

Random Sums and Graphs

Probability

Events, probabilities,
conditional probabilities,
union bound

Random variables,
expected value,
linearity of expectation
Markov's inequality

Algorithms

Approx. 3-SAT,

Big idea: we only want the average

$$\text{Linearity of Expectation} \\ E[X+Y] = E[X] + E[Y] \quad (\text{stochastic variable}) \\ \text{"average sum = sum of averages"}$$

let $Y_i = \begin{cases} 1 & \text{if } i\text{th clause satisfied} \\ 0 & \text{otherwise} \end{cases} \quad (i=1, \dots, m)$

$$E[Y_i] = 7/8 \quad (1 \text{ clause case})$$

$$E[\text{\# clauses satisfied}] = E\left[\sum_{i=1}^m Y_i\right] = \sum_{i=1}^m E[Y_i] = 7/8 m$$

let $Y_i = \begin{cases} 1 & \text{if } i\text{th clause satisfied} \\ 0 & \text{otherwise} \end{cases}$

$$Z = \sum_{i=1}^m Y_i = \text{\# clauses satisfied}$$

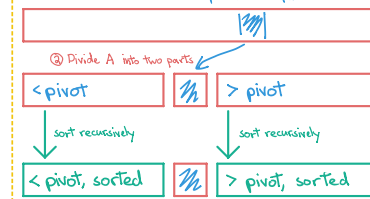
$$E[Z] = \frac{1}{2} E[Z | x_1 = \text{true}] + \frac{1}{2} E[Z | x_1 = \text{false}]$$

$\Rightarrow$ either $E[Z | x_1 = \text{true}]$ or $E[Z | x_1 = \text{false}]$ is $\geq E[Z]$!

QuickSort,

Random divide and conquer

① pick random 'pivot'



Expected running time of QuickSort

For each $i, j \in [n]$ w/ $i < j$,

$X_{ij} = \begin{cases} 1 & \text{if } i\text{th smallest element is compared to } j\text{th smallest} \\ 0 & \text{otherwise} \end{cases}$

$\sum_{i < j} X_{ij}$ = total # comparisons made by the algorithm
 $\approx$ total running time

$E[\sum_{i < j} X_{ij}]$ = average running time

$$E[\sum_{i < j} X_{ij}] = \sum_{i < j} E[X_{ij}]$$

now analyze $E[X_{ij}]$ in isolation

$$E[X_{ij}] = \Pr[X_{ij} = 1] \\ = \Pr[\text{\#th element is compared to } j\text{th}]$$

i th and j th elem selected before any element in between happens w/ probability $\frac{2}{j-i+1}$

$E[X_{ij}] = \frac{2}{j-i+1}$

by linearity of expectation

$$E[\sum_{i < j} X_{ij}] = \sum_{i < j} E[X_{ij}] = \sum_{i < j} \frac{2}{j-i+1}$$

$$\leq 2n \left(\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} \right) \leq O(n \log n) \quad \text{with harmonic series}$$

Quickselect (HW)

Probability

Hash Functions,

Universal Hash Functions

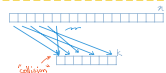
$h: [n] \rightarrow k$ s.t. for all pairs $i, j \in [n]$,
 $\Pr[h(i) = h(j)] \leq \frac{1}{k}$ (much weaker than ideal hash)

e.g. $h(x) = (ax + b) \bmod p \bmod k$

where • p prime, $> k$

• a in $\{1, \dots, p-1\}$ unif. random

• b in $\{0, \dots, p-1\}$ unif. random



Markov's Inequality

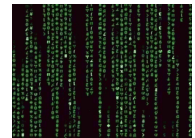
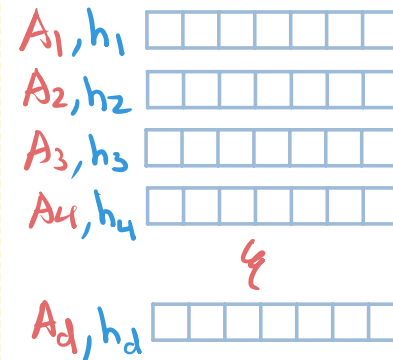
Markov's Inequality (special case)

Let $X \geq 0$ be nonnegative RV

$$\Pr[X \geq 2E[X]] \leq \frac{1}{2}$$

Algorithms

Frequency Estimation, Heavy Hitters (in streams)



estimate f_i w/
 $\min_{j=1, \dots, d} A_j[h_j(i)]$

Probability

k-wise independence,
higher order moments
(generalizing universal hash
functions and Markov's inequality)

Algorithms

Hash tables w/
chaining +
linear probing

k-wise independent hash functions

$$h: [U] \rightarrow [m]$$

s.t. for any k keys $x_1, x_2, \dots, x_k \in [U]$,
 k values $y_1, y_2, \dots, y_k \in [m]$,

$$P[h(x_1)=y_1, h(x_2)=y_2, \dots, h(x_k)=y_k] = \frac{1}{m^k}$$

eg. $h(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \pmod{p}$

where $p \geq U$ prime,
 $a_0, a_1, \dots, a_{k-1} \in [p]$ indep, uniformly random

