

CMPSCI 711: “Really Advanced Algorithms”

Lecture 11, 12, & 13 – Probability Amplification and Expanders

Andrew McGregor

Outline

Probability Amplification with Two Point Sampling

Probability Amplification with Expanding Graphs

Probability Amplification with Random Walks on Expanders

Bonus Section! Connectivity and Eigenvectors

Readings

Probability Amplification

- ▶ Consider language L and randomized algorithm $\mathcal{A}$ such that for random $r \in \{0, \dots, p-1\}$ (p is prime),
 - ▶ If $x \in L$, then $\mathbb{P}[A(x, r) = 1] \geq 1/2$
 - ▶ If $x \notin L$, then $\mathbb{P}[A(x, r) = 0] = 1$

Probability Amplification

- ▶ Consider language L and randomized algorithm $\mathcal{A}$ such that for random $r \in \{0, \dots, p-1\}$ (p is prime),
 - ▶ If $x \in L$, then $\mathbb{P}[A(x, r) = 1] \geq 1/2$
 - ▶ If $x \notin L$, then $\mathbb{P}[A(x, r) = 0] = 1$
- ▶ If algorithm has worst case polynomial running time in $|x|$, we call it an **RP algorithm**.

Probability Amplification

- ▶ Consider language L and randomized algorithm $\mathcal{A}$ such that for random $r \in \{0, \dots, p-1\}$ (p is prime),
 - ▶ If $x \in L$, then $\mathbb{P}[A(x, r) = 1] \geq 1/2$
 - ▶ If $x \notin L$, then $\mathbb{P}[A(x, r) = 0] = 1$
- ▶ If algorithm has worst case polynomial running time in $|x|$, we call it an **RP algorithm**.
- ▶ We say r is a witness for $x \in L$ if $A(x, r) = 1$

Probability Amplification

- ▶ Consider language L and randomized algorithm $\mathcal{A}$ such that for random $r \in \{0, \dots, p-1\}$ (p is prime),
 - ▶ If $x \in L$, then $\mathbb{P}[A(x, r) = 1] \geq 1/2$
 - ▶ If $x \notin L$, then $\mathbb{P}[A(x, r) = 0] = 1$
- ▶ If algorithm has worst case polynomial running time in $|x|$, we call it an **RP algorithm**.
- ▶ We say r is a witness for $x \in L$ if $A(x, r) = 1$
- ▶ Easy to boost the probability of returning 1 for $x \in L$ up to $1 - 2^{-t}$ using $O(t \log p)$ random bits.

Probability Amplification

- ▶ Consider language L and randomized algorithm $\mathcal{A}$ such that for random $r \in \{0, \dots, p-1\}$ (p is prime),
 - ▶ If $x \in L$, then $\mathbb{P}[A(x, r) = 1] \geq 1/2$
 - ▶ If $x \notin L$, then $\mathbb{P}[A(x, r) = 0] = 1$
- ▶ If algorithm has worst case polynomial running time in $|x|$, we call it an **RP algorithm**.
- ▶ We say r is a witness for $x \in L$ if $A(x, r) = 1$
- ▶ Easy to boost the probability of returning 1 for $x \in L$ up to $1 - 2^{-t}$ using $O(t \log p)$ random bits.
- ▶ What if we only have $O(\log p)$ bits?

Two Point Sampling

- ▶ Let p be a prime and let a, b be chosen uniformly at random from $\{0, 1, \dots, p-1\}$.
- ▶ Define $r_0, \dots, r_{t-1}$ where $r_i = ai + b \pmod{p}$.

Two Point Sampling

- ▶ Let p be a prime and let a, b be chosen uniformly at random from $\{0, 1, \dots, p-1\}$.
- ▶ Define $r_0, \dots, r_{t-1}$ where $r_i = ai + b \pmod{p}$.
- ▶ **Exercise:** r_i are pairwise independent (but not three-wise)

Two Point Sampling

- ▶ Let p be a prime and let a, b be chosen uniformly at random from $\{0, 1, \dots, p-1\}$.
- ▶ Define $r_0, \dots, r_{t-1}$ where $r_i = ai + b \pmod{p}$.
- ▶ **Exercise:** r_i are pairwise independent (but not three-wise)
- ▶ Let $Y = \sum_{i=1}^t A(x, r_i)$

Two Point Sampling

- ▶ Let p be a prime and let a, b be chosen uniformly at random from $\{0, 1, \dots, p-1\}$.
- ▶ Define $r_0, \dots, r_{t-1}$ where $r_i = ai + b \pmod{p}$.
- ▶ **Exercise:** r_i are pairwise independent (but not three-wise)
- ▶ Let $Y = \sum_{i=1}^t A(x, r_i)$
- ▶ **Exercise:** If $x \in L$, $\mathbb{P}[Y = 0] \leq 1/t$

Two Point Sampling

- ▶ Let p be a prime and let a, b be chosen uniformly at random from $\{0, 1, \dots, p-1\}$.
- ▶ Define $r_0, \dots, r_{t-1}$ where $r_i = ai + b \pmod{p}$.
- ▶ **Exercise:** r_i are pairwise independent (but not three-wise)
- ▶ Let $Y = \sum_{i=1}^t A(x, r_i)$
- ▶ **Exercise:** If $x \in L$, $\mathbb{P}[Y = 0] \leq 1/t$
- ▶ Hence, with $O(\log p)$ random bits, can boost probability to $1 - 1/t$ given t trials.

