Expander graphs and their applications

Michał Pilipczuk

September 26^{th}, 2013

Part I:
Expansion and the spectral gap

Boundaries

- **Expanders** are graphs that have good expansion properties.

Boundaries

- **Expanders** are graphs that have good expansion properties.
- We need a way to measure expansion.

Boundaries

- **Expanders** are graphs that have good expansion properties.
- We need a way to measure expansion.
- Consider some subset $S \subseteq V(G)$; we want to measure the *boundary* of S.

Boundaries

- **Expanders** are graphs that have good expansion properties.
- We need a way to measure expansion.
- Consider some subset $S \subseteq V(G)$; we want to measure the *boundary* of S.
- **Edge boundary**: $E(S, \overline{S})$ $\qquad\qquad$ $(\overline{S} = V(G) \setminus S)$

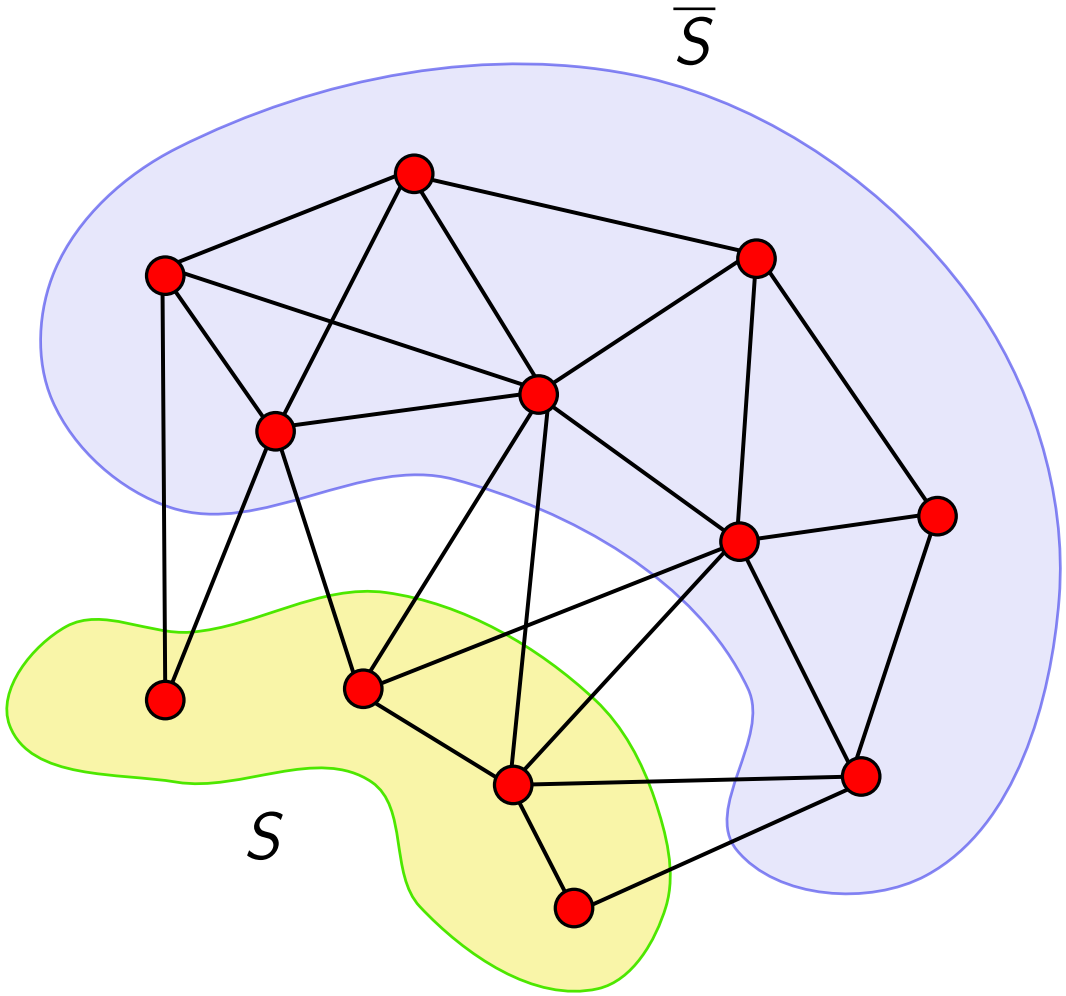
Boundaries

- **Expanders** are graphs that have good expansion properties.
- We need a way to measure expansion.
- Consider some subset $S \subseteq V(G)$; we want to measure the *boundary* of S.
- **Edge boundary**: $E(S, \overline{S})$ $\qquad\qquad$ $(\overline{S} = V(G) \setminus S)$
- **Vertex boundary**: $\Gamma(S) = \{v \mid uv \in E(G) \text{ for some } u \in S\}$

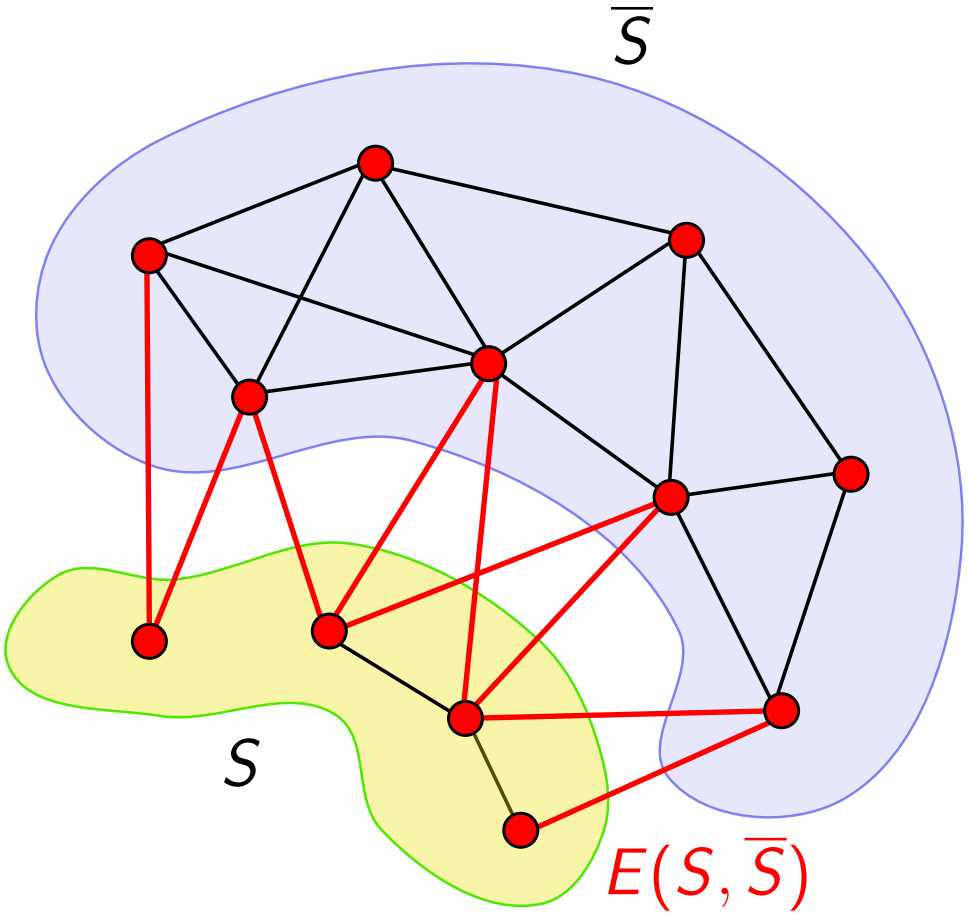
Boundaries

- **Expanders** are graphs that have good expansion properties.
- We need a way to measure expansion.
- Consider some subset $S \subseteq V(G)$; we want to measure the *boundary* of S.
- **Edge boundary**: $E(S, \overline{S})$ $\qquad\qquad$ $(\overline{S} = V(G) \setminus S)$
- **Vertex boundary**: $\Gamma(S) = \{v \mid uv \in E(G) \text{ for some } u \in S\}$
  - All vertices that can be reached within one step from S.