Important lemma

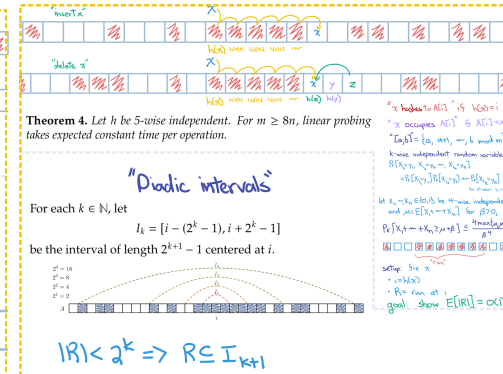
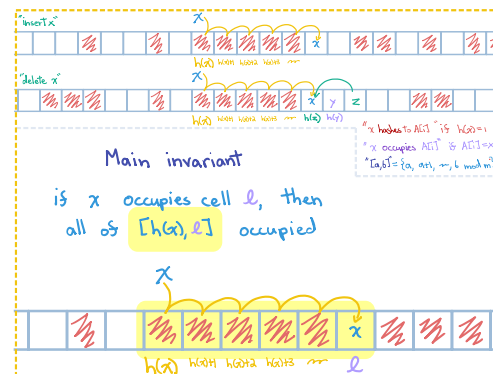
k-wise independent random variables

$$P[X_1=y_1, X_2=y_2, \dots, X_k=y_k] \\ = P[X_1=y_1]P[X_2=y_2] \dots P[X_k=y_k]$$

for all values $y_1, \dots, y_k$

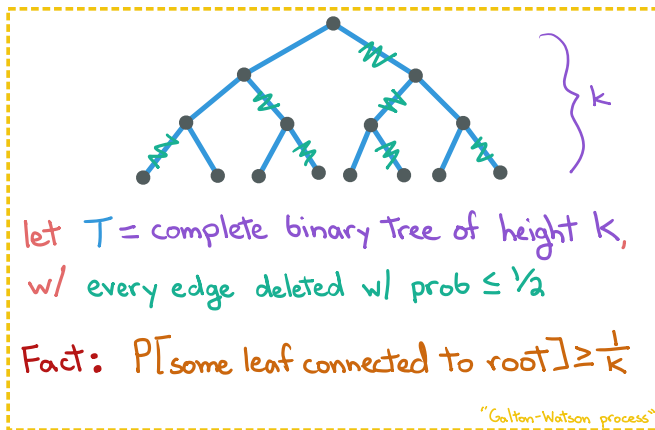
let $X_1, \dots, X_n \in \{0, 1\}$ be 4-wise independent
and $\mu = E[X_1 + \dots + X_n]$. then for $\beta > 0$,

$$P[X_1 + \dots + X_n \geq \mu + \beta] \leq \frac{4 \max\{\mu, \mu^3\}}{\beta^4}$$



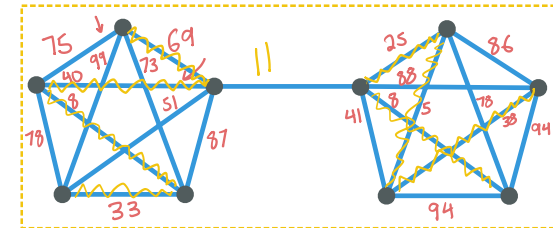
Probability

Galton-Watson processes



Algorithms

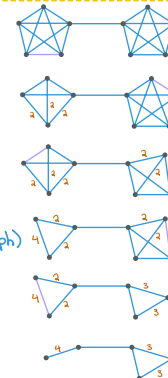
Random Contractions for min cut



Randomized contractions

Input: $G=(V,E)$, weights $c \in \mathbb{R}_{>0}^E$ (unweighted)

- ① while $|E| > 1$
 - Ⓐ sample $e \in E$ in proportion to c
 - Ⓑ "contract" e
- ② return set of edges (in original graph) contracted to remaining edge

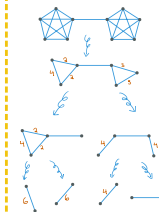


Amplification by branching

Instead of restarting at the beginning, restart partway through

High-level algorithm

- ① randomly contract until prob. of ruining the min-cut is $\sim 1/2$
- ② Branch: make two copies of current graph recurse on both copies



Probability

Multiplicative
Chernoff Bound

Algorithms (/ results)

Random graphs
& the giant component

Probability

Multiplicative
Chernoff Bound

Algorithms (/ results)

Random graphs
& the giant component



Flip 100 coins.

50 come up heads.

Should you be surprised?

(Maybe a little: $\approx 8\%$ chance)



Flip 100 coins.

0 come up heads.

Should you be surprised?

Absolutely: $\frac{1}{2^{100}}$ chance



Flip 100 coins.

≤ 25 come up heads.

Should you be surprised?

Yes: $\approx 2.818 \times 10^{-7} \%$



Flip 10 coins.

≤ 4 come up heads.

Should you be surprised?

No: $\approx 37.7\%$



Flip 1000 coins.

$\leq 40\%$ come up heads.

Should you be surprised?

Yes: $\approx 1.364 \times 10^{-10}$ probability



10 coins.

≤ 4 heads.

$\approx 37.7\%$

1000 coins.

$\leq 40\%$ heads.

