Lecture 10 — November 18, 2002

Lecturer: Shang-Hua Teng *Scribe: Marwan Fayed*

10.1 Expander Graphs: Some Properties and Applications

Expander graphs are important not only from a theoretical standpoint, but also in applications and engineering. Conceivably, an expander graph allows us to build communication networks with desirable properties. Such properties include (but are not limited to) guarantees with respect to making connections between two nodes, or routing messages. Moreover, the removal of an edge in an expander graph changes its properties only minimally. Hence, it is useful for constructing networks that are fault-tolerant. Expanders also have applications in other settings, including random sampling, cryptography, and coding theory.

But what is an expander graph? For now, we will say that intuitively, an expander graph is a graph for which any "small" subset of vertices has a relatively "large" neighbourhood.

All discussions rely on undirected graphs $G = (v, E)$, where V is the set of vertices or nodes, and E is the set of edges.

10.1.1 Vocabulary

Before we continue, we need to learn some new vocabulary.

- The **neighbourhood of a vertex** v is the set of all vertices adjacent to v, and is denoted by $\Gamma(v) = \{u \in V : (v, u) \in E\}$.
- This can be extended to determine the **neighbourhood of a set** of vertices $U \subset V$ by $\Gamma(U) = \cup_{u \in U} \Gamma(u)$.
- The **vertex set boundary** of a subset of vertices $U \subset V$ is denoted by $\partial U = \Gamma(U) \setminus U$. Think of the boundary as lying between those vertices in U, and those not in U. Then the boundary can be defined by the set of edges that cross it. We can then say $\partial U = \partial(V \setminus U)$.
- Lastly, a **d-regular graph** is most simply described as a graph where each vertex has degree d.

10.1.2 Combinatorics of Expanders

We first look at some of the properties of expanders that can be learned by counting methods.

Definition 10.1. *A d-regular graph is a (d, c)-expander graph (or has a c-expansion) for some $c > 0$, if and only if for every subset $U \subset V$ of size at most $|V|/2$, it is true that $|\partial U| \geq c|U|$.*

This definition says that the number of edges to grow linearly with the number of vertices. While it may not be an optimal construction in communication networks, it does guarantee good connectivity from a minimal number of edges.

There are a number of interesting (and desirable) properties with respect to connectivity in expanders that follow Definition 10.1. Suppose a node A wishes to send a message to node B. We can make the following set of remarks.

- There are at least $(1 + d)(1 + c)$ nodes sitting at distance ≤ 2 from A.
- Generally speaking, $(1 + d)(1 + c)^k$ nodes sit at distance $\leq k$ from B.
- If we continue to expand the reachable set of nodes, V_A, then eventually the number of reachable nodes will be $\geq |V|/2$. The node B may not be in V_A, but if we start from B then V_B will eventually grow to be $\geq |V|/2$.
- Since each set as at least $|V|/2$ nodes, **the sets must overlap**.
- Then we can say the overlap contains vertices from both sets, and that there exists a path from A to B of length at most $2(k + 1)$, where $k = \log_{c+1}(|V|/2)$.

A natural consequence of this set of remarks is that as c grows, the expected path length between a pair of vertices shrinks. This also leads to the following proposition.

Proposition 10.2. *For all $c >$ and for all sufficiently large n, there exists* **no** *$(2, c)$-expander graph with n vertices.*

Proof: For some arbitrary $c > 0$, consider an n-vertex graph which is 2-regular. Assume this graph is connected. Such a graph must be a closed cycle. Pick any subset of $n/2$ vertices. The size of the boundary of any such subset is 2. Now choose the number of vertices in the graph such that $c \cdot n/2 > 2$. □

However, we have yet to really define any "expanding" property of a graph. To do this, one must consider the *isoperimetric constant*, which is sometimes called the *expanding constant* of G.

Definition 10.3. *The isoperimetric constant or the expanding constant of a graph $G = (V, E)$ is*

$$h(G) = \inf \left\{ \frac{|\partial U|}{\min\{|U|, |V \setminus U|\}} : U \subset V, 0 < |U| < +\infty \right\}$$

which can be rephrased as,

$$h(G) = \min \left\{ \frac{|\partial U|}{|U|} : U \subset V,\ 0 < |U| < n/2 \right\}$$

To better understand the impact of $h(G)$, an analogy is given. If G is a network transmitting information, then $h(G)$ is a measure of the quality of the network (ie. if $h(G)$ is large, information travels efficiently through G). The extreme cases are described two examples.

Complete graph K_n of n vertices: if $|U| = l$, then the boundary of U has $l(n-1)$ edges, and $h(K_n) = n - (n/2) \approx n/2$.

Cycle C_n of n vertices: if $|U| = n/2$ then the boundary of $|U|$ has 2 edges, and $h(C_n) \leq 4/n$.

This tells us that as these two graphs grow, the complete graph keeps a large expansion constant, while the expansion constant in the cycle goes to 0.

10.1.3 Spectral Properties of Expanders

Any graph can be represented by an *adjacency matrix*, A. It is an nxn symmetric matrix (recall that edges are not directed) with real eigenvalues counting multiplicities, $\mu_0 \leq \mu_1 \leq ... \leq \mu_{n-1}$. Assuming G is a k-regular graph of n vertices, the following statements are true:

i. the largest eigenvalue $\mu_) = k$,

ii. every eigenvalue μ_i, for $1 \leq i \leq n-1$ satisfies $|\mu_i| \leq k$, and

iii. μ_0 has multiplicity 1 if and only if G is connected.

Recall in a *bipartite graph*, each node can be coloured so that no two adjacent nodes have the same colour. If G is a connected, k-regular graph of n vertices, then the following statements are equivalent.

i. G is bipartite.

ii. The spectrum of G is symmetric about 0.

iii. The smallest eigenvalue is $\mu_{n-1} = -k$.

The *spectral gap* of any finite, connected graph G is defined as $\triangle(G) = \mu_0 - \mu_1 k - \mu_1$. The spectral gap is a measure of the quality of the expander. The larger the spectral gap, the better the quality of the expander. This, however, is only true up to some bound. This is a result of the Theorem 10.4:

Theorem 10.4. *Let (G_n) be a family of finite connected k-regular graphs with $|V_n| \to \infty$ when $n \to \infty$. Then,* $\liminf_{N \to +\infty} \mu_1(G_N) \geq 2\sqrt{k-1}$.

10.1.4 Constructibility

All of these definitions and properties are nice, but how much time does it take to construct graphs with such elegant properties?

Consider a family of expander graphs G_N and assume that $N = 2^n$, for some n. Then the vertices of G_N are the 2^n strings of length n.

Definition 10.5. G_N **is weakly constructible** *if an explicit representation can be provided in polytime*(N).

Definition 10.6. G_N **is strongly constructible** *if, when given an n-bit long vertex of G_N, we can construct a list of its neighbours in polytime*(N).

An explicit representation is simply an adjacency matrix (or some other equivalent representation).

Two methods[1] mentioned to construct expander graphs are given by Gabber and Galil, and Reihgold, Vadham, and Wigderson, who use bipartite graphs and zig-zag graph products, respectively.

Special thanks are due to Mohamed Alimi, who was gracious enough to review presented material, and clarify where necessary.

[1] For explicit construction, see references given in survey report.