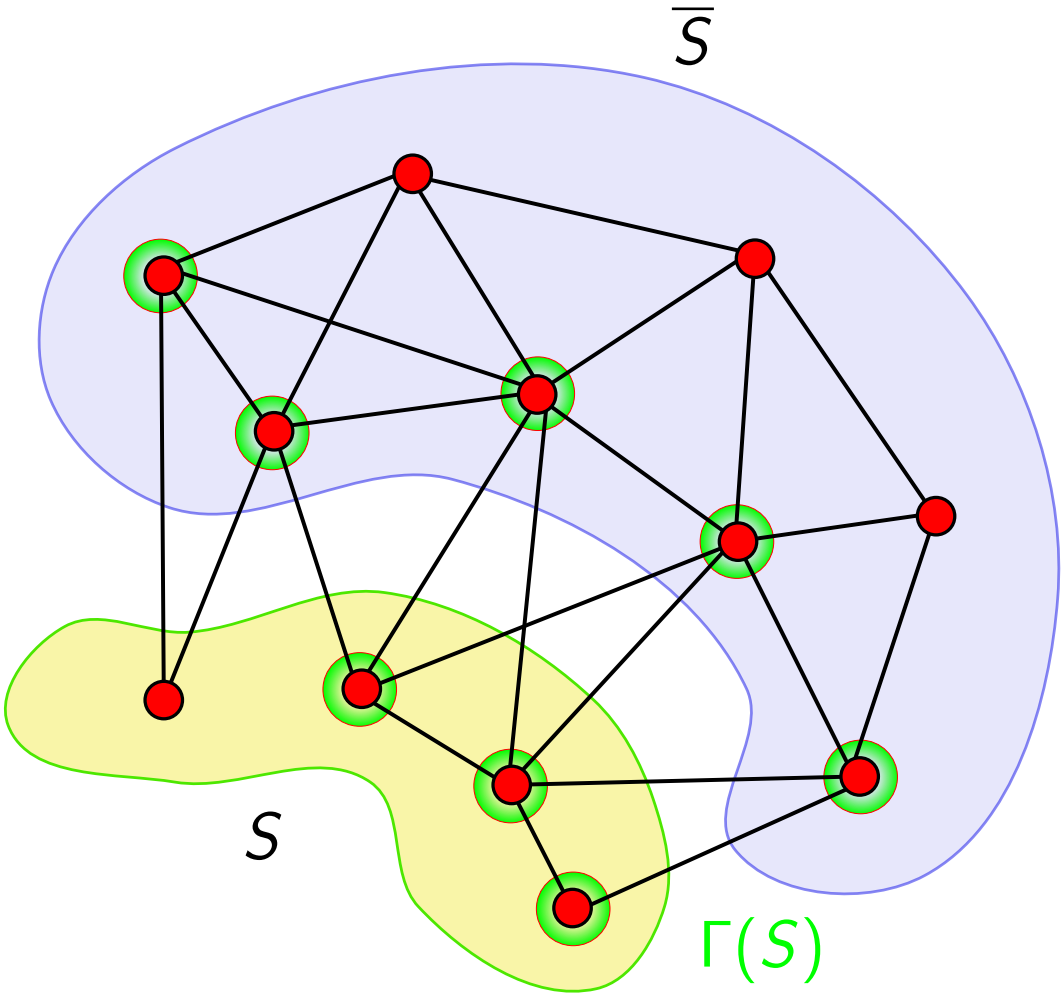
Expanding via edges and to vertices



Expanding via edges and to vertices



Expanding via edges and to vertices



Edge and vertex expansion

Edge expansion

Edge expansion of a graph G is defined as

$$h^E(G) = \min_{|S| \leq |V(G)|/2} \frac{|E(S, \overline{S})|}{|S|}.$$

Vertex expansion

Vertex expansion of a graph G is defined as

$$h^V(G) = \min_{|S| \leq |V(G)|/2} \frac{|\Gamma(S)| - |S|}{|S|}.$$

Edge and vertex expansion

Edge expansion

Edge expansion of a graph G is defined as

$$h^E(G) = \min_{|S| \leq |V(G)|/2} \frac{|E(S, \overline{S})|}{|S|}.$$

Vertex expansion

Vertex expansion of a graph G is defined as

$$h^V(G) = \min_{|S| \leq |V(G)|/2} \frac{|\Gamma(S)| - |S|}{|S|}.$$

- How to certify that a graph has a good expansion?

Adjacency matrix

- We will measure expansion by examining properties of the spectrum of the adjacency matrix of a graph.

Adjacency matrix

- We will measure expansion by examining properties of the spectrum of the adjacency matrix of a graph.
- We consider multigraphs with loops. Let $v_1, v_2, \ldots, v_n$ be an arbitrary ordering of $V(G)$.

Adjacency matrix

- We will measure expansion by examining properties of the spectrum of the adjacency matrix of a graph.
- We consider multigraphs with loops. Let $v_1, v_2, \ldots, v_n$ be an arbitrary ordering of $V(G)$.
- Adjacency matrix of a graph G is a matrix $A(G) = [a_{ij}]_{1 \leq i,j \leq n}$ such that a_{ij} is the number of edges between v_i and v_j.

Adjacency matrix

- We will measure expansion by examining properties of the spectrum of the adjacency matrix of a graph.
- We consider multigraphs with loops. Let $v_1, v_2, \ldots, v_n$ be an arbitrary ordering of $V(G)$.
- Adjacency matrix of a graph G is a matrix $A(G) = [a_{ij}]_{1 \leq i,j \leq n}$ such that a_{ij} is the number of edges between v_i and v_j.
- **Note**: $A(G)$ is a symmetric real matrix.

Eigenvectors and eigenvalues

- **Fact**: Any symmetric real matrix A has an orthonormal basis of eigenvectors.

Eigenvectors and eigenvalues

- **Fact**: Any symmetric real matrix A has an orthonormal basis of eigenvectors.
- In other words, one can find vectors $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$ and values $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ such that:

Eigenvectors and eigenvalues

- **Fact**: Any symmetric real matrix A has an orthonormal basis of eigenvectors.
- In other words, one can find vectors $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$ and values $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ such that:
  - $||e_i|| = 1$ and $\langle e_i, e_j \rangle = 0$ for $i \neq j$;

Eigenvectors and eigenvalues

- **Fact**: Any symmetric real matrix A has an orthonormal basis of eigenvectors.
- In other words, one can find vectors $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$ and values $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ such that:
  - $||e_i|| = 1$ and $\langle e_i, e_j \rangle = 0$ for $i \neq j$;
  - $Ae_i = \lambda_i \cdot e_i$

Eigenvectors and eigenvalues

- **Fact**: Any symmetric real matrix A has an orthonormal basis of eigenvectors.
- In other words, one can find vectors $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$ and values $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ such that:
  - $||e_i|| = 1$ and $\langle e_i, e_j \rangle = 0$ for $i \neq j$;
  - $Ae_i = \lambda_i \cdot e_i$
  - **Hence**: $A(b_1 e_1 + \ldots + b_n e_n) = (\lambda_1 b_1)e_1 + \ldots + (\lambda_n b_n)e_n$.