Outline

Probability Amplification with Two Point Sampling

Probability Amplification with Expanding Graphs

Probability Amplification with Random Walks on Expanders

Bonus Section! Connectivity and Eigenvectors

Readings

Probability Amplification with Expanding Graphs

- ▶ We'll show approach with error probability $\approx 1/n^{\log n}$ using $\log^2 n$ random bits (where there are $O(n)$ witnesses).

Probability Amplification with Expanding Graphs

- ▶ We'll show approach with error probability $\approx 1/n^{\log n}$ using $\log^2 n$ random bits (where there are $O(n)$ witnesses).
- ▶ Approach is based on “sparse expanding graphs”

Probability Amplification with Expanding Graphs

- ▶ We'll show approach with error probability $\approx 1/n^{\log n}$ using $\log^2 n$ random bits (where there are $O(n)$ witnesses).
- ▶ Approach is based on “sparse expanding graphs”

Theorem

For sufficiently large n , there is a bipartite graph $G = (L, R, E)$ with $|L| = n$, $|R| = 2^{\log^2 n}$ with:

- 1. Every subset of $n/2$ vertices from L has at least $2^{\log^2 n} - n$ neighbors in R .*
- 2. No vertex of R has more than $12 \log^2 n$ neighbors.*

Proof of Theorem

- ▶ By probabilistic method: For each vertex in L , pick $d = 2^{\log^2 n} (4 \log^2 n) / n$ neighbors in R (with replacement).

Proof of Theorem

- ▶ By probabilistic method: For each vertex in L , pick $d = 2^{\log^2 n}(4 \log^2 n)/n$ neighbors in R (with replacement).
- ▶ Probability there is a set of $n/2$ vertices in L with fewer than $2^{\log^2 n} - n$ neighbors in R is at most

$$\binom{n}{n/2} \binom{2^{\log^2 n}}{n} \left(\frac{2^{\log^2 n} - n}{2^{\log^2 n}} \right)^{dn/2}$$

Proof of Theorem

- ▶ By probabilistic method: For each vertex in L , pick $d = 2^{\log^2 n}(4 \log^2 n)/n$ neighbors in R (with replacement).
- ▶ Probability there is a set of $n/2$ vertices in L with fewer than $2^{\log^2 n} - n$ neighbors in R is at most

$$\binom{n}{n/2} \binom{2^{\log^2 n}}{n} \left(\frac{2^{\log^2 n} - n}{2^{\log^2 n}} \right)^{dn/2}$$

- ▶ Usual tricks shows this is $\ll 1/2$.

Proof of Theorem

- ▶ By probabilistic method: For each vertex in L , pick $d = 2^{\log^2 n}(4 \log^2 n)/n$ neighbors in R (with replacement).
- ▶ Probability there is a set of $n/2$ vertices in L with fewer than $2^{\log^2 n} - n$ neighbors in R is at most

$$\binom{n}{n/2} \binom{2^{\log^2 n}}{n} \left(\frac{2^{\log^2 n} - n}{2^{\log^2 n}} \right)^{dn/2}$$

- ▶ Usual tricks shows this is $\ll 1/2$.
- ▶ Second condition: expected number of neighbors of $v \in R$ is $4 \log^2 n$.

Proof of Theorem

- ▶ By probabilistic method: For each vertex in L , pick $d = 2^{\log^2 n}(4 \log^2 n)/n$ neighbors in R (with replacement).
- ▶ Probability there is a set of $n/2$ vertices in L with fewer than $2^{\log^2 n} - n$ neighbors in R is at most

$$\binom{n}{n/2} \binom{2^{\log^2 n}}{n} \left(\frac{2^{\log^2 n} - n}{2^{\log^2 n}} \right)^{dn/2}$$

- ▶ Usual tricks shows this is $\ll 1/2$.
- ▶ Second condition: expected number of neighbors of $v \in R$ is $4 \log^2 n$.
- ▶ Chernoff bound shows that there exists $v \in R$ with more than $12 \log^2 n$ neighbors with probability $\leq |R|(e/3)^{12 \log^2 n} \ll 1/2$

Back to probability amplification...

- Pick $v \in_R R$: Uses $O(\log^2 n)$ random bits.

Back to probability amplification...

- ▶ Pick $v \in_R R$: Uses $O(\log^2 n)$ random bits.
- ▶ Consider neighbors of v .

