Randomized Methods in Computation*
Lecture 9: Expanders and Eigenvalues

Notes taken by Ya'ara Goldschmidt, Eran Keydar, Yaki Setty

Spring 2001

Summary: This lecture is about expander graphs, which are very useful in many probabilistic applications. First, we would describe some of the combinatorial definitions and properties of an expander graph. Second, we would see one application which uses expander graphs, and finally, we would discuss some of the algebraic properties of such graphs.

1 Introduction

1.1 Motivation

We have already seen (in Lecture 2) a proof, using the probabilistic method, for the existence of 3-regular expander graphs. In the following lectures we study expanders, their applications and constructions, at greater depth.
As was presented in Lecture 2, expander graphs are sparse graphs with the property that every subset of vertices (which is not too large), has "many" adjacent neighbors. This implies the existence of a "short" path between any two vertices.
These properties are very useful in many probabilistic applications. For example they ensure that when performing a random walk on an expander graph, the distribution of reaching any of the vertices will converge to uniformity, relatively fast.

1.2 Family of Expander Graphs

Usually, when speaking on an expander graph G_N, we actually mean a family of graphs $\{G_N\}_{N \in S}$, where S is some infinite subset of the natural numbers. The members of the family are d-regular graphs (d is fixed for the entire family) and have the same expansion coefficient $c > 0$.
Three remarks for the definition of the set of graphs:

1. The graphs are not necessarily simple; that is, self-loops and parallel edges are allowed. That means that the adjacency matrix representing such a graph can have entries in the range 0 to d instead of only boolean entries.

2. In fact, we assume that all vertices have self-loops; that is, the adjacency matrix has 1's on the diagonal.

3. For our purpose, it is convenient to assume that N is equal to 2^n for some n, and that the vertices of the graph are the 2^n strings of length n (i.e., $\{0,1\}^n$).

* Lecture Notes for a course given by Oded Goldreich at the Weizmann Institute of Science, Israel.

1.3 Definitions of Neighborhood Sets

Before formally defining what an expander graph is, we define some notations about neighborhood sets. For a set of vertices U in graph $G(V, E)$, we define the following three neighborhood sets:

Definition 1 $\Gamma(U) \triangleq \{v : \exists u \in U \ , \ (u,v) \in E\}$*; the set of all vertices reachable from any vertex of* U *in exactly one step (may include vertices in* U*).*

Definition 2 $\Gamma^*(U) \triangleq \Gamma(U) \backslash U$*; the set of all vertices reachable in one step from vertices in* U*, excluding* U*. This is called the boundary of* U*.*

Definition 3 $\Gamma^+(U) \triangleq \Gamma(U) \cup U$*; the set of all vertices reachable in at most one step from* U*.*

Notice: under the assumption that all vertices have a self-loop, $\Gamma^+(U) = \Gamma(U)$.

1.4 Definitions of Expander Graphs

We can now formally define an expander graph.

Definition 4 [First Definition] *N-vertex graph has expansion coefficient $c > 0$, if $\forall$ set U of vertices with size $\leq \frac{N}{2}$: $|\Gamma^*(U)| \geq c \cdot |U|$*

Sometimes one would find it more convenient to use the following definition for an expander graph:

Definition 5 [Second Definition] *N-vertex graph has expansion $c > 0$, if $\forall$ set U of vertices:* $|\Gamma^+(U)| \geq \min\left\{(1+c)|U|, \frac{N}{2}+1\right\}$

Notice: any graph G satisfying Definition 4 also satisfies Definition 5, but the converse is not necessarily true.
Definition 5 implies that every expander graph is connected, as stated in the following proposition:

Proposition 1.1 *Any expander graph is a connected graph.*

Proof: Let $G_N(V, E)$ be an expander graph with expansion coefficient $c > 0$. Suppose in contradiction that G_N is not connected. In that case, V is composed of at least 2 disjoint subsets of vertices, with no edges connecting them. Hence for any such subset U, $\Gamma^+(U) = U$. Let $U_{\min}$ be the subset of smallest size, clearly $|U_{\min}| \leq \frac{N}{2}$, hence $|\Gamma^+(U_{\min})| < \min\left\{(1+c)|U_{\min}|, \frac{N}{2}+1\right\}$. This contradicts the second definition of expander graph (Definition 5). ■

1.5 Constructibility

When speaking on expander graphs, one should consider the time required to construct the graph. This is the requirement of constructibility. There are two natural versions for this requirement: a weak version and a strong one.