1.364×10^{-10} prob.

scale matters

Concentration phenomena

let $X_1, \dots, X_n \in [0, 1]$ be independent

$$\mu = E[X_1 + \dots + X_n]$$

Q: probability that

$X_1 + \dots + X_n$ is close to μ ?
(multiplicatively)

A: error probability exponentially small in μ

Multiplicative Chernoff bound

let $X_1, \dots, X_n \in [0, 1]$ be independent

$$\mu = E[X_1 + \dots + X_n]$$

$$\epsilon \in (0, 1)$$

$$\bullet \quad P[X_1 + \dots + X_n \geq (1 + \epsilon)\mu] \leq e^{-\epsilon^2 \mu / 3}$$

$$\bullet \quad P[X_1 + \dots + X_n \leq (1 - \epsilon)\mu] \leq e^{-\epsilon^2 \mu / 2}$$

(proof at end if time permits)

Probability

Multiplicative
Chernoff Bound

Algorithms (/ results)

Random graphs
& the giant component

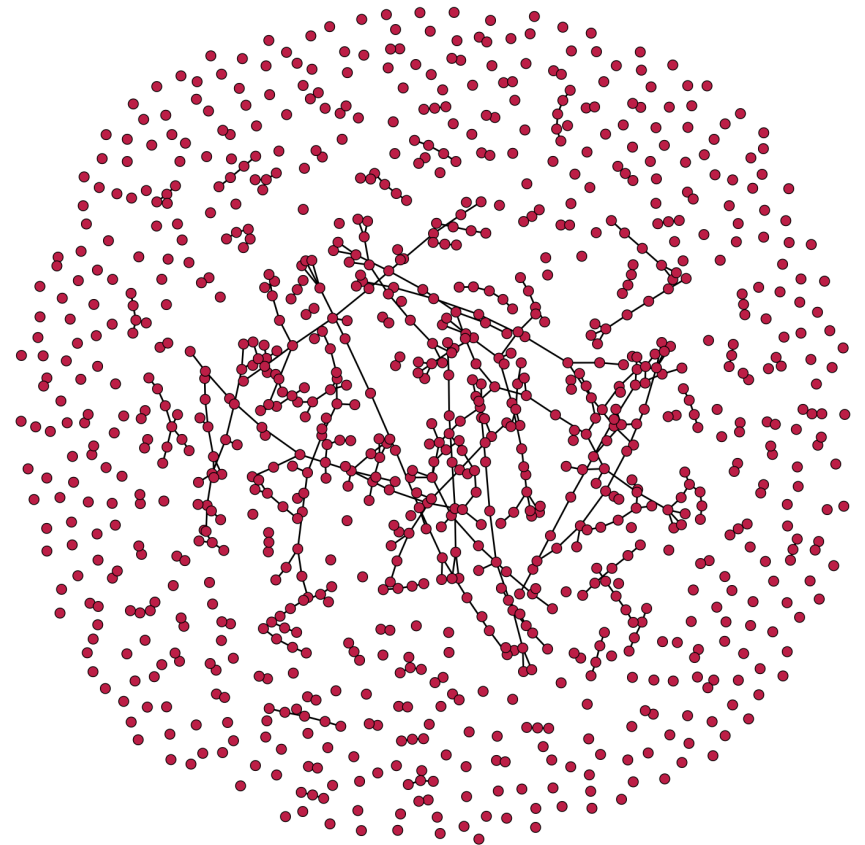
Erdős-Rényi graphs $G(n, p)$

(1959)

- n vertices
- each edge sampled independently
w/ probability p

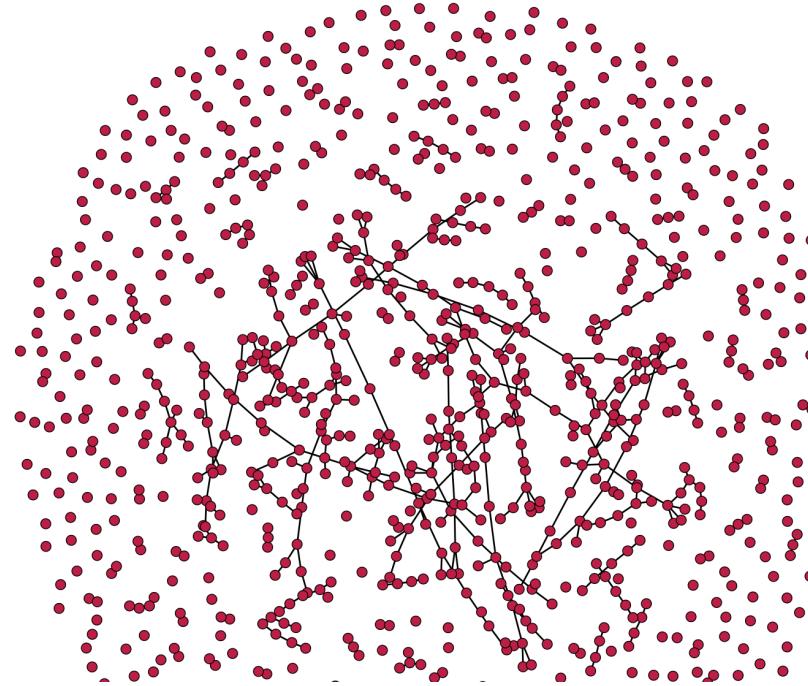
Q: what does such a graph
look like?

does it consistently have
certain properties?