Eigenvectors and eigenvalues

- **Fact**: Any symmetric real matrix A has an orthonormal basis of eigenvectors.
- In other words, one can find vectors $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$ and values $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ such that:
  - $||e_i|| = 1$ and $\langle e_i, e_j \rangle = 0$ for $i \neq j$;
  - $Ae_i = \lambda_i \cdot e_i$
  - **Hence**: $A(b_1 e_1 + \ldots + b_n e_n) = (\lambda_1 b_1)e_1 + \ldots + (\lambda_n b_n)e_n$.
- Multiset $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ is called the **spectrum** of A (denoted $\sigma(A)$).

Spectrum of a d-regular graph

- From now on, (almost) all the considered graphs will be d-regular for some constant d.

Spectrum of a d-regular graph

- From now on, (almost) all the considered graphs will be d-regular for some constant d.
- Let G be a d-regular graph with adjacency matrix $A(G)$.

Spectrum of a d-regular graph

- From now on, (almost) all the considered graphs will be d-regular for some constant d.
- Let G be a d-regular graph with adjacency matrix $A(G)$.
- Let $\mathbf{1} = (1, 1, \ldots, 1)$. Then $A\mathbf{1} = d \cdot \mathbf{1}$ since the graph is d-regular.

Spectrum of a d-regular graph

- From now on, (almost) all the considered graphs will be d-regular for some constant d.
- Let G be a d-regular graph with adjacency matrix $A(G)$.
- Let $\mathbf{1} = (1, 1, \ldots, 1)$. Then $A\mathbf{1} = d \cdot \mathbf{1}$ since the graph is d-regular.
- We have one eigenvector: $\frac{1}{\sqrt{n}} \cdot \mathbf{1}$, with eigenvalue d.

Spectrum of a d-regular graph

- Let us examine $u = e_i$ in the standard basis, and let $||u||_1 = \sum_{j=1}^{n} |u_j|$.

Spectrum of a d-regular graph

- Let us examine $u = e_i$ in the standard basis, and let $||u||_1 = \sum_{j=1}^{n} |u_j|$.

$$
\begin{aligned}
|\lambda_i| \cdot ||u||_1 &= ||Au||_1 = \sum_{j=1}^{n} \left| \sum_{k=1}^{n} a_{jk} u_k \right| \\
&\leq \sum_{j=1}^{n} \sum_{k=1}^{n} |a_{jk}| \cdot |u_k| = \sum_{k=1}^{n} \sum_{j=1}^{n} |a_{jk}| \cdot |u_k| \\
&= \sum_{k=1}^{n} |u_k| \cdot \sum_{j=1}^{n} |a_{jk}| = \sum_{k=1}^{n} |u_k| \cdot d = d \cdot ||u||_1
\end{aligned}
$$

Spectrum of a d-regular graph

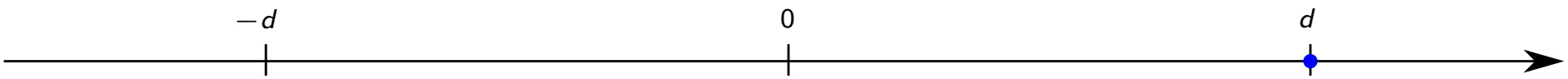
- Let us examine $u = e_i$ in the standard basis, and let $||u||_1 = \sum_{j=1}^{n} |u_j|$.

$$\begin{aligned} |\lambda_i| \cdot ||u||_1 &= ||Au||_1 = \sum_{j=1}^{n} \left| \sum_{k=1}^{n} a_{jk} u_k \right| \\ &\leq \sum_{j=1}^{n} \sum_{k=1}^{n} |a_{jk}| \cdot |u_k| = \sum_{k=1}^{n} \sum_{j=1}^{n} |a_{jk}| \cdot |u_k| \\ &= \sum_{k=1}^{n} |u_k| \cdot \sum_{j=1}^{n} |a_{jk}| = \sum_{k=1}^{n} |u_k| \cdot d = d \cdot ||u||_1 \end{aligned}$$

- Ergo $|\lambda_i| \leq d$ for all i, and $\lambda_1 = d$.

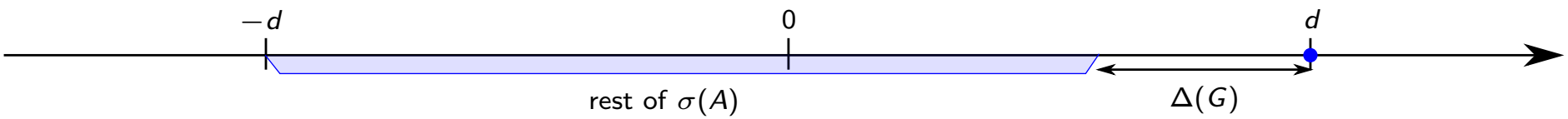
Spectral gap

- Spectral gaps: lower eigenvalues are separated from $\lambda_1 = d$.



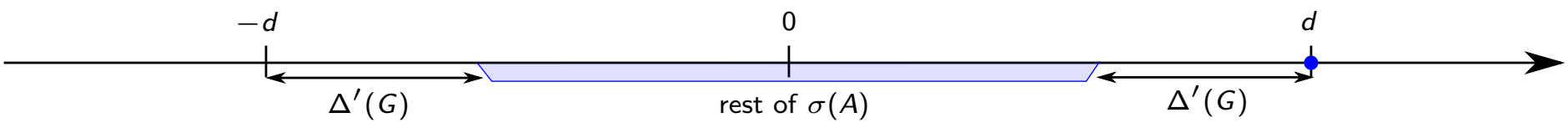
Spectral gap

- Spectral gaps: lower eigenvalues are separated from $\lambda_1 = d$.
- **Spectral gap**: $\Delta(G) = d - \lambda_2$.



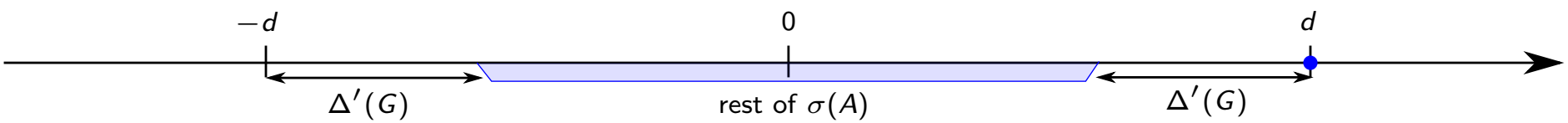
Spectral gap

- Spectral gaps: lower eigenvalues are separated from $\lambda_1 = d$.
- **Spectral gap**: $\Delta(G) = d - \lambda_2$.
- **Absolute spectral gap**: $\Delta'(G) = d - \max(|\lambda_2|, |\lambda_n|)$.



Spectral gap

- Spectral gaps: lower eigenvalues are separated from $\lambda_1 = d$.
- **Spectral gap**: $\Delta(G) = d - \lambda_2$.
- **Absolute spectral gap**: $\Delta'(G) = d - \max(|\lambda_2|, |\lambda_n|)$.
- G is an (n, d, α)-**expander** if $|V(G)| = n$, G is d-regular, and $|\lambda_i| \leq \alpha \cdot d$ for all $i = 2, 3, \ldots, n$.