Definition 6 [Weak Version] *An expander graph G_N is (weakly) constructible, if an explicit representation of it can be given in time* $\text{poly}(N)$*.*

An explicit representation means an adjacency matrix or a neighbors list.
This definition is weak, since the construction is polynomial in the number of vertices. As mentioned before, in some applications we would like to relate to vertices as strings over $\{0,1\}^n$, and then the output would be exponential in n. This leads to the stronger definition of constructibility:

Definition 7 [Strong Version] *An expander graph G_N is (strongly) constructible, if when given a string of length n bits, representing vertex v in G_N ($N = 2^n$), we can construct a list of all its neighbors in time* $\mathrm{poly}(n)$.

Clearly, Definition 7 implies Definition 6.

2 On the Diameter of Expander Graphs

In this section we prove that there is a relatively short path between any two vertices in an expander graph.

Definition 8 *The diameter of a connected graph G, denoted $Diam(G)$, is the maximal distance between any two vertices in the graph.*

Theorem 9 [Logarithmic Diameter]
Let G_N be an expander graph with an expansion coefficient c, then:

$$Diam(G_N) \leq \frac{2\log(N)}{\log(1+c)}$$

Proof: In order to prove the theorem, we would prove that for every two vertices u and v, there exists a path connecting u and v of length at most $\frac{2\log((N/2)+1)}{\log(1+c)}$.
Define $l = \log_{1+c}(\frac{N}{2}+1)$, and define the following sets inductively:

$$\begin{aligned} U_0 &= \{u\} \\ U_i &= \Gamma^+(U_{i-1}) \end{aligned}$$

Then, U_i is the set of the vertices reachable from u in at most i steps. Using the second definition of expansion (Definition 5) we conclude:

$$\begin{aligned} |U_i| &= |\Gamma^+(U_{i-1})| \\ &\geq \min\left\{(1+c)|U_{i-1}|, \frac{N}{2}+1\right\} \\ &\geq \min\left\{(1+c)^i, \frac{N}{2}+1\right\} \end{aligned}$$

Using $i = l$, we get $|U_l| > \min\left\{(1+c)^l, \frac{N}{2}+1\right\}$, which is at least $\frac{N}{2}+1$ provided $(1+c)^l > \frac{N}{2}$. The latter is correct by the definition of l. Applying the same argument for v we get $|V_l| > \frac{N}{2}$. Remember that U_l and V_l are the sets of vertices reachable in at most l steps from u and v, respectively. Both U_l and V_l are subsets of the set of N vertices, therefore these two sets must have non-empty intersection. Therefore there must be a path between u and v of length at most:

$$2l = 2 \cdot \frac{\log(\frac{N}{2}+1)}{\log(1+c)} \leq \frac{2\log(N)}{\log(1+c)}$$

■

3 Amplification of Expander Graphs

For some applications we would need an expansion coefficient that is larger than the one associated with the $\{G_N\}_{N\in S}$ which we are given or have been constructed. To achieve this we amplify the graph G_N, to get a graph with larger expansion coefficient, but also with more edges.

3.1 The Amplified Graph

Given the graph G_N with vertex set $[N]$, we can construct the graph G_N^k in the following way:

$$G_N^k \triangleq \left([N], \left\{(u,v) : \begin{array}{c} \exists \text{ path of length exactly } k \\ \text{between } u \text{ and } v \text{ in } G_N \end{array} \right\}\right)$$

Given a representation of G_N^k as an adjacency matrix - M_N, the adjacency matrix M_N^k of G_N^k can be calculated by raising M_N to the k-th power: $M_N^k = (M_N)^k$. We can now present the following proposition about G_N^k constructed from an expander graph G_N which is d-regular and has expansion c.

