CS5275 – The Algorithm Designer's Toolkit (S2 AY2025/26)

Lecture 8:

Expanders – Ramanujan graphs

Quasirandomness

- **Observation:**
  - For n-vertex d-regular graphs, the following two statements are equivalent.

For any cut $(S, V \setminus S)$, we have:

$$|E(S, V \setminus S)| \in \Theta\left(\frac{d}{n} \cdot |S||V \setminus S|\right)$$

$G = (V, E)$ is an $\Omega(1)$-expander.

Quasirandomness

- **Observation:**
  - For n-vertex d-regular graphs, the following two statements are equivalent.

For any cut $(S, V \setminus S)$, we have:

$$|E(S, V \setminus S)| \in \Theta\left(\frac{d}{n} \cdot |S||V \setminus S|\right)$$

This is the expected number of edges in $E(S, V \setminus S)$ if G is a random n-vertex d-regular graph.

$G = (V, E)$ is an $\Omega(1)$-expander.

This can be seen as a **quasirandomness** property.

Quasirandomness

- **Observation:**
  - For n-vertex d-regular graphs, the following two statements are equivalent.

For any cut $(S, V \setminus S)$, we have:

$$|E(S, V \setminus S)| \in \Theta\left(\frac{d}{n} \cdot |S||V \setminus S|\right)$$

$G = (V, E)$ is an $\Omega(1)$-expander.

This is the expected number of edges in $E(S, V \setminus S)$ if G is a random n-vertex d-regular graph.

This can be seen as a **quasirandomness** property.

Question: Can we extend this to $E(S, T)$ for any two subsets $S \subseteq V$ and $T \subseteq V$?

Notation

- For simplicity, we restrict ourselves to n-vertex d-regular graphs.

$e(A,B) = |(a,b) \in A \times B : \{a,b\} \in E|$

- This is the number of edges between A and B.
- If $\{u,v\} \in E$ satisfies $\{u,v\} \subseteq A \cap B$, then $\{u,v\}$ is counted twice.

$\sigma_2 = \max\{|\lambda_2|, |\lambda_3|, \dots, |\lambda_n|\}$,

- where $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq -d$ are the eigenvalues of the adjacency matrix $\boldsymbol{A}$.

Expander mixing lemma

- For simplicity, we restrict ourselves to n-vertex d-regular graphs.

$e(A,B) = |(a,b) \in A \times B : \{a,b\} \in E|$

- This is the number of edges between A and B.
- If $\{u,v\} \in E$ satisfies $\{u,v\} \subseteq A \cap B$, then $\{u,v\}$ is counted twice.

$\sigma_2 = \max\{|\lambda_2|, |\lambda_3|, \dots, |\lambda_n|\}$,

- where $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq -d$ are the eigenvalues of the adjacency matrix $\boldsymbol{A}$.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

The number of edges between S and T is close to the expected number of edges between them in a random d-regular graph.

Proof of the lemma

- $e(S,T) = \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T$
- $|S||T| = \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T$, where $\boldsymbol{J}$ is the all-1 $(n \times n)$ matrix.

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| = \left| \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T - \frac{d}{n} \cdot \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T \right| = \left| \mathbf{1}_S^\top \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right|$$

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Proof of the lemma

- $e(S,T) = \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T$
- $|S||T| = \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T$, where $\boldsymbol{J}$ is the all-1 $(n \times n)$ matrix.

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| = \left| \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T - \frac{d}{n} \cdot \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T \right| = \left| \mathbf{1}_S^\top \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right|$$

$$\leq \|\mathbf{1}_S\| \cdot \left\| \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right\|$$

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Eigenvalues

Eigenvectors	$\boldsymbol{A}$	$\frac{d}{n}\boldsymbol{J}$	$\boldsymbol{A} - \frac{d}{n}\boldsymbol{J}$
$\boldsymbol{v}_1 = \frac{1}{\sqrt{n}}\mathbf{1}$	$\lambda_1 = d$	d	0
$\boldsymbol{v}_2$	λ_2	0	λ_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\boldsymbol{v}_n$	λ_n	0	λ_n

Proof of the lemma

- $e(S,T) = \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T$
- $|S||T| = \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T$, where $\boldsymbol{J}$ is the all-1 $(n \times n)$ matrix.