Cheeger's inequalities

$$\begin{array}{ccccc} \Delta(G)/2 & \leq & h^E(G) & \leq & \sqrt{2d\Delta(G)} \\ \frac{d^2-(d-\Delta'(G))^2}{d^2+(d-\Delta'(G))^2} & \leq & h^V(G) & \leq & d\sqrt{2}\sqrt{d^2-(d-\Delta'(G))^2} \end{array}$$

Cheeger's inequalities

$$\begin{array}{ccccc} \Delta(G)/2 & \leq & h^E(G) & \leq & \sqrt{2d\Delta(G)} \\ \frac{d^2-(d-\Delta'(G))^2}{d^2+(d-\Delta'(G))^2} & \leq & h^V(G) & \leq & d\sqrt{2}\sqrt{d^2-(d-\Delta'(G))^2} \end{array}$$

- To ensure good expansion it suffices to ensure good spectral gap, and vice versa.

Cheeger's inequalities

$$\begin{array}{ccccc} \Delta(G)/2 & \leq & h^E(G) & \leq & \sqrt{2d\Delta(G)} \\ \frac{d^2-(d-\Delta'(G))^2}{d^2+(d-\Delta'(G))^2} & \leq & h^V(G) & \leq & d\sqrt{2}\sqrt{d^2-(d-\Delta'(G))^2} \end{array}$$

- To ensure good expansion it suffices to ensure good spectral gap, and vice versa.
- Spectral properties are much easier to control.

Part II:
Random walks on expanders

Markov chains on graphs

- Let G be a d-regular multigraph.

Markov chains on graphs

- Let G be a d-regular multigraph.
- Consider the following Markov chain: we start in some vertex $v_1 \in V(G)$ and at each step we move along one of d edges incident to the current vertex, chosen uniformly at random.

Markov chains on graphs

- Let G be a d-regular multigraph.
- Consider the following Markov chain: we start in some vertex $v_1 \in V(G)$ and at each step we move along one of d edges incident to the current vertex, chosen uniformly at random.
- Let p^t be the vector of probabilities of being in vertices of G after t steps:

Markov chains on graphs

- Let G be a d-regular multigraph.
- Consider the following Markov chain: we start in some vertex $v_1 \in V(G)$ and at each step we move along one of d edges incident to the current vertex, chosen uniformly at random.
- Let p^t be the vector of probabilities of being in vertices of G after t steps:
  - $(p^t)_j = \mathbb{P}(\text{after } t \text{ steps we are in } v_j)$,

Markov chains on graphs

- Let G be a d-regular multigraph.
- Consider the following Markov chain: we start in some vertex $v_1 \in V(G)$ and at each step we move along one of d edges incident to the current vertex, chosen uniformly at random.
- Let p^t be the vector of probabilities of being in vertices of G after t steps:
  - $(p^t)_j = \mathbb{P}(\text{after } t \text{ steps we are in } v_j)$,
  - $p^0 = (1, 0, 0, \ldots, 0)$ in the standard basis,

Markov chains on graphs

- Let G be a d-regular multigraph.
- Consider the following Markov chain: we start in some vertex $v_1 \in V(G)$ and at each step we move along one of d edges incident to the current vertex, chosen uniformly at random.
- Let p^t be the vector of probabilities of being in vertices of G after t steps:
  - $(p^t)_j = \mathbb{P}(\text{after } t \text{ steps we are in } v_j)$,
  - $p^0 = (1, 0, 0, \ldots, 0)$ in the standard basis,
  - $(p^t)_j = \sum_i \frac{a_{ij}}{d} \cdot (p^{t-1})_i$.

Markov chains on graphs

- Let G be a d-regular multigraph.
- Consider the following Markov chain: we start in some vertex $v_1 \in V(G)$ and at each step we move along one of d edges incident to the current vertex, chosen uniformly at random.
- Let p^t be the vector of probabilities of being in vertices of G after t steps:
  - $(p^t)_j = \mathbb{P}(\text{after } t \text{ steps we are in } v_j)$,
  - $p^0 = (1, 0, 0, \ldots, 0)$ in the standard basis,
  - $(p^t)_j = \sum_i \frac{a_{ij}}{d} \cdot (p^{t-1})_i$.
  - Hence $p^t = \tilde{A}p^{t-1} = \tilde{A}^t p^0$, where $\tilde{A} = \frac{1}{d} \cdot A$.

Spectrum of $\tilde{A}$

- $\tilde{A} = \frac{1}{d} \cdot A$.

Spectrum of $\tilde{A}$

- $\tilde{A} = \frac{1}{d} \cdot A$.
- So $\tilde{A}$ has the same eigenvectors as A, with eigenvalues $\tilde{\lambda}_i = \frac{1}{d} \cdot \lambda_i$.

Spectrum of $\tilde{A}$

- $\tilde{A} = \frac{1}{d} \cdot A$.
- So $\tilde{A}$ has the same eigenvectors as A, with eigenvalues $\tilde{\lambda}_i = \frac{1}{d} \cdot \lambda_i$.
- If G is an (n, d, α)-expander, then $\tilde{\lambda}_1 = 1$ and $|\tilde{\lambda}_i| \leq \alpha$ for $i = 2, 3, \ldots, n$.

Iterating $\tilde{A}$

- Let $p^0 = (b_1, b_2, \ldots, b_n)$ in basis $(e_1, e_2, \ldots, e_n)$.
  Note that $e_1 = \frac{1}{\sqrt{n}} \cdot \mathbf{1}$, so $b_1 = \langle p^0, e_1 \rangle = \langle p^0, \frac{1}{\sqrt{n}} \cdot \mathbf{1} \rangle = \frac{1}{\sqrt{n}}$.

Iterating $\tilde{A}$

- Let $p^0 = (b_1, b_2, \ldots, b_n)$ in basis $(e_1, e_2, \ldots, e_n)$.
  Note that $e_1 = \frac{1}{\sqrt{n}} \cdot \mathbf{1}$, so $b_1 = \langle p^0, e_1 \rangle = \langle p^0, \frac{1}{\sqrt{n}} \cdot \mathbf{1} \rangle = \frac{1}{\sqrt{n}}$.
- Then $\tilde{A}^t p^0 = (b_1, \tilde{\lambda}_2^t \cdot b_2, \ldots, \tilde{\lambda}_n^t \cdot b_n)$.

Iterating $\tilde{A}$

- Let $p^0 = (b_1, b_2, \ldots, b_n)$ in basis $(e_1, e_2, \ldots, e_n)$.
  Note that $e_1 = \frac{1}{\sqrt{n}} \cdot \mathbf{1}$, so $b_1 = \langle p^0, e_1 \rangle = \langle p^0, \frac{1}{\sqrt{n}} \cdot \mathbf{1} \rangle = \frac{1}{\sqrt{n}}$.
- Then $\tilde{A}^t p^0 = (b_1, \tilde{\lambda}_2^t \cdot b_2, \ldots, \tilde{\lambda}_n^t \cdot b_n)$.
- So we get

$$\begin{aligned} ||\tilde{A}^t p^0 - b_1 e_1|| &= ||\tilde{\lambda}_2^t b_2 e_2 + \ldots + \tilde{\lambda}_n^t b_n e_n|| \\ &= \sqrt{\tilde{\lambda}_2^{2t} \cdot b_2^2 + \ldots + \tilde{\lambda}_n^{2t} \cdot b_n^2} \\ &\leq \alpha^t \cdot ||p^0|| = \alpha^t. \end{aligned}$$

