional Expectations for Cuts

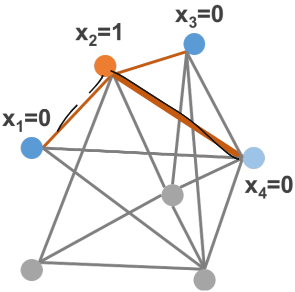
How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?



$\mathbb{E}[X|x_1 = 0, \ldots, x_4 = 1] \overset{+2}{=} \underbrace{\frac{1}{2} \cdot 10}\underbrace{+ 2} = 9$

Conditional Expectations for Cuts

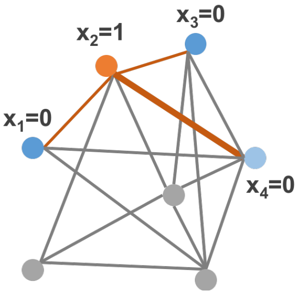
How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?



$\mathbb{E}[X|x_1 = 0, \ldots, x_4 = 0] = \overset{2+}{\frac{1}{2}} \cdot 10 + 1 = 8$

Conditional Expectations for Cuts

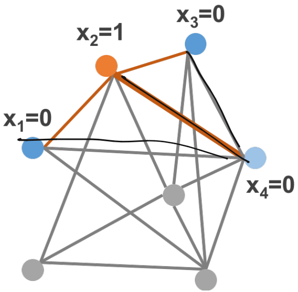
How can we pick v_i such that $\mathbb{E}[X|x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?



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 $\mathbb{E}[X | x_1 = v_1, \ldots, x_{i-1} = v_{i-1}] \geq \frac{m}{2}$?

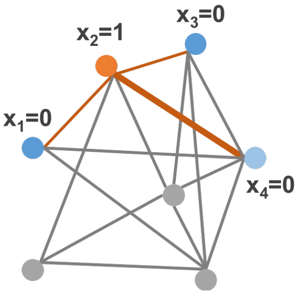


Natural greedy approach: add vertex *i* to the side of the cut to which it has fewest edges.

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

Conditional Expectations for Cuts

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

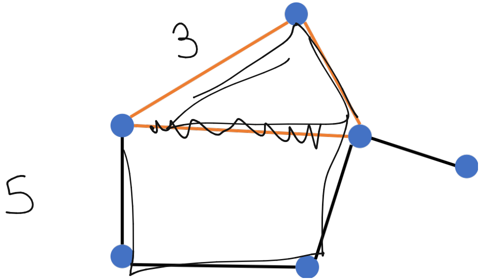


Natural greedy approach: add vertex i to the side of the cut to which it has fewest edges.

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

Large Girth Graphs

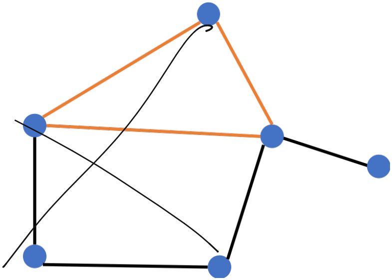
The girth of a graph is the length of its shortest cycle.



Large Girth Graphs

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

3

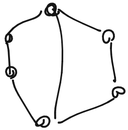


Natural Question: How large can the girth be for a graph with *m* edges?

$\binom{n}{2}$

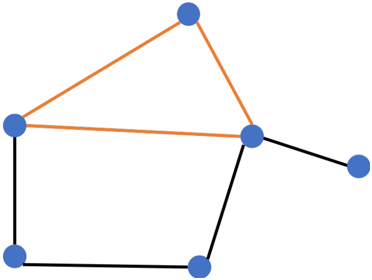
n edges

$n+1$ edges



Large Girth Graphs

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

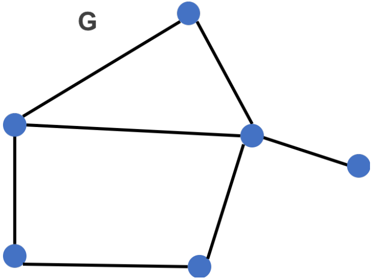


Natural Question: How large can the girth be for a graph with m edges?