Proposition 3.1 *Let G_N be a d-regular expander graph with expansion coefficient c, and let k be an integer. Then G_N^k has the following properties:*

1. *G_N^k is d^k-regular.*
2. *The expansion coefficient of G_N^k is $(1+c)^k - 1$.*

Proof:

1. By the construction of G_N^k, the degree of each vertex in G_N^k is the number of paths (not necessarily simple) of length k in G_N. Since G_N is d-regular, the number of paths is exactly d^k. Hence G_N^k is d^k-regular.
2. For any set U, we denote by U_i the set of vertices reachable from U in at most i steps in the graph G_N. Then $U_0 = U$, $U_1 = \Gamma^+(U)$, and in general $U_i = \Gamma^+(U_{i-1})$.

$$\begin{array}{rcl} |U_0| &=& |U| \\ |U_i| &\geq& \min\left\{(1+c)|U_{i-1}|, \frac{N}{2}+1\right\} \\ &\geq& \min\left\{(1+c)^i|U|, \frac{N}{2}+1\right\} \end{array}$$

In G_N^k the set $\Gamma_{G_N^k}(U)$ is the set of all vertices reachable from U in exactly one step, that is, it is equal to the set of vertices reachable in exactly k steps from U in G_N. But since every vertex in G_N has a self-loop, $\Gamma_{G_N^k}(U)$ also equals to the set of vertices reachable from U in at most k steps. This also implies that U is a subset of $\Gamma_{G_N^k}(U)$, hence $\Gamma^+_{G_N^k}(U) = \Gamma_{G_N^k}(U) = U_k$. Therefore $|\Gamma^+_{G_N^k}(U)| \geq \min\left\{(1+c)^k|U|, \frac{N}{2}+1\right\}$. Using the second definition of expansion, the expansion coefficient of G_N^k is $(1+c)^k - 1$.

■

3.2 Constructibility of G_N^k

We now present two claims about the constructibility of G_N^k:

Claim 3.2 *Let G_N be a d-regular expander graph which is weakly constructibility, and let k be an integer, then G_N^k is weakly constructible as well.*

Proof: We notice that if we take k to be as large as the diameter of the graph, then G_N^k is a complete graph, therefore we can assume that k is not larger than the diameter of the graph. Based on Theorem 9, $k = O(\log(N))$. If G_N is weakly constructible then we can construct its adjacency matrix in time poly(N). Raising it to the k-th power, requires at most k times poly(N)-time operations. Since we assumed $k = O(\log(N))$ the whole construction takes poly(N) time. ■

Claim 3.3 *Let G_N be a d-regular expander graph which is strongly constructible, and let k be an integer. Then the generation of the list of neighbors of each vertex in G_N^k takes* $\mathrm{poly}(n \cdot |output|)$*; that is,* $\mathrm{poly}(n \cdot d^k)$.

Notice that since k may not be constant, the number of neighbors of a vertex in G_N^k can be exponential in n, therefore G_N^k is not necessarily strongly constructible.
Proof: If G_N is strongly constructible, then the generation of the neighbors list of v in G_N^k can be done by using a BFS search on G_N for depth k. The number of vertices in depth till k is upper bounded by $\sum_{i=1}^{k} d^i$, that is $O(d^k)$. Since finding the neighbors of a vertex in G_N takes poly(n) time, the complexity of the BFS is $\mathrm{poly}(n \cdot d^k)$. And this is the most expensive operation of the construction. Notice that if d^k is polynomial in n, then G_N^k is strongly constructible. ■

4 An Application of Expander Graphs

The following section presents one application of expander graphs.

4.1 The Problem

Consider the following problem: Suppose W is a set of witnesses, $W \subseteq \{0,1\}^n$ such that $|W| \geq \frac{1}{2} \cdot 2^n$. Our aim is to present a randomized algorithm that when given $\delta < \frac{1}{2}$ (e.g. $\delta = 0.01$) satisfies:

$$\Pr[\text{Output of the Alg} \in W] > 1 - \delta$$

An obvious solution would be to pick $\log\left(\frac{1}{\delta}\right)$ strings independently (each giving a probability of at least $\frac{1}{2}$ to hit W). But we seek for a solution which would satisfy the following restrictions:

1. Running time should be $\mathrm{poly}(\frac{n}{\delta})$
2. At most n bits of randomness are allowed to be used.

The second restriction prevents us from using the above (obvious) solution, and even does not allow to construct a pairwise independent sample space.