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| = \left| \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T - \frac{d}{n} \cdot \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T \right| = \left| \mathbf{1}_S^\top \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right|$$

$$\leq \|\mathbf{1}_S\| \cdot \left\| \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right\| \leq \|\mathbf{1}_S\| \cdot \sigma_2 \cdot \|\mathbf{1}_T\|$$

$$\left\| \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right\| = \left\| \sum_{i=2}^{n} \lambda_i \langle \mathbf{1}_T, \boldsymbol{v}_i \rangle \boldsymbol{v}_i \right\|$$

$$= \sqrt{\sum_{i=2}^{n} \lambda_i^2 \langle \mathbf{1}_T, \boldsymbol{v}_i \rangle^2} \leq \sigma_2 \cdot \sqrt{\sum_{i=2}^{n} \langle \mathbf{1}_T, \boldsymbol{v}_i \rangle^2} \leq \sigma_2 \cdot \|\mathbf{1}_T\|$$

$$\sigma_2 = \max\{|\lambda_2|, |\lambda_3|, \dots, |\lambda_n|\}$$

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Eigenvalues

Eigenvectors	$\boldsymbol{A}$	$\frac{d}{n}\boldsymbol{J}$	$\boldsymbol{A} - \frac{d}{n}\boldsymbol{J}$
$\boldsymbol{v}_1 = \frac{1}{\sqrt{n}}\mathbf{1}$	$\lambda_1 = d$	d	0
$\boldsymbol{v}_2$	λ_2	0	λ_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\boldsymbol{v}_n$	λ_n	0	λ_n

Proof of the lemma

- $e(S,T) = \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T$
- $|S||T| = \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T$, where $\boldsymbol{J}$ is the all-1 $(n \times n)$ matrix.

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| = \left| \mathbf{1}_S^\top \boldsymbol{A} \mathbf{1}_T - \frac{d}{n} \cdot \mathbf{1}_S^\top \boldsymbol{J} \mathbf{1}_T \right| = \left| \mathbf{1}_S^\top \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right|$$

$$\leq \|\mathbf{1}_S\| \cdot \left\| \left(\boldsymbol{A} - \frac{d}{n} \boldsymbol{J} \right) \mathbf{1}_T \right\| \leq \|\mathbf{1}_S\| \cdot \sigma_2 \cdot \|\mathbf{1}_T\| = \sigma_2 \cdot \sqrt{|S||T|}$$

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs

- How small σ_2 can be?
  - **Answer:** $2\sqrt{d-1}$

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs

- How small σ_2 can be?
  - **Answer:** $2\sqrt{d-1}$

Alon–Boppana bound: For every d and $\epsilon > 0$, there exists n_0 such that all graphs with $\geq n_0$ vertices have $\sigma_2 > 2\sqrt{d-1} - \epsilon$.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs

- How small σ_2 can be?
  - **Answer:** $2\sqrt{d-1}$

Alon–Boppana bound: For every d and $\epsilon > 0$, there exists n_0 such that all graphs with $\geq n_0$ vertices have $\sigma_2 > 2\sqrt{d-1} - \epsilon$.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Proof of a weaker bound:

$\sigma_2 \in \Omega\left(\sqrt{d}\right)$ when $d \leq 0.99 \cdot n$

$$\mathrm{tr}(\boldsymbol{A}^2) = nd$$

The trace of a matrix is the sum of its diagonal entries and equals the sum of its eigenvalues.

$$\mathrm{tr}(\boldsymbol{A}^2) = \sum_{i=1}^{n} \lambda_i^2 \leq d^2 + (n-1)\sigma_2^2$$

$$\sigma_2 \geq \sqrt{\frac{nd - d^2}{n-1}} \in \Omega\left(\sqrt{d}\right)$$

Ramanujan graphs

The name comes from the Ramanujan–Petersson conjecture, which was used in a construction of some of these graphs.

- How small σ_2 can be?
  - **Answer:** $2\sqrt{d-1}$

The graphs with $\sigma_2 \leq 2\sqrt{d-1}$ are called **Ramanujan graphs**.

Alon–Boppana bound: For every d and $\epsilon > 0$, there exists n_0 such that all graphs with $\geq n_0$ vertices have $\sigma_2 > 2\sqrt{d-1} - \epsilon$.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs

The name comes from the Ramanujan–Petersson conjecture, which was used in a construction of some of these graphs.

- How small σ_2 can be?
  - **Answer:** $2\sqrt{d-1}$

The graphs with $\sigma_2 \le 2\sqrt{d-1}$ are called **Ramanujan graphs**.