Back to probability amplification...

- ▶ Pick $v \in_R R$: Uses $O(\log^2 n)$ random bits.
- ▶ Consider neighbors of v .
- ▶ At least $n/2$ of nodes in L are witnesses if $x \in L$.

Back to probability amplification...

- ▶ Pick $v \in_R R$: Uses $O(\log^2 n)$ random bits.
- ▶ Consider neighbors of v .
- ▶ At least $n/2$ of nodes in L are witnesses if $x \in L$.
- ▶ Probability we find a witness is at least $1 - n/2^{\log^2 n}$.

Outline

Probability Amplification with Two Point Sampling

Probability Amplification with Expanding Graphs

Probability Amplification with Random Walks on Expanders

Bonus Section! Connectivity and Eigenvectors

Readings

Expanders

Definition

An (n, d, c) -expander is a d -regular bipartite (multi-)graph $G = (X, Y, E)$ with $|X| = |Y| = n/2$ such that for any $S \subset X$,

$$|\Gamma(S)| \geq \left(1 + c \left(1 - \frac{2|S|}{n}\right)\right) |S|.$$

Expanders

Definition

An (n, d, c) -expander is a d -regular bipartite (multi-)graph $G = (X, Y, E)$ with $|X| = |Y| = n/2$ such that for any $S \subset X$,

$$|\Gamma(S)| \geq \left(1 + c \left(1 - \frac{2|S|}{n}\right)\right) |S|.$$

Example (Gabber-Galil expanders)

For positive integer m , let $n = 2m^2$. Each vertex in X has distinct label consisting of a pair (a, b) for $a, b \in \{0, \dots, m-1\}$. Similarly for Y . $(x, y) \in X$ has neighbors in Y with labels:

$$(x, y), (x, 2x + y), (x, 2x + y + 1), (x, 2x + y + 2)$$

$$(x + 2y, y), (x + 2y + 1, y), (x + 2y + 2, y)$$

where addition is modulo m . Resulting graph is a $(n, 7, 2\alpha)$ example where $\alpha = (2 - \sqrt{3})/4$.

Expanders

Definition

An (n, d, c) -expander is a d -regular bipartite (multi-)graph $G = (X, Y, E)$ with $|X| = |Y| = n/2$ such that for any $S \subset X$,

$$|\Gamma(S)| \geq \left(1 + c \left(1 - \frac{2|S|}{n}\right)\right) |S|.$$

Example (Gabber-Galil expanders)

For positive integer m , let $n = 2m^2$. Each vertex in X has distinct label consisting of a pair (a, b) for $a, b \in \{0, \dots, m-1\}$. Similarly for Y . $(x, y) \in X$ has neighbors in Y with labels:

$$(x, y), (x, 2x + y), (x, 2x + y + 1), (x, 2x + y + 2)$$

$$(x + 2y, y), (x + 2y + 1, y), (x + 2y + 2, y)$$

where addition is modulo m . Resulting graph is a $(n, 7, 2\alpha)$ example where $\alpha = (2 - \sqrt{3})/4$.

Eigenvalues and Algebraic Graph Theory

Fact

For symmetric $n \times n$ matrix A , there exists n orthonormal eigenvectors $e_1, \dots, e_n$ with eigenvalues $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$: i.e.,

$$e_i A = \lambda_i e_i \quad \text{and} \quad e_i \cdot e_j = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

If A is adjacency matrix of graph G , then G connected implies $\lambda_2 < \lambda_1$. If G is d -regular and bipartite, $\lambda_1 = d$ and $\lambda_n = -d$.

Eigenvalues and Algebraic Graph Theory

Fact

For symmetric $n \times n$ matrix A , there exists n orthonormal eigenvectors $e_1, \dots, e_n$ with eigenvalues $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$: i.e.,

$$e_i A = \lambda_i e_i \quad \text{and} \quad e_i \cdot e_j = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

If A is adjacency matrix of graph G , then G connected implies $\lambda_2 < \lambda_1$. If G is d -regular and bipartite, $\lambda_1 = d$ and $\lambda_n = -d$.

Theorem (Alon '86)

If G is an (n, d, c) -expander then $|\lambda_2| \leq d - \frac{c^2}{1024 + 2c^2}$. If $|\lambda_2| \leq d - \epsilon$ then G is an (n, d, c) -expander with $c \geq \frac{2d\epsilon - \epsilon^2}{d^2}$.

Expanders are Rapidly Mixing

Definition

Let G be an (n, d, c) -expander and let Q be transition matrix on G with $Q_{uu} = 1/2$ and $Q_{uv} = 1/(2d)$ if v is a neighbor of u . Let λ_i be eigenvalues of G and $\mu_i = (1 + \lambda_i/d)/2$ be eigenvalues of Q .