4.2 The Algorithm

We start with a d-regular expander graph G_N with expansion c, we then construct the graph G_N^l (as explained in Section 3), which is d^l-regular and has expansion coefficient $(1+c)^l - 1$. By choosing l to be $\frac{\log(1/\delta)}{\log(1+c)}$, we ensure that the expansion coefficient of G_N^l is approximately $\frac{1}{\delta}$.
Using this construction, consider the following algorithm:

1. Select at random a vertex v in G_N^l.
2. Scan the neighbors of v, and output a neighbor in W if such exists, else fail.

Three remarks:

1. Each vertex is represented as a string of length n bits, thus only n bits of randomness are required for Stage 1.
2. We actually do not explicitly construct G_N^k. Instead, after randomly selecting the string v (in Stage 1), we use the fact that G_N is strongly constructible to generate the neighbors of v in G_N^k in time poly($\frac{n}{\delta}$).
3. Since the graph has self-loops, in Stage 2 of the algorithm v is scanned along with its neighbors.

4.3 Analysis of the Algorithm

4.3.1 Time Complexity

Using Claim 3.3, the time complexity of Stage 2 of the algorithm is poly($n \cdot d^l$), where:

$$d^l = d^{O\left(log\left(\frac{1}{\delta}\right)\right)} = \exp\left(\log\left(\frac{1}{\delta}\right)\right) = \text{poly}\left(\frac{1}{\delta}\right)$$

provided that d is constant. That is, the complexity of Stage 2 is poly($\frac{n}{\delta}$). This is the most expensive operation of the algorithm, hence this determines its time complexity.

4.3.2 Correctness

We now analyze the probability of the algorithm to fail, which happens when none of the neighbors of the chosen v are in W. We define a vertex as *bad* if all its neighbors (and itself) are in $\{0,1\}^n \backslash W$. Denote $B = \{v : v \text{ is } bad\}$.

Claim 4.1 $|B| < \delta \cdot 2^n$

Proof: Suppose in contradiction that $|B| \geq \delta \cdot 2^n (= \delta \cdot N)$. Using the second definition of expansion on $\Gamma^+(B)$ we get:

$$|\Gamma^+(B)| = \min\left\{\underbrace{((1+c)^l - 1)}_{>\frac{1}{\delta}} \cdot \delta N, \frac{N}{2} + 1\right\} = \frac{N}{2} + 1$$

Hence $|\Gamma^+(B)| \geq \frac{N}{2}$, but also $\Gamma^+(B) \cap W = \phi$. This contradicts the hypothesis that $|W| > \frac{N}{2}$. ■

5 Algebraic Definition of Expanders

Until now we have been discussing the combinatorial properties of expanders. In the following section we will talk about some algebraic properties of expander graphs. This will lead us, in the next lecture, to the algebraic definition of an expander graph and to the relations between the combinatorial and algebraic definitions. We will study the algebraic properties by exploring the connection they have with a random walk on the graph.
A *random walk* is a sequence of random steps, at which we start from an initial vertex and uniformly select one of its outgoing edges. We follow that edge and repeat the random selection for the vertex we have reached, and so on for any desired number of steps. Since the selection of an outgoing edge in each step is uniform, the probability to reach each vertex in that step is proportional to the number of edges connecting the current vertex to it.

5.1 The Normalized Adjacency Matrix

Consider the symmetric adjacency matrix of an undirected d-regular graph with vertex set $[N]$. The entries in the matrix are between 0 and d (since we allow self-loops and parallel edges). We define the *normalized adjacency matrix* to be the above matrix divided by d. This devision ensures that all the entries are in $[0,1]$, and the sum of each column and each row is 1. The *normalized adjacency matrix* is a stochastic matrix, and as such it can be used to describe a random walk on the graph. Denote the *normalized adjacency matrix* by A, then entry a_{ij} is the probability to reach vertex i in one random step, given that we are now in vertex j. We denote this probability by $\Pr[\,i\,|\,j\,]$. We can now look at the following operation:

$$\overbrace{\begin{bmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{bmatrix}}^{A:N\times N} \underbrace{\begin{bmatrix} p_1 \\ \vdots \\ p_N \end{bmatrix}}_{P:N\times 1} = \underbrace{\begin{bmatrix} p'_1 \\ \vdots \\ p'_N \end{bmatrix}}_{P':N\times 1}$$