Alon–Boppana bound: For every d and $\epsilon > 0$, there exists n_0 such that all graphs with $\ge n_0$ vertices have $\sigma_2 > 2\sqrt{d-1} - \epsilon$.

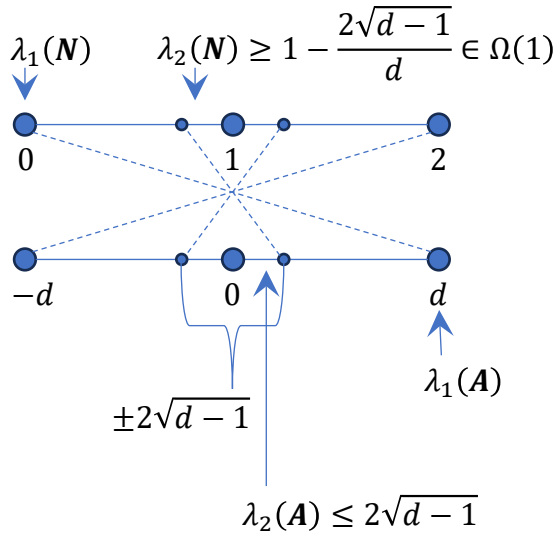
Ramanujan graphs are $\Omega(1)$-expanders.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \le \sigma_2 \cdot \sqrt{|S||T|}$$

Eigenvalues of $\boldsymbol{N}$:

Eigenvalues of $\boldsymbol{A}$:



$$\boldsymbol{N} = \boldsymbol{I} - \frac{1}{d}\boldsymbol{A}$$

Ramanujan graphs

The name comes from the Ramanujan–Petersson conjecture, which was used in a construction of some of these graphs.

- How small σ_2 can be?
  - **Answer:** $2\sqrt{d-1}$

The graphs with $\sigma_2 \leq 2\sqrt{d-1}$ are called **Ramanujan graphs**.

Alon–Boppana bound: For every d and $\epsilon > 0$, there exists n_0 such that all graphs with $\geq n_0$ vertices have $\sigma_2 > 2\sqrt{d-1} - \epsilon$.

Ramanujan graphs are $\Omega(1)$-expanders.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Some $\Omega(1)$-expanders are not Ramanujan.

$\sigma_2 = d$ for any bipartite graph.

Random graphs are nearly Ramanujan

- For every d and $\epsilon > 0$, the probability that a random d-regular graph satisfies $\sigma_2 < 2\sqrt{d-1} + \epsilon$ tends to 1 as $n \to \infty$.

  - Joel Friedman (Duke Mathematical Journal, 2003)

Algebraic constructions

- There is an infinite family of d-regular Ramanujan graphs, whenever $d-1$ is a prime power.

  - Alexander Lubotzky, Ralph Phillips, and Peter Sarnak (Combinatorica, 1988)
  - Moshe Morgenstern (Journal of Combinatorial Theory, Series B, 1994).

Algebraic constructions

- There is an infinite family of d-regular Ramanujan graphs, whenever $d-1$ is a prime power.

- Alexander Lubotzky, Ralph Phillips, and Peter Sarnak (Combinatorica, 1988)
- Moshe Morgenstern (Journal of Combinatorial Theory, Series B, 1994).

Open problem: Show this for all $d \geq 3$.

Algebraic constructions

- There is an infinite family of d-regular Ramanujan graphs, whenever $d-1$ is a prime power.

- Alexander Lubotzky, Ralph Phillips, and Peter Sarnak (Combinatorica, 1988)
- Moshe Morgenstern (Journal of Combinatorial Theory, Series B, 1994).

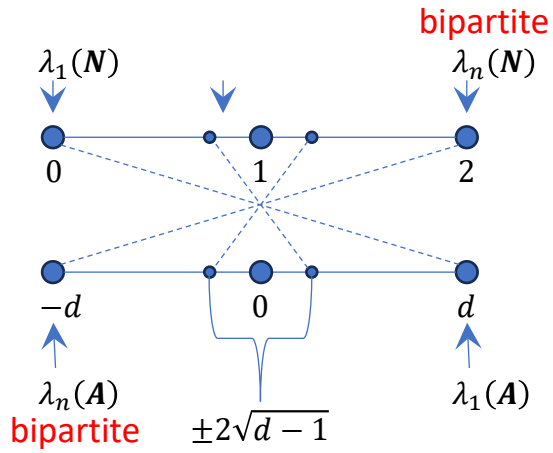
Open problem: Show this for all $d \geq 3$.