Expanders are Rapidly Mixing

Definition

Let G be an (n, d, c) -expander and let Q be transition matrix on G with $Q_{uu} = 1/2$ and $Q_{uv} = 1/(2d)$ if v is a neighbor of u . Let λ_i be eigenvalues of G and $\mu_i = (1 + \lambda_i/d)/2$ be eigenvalues of Q .

Theorem

Consider aperiodic random walk on G defined by Q . Distribution at time t ,

$$|q^{(t)} - \pi| \leq 2\sqrt{n}\mu_2^t$$

This is at most $\sqrt{n}(1 - \epsilon/2d)^t$ if $\lambda_2 \leq d - \epsilon$.

Expanders are Rapidly Mixing

Definition

Let G be an (n, d, c) -expander and let Q be transition matrix on G with $Q_{uu} = 1/2$ and $Q_{uv} = 1/(2d)$ if v is a neighbor of u . Let λ_i be eigenvalues of G and $\mu_i = (1 + \lambda_i/d)/2$ be eigenvalues of Q .

Theorem

Consider aperiodic random walk on G defined by Q . Distribution at time t ,

$$|q^{(t)} - \pi| \leq 2\sqrt{n}\mu_2^t$$

This is at most $\sqrt{n}(1 - \epsilon/2d)^t$ if $\lambda_2 \leq d - \epsilon$.

Lemma

For any vector $v \in \mathbb{R}^n$, $\|v\|_2 \leq \|v\|_1 \leq \sqrt{n}\|v\|_2$ where

$$\|v\|_1 = \sum_i |v_i| \text{ and } \|v\|_2 = \sqrt{\sum_i v_i^2}.$$

Proof of Theorem

- Distribution at time t is $q^{(t)} = q^{(0)} Q^t$

Proof of Theorem

- ▶ Distribution at time t is $q^{(t)} = q^{(0)} Q^t$
- ▶ Choose orthonormal eigenvectors $e_1, \dots, e_n$ for Q .

Proof of Theorem

- ▶ Distribution at time t is $q^{(t)} = q^{(0)} Q^t$
- ▶ Choose orthonormal eigenvectors $e_1, \dots, e_n$ for Q .
- ▶ Express $q^{(0)}$ as $q^{(0)} = \sum_{i \in [n]} c_i e_i$

Proof of Theorem

- ▶ Distribution at time t is $q^{(t)} = q^{(0)} Q^t$
- ▶ Choose orthonormal eigenvectors $e_1, \dots, e_n$ for Q .
- ▶ Express $q^{(0)}$ as $q^{(0)} = \sum_{i \in [n]} c_i e_i$
- ▶ Orthonormality implies $1 = \|q^{(0)}\|_1 \geq \|q^{(0)}\|_2 = \sqrt{\sum_i c_i^2}$

Proof of Theorem

- ▶ Distribution at time t is $q^{(t)} = q^{(0)} Q^t$
- ▶ Choose orthonormal eigenvectors $e_1, \dots, e_n$ for Q .
- ▶ Express $q^{(0)}$ as $q^{(0)} = \sum_{i \in [n]} c_i e_i$
- ▶ Orthonormality implies $1 = \|q^{(0)}\|_1 \geq \|q^{(0)}\|_2 = \sqrt{\sum_i c_i^2}$
- ▶ Then $q^{(t)} = \sum_{i \in [n]} c_i e_i Q^t = \sum_{i \in [n]} c_i e_i \mu_i^t$

Proof of Theorem

- ▶ Distribution at time t is $q^{(t)} = q^{(0)} Q^t$
- ▶ Choose orthonormal eigenvectors $e_1, \dots, e_n$ for Q .
- ▶ Express $q^{(0)}$ as $q^{(0)} = \sum_{i \in [n]} c_i e_i$
- ▶ Orthonormality implies $1 = \|q^{(0)}\|_1 \geq \|q^{(0)}\|_2 = \sqrt{\sum_i c_i^2}$
- ▶ Then $q^{(t)} = \sum_{i \in [n]} c_i e_i Q^t = \sum_{i \in [n]} c_i e_i \mu_i^t$

Proof of Theorem

- ▶ Distribution at time t is $q^{(t)} = q^{(0)} Q^t$
- ▶ Choose orthonormal eigenvectors $e_1, \dots, e_n$ for Q .
- ▶ Express $q^{(0)}$ as $q^{(0)} = \sum_{i \in [n]} c_i e_i$
- ▶ Orthonormality implies $1 = \|q^{(0)}\|_1 \geq \|q^{(0)}\|_2 = \sqrt{\sum_i c_i^2}$
- ▶ Then $q^{(t)} = \sum_{i \in [n]} c_i e_i Q^t = \sum_{i \in [n]} c_i e_i \mu_i^t$
- ▶ Let $x = c_1 e_1$ and using previous lemma:

$$\|q^{(t)} - x\|_1 \leq \sqrt{n} \|q^{(t)} - x\|_2 = \sqrt{n} \left\| \sum_{i=2}^n c_i e_i \mu_i^t \right\|_2$$

