Introduction to Expander Graphs

Michael Lampis, Valia Mitsou

NTUA

Outline

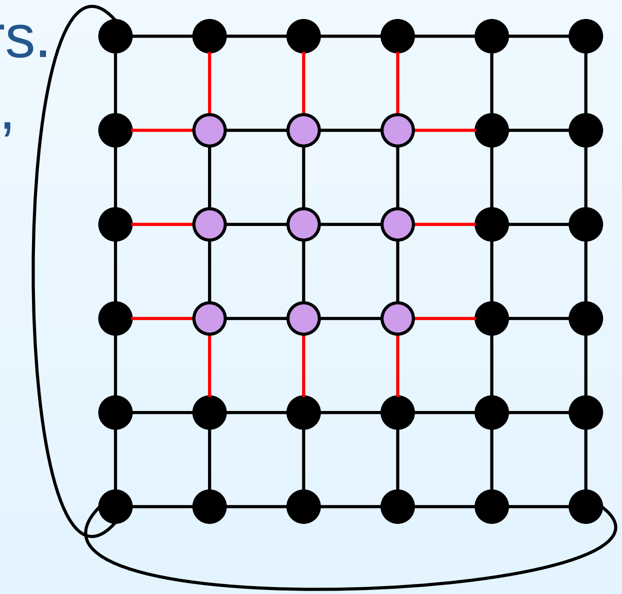
- Definition
- Examples
- Algebraic methods and the spectral gap theorem
- Applications

Definition

- Informally: an expander graph is a (multi)graph in which every subset S of vertices expands quickly, i.e. many edges connect it to $\bar{S}$.
- Formally:
  - ϑS : the set of edges connecting S to $\bar{S}$.
  - *Expansion parameter*: $h(G) \equiv \min_{S:|S|\leq n/2} \frac{|\vartheta S|}{|S|}$
- A family of graphs G_n is an expander family when
  - $\forall i, G_i$ is d-regular, for some constant d (therefore, all the graphs in the family are sparse).
  - $h(G_i) > \epsilon > 0$, for some constant ϵ.