We claim that the above operation describes one step of a random walk on the graph: That is, if P is the probability distribution of being in any vertex at the current stage, then P' is the distribution after doing one random step. To explain this claim we look at the i-th entry of P' which is:

$$\begin{array}{rcccccccc} p'_i & = & a_{i1}\cdot p_1 & + & a_{i2}\cdot p_2 & + & \ldots & + & a_{iN}\cdot p_N \\ & = & \Pr[\,i\,|\,1\,]\cdot p_1 & + & \Pr[\,i\,|\,2\,]\cdot p_2 & + & \ldots & + & \Pr[\,i\,|\,N\,]\cdot p_N \end{array}$$

That is, p'_i describes the probability to reach vertex i after that step, so P' is the probability distribution after that step. Basically, if we start with initial distribution vector $P^{(0)}$, then the distribution after one random step is $P^{(1)} = AP^{(0)}$. After another random step the distribution is $P^{(2)} = AP^{(1)} = A^2P^{(0)}$. In general, the distribution after t random steps would be $P^{(t)} = A^tP^{(0)}$.

We call a distribution P a *stationary distribution* if $AP = P$. Clearly, if for some $t > 0$ it holds that $A^tP^{(0)} = P^{(t)}$ is the stationary distribution, then for any $t' \geq t$, the distribution $P^{(t')}$ remains the stationary distribution. We say that a random walk *converges* if for any initial distribution $P^{(0)}$, and for every $\epsilon > 0$ there exists $t > 0$ such that $A^tP^{(0)} = P^{(t)}$ is ϵ-close (in variation distnace) to the stationary distribution. As a corollary to the facts proven in the next section, one may conclude that for any connected bipartite (regular) graph a random walk on its vertices converges to the uniform distribution. In the next lecture, we shall see that the rate of convergence (i.e., the dependence of t on ϵ) depends on the eigenvalues of the adjacency matrix.

5.2 Eigenvectors and Eigenvalues of the Matrix

First, we would explore the eigenvalues and eigenvectors of the (normalized) adjacency matrix:

Fact 5.1 *All eigenvalues are real.*

This follows from the fact that the adjacency matrix is symmetric.

Fact 5.2 *The eigenvectors form a basis.*

This again follows from the fact that the adjacency matrix is symmetric and therefore diagonalizable.

Fact 5.3 *The value* 1 *is an eigenvalue corresponding to the uniform eigenvector* $\bar{e}_1 = (\frac{1}{N}, \ldots, \frac{1}{N})$.

That is: $A \cdot \bar{e}_1 = \bar{e}_1$.
Proof: Indeed examine $\bar{p} = A \cdot \bar{e}_1$. For any entry $1 \leq i \leq N$ in $\bar{p}$:

$$p_i = \sum_{j=1}^{N} a_{ij} \frac{1}{N} = \frac{1}{N} \sum_{j=1}^{N} a_{ij} = \frac{1}{N} \cdot 1 = \frac{1}{N}$$

■

Remark : $\bar{e}_1$ is the *stationary distribution.*

Fact 5.4 *Eigenvectors corresponding to distinct eigenvalues are orthogonal. That is, if $A\bar{v_1} = \lambda_1 \bar{v_1}$, $A\bar{v_2} = \lambda_2 \bar{v_2}$ and $\lambda_1 \neq \lambda_2$, then $\bar{v_1}^\top \bar{v_2} = 0$ (i.e. $\bar{v_1} \perp \bar{v_2}$).*