Erdős-Rényi graphs $G(n, p)$

- n vertices
- each edge sampled independently w/ probability p

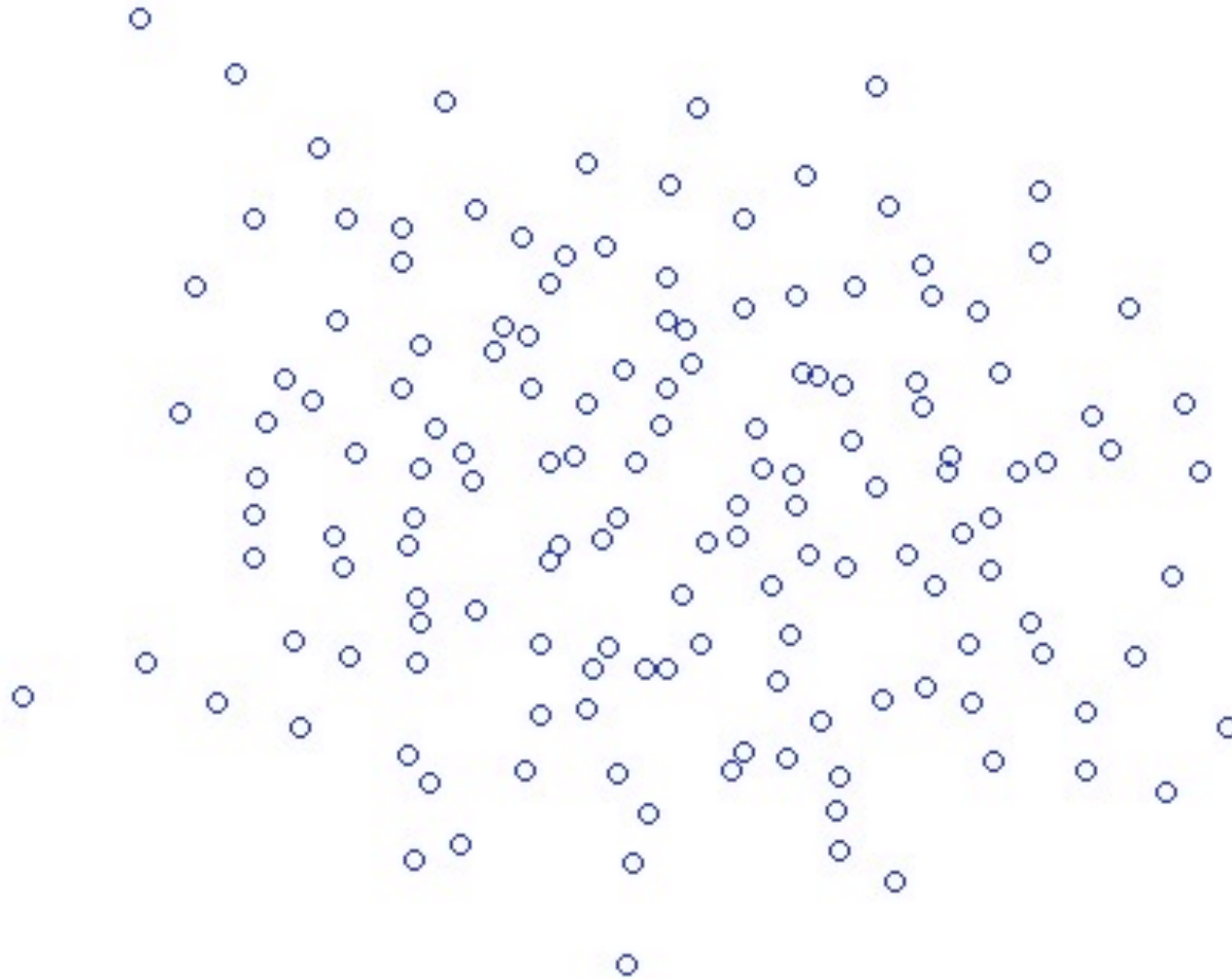


Theorem 5.3. Consider a random graph $G \sim \mathcal{G}(n, p)$ for $p = c/n$, where c is a constant.

1. If $c > 1$, then with high probability, there is exactly one connected component of G with $\Omega(n)$ vertices, and all other components have size $\leq O(\log n)$.
2. For $c < 1$, then with high probability, all connected components of G have size $< O(\log n)$.

"threshold phenomena"

$$p = 0$$
$$p \cdot n = 0$$



Theorem 5.3. Consider a random graph $G \sim \mathcal{G}(n, p)$ for $p = c/n$, where c is a constant.

Proof outline ($c > 1$)

1. If $c > 1$, then with high probability, there is exactly one connected component of G with $\Omega(n)$ vertices, and all other components have size $\leq O(\log n)$.
2. For $c < 1$, then with high probability, all connected components of G has size $< O(\log n)$.

① Gap theorem let $p = (1 + \varepsilon)/n$. w/ high probability,
all components have size
 $\overset{\text{"small component"}}{\leq O\left(\frac{\log n}{\varepsilon^2}\right)}$ or $\overset{\text{"large component"}}{\geq \Omega(\varepsilon n)}$