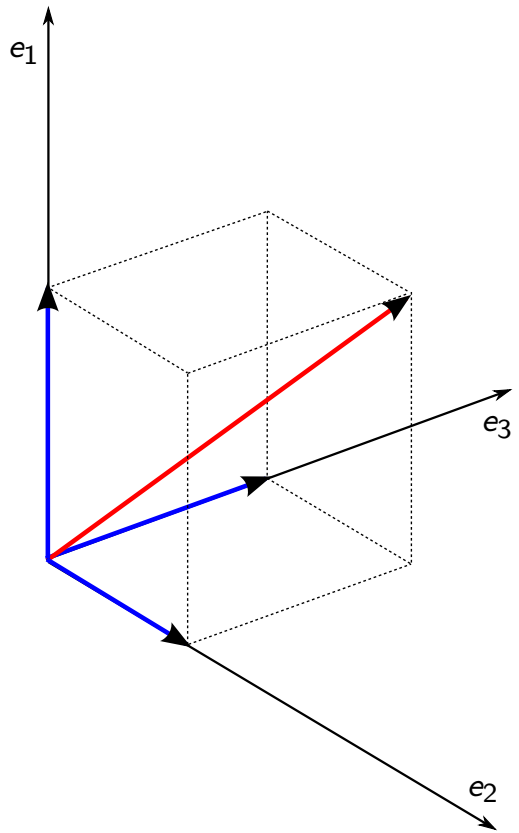
Iterating $\tilde{A}$

- Let $p^0 = (b_1, b_2, \ldots, b_n)$ in basis $(e_1, e_2, \ldots, e_n)$.
  Note that $e_1 = \frac{1}{\sqrt{n}} \cdot \mathbf{1}$, so $b_1 = \langle p^0, e_1 \rangle = \langle p^0, \frac{1}{\sqrt{n}} \cdot \mathbf{1} \rangle = \frac{1}{\sqrt{n}}$.
- Then $\tilde{A}^t p^0 = (b_1, \tilde{\lambda}_2^t \cdot b_2, \ldots, \tilde{\lambda}_n^t \cdot b_n)$.
- So we get

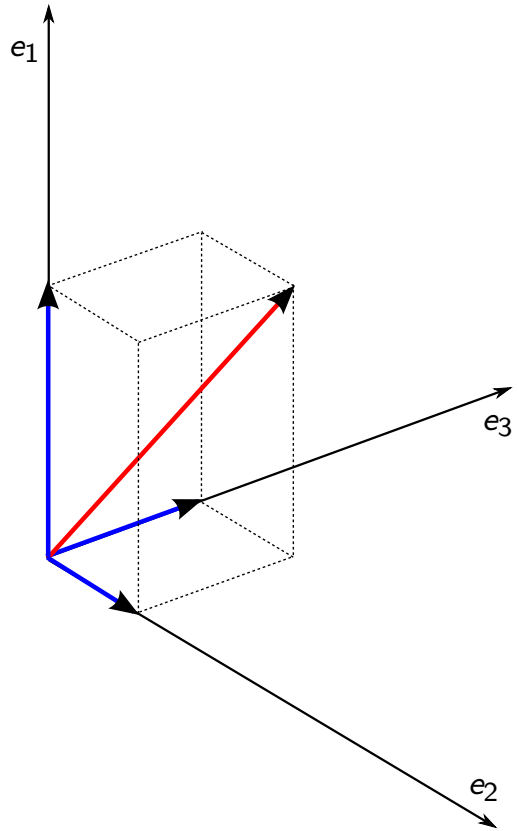
$$\begin{aligned} ||\tilde{A}^t p^0 - b_1 e_1|| &= ||\tilde{\lambda}_2^t b_2 e_2 + \ldots + \tilde{\lambda}_n^t b_n e_n|| \\ &= \sqrt{\tilde{\lambda}_2^{2t} \cdot b_2^2 + \ldots + \tilde{\lambda}_n^{2t} \cdot b_n^2} \\ &\leq \alpha^t \cdot ||p^0|| = \alpha^t. \end{aligned}$$

- **Note**: $b_1 e_1 = \frac{1}{n} \cdot \mathbf{1}$, so p^t converges to uniform distribution exponentially fast.

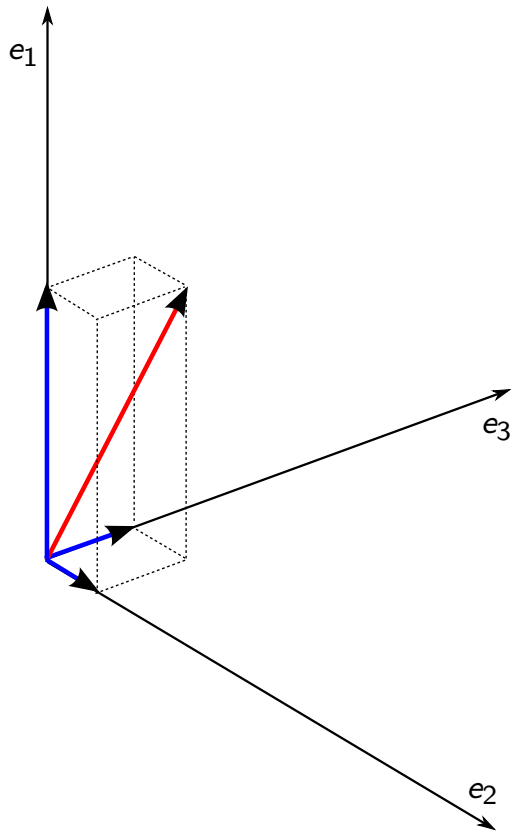
The proof on the picture



The proof on the picture



The proof on the picture



What does it mean?

- **Iterating $\tilde{A}$ extinguishes non-main coefficients.**

What does it mean?

- **Iterating $\tilde{A}$ extinguishes non-main coefficients.**
- Random walk on an expander converges to the uniform distribution $\frac{1}{n} \cdot \mathbf{1}$ exponentially quickly.

What does it mean?

- **Iterating $\tilde{A}$ extinguishes non-main coefficients.**
- Random walk on an expander converges to the uniform distribution $\frac{1}{n} \cdot \mathbf{1}$ exponentially quickly.
  - We say that random walks are *rapidly mixing*.

What does it mean?

- **Iterating $\tilde{A}$ extinguishes non-main coefficients.**
- Random walk on an expander converges to the uniform distribution $\frac{1}{n} \cdot \mathbf{1}$ exponentially quickly.
  - We say that random walks are *rapidly mixing*.
- **Corollary**: an (n, d, α)-expander has diameter $\mathcal{O}(\log n)$.

Application: sampling via expander walks

- Given: universe U, $|U| = n$, and a *bad* subset $B \subseteq U$ of size βn.

Application: sampling via expander walks

- Given: universe U, $|U| = n$, and a *bad* subset $B \subseteq U$ of size βn.
- We want to sample elements of the universe to get at least one *good* element.

Application: sampling via expander walks

- Given: universe U, $|U| = n$, and a *bad* subset $B \subseteq U$ of size βn.
- We want to sample elements of the universe to get at least one *good* element.
- Sample t elements uniformly at random: $\mathbb{P}(\text{all bad}) = \beta^t$, and $t \log n$ random bits used.

Application: sampling via expander walks

- Given: universe U, $|U| = n$, and a *bad* subset $B \subseteq U$ of size βn.
- We want to sample elements of the universe to get at least one *good* element.
- Sample t elements uniformly at random: $\mathbb{P}(\text{all bad}) = \beta^t$, and $t \log n$ random bits used.
- **Idea**: since random walks on expanders mix rapidly, maybe we can improve by taking a random walk on some constant-degree expander?