Solved for <u>bipartite</u> Ramanujan graphs:

$$\max\{|\lambda_2|, |\lambda_3|, \dots, |\lambda_{n-1}|\} \leq 2\sqrt{d-1}$$

Eigenvalues of $\boldsymbol{N}$:

Eigenvalues of $\boldsymbol{A}$:



- Adam Marcus, Daniel Spielman and Nikhil Srivastava (Annals of Mathematics, 2015)

Properties of Ramanujan graphs

- **Claim:** For any $S, T \subseteq V$, if $|S| \cdot |T| \cdot d \geq 4n^2$, then $e(S,T) > 0$.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs: $\sigma_2 \leq 2\sqrt{d-1}$

Properties of Ramanujan graphs

- **Claim:** For any $S, T \subseteq V$, if $|S| \cdot |T| \cdot d \geq 4n^2$, then $e(S,T) > 0$.

$$\sqrt{d|S||T|} \geq 2n$$

$$\downarrow$$

$$\frac{d}{n} \cdot |S||T| \geq 2\sqrt{d|S||T|} > \sigma_2 \cdot \sqrt{|S||T|}$$

$$\downarrow$$

$$e(S,T) \geq \frac{d}{n} \cdot |S||T| - \sigma_2 \cdot \sqrt{|S||T|} > 0$$

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs: $\sigma_2 \leq 2\sqrt{d-1}$

Properties of Ramanujan graphs

- **Claim:** For any $S, T \subseteq V$, if $|S| \cdot |T| \cdot d \geq 4n^2$, then $e(S,T) > 0$.

Exercise: The result is asymptotically the best possible.
- If you change $4n^2$ to ϵn^2 for some sufficiently small constant $\epsilon > 0$,
  - then this claim is false for every large enough d-regular graph.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs: $\sigma_2 \leq 2\sqrt{d-1}$

Properties of Ramanujan graphs

- **Claim:** For any $S, T \subseteq V$, if $|S| \cdot |T| \cdot d \geq 4n^2$, then $e(S,T) > 0$.

Corollary 1: Any independent set S has size $|S| < \frac{2n}{\sqrt{d}}$.

If $|S| \geq \frac{2n}{\sqrt{d}}$, then $|S|^2 d \geq 4n^2$, so $e(S,S) > 0$.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs: $\sigma_2 \leq 2\sqrt{d-1}$

Properties of Ramanujan graphs

- **Claim:** For any $S, T \subseteq V$, if $|S| \cdot |T| \cdot d \geq 4n^2$, then $e(S,T) > 0$.

Corollary 1: Any independent set S has size $|S| < \frac{2n}{\sqrt{d}}$.

Corollary 2: Chromatic number $> \frac{\sqrt{d}}{2}$.

If a proper coloring with $\leq \frac{\sqrt{d}}{2}$ colors exists, then $n < \frac{\sqrt{d}}{2} \cdot \frac{2n}{\sqrt{d}} = n$, which is impossible.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs: $\sigma_2 \leq 2\sqrt{d-1}$

Properties of Ramanujan graphs

- **Claim:** For any $S, T \subseteq V$, if $|S| \cdot |T| \cdot d \geq 4n^2$, then $e(S,T) > 0$.

Corollary 1: Any independent set S has size $|S| < \frac{2n}{\sqrt{d}}$.

Corollary 2: Chromatic number $> \frac{\sqrt{d}}{2}$.

These results have been used to give lower bounds on the number of communication rounds needed to compute certain colorings and independent sets in a distributed network.

Expander mixing lemma:

$$\left| e(S,T) - \frac{d}{n} \cdot |S||T| \right| \leq \sigma_2 \cdot \sqrt{|S||T|}$$

Ramanujan graphs: $\sigma_2 \leq 2\sqrt{d-1}$

- Marijke H.L. Bodlaender, Magnús M. Halldórsson, Christian Konrad, and Fabian Kuhn. "Brief announcement: Local independent set approximation." *Proceedings of the ACM Symposium on Principles of Distributed Computing* (PODC 2016).
- Nathan Linial. "Locality in distributed graph algorithms." *SIAM Journal on computing* (1992).

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.
- **Standard solution:** Repeat for $x = \left\lceil \log \frac{1}{f} \right\rceil$ times.