Proof of Theorem

- ▶ Distribution at time t is $q^{(t)} = q^{(0)} Q^t$
- ▶ Choose orthonormal eigenvectors $e_1, \dots, e_n$ for Q .
- ▶ Express $q^{(0)}$ as $q^{(0)} = \sum_{i \in [n]} c_i e_i$
- ▶ Orthonormality implies $1 = \|q^{(0)}\|_1 \geq \|q^{(0)}\|_2 = \sqrt{\sum_i c_i^2}$
- ▶ Then $q^{(t)} = \sum_{i \in [n]} c_i e_i Q^t = \sum_{i \in [n]} c_i e_i \mu_i^t$
- ▶ Let $x = c_1 e_1$ and using previous lemma:

$$\|q^{(t)} - x\|_1 \leq \sqrt{n} \|q^{(t)} - x\|_2 = \sqrt{n} \left\| \sum_{i=2}^n c_i e_i \mu_i^t \right\|_2$$

- ▶ Because $\mu_2 \geq \mu_3 \geq \dots \mu_n \geq 0$,

$$\|q^{(t)} - x\|_1 \leq \sqrt{n} \mu_2^t \left\| \sum_{i=2}^n c_i e_i \right\|_2 \leq \sqrt{n} \mu_2^t$$

BPP and Probability Amplification

- ▶ Consider language L and randomized algorithm $\mathcal{A}$ such that for random $r \in \{0, 1\}^n$,
 - ▶ If $x \in L$, then $\mathbb{P}[A(x, r) = 1] \geq 99/100$
 - ▶ If $x \notin L$, then $\mathbb{P}[A(x, r) = 0] \geq 99/100$

BPP and Probability Amplification

- ▶ Consider language L and randomized algorithm $\mathcal{A}$ such that for random $r \in \{0, 1\}^n$,
 - ▶ If $x \in L$, then $\mathbb{P}[A(x, r) = 1] \geq 99/100$
 - ▶ If $x \notin L$, then $\mathbb{P}[A(x, r) = 0] \geq 99/100$
- ▶ If algorithm has worst case polynomial running time in $|x|$, we call it an *BPP algorithm*.

Probability Amplification via Expanders

- ▶ Let G be a $(N, 7, 2\alpha)$ Gabber-Galil expander where $N = 2^n$ and nodes are labelled by $\{0, 1\}^n$

Probability Amplification via Expanders

- ▶ Let G be a $(N, 7, 2\alpha)$ Gabber-Galil expander where $N = 2^n$ and nodes are labelled by $\{0, 1\}^n$
- ▶ Consider random walk on G with prob. $1/2$ of not moving in a given step and random starting position:

$$X_0, X_1, X_2, \dots, X_{7k\beta}$$

where $\beta = O(1)$ satisfies $\lambda_2^\beta \leq 1/10$.

Probability Amplification via Expanders

- ▶ Let G be a $(N, 7, 2\alpha)$ Gabber-Galil expander where $N = 2^n$ and nodes are labelled by $\{0, 1\}^n$
- ▶ Consider random walk on G with prob. $1/2$ of not moving in a given step and random starting position:

$$X_0, X_1, X_2, \dots, X_{7k\beta}$$

where $\beta = O(1)$ satisfies $\lambda_2^\beta \leq 1/10$.

- ▶ Total random bits requires $n + O(k)$

Probability Amplification via Expanders

- ▶ Let G be a $(N, 7, 2\alpha)$ Gabber-Galil expander where $N = 2^n$ and nodes are labelled by $\{0, 1\}^n$
- ▶ Consider random walk on G with prob. $1/2$ of not moving in a given step and random starting position:

$$X_0, X_1, X_2, \dots, X_{7k\beta}$$

where $\beta = O(1)$ satisfies $\lambda_2^\beta \leq 1/10$.

- ▶ Total random bits requires $n + O(k)$
- ▶ For $0 \leq i \leq 7k$, let r_i be label of $X_{i\beta}$

Probability Amplification via Expanders

- ▶ Let G be a $(N, 7, 2\alpha)$ Gabber-Galil expander where $N = 2^n$ and nodes are labelled by $\{0, 1\}^n$
- ▶ Consider random walk on G with prob. $1/2$ of not moving in a given step and random starting position:

$$X_0, X_1, X_2, \dots, X_{7k\beta}$$

where $\beta = O(1)$ satisfies $\lambda_2^\beta \leq 1/10$.

- ▶ Total random bits requires $n + O(k)$
- ▶ For $0 \leq i \leq 7k$, let r_i be label of $X_{i\beta}$

Theorem

Majority of $A(x, r_0), \dots, A(x, r_{7k})$ are correct with prob. $1 - 1/2^k$.