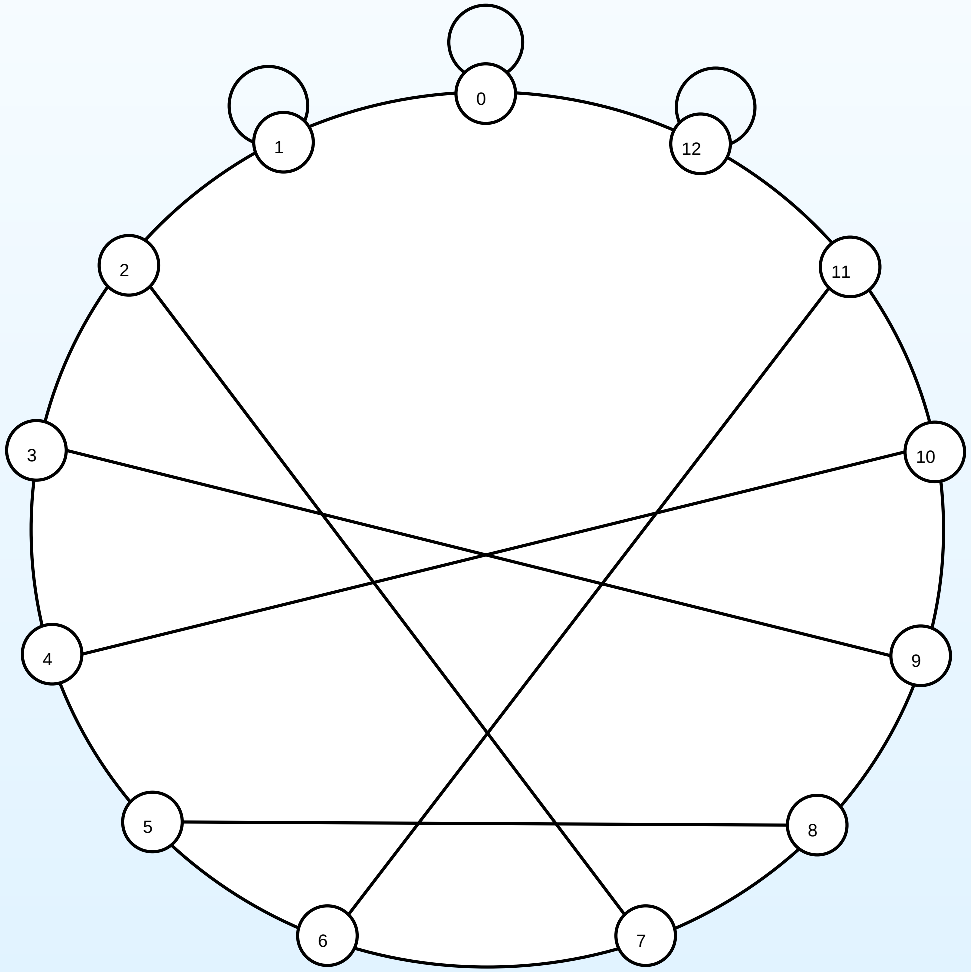
(Counter-)Examples

- A clique would be an expander graph, if it was sparse.
  Any subset S has $|\vartheta S| = |S|(n - |S|)$. Thus,
  $h(K_n) = \min_{|S| \leq n/2}(n - |S|) = \frac{n}{2}$.
- Cycles C_n are not expanders.
  The subset S of $n/2$ consecutive vertices has $\vartheta S = 2$. Thus,
  $h(C_n) \leq \frac{2}{n/2} = \frac{4}{n} \to 0$.
- Toroidal $n \times n$ grids are not expanders.
  An $\frac{n}{2} \times \frac{n}{2}$ subgrid has $\vartheta S = 2n$. Thus,
  $h(G_n) \leq \frac{2n}{n^2/4} = \frac{8}{n} \to 0$



Example

- For p prime, $G_p = (\mathbb{Z}_p, E_p)$, where
  $E_p = \{(x,y) | y \equiv_p x \pm 1 \vee y \equiv_p x^{-1}\} \cup \{(0,1),(0,p-1)\}$



Expander graph constructions

- Mildly Explicit Construction: There is a poly-time algorithm that given input 1^n (in unary) produces the graph in the family with n vertices.
- Very Explicit Construction: There is a poly-time algorithm that given input (n, v) (in binary) produces a list of all of v's neighbors in the graph.
- Very Explicit Construction $\Rightarrow$ Mildly Explicit Construction.
- Very Explicit Constructions allow us to perform random walks on expander graphs of exponential size.
- The previous example was a Very Explicit Construction.

Deciding on the Expansion property

- Given a graph G, it is hard (co-NP-complete) to decide whether G is an expander.
- Intuition: there are exponentially many subsets that may serve as a NO-certificate.
- Algebraic methods can be used to prove that specific explicitly constructed families are indeed expanders.

Algebra

- Let A be the adjacency matrix of an expander graph. Its rows and columns sum up to d.
- Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of A.
- $A\mathbb{1} = d\mathbb{1}$. Thus, d is an eigenvalue of A. Its corresponding eigenvector is $\mathbb{1}$.
- A can have no eigenvalue greater than d, therefore, $\lambda_1 = d$.
- The eigenvectors $\{\mathbb{1}, v_2, \ldots, v_n\}$ of A form an orthogonal basis, because A is symmetric.
- We will show that $h(G) \geq \frac{\lambda_1 - \lambda_2}{2}$

The eigenvalue gap

$$\frac{\lambda_1 - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(\lambda_1 - \lambda_2)}$$

- We will show that $\lambda_2 \geq d - 2h(G)$.
- $d - 2h(G) = d - 2\frac{|\vartheta S|}{|S|}$, for some appropriate subset S, with $|S| \leq n/2 \Rightarrow |\bar{S}| \geq n/2 \geq |S|$.
- $d - 2\frac{|\vartheta S|}{|S|} \leq d - |\vartheta S|(\frac{1}{|S|} + \frac{1}{|\bar{S}|})$
- Take a vector v s.t. $v = \frac{\mathbb{1}_S}{|S|} - \frac{\mathbb{1}_{\bar{S}}}{|\bar{S}|}$. (The vector $\mathbb{1}_S$ is the vector with 1's for the vertices of S and 0 elsewhere).
  We will show that $d - |\vartheta S|(\frac{1}{|S|} + \frac{1}{|\bar{S}|}) = \frac{v^T A v}{v^T v}$.

The eigenvalue gap

- $v^T v = \frac{|S|}{|S|^2} + \frac{|\bar{S}|}{|\bar{S}|^2} = \frac{1}{|S|} + \frac{1}{|\bar{S}|}$
- Observe that $\mathbb{1}_S^T A \mathbb{1}_T = |E(S,T)|$ for $S \cap T = \emptyset$, and $\mathbb{1}_S^T A \mathbb{1}_S = 2|E(S,S)|$
- $v^T A v = \frac{2}{|S|^2}|E(S,S)| + \frac{2}{|\bar{S}|^2}|E(\bar{S},\bar{S})| - \frac{2}{|S||\bar{S}|}|E(S,\bar{S})|$
- $2|E(S,S)| + |E(S,\bar{S})| = d|S|, \quad 2|E(\bar{S},\bar{S})| + |E(S,\bar{S})| = d|\bar{S}|$
- $E(S,\bar{S}) = \vartheta S$.
- $\ldots \Rightarrow d - |\vartheta S|(\frac{1}{|S|} + \frac{1}{|\bar{S}|}) = \frac{v^T A v}{v^T v}$

The eigenvalue gap

- All we need now is $\frac{v^T A v}{v^T v} \leq \lambda_2$.
- But $tr(v) = 0 \Rightarrow v \perp \mathbb{1}$.
- v can be written as $v = a_2\tilde{v}_2 + a_3\tilde{v}_3 + \ldots + a_n\tilde{v}_n$. ($\tilde{v}_i$ are the normalized eigenvectors).
- $\frac{v^T A v}{v^T v} = \frac{\sum a_i^2 \lambda_i}{\sum a_i^2} \leq \lambda_2$
- The theorem follows!

$$\frac{\lambda_1 - \lambda_2}{2} \leq h(G)$$

Applications

- Error-correcting codes.
- New proof of PCP theorem.
- Hardness of approximation proofs.
- Reduction of random bits for randomized algorithms.