② Existence of large component

③ Uniqueness of large component

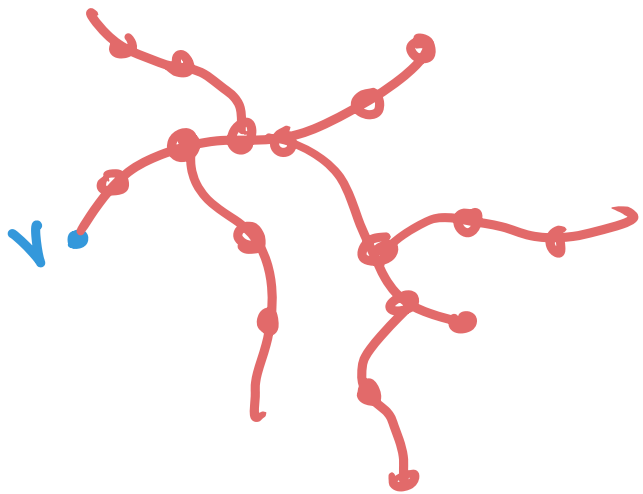
① Gap theorem let $p = (1+\epsilon)/n$. w/ high probability,
all components have size

$$\leq O\left(\frac{\log n}{\epsilon^2}\right) \quad \text{or} \quad \geq \Omega(\epsilon n)$$

Setup

fix vertex v .

let $C(v) \subseteq V$ = connected component of v



to analyze $C(v)$, imagine
revealing $C(v)$ w/ a search algo

Fix vertex v . $C(v) \subseteq V =$ connected component of v

"Search algo"

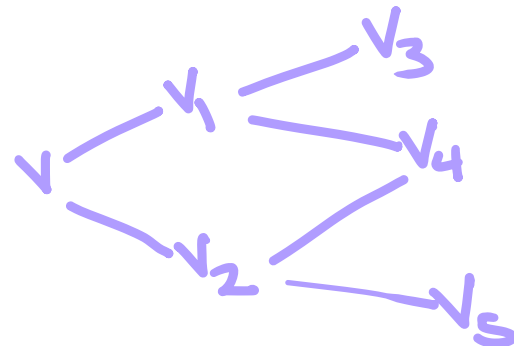
$A = \{\text{vertices known to be in } C(v)\}$ (initially $A = \{v\}$)

$B = \{\text{explored vertices}\}$ (initially $B = \emptyset$)

① while there is a vertex $v_i \in A \setminus B$

 Ⓐ add all neighbors of v_i to A

 Ⓑ add v_i to B



~

Indexed version of "Search algo"

$A_i = \{\text{vertices known to be in } C(v) \text{ after } i \text{ iter.}\}$
($A_0 = \{v\}$)

$B_i = \{\text{explored vertices after } i \text{ iterations}\}$ ($B_0 = \emptyset$)

1. For $i = 1, 2, \dots$ until $A_i = B_i$

a. Let $v_i \in A_{i-1} \setminus B_{i-1}$

b. $A_i = A_{i-1} \cup N(v_i)$

c. $B_i = B_{i-1} \cup \{v_i\}$

Observation 1

algo terminates iff $|A_i| = i$

Observation 2 $A_{i+1} = A_i \cup S_{i+1}$

where S_{i+1} samples each $v \in V \setminus A_i$ independently
w/ probability p

$A_i = \{\text{vertices known to be in } C(v) \text{ after } i \text{ iter.}\}$
($A_0 = \{v\}$)

$B_i = \{\text{explored vertices after } i \text{ iterations}\}$ ($B_0 = \emptyset$)

1. For $i=1, 2, \dots$ until $A_i = B_i$

a. Let $v_i \in A_{i-1} \setminus B_{i-1}$

b. $A_i = A_{i-1} \cup N(v_i)$

c. $B_i = B_{i-1} \cup \{v_i\}$

Observation 1 algo terminates iff $|A_i| = i$

Observation 2 $A_{i+1} = A_i \cup S_{i+1}$

where S_{i+1} samples each $v \in V \setminus A_i$ independently w/ probability p

1. For $i=1,2,\dots$ until $A_i = B_i$

a. Let $v_i \in A_{i-1} \setminus B_{i-1}$

b. $A_i = A_{i-1} \cup N(v_i)$

c. $B_i = B_{i-1} \cup \{v_i\}$

1. For $i=1,2,\dots$ until $|A_i| = i$

a. Let S_i randomly sample $V \setminus A_{i-1}$ w/ probability p

b. $A_i = A_{i-1} \cup S_i$

(equivalent)

let $i \leq \frac{\epsilon n}{4}$.

Lemma 1. $E[|A_i|] \geq (1+\epsilon)i$

① Gap theorem let $p = (1+\epsilon)/n$. w/ high probability, all components have size $\leq O(\frac{\log n}{\epsilon^2})$ or $\geq \Omega(\epsilon n)$

Multiplicative Chernoff bound
let $X_1, \dots, X_n \in [0, 1]$ be independent

$$\mu = E[X_1 + \dots + X_n] \in (0, 1)$$

$$P[X_1 + \dots + X_n \leq (1-\epsilon)\mu] \leq e^{-\epsilon^2 \mu / 2}$$

1. For $i=1, 2, \dots$ until $|A_i| = i$
 - a. Let S_i randomly sample $V \setminus A_{i-1}$ w/ probability p
 - b. $A_i = A_{i-1} \cup S_i$

let $i \leq \frac{\epsilon n}{4}$.

Lemma 1. $E[|A_i|] \geq (1+\epsilon)i$

Lemma 2.

$$P[|A_i| \leq i] \leq e^{-\epsilon^2 i / 8}$$

① Gap theorem let $p = (1+\epsilon)/n$. w/ high probability, all components have size $\leq O(\frac{\log n}{\epsilon^2})$ or $\geq \Omega(\epsilon n)$

Multiplicative Chernoff bound
let $X_1, \dots, X_n \in [0,1]$ be independent

$$\mu = E[X_1 + \dots + X_n] \in (0,1)$$

$$P[X_1 + \dots + X_n \leq (1-\epsilon)\mu] \leq e^{-\epsilon^2 \mu / 2}$$

1. For $i=1,2,\dots$ until $|A_i|=i$
 - a. Let S_i randomly sample $V \setminus A_{i-1}$ w/ probability p
 - b. $A_i = A_{i-1} \cup S_i$

let $i \leq \frac{\epsilon n}{4}$.