Proof of Theorem

- ▶ Let $W \in \{0, 1\}^{N \times N}$ with $W_{uu} = 1$ iff node u is “good”

Proof of Theorem

- ▶ Let $W \in \{0, 1\}^{N \times N}$ with $W_{uu} = 1$ iff node u is “good”
- ▶ Let $B = Q^t$. For $A \in [7k]$, probability r_i 's are good for $i \in A$ and r_i 's are not good for $i \notin A$ is:

$$\|q^{(0)}BS_1 \dots BS_{7k}\|_1$$

where $S_i = W$ if $i \in A$ and $S_i = \bar{W} = I - W$ if $i \notin A$.

Proof of Theorem

- ▶ Let $W \in \{0, 1\}^{N \times N}$ with $W_{uu} = 1$ iff node u is “good”
- ▶ Let $B = Q^t$. For $A \in [7k]$, probability r_i 's are good for $i \in A$ and r_i 's are not good for $i \notin A$ is:

$$\|q^{(0)}BS_1 \dots BS_{7k}\|_1$$

where $S_i = W$ if $i \in A$ and $S_i = \bar{W} = I - W$ if $i \notin A$.

Claim

For any $p \in \mathbb{R}^N$, $\|pBW\|_2 \leq \|p\|_2$ and $\|pB\bar{W}\|_2 \leq \|p\|_2/5$

Proof of Theorem

- ▶ Let $W \in \{0, 1\}^{N \times N}$ with $W_{uu} = 1$ iff node u is “good”
- ▶ Let $B = Q^t$. For $A \in [7k]$, probability r_i ’s are good for $i \in A$ and r_i ’s are not good for $i \notin A$ is:

$$\|q^{(0)}BS_1 \dots BS_{7k}\|_1$$

where $S_i = W$ if $i \in A$ and $S_i = \bar{W} = I - W$ if $i \notin A$.

Claim

For any $p \in \mathbb{R}^N$, $\|pBW\|_2 \leq \|p\|_2$ and $\|pB\bar{W}\|_2 \leq \|p\|_2/5$

- ▶ Applying claim repeatedly,

$$\begin{aligned}\|q^{(0)}BS_1 \dots BS_{7k}\|_1 &\leq \sqrt{N}\|q^{(0)}BS_1 \dots BS_{7k}\|_2 \\ &\leq \sqrt{N}(1/5)^{7k-|A|}\|q^{(0)}\|_2 = (1/5)^{7k-|A|}\end{aligned}$$

Proof of Theorem

- ▶ Let $W \in \{0, 1\}^{N \times N}$ with $W_{uu} = 1$ iff node u is “good”
- ▶ Let $B = Q^t$. For $A \in [7k]$, probability r_i ’s are good for $i \in A$ and r_i ’s are not good for $i \notin A$ is:

$$\|q^{(0)}BS_1 \dots BS_{7k}\|_1$$

where $S_i = W$ if $i \in A$ and $S_i = \bar{W} = I - W$ if $i \notin A$.

Claim

For any $p \in \mathbb{R}^N$, $\|pBW\|_2 \leq \|p\|_2$ and $\|pB\bar{W}\|_2 \leq \|p\|_2/5$

- ▶ Applying claim repeatedly,

$$\begin{aligned}\|q^{(0)}BS_1 \dots BS_{7k}\|_1 &\leq \sqrt{N}\|q^{(0)}BS_1 \dots BS_{7k}\|_2 \\ &\leq \sqrt{N}(1/5)^{7k-|A|}\|q^{(0)}\|_2 = (1/5)^{7k-|A|}\end{aligned}$$

- ▶ Probability $|A| \leq 7k/2$ is at most $2^{7k}(1/5)^{7k/2} < 1/2^k$

Finishing the Theorem: Proof of Claim

- Express p in eigenvector basis $p = \sum_{i \in [n]} c_i e_i$

Finishing the Theorem: Proof of Claim

- ▶ Express p in eigenvector basis $p = \sum_{i \in [n]} c_i e_i$
- ▶ Because eigenvectors are in $[0, 1]$:

$$\|pBW\|_2 \leq \|pB\|_2 = \left\| \sum_{i \in [n]} c_i \lambda_i^\beta e_i \right\|_2 = \sqrt{\sum_{i \in [n]} c_i^2 \lambda_i^{2\beta}} \leq \sqrt{\sum_{i \in [n]} c_i^2}$$

Finishing the Theorem: Proof of Claim

- ▶ Express p in eigenvector basis $p = \sum_{i \in [n]} c_i e_i$
- ▶ Because eigenvectors are in $[0, 1]$:

$$\|pBW\|_2 \leq \|pB\|_2 = \left\| \sum_{i \in [n]} c_i \lambda_i^\beta e_i \right\|_2 = \sqrt{\sum_{i \in [n]} c_i^2 \lambda_i^{2\beta}} \leq \sqrt{\sum_{i \in [n]} c_i^2}$$