Probability of no success is $\frac{1}{2^x} \leq f$.

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.
- **Standard solution:** Repeat for $x = \left\lceil \log \frac{1}{f} \right\rceil$ times. ← This requires $rx = r\left\lceil \log \frac{1}{f} \right\rceil$ random bits.

Probability of no success is $\frac{1}{2^x} \leq f$.

Question: Is it possible to reduce the failure probability without using more than r random bits?

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

- Set $d = \left\lceil \frac{8}{f} \right\rceil$.
- Take a d-regular Ramanujan graph with $n = 2^r$ vertices.
  - Each vertex corresponds to an r-bit string.

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

- Set $d = \left\lceil \frac{8}{f} \right\rceil$.
- Take a d-regular Ramanujan graph with $n = 2^r$ vertices.
  - Each vertex corresponds to an r-bit string.
  - $S =$ the set of vertices that lead to a successful execution of the algorithm.
    - $|S| = \frac{n}{2}$.
  - $T =$ the set of vertices that do not have a neighbor in S.
    - $|S| \cdot |T| \cdot d < 4n^2 \rightarrow |T| < fn$.

Recall: For any $S, T \subseteq V$, if $|S| \cdot |T| \cdot d \geq 4n^2$, then $e(S,T) > 0$.

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

- Set $d = \left\lceil \frac{8}{f} \right\rceil$.
- Take a d-regular Ramanujan graph with $n = 2^r$ vertices.
  - Each vertex corresponds to an r-bit string.
  - $S =$ the set of vertices that lead to a successful execution of the algorithm.
    - $|S| = \frac{n}{2}$.
  - $T =$ the set of vertices that do not have a neighbor in S.
    - $|S| \cdot |T| \cdot d < 4n^2 \rightarrow |T| < fn$.
- Sample a vertex v uniformly at random, for each neighbor u of v, run the algorithm using the r-bit string of u.
  - Successful $\leftrightarrow v \notin T$
  - This happens with probability at least $1 - f$.

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

- Set $d = \left\lceil \frac{8}{f} \right\rceil$.
- Take a d-regular Ramanujan graph with $n = 2^r$ vertices.
  - Each vertex corresponds to an r-bit string.
  - $S =$ the set of vertices that lead to a successful execution of the algorithm.
    - $|S| = \frac{n}{2}$.
  - $T =$ the set of vertices that do not have a neighbor in S.
    - $|S| \cdot |T| \cdot d < 4n^2 \rightarrow |T| < fn$.
- Sample a vertex v uniformly at random, for each neighbor u of v, run the algorithm using the r-bit string of u.
  - Successful $\leftrightarrow v \notin T$
  - This happens with probability at least $1 - f$.

	Time	Random bits
Standard	$O\left(t \log \frac{1}{f}\right)$	$O\left(r \log \frac{1}{f}\right)$
Ramanujan	$O\left(\frac{t}{f}\right)$	r

Here we omit the cost for simulating a Ramanujan graph.

Success probability amplification

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

- Set $d = \left\lceil \frac{8}{f} \right\rceil$.
- Take a d-regular Ramanujan graph with $n = 2^r$ vertices.
  - Each vertex corresponds to an r-bit string.
  - $S =$ the set of vertices that lead to a successful execution of the algorithm.
    - $|S| = \frac{n}{2}$.
  - $T =$ the set of vertices that do not have a neighbor in S.
    - $|S| \cdot |T| \cdot d < 4n^2 \rightarrow |T| < f$.
- Sample a vertex v uniformly at random, for each neighbor u of v, run the algorithm using the r-bit string of u.
  - Successful $\leftrightarrow v \notin T$
  - This happens with probability at least $1 - f$.

	Time	Random bits
Standard	$O\left(t \log \frac{1}{f}\right)$	$O\left(r \log \frac{1}{f}\right)$
Ramanujan	$O\left(\frac{t}{f}\right)$	r
Next	$O\left(t \log \frac{1}{f}\right)$	$O\left(r + \log \frac{1}{f}\right)$

A Chernoff Bound for random walks

- Let $G = (V, E)$ be an n-vertex d-regular regular graph.
- Let $(v_1, v_2, \ldots, v_\ell)$ be an $(\ell - 1)$-step random walk starting from a uniformly random vertex.
- Let $f : V \to [0, 1]$ be a function.
- Let $\mu = \frac{1}{n}\sum_{v \in V} f(v)$.
- Let $\epsilon > 0$.

$$\Pr\left[\frac{1}{\ell}\sum_{i=1}^{\ell} f(v_i) \geq \mu + \epsilon + \frac{\sigma_2}{d}\right] \in e^{-\Omega(\epsilon^2 \ell)}$$

The proof is omitted.