Lemma 1. $E[|A_i|] \geq (1+\epsilon)i$

Lemma 2.

$$P[|A_i| \leq i] \leq e^{-\epsilon^2 i / 8}$$

for $i \geq 32 \log n / \epsilon^2$, $\uparrow \leq \frac{1}{n^4}$

by union bound over $\frac{32 \log n}{\epsilon^2} \leq i \leq \frac{\epsilon n}{4}$,

$$P\left[\frac{32 \log n}{\epsilon^2} \leq |A_i| \leq \frac{\epsilon n}{4}\right] \leq \frac{1}{n^3}$$

① Gap theorem let $p = (1+\epsilon)/n$. w/ high probability, all components have size $\leq O(\frac{\log n}{\epsilon^2})$ or $\geq \Omega(\epsilon n)$

Multiplicative Chernoff bound
let $X_1, \dots, X_n \in [0, 1]$ be independent

$$\mu = E[X_1 + \dots + X_n] \in (0, 1)$$

$$P[X_1 + \dots + X_n \leq (1-\epsilon)\mu] \leq e^{-\epsilon^2 \mu / 2}$$

1. For $i=1, 2, \dots$ until $|A_i| = i$
 - a. Let S_i randomly sample $V \setminus A_{i-1}$ w/ probability p
 - b. $A_i = A_{i-1} \cup S_i$

Theorem 5.3. Consider a random graph $G \sim \mathcal{G}(n, p)$ for $p = c/n$, where c is a constant.

Proof outline ($c > 1$)

1. If $c > 1$, then with high probability, there is exactly one connected component of G with $\Omega(n)$ vertices, and all other components have size $\leq O(\log n)$.
2. For $c < 1$, then with high probability, all connected components of G has size $< O(\log n)$.

✓ ① Gap theorem let $p = (1 + \varepsilon)/n$. w/ high probability,
all components have size
 $\leq O\left(\frac{\log n}{\varepsilon^2}\right)$ or $\geq \Omega(\varepsilon n)$

② Existence of large component

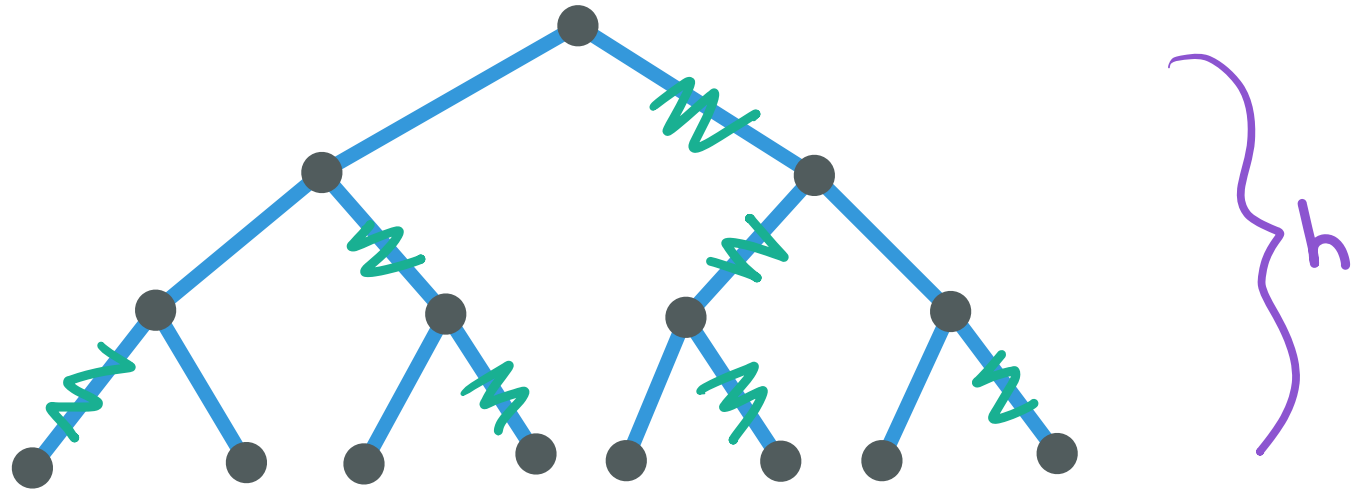
③ Uniqueness of large component

② Existence of large component

Lemma 5.5. *Let $p = (1 + \epsilon)/n$ for $\epsilon > 0$. Let $v \in V$ be a vertex. For all $3 \leq h \leq \epsilon n$, with probability at least $1/h$, v has at least $1 + h$ vertices in its connected component.*

Lemma 5.5. Let $p = (1 + \epsilon)/n$ for $\epsilon > 0$. Let $v \in V$ be a vertex. For all $3 \leq h \leq \epsilon n$, with probability at least $1/h$, v has at least $1 + h$ vertices in its connected component.