- ▶ Write $p = c_1 e_1 + y$ for $y = \sum_{i \geq 2} c_i e_i$. $\lambda_2^\beta \leq 1/10$ implies:

$$\|yB\bar{W}\|_2 \leq \|yB\|_2 = \left\| \sum_{i \geq 2} c_i \lambda_i^\beta e_i \right\|_2 \leq \lambda_2^\beta \sqrt{\sum_{i \geq 2} c_i^2} \leq \|y\|_2 / 10$$

Finishing the Theorem: Proof of Claim

- ▶ Express p in eigenvector basis $p = \sum_{i \in [n]} c_i e_i$
- ▶ Because eigenvectors are in $[0, 1]$:

$$\|pBW\|_2 \leq \|pB\|_2 = \left\| \sum_{i \in [n]} c_i \lambda_i^\beta e_i \right\|_2 = \sqrt{\sum_{i \in [n]} c_i^2 \lambda_i^{2\beta}} \leq \sqrt{\sum_{i \in [n]} c_i^2}$$

- ▶ Write $p = c_1 e_1 + y$ for $y = \sum_{i \geq 2} c_i e_i$. $\lambda_2^\beta \leq 1/10$ implies:

$$\|yB\bar{W}\|_2 \leq \|yB\|_2 = \left\| \sum_{i \geq 2} c_i \lambda_i^\beta e_i \right\|_2 \leq \lambda_2^\beta \sqrt{\sum_{i \geq 2} c_i^2} \leq \|y\|_2 / 10$$

- ▶ Since $e_1 = (1, \dots, 1)/\sqrt{n}$ and $\lambda_1 = 1$:

$$\|c_1 e_1 B\bar{W}\|_2 \leq \|c_1 e_1 \hat{W}\|_2 \leq \|c_1 e_1\|_2 / 10$$

Finishing the Theorem: Proof of Claim

- ▶ Express p in eigenvector basis $p = \sum_{i \in [n]} c_i e_i$
- ▶ Because eigenvectors are in $[0, 1]$:

$$\|pBW\|_2 \leq \|pB\|_2 = \left\| \sum_{i \in [n]} c_i \lambda_i^\beta e_i \right\|_2 = \sqrt{\sum_{i \in [n]} c_i^2 \lambda_i^{2\beta}} \leq \sqrt{\sum_{i \in [n]} c_i^2}$$

- ▶ Write $p = c_1 e_1 + y$ for $y = \sum_{i \geq 2} c_i e_i$. $\lambda_2^\beta \leq 1/10$ implies:

$$\|yB\bar{W}\|_2 \leq \|yB\|_2 = \left\| \sum_{i \geq 2} c_i \lambda_i^\beta e_i \right\|_2 \leq \lambda_2^\beta \sqrt{\sum_{i \geq 2} c_i^2} \leq \|y\|_2 / 10$$

- ▶ Since $e_1 = (1, \dots, 1)/\sqrt{n}$ and $\lambda_1 = 1$:

$$\|c_1 e_1 B\bar{W}\|_2 \leq \|c_1 e_1 \hat{W}\|_2 \leq \|c_1 e_1\|_2 / 10$$

- ▶ Putting it together:

$$\|pB\bar{W}\|_2 \leq \|c_1 e_1 B\bar{W}\|_2 + \|yB\bar{W}\|_2 \leq (\|c_1 e_1\|_2 + \|y\|_2) \leq \|p\|_2 / 5$$

Outline

Probability Amplification with Two Point Sampling

Probability Amplification with Expanding Graphs

Probability Amplification with Random Walks on Expanders

Bonus Section! Connectivity and Eigenvectors

Readings

Connectivity and Eigenvectors

Theorem

Let A be the adjacency matrix of a d -regular graph. Then a) $\lambda_1 = d$, and b) $\lambda_2 = d$ iff graph is disconnected.

Proof.

Connectivity and Eigenvectors

Theorem

Let A be the adjacency matrix of a d -regular graph. Then a) $\lambda_1 = d$, and b) $\lambda_2 = d$ iff graph is disconnected.

Proof.

- Part a): Let $x \in \mathbb{R}^n$ satisfy $\|x\|_2 = 1$ and $xA = \lambda_1 x$:

$$\begin{aligned} 0 \leq \sum_{u,v} A_{u,v} (x(u) - x(v))^2 &= 2d \sum_v x(v)^2 - 2 \sum_{u,v} x(u)x(v)A_{u,v} \\ &= 2d - 2xAx^T = 2d - 2\lambda_1 \end{aligned}$$

Connectivity and Eigenvectors

Theorem

Let A be the adjacency matrix of a d -regular graph. Then a) $\lambda_1 = d$, and b) $\lambda_2 = d$ iff graph is disconnected.

Proof.