A Chernoff Bound for random walks

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

- Let $G = (V, E)$ be an n-vertex d-regular regular graph.
- Let $(v_1, v_2, \dots, v_\ell)$ be an $(\ell - 1)$-step random walk starting from a uniformly random vertex.
- Let $f : V \to [0, 1]$ be a function.
- Let $\mu = \frac{1}{n}\sum_{v \in V} f(v)$.
- Let $\epsilon > 0$.

$$\Pr\left[\frac{1}{\ell}\sum_{i=1}^{\ell} f(v_i) \geq \mu + \epsilon + \frac{\sigma_2}{d}\right] \in e^{-\Omega(\epsilon^2 \ell)}$$

	Time	Random bits
Standard	$O\left(t \log\frac{1}{f}\right)$	$O\left(r \log\frac{1}{f}\right)$
Ramanujan	$O\left(\frac{t}{f}\right)$	r
Next	$O\left(t \log\frac{1}{f}\right)$	$O\left(r + \log\frac{1}{f}\right)$

New approach:

- Take $d \in O(1)$ and $n = 2^r$.
- Construct a random walk $(v_1, v_2, \dots, v_\ell)$ with $\ell \in O\left(\log\frac{1}{f}\right)$.
- Run the algorithm with these bit strings.

A Chernoff Bound for random walks

It uses r random bits and takes t time.

- Consider a randomized algorithm that succeeds with probability $\frac{1}{2}$.
- **Goal:** Amplify the success probability to $1 - f$.

$n = 2^r$ $\quad$ $d \in O(1)$ is large enough so that $\frac{\sigma_2}{d} \leq \frac{1}{8}$.

- Let $G = (V, E)$ be an n-vertex d-regular regular graph.
- Let $(v_1, v_2, \ldots, v_\ell)$ be an $(\ell - 1)$-step random walk starting from a uniformly random vertex.
- Let $f : V \to [0, 1]$ be a function. (0 : the algorithm succeeds. 1 : the algorithm fails.)
- Let $\mu = \frac{1}{n}\sum_{v \in V} f(v)$.
- Let $\epsilon > 0$.

$$\Pr\left[\frac{1}{\ell}\sum_{i=1}^{\ell} f(v_i) \geq \underbrace{\mu + \epsilon + \frac{\sigma_2}{d}}_{\leq \frac{3}{4}}\right] \in e^{-\Omega(\epsilon^2 \ell)}$$

($\mu \leq \frac{1}{2}$, $\epsilon \leq \frac{1}{8}$, $\frac{\sigma_2}{d} \leq \frac{1}{8}$)

$\ell \in O\left(\log \frac{1}{f}\right)$ is large enough so that the error probability $e^{-\Omega(\epsilon^2 \ell)}$ is at most f.

$\frac{1}{\ell}\sum_{i=1}^{\ell} f(v_i) < 1 \rightarrow$ some of $v_1, v_2, \ldots, v_\ell$ make the algorithm successful.

Further applications

- Ramanujan graphs can be used to construct error correcting codes.

  Michael Sipser and Daniel A. Spielman.
  “Expander codes.”
  IEEE transactions on Information Theory, 2002.

- Ramanujan graphs can be used to construct cryptographic hash functions.

  Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter.
  “Cryptographic hash functions from expander graphs.”
  Journal of Cryptology, 2009.

Outlook

- **Next:**
  - An interesting application of Ramanujan graphs for graph algorithm design.

for general graphs

References

- **Main reference:**
  - Lecture 5.1 of https://sites.google.com/site/thsaranurak/teaching/Expander
  - Chapter 21 of https://lucatrevisan.github.io/books/expanders-2016.pdf

- **Additional/optional reading:**
  - https://en.wikipedia.org/wiki/Expander_mixing_lemma
  - https://en.wikipedia.org/wiki/Ramanujan_graph
  - Shlomo Hoory, Nathan Linial, and Avi Wigderson. “Expander graphs and their applications.” *Bulletin of the American Mathematical Society* 43.4 (2006): 439-561.