Application: sampling via expander walks

- Given: universe U, $|U| = n$, and a *bad* subset $B \subseteq U$ of size βn.
- We want to sample elements of the universe to get at least one *good* element.
- Sample t elements uniformly at random: $\mathbb{P}(\text{all bad}) = \beta^t$, and $t \log n$ random bits used.
- **Idea**: since random walks on expanders mix rapidly, maybe we can improve by taking a random walk on some constant-degree expander?
- Sample one element u, and perform a random walk of length t from u to collect t samples.

Application: sampling via expander walks

Random sampling of expander walks

Assume that G is a (n, d, α)-expander for some constants d, α, and $B \subseteq V(G)$ is a vertex subset of size βn. Then the probability that a random walk of length t from a vertex chosen uniformly at random is entirely contained in B, is at most $(\beta + \alpha)^t$.

Application: sampling via expander walks

Random sampling of expander walks

Assume that G is a (n, d, α)-expander for some constants d, α, and $B \subseteq V(G)$ is a vertex subset of size βn. Then the probability that a random walk of length t from a vertex chosen uniformly at random is entirely contained in B, is at most $(\beta + \alpha)^t$.

- Sample a random walk of length t from a randomly chosen vertex: $\mathbb{P}(\text{all bad}) \leq (\beta + \alpha)^t$, but for constant d we use only $\log n + \mathcal{O}(t \log d) = \log n + \mathcal{O}(t)$ random bits.

Application: reducing randomness for **RP**

- Assume $\mathcal{A}$ is a one-sided error algorithm:
  on a NO-instance it always says NO, but on a YES-instance it says YES with probability $\geq \frac{1}{2}$.

Application: reducing randomness for **RP**

- Assume $\mathcal{A}$ is a one-sided error algorithm:
  on a NO-instance it always says NO, but on a YES-instance it says YES with probability $\geq \frac{1}{2}$.
- Let r be the number of random bits used by the algorithm. We would like to reduce the error probability to $\leq \frac{1}{n}$.

Application: reducing randomness for **RP**

- Assume $\mathcal{A}$ is a one-sided error algorithm:
  on a NO-instance it always says NO, but on a YES-instance it says YES with probability $\geq \frac{1}{2}$.
- Let r be the number of random bits used by the algorithm. We would like to reduce the error probability to $\leq \frac{1}{n}$.
- **Strategy 1**: $\log n$ independent repetitions, $r \log n$ random bits.

Application: reducing randomness for **RP**

- Assume $\mathcal{A}$ is a one-sided error algorithm:
  on a NO-instance it always says NO, but on a YES-instance it says YES with probability $\geq \frac{1}{2}$.
- Let r be the number of random bits used by the algorithm. We would like to reduce the error probability to $\leq \frac{1}{n}$.
- **Strategy 1**: $\log n$ independent repetitions, $r \log n$ random bits.
- **Strategy 2**: random walk of length $(1+\varepsilon)\log n$ on an arbitrary $(2^r, d, \alpha)$-expander constructed on the set of all possible bit sequences given to the algorithm.

Application: reducing randomness for **RP**

- Assume $\mathcal{A}$ is a one-sided error algorithm:
  on a NO-instance it always says NO, but on a YES-instance it says YES with probability $\geq \frac{1}{2}$.
- Let r be the number of random bits used by the algorithm. We would like to reduce the error probability to $\leq \frac{1}{n}$.
- **Strategy 1**: $\log n$ independent repetitions, $r \log n$ random bits.
- **Strategy 2**: random walk of length $(1+\varepsilon)\log n$ on an arbitrary $(2^r, d, \alpha)$-expander constructed on the set of all possible bit sequences given to the algorithm.
  - $r + \mathcal{O}(\log n)$ random bits used.

Application: reducing randomness for **RP**

- Assume $\mathcal{A}$ is a one-sided error algorithm:
  on a NO-instance it always says NO, but on a YES-instance it says YES with probability $\geq \frac{1}{2}$.
- Let r be the number of random bits used by the algorithm. We would like to reduce the error probability to $\leq \frac{1}{n}$.
- **Strategy 1**: $\log n$ independent repetitions, $r \log n$ random bits.
- **Strategy 2**: random walk of length $(1+\varepsilon)\log n$ on an arbitrary $(2^r, d, \alpha)$-expander constructed on the set of all possible bit sequences given to the algorithm.
  - $r + \mathcal{O}(\log n)$ random bits used.
  - **Note**: with poly(n) overhead we can iterate through these $\mathcal{O}(\log n)$ additional bits, so we can reduce the error probability to $\frac{1}{n}$ with poly(n, r) overhead **without** increasing the number of random bits used.

What do we need?

- To perform the above randomness reduction, we need a good family of expanders.

What do we need?

- To perform the above randomness reduction, we need a good family of expanders.

Deterministic construction of expanders

For every $\alpha_0 > 0$ there exists a constant d and a sequence of graphs $G_1, G_2, G_3, \ldots$ such that G_k is an (n_k, d, α_0)-expander, where n_k grows to infinity.

What do we need?

- To perform the above randomness reduction, we need a good family of expanders.

Deterministic construction of expanders

For every $\alpha_0 > 0$ there exists a constant d and a sequence of graphs $G_1, G_2, G_3, \ldots$ such that G_k is an (n_k, d, α_0)-expander, where n_k grows to infinity.
Moreover, graph G_k may be traversed efficiently, that is, given an $\mathcal{O}(\log n_k)$-representation of a vertex of G_k one can list its neighbours in $\mathrm{poly}(\log n_k)$ deterministic time.

What do we need?

- To perform the above randomness reduction, we need a good family of expanders.

Deterministic construction of expanders

For every $\alpha_0 > 0$ there exists a constant d and a sequence of graphs $G_1, G_2, G_3, \ldots$ such that G_k is an (n_k, d, α_0)-expander, where n_k grows to infinity.
Moreover, graph G_k may be traversed efficiently, that is, given an $\mathcal{O}(\log n_k)$-representation of a vertex of G_k one can list its neighbours in $\mathrm{poly}(\log n_k)$ deterministic time.

- We now sketch a construction of an infinite family of constant-degree expanders for $\alpha_0 = \frac{1}{2}$ (without traversing).

Part III:
Construction of an expander

The strategy

- For some constant d, there exists an explicit $(d^4, d, \frac{1}{100})$-expander H. (probabilistic or algebraic)

The strategy

- For some constant d, there exists an explicit $(d^4, d, \frac{1}{100})$-expander H. (probabilistic or algebraic)
- We show a construction for $\alpha_0 = \frac{1}{2}$ and the degree d^2.

The strategy

- For some constant d, there exists an explicit $(d^4, d, \frac{1}{100})$-expander H. (probabilistic or algebraic)
- We show a construction for $\alpha_0 = \frac{1}{2}$ and the degree d^2.
- Start with some G_1 we define in a moment, and construct $G_2, G_3, \ldots$ by applying at each step two operations:

The strategy

- For some constant d, there exists an explicit $(d^4, d, \frac{1}{100})$-expander H. (probabilistic or algebraic)
- We show a construction for $\alpha_0 = \frac{1}{2}$ and the degree d^2.
- Start with some G_1 we define in a moment, and construct $G_2, G_3, \ldots$ by applying at each step two operations:
  1. Taking **power** of the current G_i: vertex count stays the same, $\alpha(\cdot)$ gets much better, but the degree explodes.