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

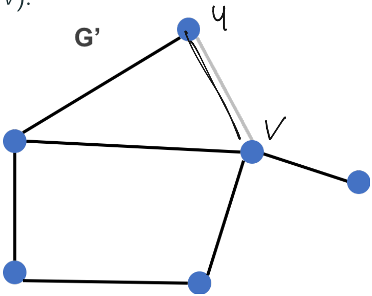
Relevance to Spanners

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

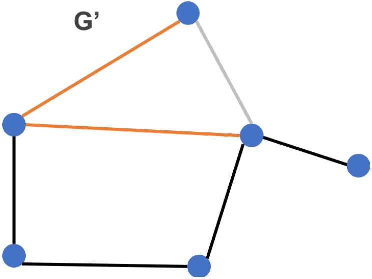
A spanner is a subgraph that approximately preserves shortest path distances. We say G' is a spanner for G with stretch t if for all u, v $d_{G'}(u, v) \leq t \cdot d_G(u, v)$.



Relevance to Spanners

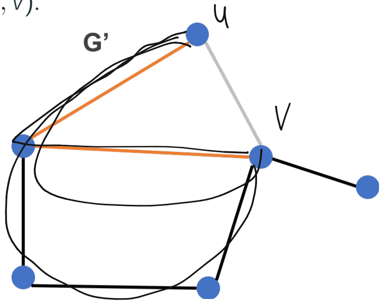
A spanner is a subgraph that approximately preserves shortest path distances. We say G' is a spanner for G with stretch t if for all u, v $d_{G'}(u, v) \leq t \cdot d_G(u, v)$.

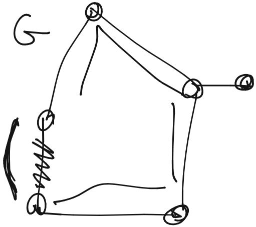
$t \geq 2$



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 $d_{G'}(u,v) \leq t \cdot d_G(u,v)$.

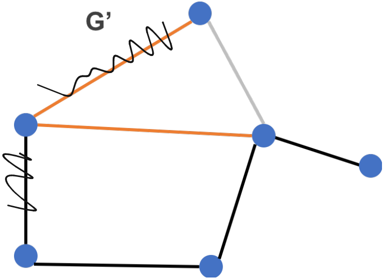




Even when G' excludes a single edge, $t \geq girth(G) - 1$.

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

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

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

$p(n-1) \approx n^{1/k}$

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 $k+1$.

Large Girth Graphs via Probabilistic Method

Theorem

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

Large Girth Graphs via Probabilistic Method

Theorem

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

$$\mathbb{E}[X] = p \cdot \binom{n}{2}$$

Large Girth Graphs via Probabilistic Method

Theorem

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

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

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

$$\frac{n(n-1)}{2} \cdot n^{1/k-1} = \frac{n-1}{2} \cdot n^{1/k}$$

Theorem

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

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

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

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

1 2 3 4

1 3 2 4

Large Girth Graphs via Probabilistic Method

Theorem

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

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

$\leq n$

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

$$\frac{n \cdot (n-1) \ldots (n-i+1)}{i \cdot (i-1) \ldots 1}$$

Large Girth Graphs via Probabilistic Method

Theorem

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

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

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

$$(n \cdot p)^i = (n \cdot n^{1/k-1})^i = (n^{1/k})^i = n^{i/k}$$

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:

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

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,

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

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,

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

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 E_j for $j \notin \Gamma(i)$ (the neighborhood of i in the dependency graph)

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.

$$\underbrace{(x_1 \vee \bar{x}_2 \vee x_3)}_{E_1} \wedge \underbrace{(x_2 \vee \bar{x}_4 \vee x_3)}_{E_2} \wedge \underbrace{(x_4 \vee x_5 \vee x_6)}_{E_3} \wedge \underbrace{(\neg x_4 \vee x_6 \vee x_7)}_{E_4} \ldots$$

$|\Gamma(1)| = 1$

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) LLL

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 $4dp \leq 1$:

$(n-1)p < 1$

dp

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

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

$\overset{0}{x_1} \vee \overset{1}{\bar{x}_2} \vee \overset{0}{x_3}$

$\frac{64}{24} \approx 2$

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. $\Pr[E_i] \leq \frac{1}{2^k}$

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

$(x_1 \vee x_2 \vee \bar{x}_3) \longleftrightarrow (x_1 \vee x_4 \vee x_5)$

Theorem

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

correlated with E_i

events

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

$|\Gamma(i)| \leq \binom{n}{k} \cdot 2^k$

$\leq k \cdot \frac{2^k}{4k} = \frac{2^k}{4}$

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. $\Pr[E_i] \leq \frac{1}{2^k} = p$.