Last time

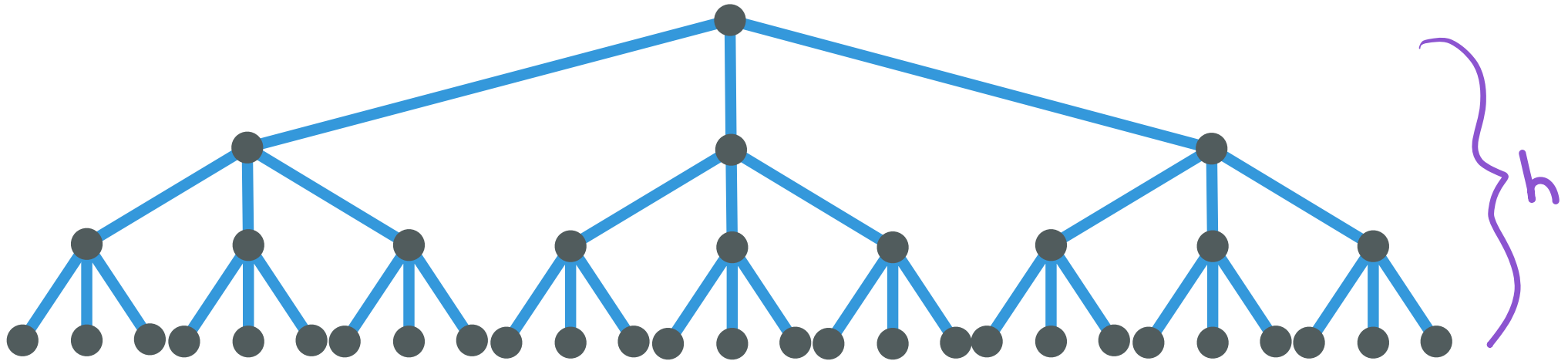


let T = complete binary tree of height h ,
w/ every edge deleted w/ prob $\leq 1/2$

Fact: $P[\text{some leaf connected to root}] \geq \frac{1}{h}$

"Galton-Watson process"

Lemma 5.5. Let $p = (1 + \epsilon)/n$ for $\epsilon > 0$. Let $v \in V$ be a vertex. For all $3 \leq h \leq \epsilon n$, with probability at least $1/h$, v has at least $1 + h$ vertices in its connected component.

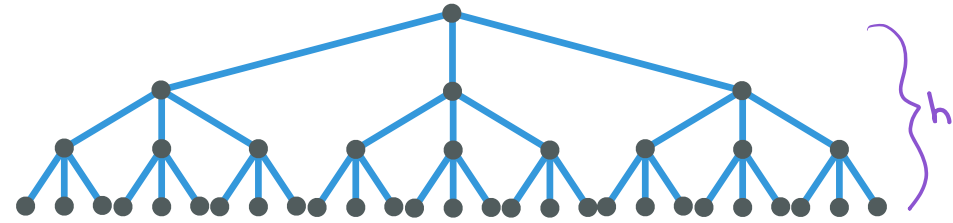


let $T =$ complete k -ary tree of height h ,
 w/ every edge deleted w/ prob $\leq 1/k$

Fact: $P[\text{some leaf connected to root}] \geq \frac{1}{h}$

"Galton-Watson process"

Lemma 5.5. Let $p = (1 + \epsilon)/n$ for $\epsilon > 0$. Let $v \in V$ be a vertex. For all $3 \leq h \leq \epsilon n$, with probability at least $1/h$, v has at least $1 + h$ vertices in its connected component.



let $T =$ complete k -ary tree of height h ,
w/ every edge deleted w/ prob $\leq 1/k$

Fact: $P[\text{some leaf connected to root}] \geq \frac{1}{h}$

"Galton-Watson process"

Equivalent process

start w/ population of size 1

Each generation, each individual flips k coins
w/ prob. $1/k$ of heads

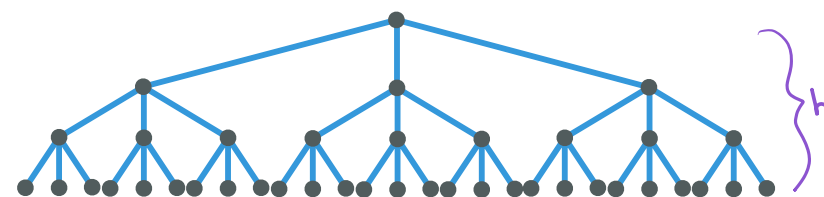
heads = # children

Fact: $P[\text{surviving } h \text{ generations}] \geq \frac{1}{h}$

Lemma 5.5. Let $p = (1 + \epsilon)/n$ for $\epsilon > 0$. Let $v \in V$ be a vertex. For all $3 \leq h \leq \epsilon n$, with probability at least $1/h$, v has at least $1 + h$ vertices in its connected component.