The strategy

- For some constant d, there exists an explicit $(d^4, d, \frac{1}{100})$-expander H. (probabilistic or algebraic)
- We show a construction for $\alpha_0 = \frac{1}{2}$ and the degree d^2.
- Start with some G_1 we define in a moment, and construct $G_2, G_3, \ldots$ by applying at each step two operations:
  1. Taking **power** of the current G_i: vertex count stays the same, $\alpha(\cdot)$ gets much better, but the degree explodes.
  2. **Zig-zag product** with H: vertex count increases, $\alpha(\cdot)$ increases only slightly, but the degree becomes again constant.

Squaring the graph

- Given some G, define graph G^2 as the graph with adjacency matrix $A(G)^2$.

Squaring the graph

- Given some G, define graph G^2 as the graph with adjacency matrix $A(G)^2$.
- Let $A(G) = [a_{ij}]$ and $A(G^2) = A(G)^2 = [b_{ij}]$. Then:

$$b_{ij} = \sum_{k=1}^{n} a_{ik} a_{kj}.$$

Squaring the graph

- Given some G, define graph G^2 as the graph with adjacency matrix $A(G)^2$.
- Let $A(G) = [a_{ij}]$ and $A(G^2) = A(G)^2 = [b_{ij}]$. Then:

$$b_{ij} = \sum_{k=1}^{n} a_{ik} a_{kj}.$$

- Hence in G^2, the number of edges between v_i and v_j is the number of walks of length 2 between v_i and v_j in G.

Squaring the graph

- Given some G, define graph G^2 as the graph with adjacency matrix $A(G)^2$.
- Let $A(G) = [a_{ij}]$ and $A(G^2) = A(G)^2 = [b_{ij}]$. Then:

$$b_{ij} = \sum_{k=1}^{n} a_{ik} a_{kj}.$$

- Hence in G^2, the number of edges between v_i and v_j is the number of walks of length 2 between v_i and v_j in G.
- Generally, G^t has adjacency matrix $A(G)^t$, and every v_i-v_j walk of length t in G contributes to one edge between v_i and v_j in G^t.

Squaring the graph

- Given some G, define graph G^2 as the graph with adjacency matrix $A(G)^2$.
- Let $A(G) = [a_{ij}]$ and $A(G^2) = A(G)^2 = [b_{ij}]$. Then:

$$b_{ij} = \sum_{k=1}^{n} a_{ik} a_{kj}.$$

- Hence in G^2, the number of edges between v_i and v_j is the number of walks of length 2 between v_i and v_j in G.
- Generally, G^t has adjacency matrix $A(G)^t$, and every v_i-v_j walk of length t in G contributes to one edge between v_i and v_j in G^t.
- **Note**: G^t has still n vertices, but is d^t-regular.

Squaring the graph: spectrum

- If $A(G)$ has eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, then $A(G)^t$ has eigenvalues $\lambda_1^t, \lambda_2^t, \ldots, \lambda_n^t$.

Squaring the graph: spectrum

- If $A(G)$ has eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, then $A(G)^t$ has eigenvalues $\lambda_1^t, \lambda_2^t, \ldots, \lambda_n^t$.
- **Corollary**: $\alpha(G^t) = \alpha(G)^t$.

Squaring the graph: spectrum

- If $A(G)$ has eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, then $A(G)^t$ has eigenvalues $\lambda_1^t, \lambda_2^t, \ldots, \lambda_n^t$.
- **Corollary**: $\alpha(G^t) = \alpha(G)^t$.
- If $\alpha(G) \leq \frac{1}{2}$ then $\alpha(G^2) \leq \frac{1}{4}$.

Zig-zag product definition

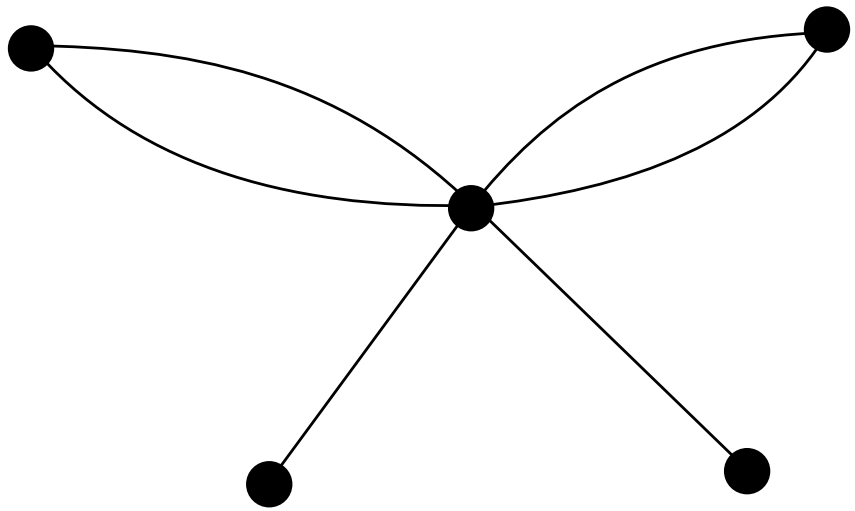
- Assume G is D-regular and has n vertices, and H is d-regular and has D vertices.

Zig-zag product definition

- Assume G is D-regular and has n vertices, and H is d-regular and has D vertices.
- Graph $G \textcircled{z} H$ has nD vertices and is d^2-regular.

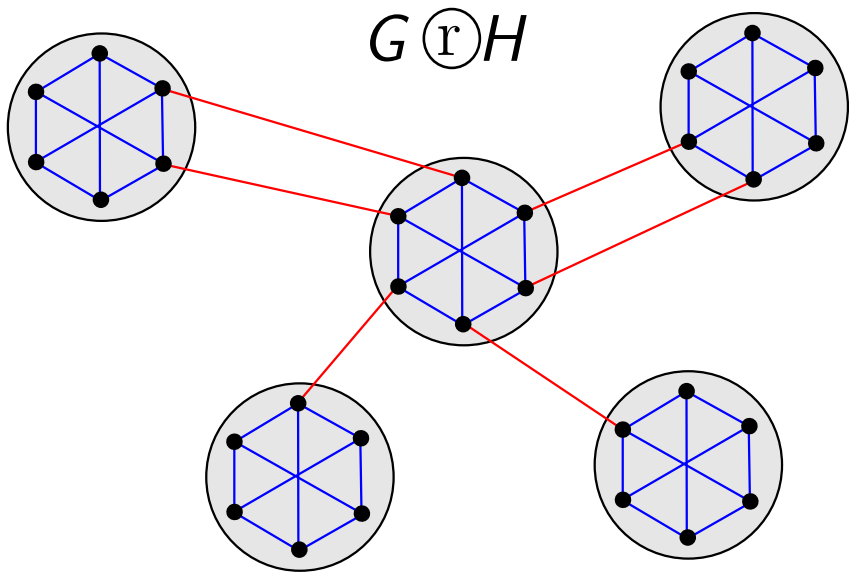
Zig-zag product definition

- Assume G is D-regular and has n vertices, and H is d-regular and has D vertices.
- Graph $G \textcircled{z} H$ has nD vertices and is d^2-regular.