Proof: Examine $\bar{v_1}^\top A \bar{v_2}$
On the one hand:

$$\bar{v_1}^\top A \bar{v_2} = (A^\top \bar{v_1})^\top \bar{v_2} \overset{(*)}{=} (A\bar{v_1})^\top \bar{v_2} = (\lambda_1 \bar{v_1})^\top \bar{v_2} = \lambda_1 \bar{v_1}^\top \bar{v_2}$$

where $(*)$ holds since $A^\top = A$.
On the other hand:

$$\bar{v_1}^\top A \bar{v_2} = \bar{v_1}^\top \lambda_2 \bar{v_2} = \lambda_2 \bar{v_1}^\top \bar{v_2}$$

Hence $\lambda_1 \bar{v_1}^\top \bar{v_2} = \lambda_2 \bar{v_1}^\top \bar{v_2}$. Thus $\lambda_1 \neq \lambda_2$ implies $\bar{v_1}^\top \bar{v_2} = 0$. ■

Fact 5.5 *Any eigenvector $\bar{v}$ corresponding to an eigenvalue $\neq 1$ has sum 0.*

Proof: This is deduced from Fact 5.4. Since $\bar{v}$ is orthogonal to the uniform vector $\bar{v}^\top \cdot \begin{bmatrix} \frac{1}{N} \\ \vdots \\ \frac{1}{N} \end{bmatrix} = 0$.
This implies that $\sum_{i=1}^{N} v_i \frac{1}{N} = 0$, therefore $\frac{1}{N} \sum_{i=1}^{N} v_i = 0$, and so $\sum_{i=1}^{N} v_i = 0$. ■

Fact 5.6 *For any eigenvalue λ, $|\lambda| \leq 1$.*

Proof: Let $\{\bar{e}_i\}$ be the eigenvectors, where $\bar{e}_1 = (\frac{1}{N}, \ldots, \frac{1}{N})$.
Any probability vector $\bar{p}$ can be represented as a linear combination of the basis $\{e_i\}$ (Fact 5.2): $\bar{p} = \sum_{i=1}^{N} c_i \bar{e}_i$.
Let $t \geq 1$ be an integer.

$$A^t \bar{p} = A^t \sum_{i=1}^{N} c_i \bar{e}_i = \sum_{i=1}^{N} c_i A^t \bar{e}_i = \sum_{i=1}^{N} c_i {\lambda_i}^t \bar{e}_i$$

If $\lambda_i > 1$ and $c_i \neq 0$ then the above sum diverges, which is not possible since $A^t \bar{p}$ is a probability vector.
However if $c_i = 0$, then we cannot conclude that $|\lambda_i| \leq 1$. Thus, for any $i \geq 2$, consider $\bar{p} = \bar{e}_1 + \epsilon \bar{e}_i$, where ϵ is small enough such that $\bar{p}$ is a probability vector. That is:

$$\epsilon \leq \frac{1}{|m|N} \quad \text{where } m = \min_{1 \leq j \leq N} \{e_{i_j}\}$$

Taking such ϵ ensures that $\bar{p}$ is a probability vector:

- All entries of $\bar{p}$ are non-negative:
  Since m is the minimal entry of $\bar{e}_i$, all entries in $\epsilon\bar{e}_i$ are greater or equal to $-\frac{1}{N}$. Moreover, all entries in $\bar{e}_1$ are $\frac{1}{N}$, therefore all the entries in $\bar{p}$ are non-negative.

- The sum of the entries of $\bar{p}$ is 1:
  The sum of entries in $\bar{e}_1$ is 1, and the sum of entries in $\bar{e}_i$ is 0 (Fact 5.5), hence the sum of entries in $\bar{e}_1 + \epsilon\bar{e}_i$ is 1.

Now consider:

$$\bar{p}' = A^t\bar{p} = A^t(\bar{e}_1 + \epsilon\bar{e}_i) = A^t\bar{e}_1 + A^t\epsilon\bar{e}_i = \bar{e}_1 + \epsilon{\lambda_i}^t\bar{e}_i$$

$\bar{p}'$ should also be a probability vector, but when $|\lambda_i| > 1$ and for t large enough, the above term diverges. Hence, we conclude that $|\lambda_i| \leq 1$ ■