Random walks on expander graphs

- A random walk is the following process: start at an arbitrary vertex and at each step select one of its edges uniformly at random. Traverse that edge and repeat the process.
- Suppose we perform a random walk on an expander graph G. We will show that after a short time we have the same probability of being on any vertex.
- Since the graph is an expander, there is a low probability of being "trapped" in a small subset of the vertices for long, because many edges leave that subset.

Random walks on expander graphs

- probability distribution p: a vector containing the probabilities of being at any vertex of G in a specific time.
- After one step the probability distribution will be $p' = \tilde{A}p$
- Since the graph is d-regular the transition matrix is $\tilde{A} = \frac{A}{d}$.
- The uniform distribution $u = \frac{1}{n}\mathbb{1}$ is the stationary distribution, since $\tilde{A}u = u$.
- The question is how fast the random walk converges to the stationary distribution.
- We will show that this happens exponentially fast.

Convergence

$$\|\tilde{A}^t p - u\|_1 \leq \sqrt{n}\tilde{\lambda}_2^t$$

- Suppose that p is the initial distribution. This theorem tells us that we converge to the uniform distribution u exponentially fast. Proof:
- We will show that $\|\tilde{A}^t p - u\|_2 \leq \tilde{\lambda}_2^t$, and the result follows because $\forall v, \|v\|_2 \leq \sqrt{n}\|v\|_1$
- $\|\tilde{A}^t p - u\|_2 = \|\tilde{A}^t(p-u)\|_2$ because $\tilde{A}u = u$
- The eigenvectors $\{u = v_1, v_2, \ldots, v_n\}$ form an orthonormal basis. Thus, $p - u = a_1 v_1 + a_2 v_2 + \ldots + a_n v_n$.
- But $p - u \perp u \Rightarrow a_1 = 0$.
- $\tilde{A}^t(p-u) = \sum_{i=2}^n \tilde{A}^t a_i v_i = \sum_{i=2}^n \tilde{\lambda}_i^t a_i v_i$
- $\|\tilde{A}^t(p-u)\|_2 \leq \|\sum_{i=2}^n \tilde{\lambda}_2^t a_i v_i\| = \tilde{\lambda}_2^t \|p-u\|_2 \leq \tilde{\lambda}_2^t$

Non-confinement

- Let B be a subset of the vertices. The probability that a random walk stays inside that subset for t steps is

$$Pr[B(t)] \leq (\tilde{\lambda}_2 + \frac{|B|}{n})^t$$

- Proof omitted...
- Note that $|B|$ must be sufficiently small so that $\tilde{\lambda}_2 + \frac{|B|}{n} < 1$.

Improving the probability of success

- Suppose we have a randomized algorithm for a problem in RP with probability of failure $\leq \frac{1}{2}$.
- A standard technique to improve this probability is to run it several times. Then probability of failure $\leq \frac{1}{2^t}$.
- Drawback: if the algorithm needed m random bits, now we need tm random bits.
- Expander graphs can help us reduce this to $m + O(t)$ without losing (much) on the amplification!

Probability Amplification: Intuition

- Observation 1: choosing m random bits is equivalent to picking uniformly at random a vertex from a graph on 2^m vertices.
- Observation 2: a random walk on an expander graph quickly converges to the uniform distribution
- Observation 3: a random walk on an expander graph costs few random bits, because vertices have constant degree.
- $\longrightarrow$ a random walk on an expander graph is a good way to save random bits, because after a while it is almost like sampling uniformly at random.

Method

- Suppose we have a randomized algorithm. Use a very explicit expander graph construction to produce a graph on 2^m vertices, where m is the number of random bits. Each vertex corresponds to a choice.
- Perform a random walk for t steps, starting from a random vertex v_0 and visiting $v_1, v_2, \ldots, v_t$.
- Run the algorithm successively with random strings $v_0, v_1, \ldots, v_t$ and output the collective answer.
- Random bits used: $\approx m + t \log d$.

Why this works

- Let B be the set of bad choices of random strings.
- Recall that the probability that a random walk is confined in B drops exponentially with t.
- $\tilde{\lambda}_2 + \frac{|B|}{n} < 1$ is achievable by repeating the algorithm $O(1)$ times to make B small enough.
- Bonus: this works for algorithms in BPP as well! Just take the majority of the outcomes.

THE END!!!