Idea:

"couple"
(i.e., relate)



let T = complete k -ary tree of height h ,
w/ every edge deleted w/ prob $\leq 1/k$

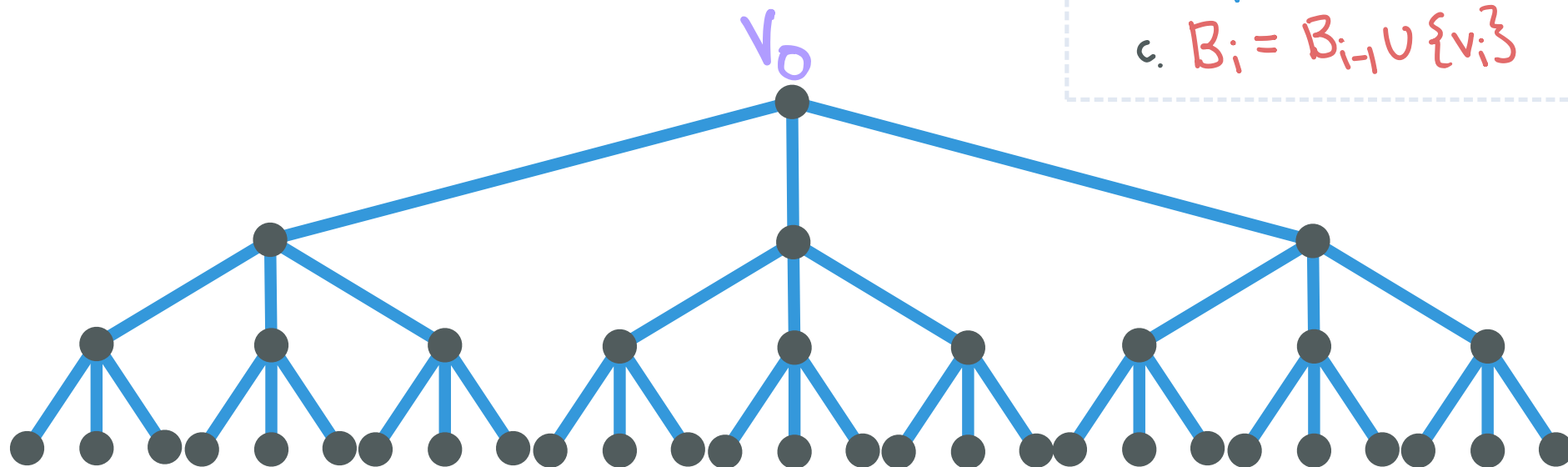
Fact: $P[\text{some leaf connected to root}] \geq \frac{1}{h}$
"Galton-Watson process"

1. For $i=1, 2, \dots$ until $A_i = B_i$:

a. Let $v_i \in A_{i-1} \setminus B_{i-1}$

b. $A_i = A_{i-1} \cup N(v_i)$

c. $B_i = B_{i-1} \cup \{v_i\}$

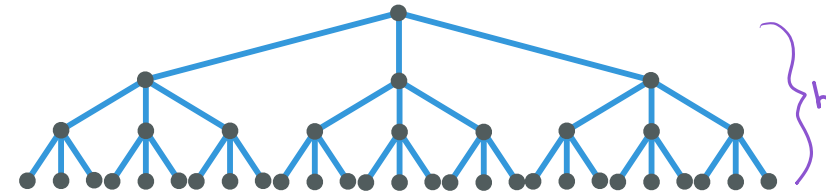


Lemma 5.5. Let $p = (1 + \epsilon)/n$ for $\epsilon > 0$. Let $v \in V$ be a vertex. For all $3 \leq h \leq \epsilon n$, with probability at least $1/h$, v has at least $1 + h$ vertices in its connected component.

Recall search algo.

conditional on $|A_{i-1}| \leq h$,

A_i/A_{i-1} is like sampling
 $n-h \geq \frac{n}{1+\epsilon}$ children of
 some node, each w/
 prob. $p = \frac{1+\epsilon}{n}$



let T = complete k -ary tree of height h ,
 w/ every edge deleted w/ prob $\leq 1/k$

Fact: $P[\text{some leaf connected to root}] \geq \frac{1}{h}$
 "Galton-Watson process"

1. For $i=1, 2, \dots$ until $A_i = B_i$:
 - a. Let $v_i \in A_{i-1} \setminus B_{i-1}$
 - b. $A_i = A_{i-1} \cup N(v_i)$
 - c. $B_i = B_{i-1} \cup \{v_i\}$

surviving h generations $\Rightarrow |A_i| > i \quad \forall i < h$
 (or reaching $|A_i| = h$)

Theorem 5.3. Consider a random graph $G \sim \mathcal{G}(n, p)$ for $p = c/n$, where c is a constant.

Proof outline ($c > 1$)

1. If $c > 1$, then with high probability, there is exactly one connected component of G with $\Omega(n)$ vertices, and all other components have size $\leq O(\log n)$.
2. For $c < 1$, then with high probability, all connected components of G has size $< O(\log n)$.

✓ ① Gap theorem let $p = (1 + \epsilon)/n$. w/ high probability,
all components have size
 $\leq O\left(\frac{\log n}{\epsilon^2}\right)$ or $\geq \Omega(\epsilon n)$

✓ ② Existence of large component

③ Uniqueness of large component

Imagine sampling $G \sim (n, p)$ as:

- ① sample $G_1 \sim (n/2, p)$
- ② sample $G_2 \sim (n/2, p)$
- ③ combine G_1 and G_2
- ④ sample cross edges

Multiplicative Chernoff bound

let $X_1, \dots, X_n \in [0, 1]$ be independent

$$\mu = E[X_1 + \dots + X_n]$$

$$\epsilon \in (0, 1)$$

$$\bullet \quad P[X_1 + \dots + X_n \geq (1 + \epsilon)\mu] \leq e^{-\epsilon^2 \mu / 3}$$

$$\bullet \quad P[X_1 + \dots + X_n \leq (1 - \epsilon)\mu] \leq e^{-\epsilon^2 \mu / 2}$$

(proof at end if time permits)