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

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. $\Pr[E_i] \le \frac{1}{2^k} = p$.

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

So $4dp = 4 \cdot \frac{1}{2^k} \cdot \frac{2^k}{4} \le 1$, 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.

$(x_1 \vee x_2 \vee \bar{x}_3)$

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.*

$4pd \leq 1$

$n \cdot p = \Theta(n/d)$

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

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

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.*

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

Entropic Proof of Algorithmic LLL

Moser's 'entropic proof' of the algorithmic LLL uses a particularly cool technique.

Focus on the case of k-SAT where $|\Gamma(i)| < d = \frac{2^k}{8} = 2^{k-3}$.

- In each iteration of rerandomization, the algorithm uses k random bits. So for T iterations it uses Tk random bits.
- We will show that if we run the algorithm for too long, then we obtain a compression of these bits into a string of $< Tk$ bits, which shouldn't be possible (since they are random bits and incompressible).

Entropic Proof of Algorithmic LLL

Moser's 'entropic proof' of the algorithmic LLL uses a particularly cool technique.

Focus on the case of k-SAT where $|\Gamma(i)| < d = \frac{2^k}{8} = 2^{k-3}$.

- In each iteration of rerandomization, the algorithm uses k random bits. So for T iterations it uses Tk random bits.
- We will show that if we run the algorithm for too long, then we obtain a compression of these bits into a string of $< Tk$ bits, which shouldn't be possible (since they are random bits and incompressible).

$\underline{2^t}$ $\quad 1+2+4+\ldots 2^{t-c}$

$\leq 2^{(t-c)+1}$

Incompressibility Fact: For any function f mapping inputs in $\{0,1\}^t$ to distinct, possibly variable length binary output strings, if s is a uniform random t-bit binary string, then for any integer c, $\Pr[length[f(s)] \leq \underline{t-c}] \leq \frac{1}{2^{c-1}}$.

$$\frac{2^{(t-c)+1}}{2^t} = \frac{1}{2^{c-1}}$$

Compressing Bits While Solving k-SAT

- Initialize random assignments for the m variables using m bits.
- Iterate through the clauses, recording '1' for each that is satisfied, and recording '0' when you reach an unsatisfied clause i.
- Run LocalCorrect(i). Then move on to the next clause.
- After completion of all clauses, record the final state of the m variables using m bits.

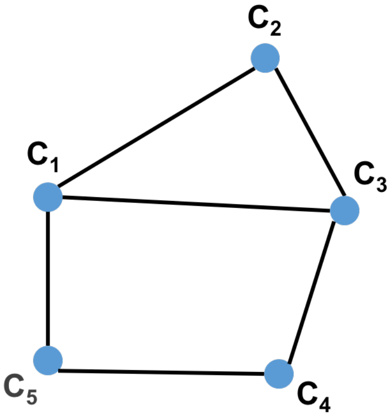
LocalCorrect(i):

- Resample random values for the variables in clause i, using k bits (but don't record them!).

$\log(2^k/8) = k-3$

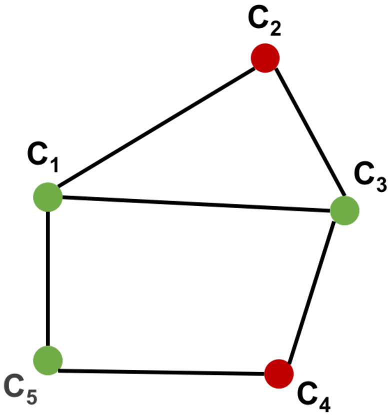
- While some clause $j \in \Gamma(i) \cup \{i\}$ is unsatisfied, pick the first such j, and record '0' along with j using $k-3$ bits. Then run LocalCorrect(j).
- Record '1' upon termination.