- Part a): Let $x \in \mathbb{R}^n$ satisfy $\|x\|_2 = 1$ and $xA = \lambda_1 x$:

$$\begin{aligned} 0 \leq \sum_{u,v} A_{u,v} (x(u) - x(v))^2 &= 2d \sum_v x(v)^2 - 2 \sum_{u,v} x(u)x(v)A_{u,v} \\ &= 2d - 2xAx^T = 2d - 2\lambda_1 \end{aligned}$$

- Hence $d \geq \lambda_1$ and therefore $d = \lambda_1$ since $\lambda_1 \geq d$

Connectivity and Eigenvectors

Theorem

Let A be the adjacency matrix of a d -regular graph. Then a) $\lambda_1 = d$, and b) $\lambda_2 = d$ iff graph is disconnected.

Proof.

- Part a): Let $x \in \mathbb{R}^n$ satisfy $\|x\|_2 = 1$ and $xA = \lambda_1 x$:

$$\begin{aligned} 0 \leq \sum_{u,v} A_{u,v} (x(u) - x(v))^2 &= 2d \sum_v x(v)^2 - 2 \sum_{u,v} x(u)x(v)A_{u,v} \\ &= 2d - 2xAx^T = 2d - 2\lambda_1 \end{aligned}$$

- Hence $d \geq \lambda_1$ and therefore $d = \lambda_1$ since $\lambda_1 \geq d$
- Part b): Let $\lambda_2 = d$ and $e_2 \perp e_1 = (1, \dots, 1)/\sqrt{n}$:

$$0 \leq \sum_{u,v} A_{u,v} (e_2(u) - e_2(v))^2 = 2d - 2\lambda_2$$

Connectivity and Eigenvectors

Theorem

Let A be the adjacency matrix of a d -regular graph. Then a) $\lambda_1 = d$, and b) $\lambda_2 = d$ iff graph is disconnected.

Proof.

- Part a): Let $x \in \mathbb{R}^n$ satisfy $\|x\|_2 = 1$ and $xA = \lambda_1 x$:

$$\begin{aligned} 0 \leq \sum_{u,v} A_{u,v} (x(u) - x(v))^2 &= 2d \sum_v x(v)^2 - 2 \sum_{u,v} x(u)x(v)A_{u,v} \\ &= 2d - 2xAx^T = 2d - 2\lambda_1 \end{aligned}$$

- Hence $d \geq \lambda_1$ and therefore $d = \lambda_1$ since $\lambda_1 \geq d$
► Part b): Let $\lambda_2 = d$ and $e_2 \perp e_1 = (1, \dots, 1)/\sqrt{n}$:

$$0 \leq \sum_{u,v} A_{u,v} (e_2(u) - e_2(v))^2 = 2d - 2\lambda_2$$

- $e_2(u) = e_2(v)$ for all u, v if graph connected so $e_2 \not\perp e_1$

Proof Continued

- ▶ Part b) other direction: Suppose G is disconnected and S , $V \setminus S$ is partition of graph.

Proof Continued

- ▶ Part b) other direction: Suppose G is disconnected and S , $V \setminus S$ is partition of graph.
- ▶ Let $p = |S|/|V|$ and $q = |V \setminus S|/|V|$ and define

$$x(v) = \begin{cases} q & \text{if } v \in S \\ -p & \text{if } v \notin S \end{cases}$$

Proof Continued

- ▶ Part b) other direction: Suppose G is disconnected and $S, V \setminus S$ is partition of graph.
- ▶ Let $p = |S|/|V|$ and $q = |V \setminus S|/|V|$ and define

$$x(v) = \begin{cases} q & \text{if } v \in S \\ -p & \text{if } v \notin S \end{cases}$$

- ▶ $x \perp e_1$ since

$$x \cdot e_1 = n^{-.5} \sum_v x(v) = n^{-.5}(q|S| - p|V \setminus S|) = n^{-.5}(qp n - pq n) = 0$$

Proof Continued

- ▶ Part b) other direction: Suppose G is disconnected and S , $V \setminus S$ is partition of graph.
- ▶ Let $p = |S|/|V|$ and $q = |V \setminus S|/|V|$ and define

$$x(v) = \begin{cases} q & \text{if } v \in S \\ -p & \text{if } v \notin S \end{cases}$$

- ▶ $x \perp e_1$ since

$$x \cdot e_1 = n^{-.5} \sum_v x(v) = n^{-.5}(q|S| - p|V \setminus S|) = n^{-.5}(qp n - pq n) = 0$$

- ▶ But x also has eigenvalue d : $xM = dx$

Outline

Probability Amplification with Two Point Sampling

Probability Amplification with Expanding Graphs

Probability Amplification with Random Walks on Expanders

Bonus Section! Connectivity and Eigenvectors

Readings

Readings

For next time, please make sure you've read:

- ▶ Chapter 3.4, 5.3 [MR].
- ▶ Chapter 6 [MR] and 11.1, 11.2 from [MU]