Fact 5.7 *If G is connected, then the eigenvalue* 1 *has a unique eigenvector.*

Proof: Suppose in contradiction, that $\bar{e}_1$ and $\bar{e}_2$ are two orthogonal eigenvectors corresponding to the eigenvalue 1. Let $\bar{p} = \bar{e}_1 + \epsilon\bar{e}_2$, where $\epsilon = \frac{1}{|m|N}$ and m is the minimal entry of $\bar{e}_2$. Such ϵ ensures that for any entry with value m in e_2, the corresponding entry in $\bar{p}$ is 0 (see the proof of Fact 5.6). That means that $\bar{p}$ has some zero entries and the rest are positive entries. Since $\lambda_1 = \lambda_2 = 1$, the following holds:

$$A\bar{p} = A(\bar{e}_1 + \epsilon\bar{e}_2) = A\bar{e}_1 + \epsilon A\bar{e}_2 = 1 \cdot \bar{e}_1 + \epsilon \cdot 1 \cdot \bar{e}_2 = \bar{e}_1 + \epsilon\bar{e}_2 = \bar{p}$$

Therefore for any positive t, $A^t\bar{p} = \bar{p}$. Let i be an index of a positive entry, and let j be an index of a zero entry. Thus, the i-th entry in $\bar{p}$ is positive, whereas the j-th entry in $A^t\bar{p}$ is zero. It follows that, for any integer $t > 0$, the probability to reach from vertex i to vertex j in t steps is 0 (since $(A^t\bar{p})_j$ is the sum of the probability of reaching j in t steps, when starting in vertex k with probability p_k). This implies that for any $t > 0$, there is no path of length t between i and j which implies that the graph is not connected, thus we get contradiction. ■

Fact 5.8 *For a connected aperiodic graph G, -1 is not an eigenvalue.*

Definition 10 *A graph G is said to be aperiodic if the GCD of its cycle* (not necessarily simple cycles) *lengths is* 1.

We first notice that the GCD of all cycle lengths is at most 2. If the GCD is 2, then the graph must be bipartite with no self loops. In this case all cycles would be of even length. However, since the graph is aperiodic its GCD is 1, hence there must exist an odd cycle on the graph.

Proof: Suppose in contradiction that $\bar{e}_2$ is an eigenvector with a corresponding eigenvalue -1. Let $\bar{p} = \bar{e}_1 + \epsilon\bar{e}_2$, where $\epsilon = \frac{1}{|m|N}$ (as in the proof of Fact 5.7). Let u be an index of a zero entry in $\bar{p}$, hence negative in $\bar{e}_2$. First we claim that since there exists an odd cycle in the graph, then there is an odd cycle going through u. Such cycle can be constructed by combining the path from u to the odd cycle, the cycle itself, and the path back to u. (The path from u to the odd cycle exists because the graph is connected.) Let l be the length of such an odd cycle. Consider $A^{l+1}\bar{p}$:
On the one hand:

$$A^{l+1}\bar{p} = A^{l+1}(\bar{e}_1 + \epsilon\bar{e}_2) = A^{l+1}\bar{e}_1 + A^{l+1}\epsilon\bar{e}_2 = {\lambda_1}^{l+1}\bar{e}_1 + \epsilon{\lambda_2}^{l+1}\bar{e}_2 = \bar{e}_1 + (-1)^{l+1}\epsilon\bar{e}_2 = \bar{p}.$$

In particular, the u-th entry of $A^{l+1}\bar{p}$ is 0 (just as this entry is in $\bar{p}$).
On the other hand:

$$A^{l+1}\bar{p} = A^l(A\bar{p}) = A^l(\lambda_1\bar{e}_1 + \epsilon\lambda_2\bar{e}_2) = A^l(\bar{e}_1 - \epsilon\bar{e}_2).$$

Since the u-th entry of $\bar{e}_2$ is negative, the u-th entry of $(\bar{e}_1 - \epsilon\bar{e}_2)$ is positive. Since u is a vertex on an odd cycle with length l, there must be a positive probability to reach u in l steps when starting from u. Hence the u-th entry of $A^l(\bar{e}_1 - \epsilon\bar{e}_2) = A^{l+1}\bar{p}$ must be positive. This contradicts the previous conclusion that the u-th entry equals 0. ■

In particular, this fact holds for expanders, since the existence of self-loops implies they are aperiodic.