Compression Illustration



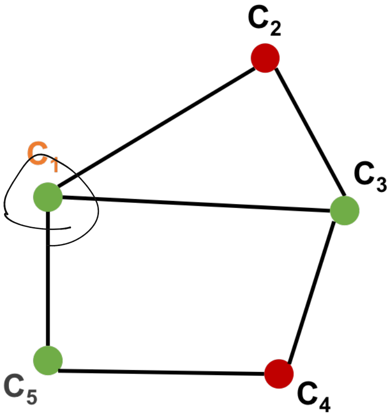
Record:
Bits Used:

Compression Illustration



Record:
Bits Used: 10110001

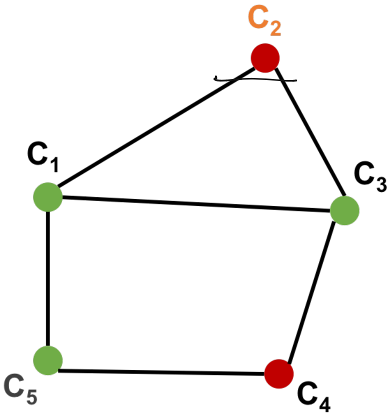
Compression Illustration



Record: 1

Bits Used: 10110001

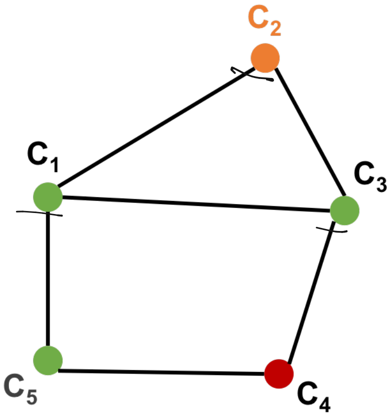
Compression Illustration



Record: 10

Bits Used: 10110001

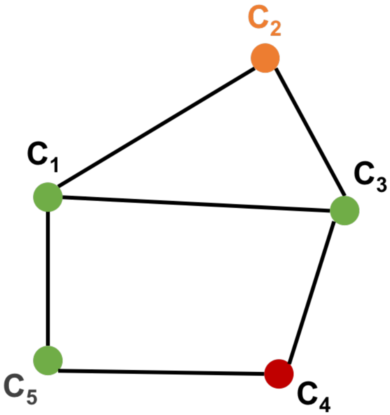
Compression Illustration



Record: 10

Bits Used: 1011000110111

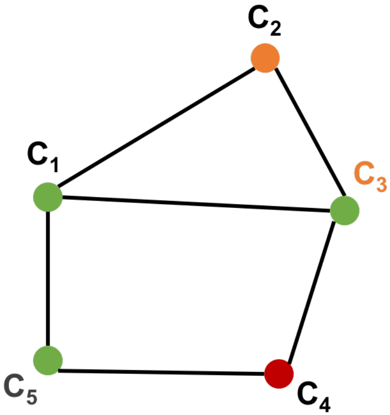
Compression Illustration



Record: 101

Bits Used: 1011000110111

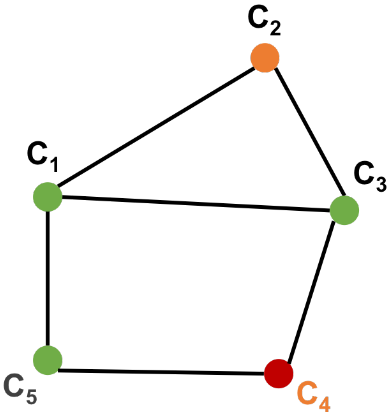
Compression Illustration



Record: 1011

Bits Used: 1011000110111

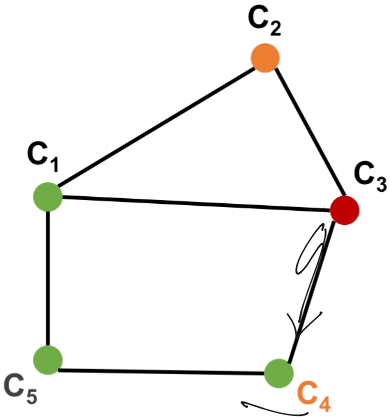
Compression Illustration



Record: 10110

Bits Used: 1011000110111

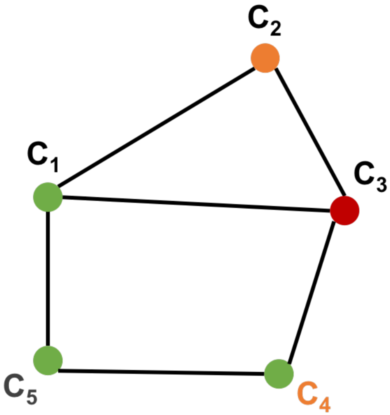
Compression Illustration



Record: 10110

Bits Used: 101100011011100100

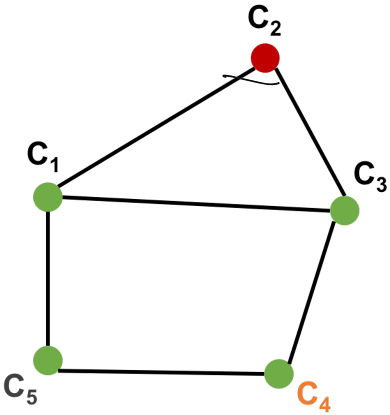
Compression Illustration



Record: 10110000

Bits Used: 1011000110111100100

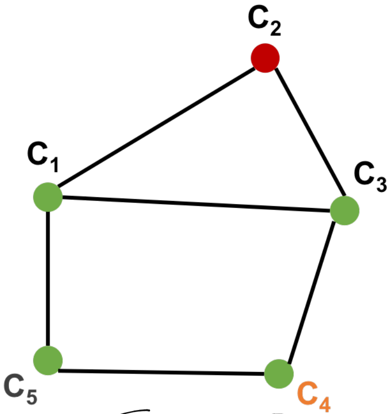
Compression Illustration



Record: 10110000

Bits Used: 1011000110111001001010101

Compression Illustration



Record: 10110000001 1100100

Bits Used: 10110001101110010010101

Compressing Bits While Solving k-SAT

Claim 1: If the algorithm runs for T iterations, it uses $m + Tk$ random bits.

Compressing Bits While Solving k-SAT

Claim 1: If the algorithm runs for T iterations, it uses $m + Tk$ random bits.

2^{k-5}

2^{k-10}

Claim 2: If the algorithms runs for T iterations it records a transcript of $m + n + T(k-1)$ bits.

Compressing Bits While Solving k-SAT

Claim 1: If the algorithm runs for T iterations, it uses $m + Tk$ random bits.

Claim 2: If the algorithms runs for T iterations it records a transcript of $m + n + T(k-1)$ bits.

