Expander Graphs and Applications

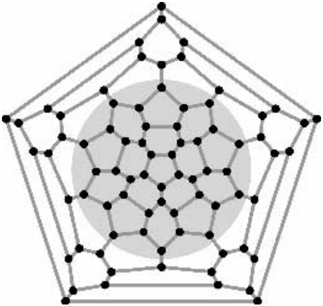
Amelia Wallace

University of North Carolina at Chapel Hill

July 22, 2009

What is an Expander Graph?

An *expander graph* is a sparse graph with high connectivity properties. Expander graphs have applications in the economical design of phone and computer networks and in various aspects of computer science, including complexity theory, coding theory and cryptography.



Definitions

Given a graph $X = (V, E)$ and $|V| = n$:

- The *edge boundary* of a set $F \subsetneq V$, $\partial F = E(F, V - F)$, is the set of edges connecting F to $V - F$.
  Note: $\partial F = \partial(V - F)$
- The *expansion parameter*, or isoperimetric constant of X, denoted $h(X)$, is defined as:

$$h(X) = \inf \left\{ \frac{|\partial F|}{\min\{|F|, |V - F|\}} : F \subsetneq V, \quad 0 < |F| < +\infty \right\}$$

Note: When X is finite, this expression can be reduced to:

$$h(X) = \min \left\{ \frac{|\partial S|}{|S|} : \; 0 < |S| \leq \frac{n}{2} \right\}$$

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Families of Expanders

A *family of expanders* is is a family $(X_m)_{m \geq 1}$ of finite, connected k-regular graphs $X_m = (V_m, E_m) \quad m \in \mathbb{N}$ such that

- $|V_m| \to +\infty$ as $m \to +\infty$
- there exists an $\epsilon > 0$ such that $h(X_m) > \epsilon$ for all $m \geq 1$

Example: For all prime p, $V_p = \mathbb{Z}_p$ and $k = 3$.
Each vertex x is connected to its neighbors and its inverse (i.e. $x + 1$, $x - 1$, and x^{-1})

Construction of Expanders

Probabilistic arguments have shown that almost all k-regular graphs ($k \geq 3$) are expanders, but their explicit construction is difficult. There are methods for constructing some expanders:

- The Gabber-Galil Construction
- Constructions using the Cayley graphs of groups; in particular $PGL(2, F_q)$.
- The Margulis construction.
- The Zig-Zag product of two expander graphs is also an expander.

Adjacency Matrix

The *adjacency matrix* of a graph G is a matrix $A = (a_{xy})$ indexed by pairs of vertices $x, y \in V$,where the entry a_{xy} is the number of edges joining x to y.

By definition, A is symmetric, so it has and orthonormal base $v_0, v_1, ..., v_{n-1}$ with real eigenvalues $\mu_0, \mu_1, ..., \mu_{n-1}$ such that for all i, we have $Av_i = \mu_i v_i$. Without loss of generality, we can sort the eigenvalues in descending order $\mu_0 \geq \mu_1 \geq ... \geq \mu_{n-1}$.

Spectrum of a Graph

The *spectrum* of G is the set of eigenvalues of the adjacency matrix of G.

The spectrum of a graph contains a lot of information about the graph. For a k-regular graph:

- $\mu_0 = k$
- The graph is connected iff $\mu_0 > \mu_1$
- The graph is bipartite iff $\mu_0 = -\mu_{n-1}$

The *spectral gap* is the difference between the two largest eigenvalues; i.e. $\mu_0 - \mu_1$ or $k - \mu_1$.

Eigenvalue Bounds

- **Theorem** (Tamner, Alon and Milman):

$$\frac{k-\mu_1}{2} \leq h(G) \leq \sqrt{2k(k-\mu_1)}$$

- **Expander Mixing Lemma:**
  Let $\lambda = \max(|\mu_1|, |\mu_{n-1}|)$
  for all $S, T \subseteq V$:

$$||E(S,T)| - \frac{d|S||T|}{n}| \leq \lambda\sqrt{|S||T|}$$

Deterministic Error Amplification for BPP

Suppose we are given a function in $\mathcal{BPP}$. This means we have a function $f : \{0,1\}^n \rightarrow \{0,1\}$ and a probabilistic polynomial time algorithm $\mathcal{A}$ that approximates f in the sense that for random $r \in \{0,1\}^m$ we have:

$$Pr_r\left[\mathcal{A}(x,r) \neq f(x)\right] \leq \frac{1}{4}$$

For t calls to $\mathcal{A}$ this uses $t \cdot m$ coin tosses. We want to reduce errors, while using a small number of coin tosses.
Let $\mathcal{B}$ be an algorithm that uses only m coin tosses: for a d-regular expander graph G with 2^m vertices, $v \in V(G)$

$$\mathcal{B}(x,v) = Majority_{u \in \Gamma(v)} \mathcal{A}(x,u)$$

Claim:

$$Pr_v[\mathcal{B}(x,v) \neq f(x)] \leq 4\left(\frac{\lambda}{d}\right)^2$$

Proof. Let S be the set of vertices on which $\mathcal{B}$ errs, and T be the set on which $\mathcal{A}$ errs.
So, $|E(S,T)| \geq |S|\frac{d}{2}$ and $|T| \leq \frac{N}{4}$.

$$\begin{aligned}
|E(S,T)| - \frac{d|S||T|}{N} &\leq \lambda\sqrt{|S||T|} \\
\frac{d|S|}{2} - \frac{d|S|}{4} &\leq \lambda\sqrt{|S|\frac{N}{4}} \\
\frac{d|S|}{4} &\leq \lambda\sqrt{|S|\frac{N}{4}} \\
Pr_v[\mathcal{B}(x,v) \neq f(x)] = \frac{|S|}{N} &\leq 4\left(\frac{\lambda}{d}\right)^2
\end{aligned}$$

References

1. Davidoff, G; Sarnak, P; Valette, A. Elementary Number Theory, Group Theory, and Ramanujan Graphs. Cambridge University Press 2003.
2. Linial, N; Wigderson, A. Expander Graphs and Their Applications. The Hebrew University. Jerusalem, Israel.
3. Reingold, O; Vadhan, S; Wigderson A. Entropy waves, the zig-zag graph product, and new constant-degree expanders. Annals of Mathematics 155, pages 157-187, 2002.
4. Xiao, D; The Evolution of Expander Graphs. (BA thesis, Harvard College, 2003)