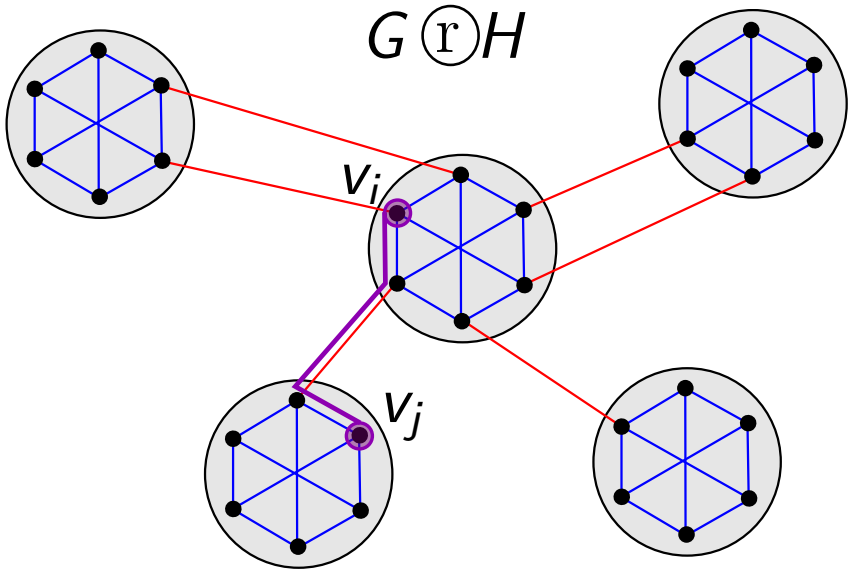
Zig-zag product definition

- Assume G is D-regular and has n vertices, and H is d-regular and has D vertices.
- Graph $G \textcircled{z} H$ has nD vertices and is d^2-regular.



Zig-zag product definition

- Assume G is D-regular and has n vertices, and H is d-regular and has D vertices.
- Graph $G \textcircled{z} H$ has nD vertices and is d^2-regular.



- $H - G - H$ walks in $G \textcircled{r} H \to$ edges in $G \textcircled{z} H$

Zig-zag product properties

- Graph $G \textcircled{z} H$ has nD vertices and is d^2-regular: every edge of $G \textcircled{z} H$ is defined by two edges of H.

Zig-zag product properties

- Graph $G \textcircled{z} H$ has nD vertices and is d^2-regular: every edge of $G \textcircled{z} H$ is defined by two edges of H.
- **Fact**: If $\beta = \alpha(H)$, then $\alpha(G \textcircled{z} H) \leq \alpha(G) + \beta + \beta^2$.

Zig-zag product properties

- Graph $G \textcircled{z} H$ has nD vertices and is d^2-regular: every edge of $G \textcircled{z} H$ is defined by two edges of H.
- **Fact**: If $\beta = \alpha(H)$, then $\alpha(G \textcircled{z} H) \leq \alpha(G) + \beta + \beta^2$.
- **Gain**: By applying the zig-zag product, we get constant degree at a small price in the spectral gap.

Whole construction

- We start the construction with $G_1 = H^2$. Then it is d^2-regular and $\alpha(G_1) \leq \frac{1}{2}$.

Whole construction

- We start the construction with $G_1 = H^2$. Then it is d^2-regular and $\alpha(G_1) \leq \frac{1}{2}$.
- We have G_i, where G_i is d^2-regular and $\alpha(G_i) \leq \frac{1}{2}$.

Whole construction

- We start the construction with $G_1 = H^2$. Then it is d^2-regular and $\alpha(G_1) \leq \frac{1}{2}$.
- We have G_i, where G_i is d^2-regular and $\alpha(G_i) \leq \frac{1}{2}$.
- Then G_i^2 is d^4-regular and has $\alpha(G_i^2) \leq \frac{1}{4}$.

Whole construction

- We start the construction with $G_1 = H^2$. Then it is d^2-regular and $\alpha(G_1) \leq \frac{1}{2}$.
- We have G_i, where G_i is d^2-regular and $\alpha(G_i) \leq \frac{1}{2}$.
- Then G_i^2 is d^4-regular and has $\alpha(G_i^2) \leq \frac{1}{4}$.
- Let $G_{i+1} = G_i^2 \textcircled{z} H$. Recall that H is d-regular and has d^4 vertices, so this is valid application.

Whole construction

- We start the construction with $G_1 = H^2$. Then it is d^2-regular and $\alpha(G_1) \leq \frac{1}{2}$.
- We have G_i, where G_i is d^2-regular and $\alpha(G_i) \leq \frac{1}{2}$.
- Then G_i^2 is d^4-regular and has $\alpha(G_i^2) \leq \frac{1}{4}$.
- Let $G_{i+1} = G_i^2 \textcircled{z} H$. Recall that H is d-regular and has d^4 vertices, so this is valid application.
- Then $\alpha(G_{i+1}) \leq \frac{1}{4} + \frac{1}{100} + \frac{1}{100^2} < \frac{1}{2}$, G_{i+1} is d^2-regular and has d^4-times more vertices.

Conclusions

- **Applications in algorithms**:
  derandomization of independent sampling.

Conclusions

- **Applications in algorithms**:
  derandomization of independent sampling.
- **Application #1**: $\mathbf{L} = \mathbf{SL}$, Reingold, 2005

Conclusions

- **Applications in algorithms**:
  derandomization of independent sampling.
- **Application #1**: **L** = **SL**, Reingold, 2005
  - Checking whether two vertices are in the same connected component of an undirected graph in **deterministic** logspace.

Conclusions

- **Applications in algorithms**:
  derandomization of independent sampling.
- **Application #1**: $\mathbf{L} = \mathbf{SL}$, Reingold, 2005
  - Checking whether two vertices are in the same connected component of an undirected graph in **deterministic** logspace.
- **Application #2**: Hardness of approximation, in particular the new proof of the PCP theorem by Irit Dinur.

Conclusions

- **Applications in algorithms**:
  derandomization of independent sampling.
- **Application #1**: $\mathbf{L} = \mathbf{SL}$, Reingold, 2005
  - Checking whether two vertices are in the same connected component of an undirected graph in **deterministic** logspace.
- **Application #2**: Hardness of approximation, in particular the new proof of the PCP theorem by Irit Dinur.
  - Controlled amplification of approximation gap using expanders.

Conclusions

- **Applications in algorithms**:
  derandomization of independent sampling.
- **Application #1**: $\mathbf{L} = \mathbf{SL}$, Reingold, 2005
  - Checking whether two vertices are in the same connected component of an undirected graph in **deterministic** logspace.
- **Application #2**: Hardness of approximation, in particular the new proof of the PCP theorem by Irit Dinur.
  - Controlled amplification of approximation gap using expanders.
- Many other connections and applications:

Conclusions

- **Applications in algorithms**:
  derandomization of independent sampling.
- **Application #1**: **L** = **SL**, Reingold, 2005
  - Checking whether two vertices are in the same connected component of an undirected graph in **deterministic** logspace.
- **Application #2**: Hardness of approximation, in particular the new proof of the PCP theorem by Irit Dinur.
  - Controlled amplification of approximation gap using expanders.
- Many other connections and applications:
  - compressed sensing, metric embeddings, correction codes, theory of random matrices, representation theory, harmonic analysis, PDEs, geometric group theory...

Further reading

- Hoory, Linial, Widgerson,
  Expander graphs and their applications, a survey.
- Lecture notes from course *Selected topics of graph theory* by Marcin Pilipczuk, Jakub Onufry Wojtaszczyk and students, editions 2010 and 2013, University of Warsaw
  (in Polish, notes about $\mathbf{L} = \mathbf{SL}$ in English).
- Script from summer school *Hardness of Approximation* by Cygan, Pilipczuk, P, Wojtaszczyk, 2010
  (in Polish).