Claim 3: The random bits used by the algorithm can be recovered uniquely from the transcript.

Compressing Bits While Solving k-SAT

Claim 1: If the algorithm runs for T iterations, it uses $m + Tk$ random bits.

Claim 2: If the algorithms runs for T iterations it records a transcript of $m + n + T(k-1)$ bits.

Claim 3: The random bits used by the algorithm can be recovered uniquely from the transcript.

We can work backward from the final state, recovering the state of the variables at each step, and hence all the random bits. Critically, when a clause is rerandomized, we know exactly how its bits were been set before rerandomization (there is just a single unsatisfying assignment for the clause).

Compressing Bits While Solving k-SAT

Claim 1: If the algorithm runs for T iterations, it uses $m + Tk$ random bits.

Claim 2: If the algorithms runs for T iterations it records a transcript of $m + n + T(k-1)$ bits.

Claim 3: The random bits used by the algorithm can be recovered uniquely from the transcript.

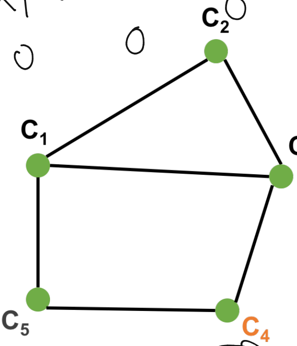
We can work backward from the final state, recovering the state of the variables at each step, and hence all the random bits. Critically, when a clause is rerandomized, we know exactly how its bits were been set before rerandomization (there is just a single unsatisfying assignment for the clause).

So we have compressed $B = m + Tk$ bits to $B' = m + n + T(k-1)$ bits. Setting, $T = n + c$ we have $B = m + Tk$ and $B' = m + Tk - c$. Thus, by our incompressibility claim, the algorithm must terminate in $n + c$ steps with probability $1 - 1/2^{c-1}$.

Recovery Illustration

$x_1 \vee x_2 \vee x_3$

0 0 0



Record: 10110000001...10111011

Bits Used: 10110001,10111,00100,10101,10111

Thanks for a great semester!