CS 880: Pseudorandomness and Derandomization 3/4/2013

Lecture 10: Expander Constructions

Instructors: Holger Dell and Dieter van Melkebeek Scribe: Xi Wu

In the previous lecture we defined expander graphs using the notion of spectral gap, and derived a number of interesting properties of expander graphs of low degree. In this lecture, we first argue that expanders with nontrivial parameters *exist*. In fact, we will see that a random d-regular graph is a good expander with high probability, and that no d-regular graph can have significantly better expansion.

This suggests a randomized construction of expanders, which however uses too many random bits for the derandomization applications that we will cover later. What we need are *explicit* constructions, i.e., families of expander graphs that can be built in an efficient deterministic way.

We consider two notions of explicitness. We say that a family of expanders is *mildly explicit* if the (multiset of) neighbors of a vertex can be computed in time $\text{poly}(N)$, where N denotes the number of vertices. We call a family *fully explicit* if, on input the label of a vertex u and an index ℓ, we can compute the label of the end point v of the ℓth outgoing edge from u in time polynomial in the length of the description of the label and the length of the index, i.e., in time $\text{poly}\log(N)$. This presupposes an ordering of the outgoing edges at every vertex u. Such an ordering facilitates the description of a random walk on G.

Ideally, the family contains an expander for every number of vertices. Typically, we will only be able to realize a subset of the natural numbers that is sufficiently dense for the applications.

There are two general approaches for constructing explicit expanders:

- *Direct Constructions*
  All known direct constructions are based on groups or, more generally, on group actions. They are simple to describe and therefore very explicit, but their analysis typically involves heavy mathematical machinery: harmonic analysis, representation theory, number theory, and additive combinatorics. We only introduce the general approach and state some of the direct constructions, but do not present their analysis. We refer to the recent survey [Yeh12] for more information.

- *Iterative Constructions*
  These constructions start from a small expander, and iteratively build larger and larger ones using simple graph operations. They are harder to describe, but their analysis is elementary and intuitive. We develop an iterative construction in full detail, namely one based on the replacement product (or the zig-zag product) of graphs.

1 Existence and Limitations of Expanders

We begin with the following theorem, which gives an upper bound on the spectral gap $1 - \lambda(G)$ as a function of the degree d.

Theorem 1 ([Alo86]). *Let d be a positive integer. Every d-regular multigraph G on N vertices satisfies $\lambda(G) \geq 2\sqrt{d-1}/d - o(1)$.*

In other words, if d is constant and N is large, then there are no regular N-vertex graph G of degree d can have $\lambda(G)$ significantly smaller than $2\sqrt{d-1}/d$. Regular multigraphs of degree d that match this bound, i.e., for which $\lambda(G) \leq 2\frac{\sqrt{d-1}}{d}$, are called *Ramanujan graphs.*

The following theorem shows that random d-regular graphs are almost Ramanujan with high probability.

Theorem 2 ([Fri08]). *Let d be a positive integer. There exists a function $f(N) = o(1)$ such that the probability that a random d-regular multigraph G on N vertices satisfies $\lambda(G) \leq 2\sqrt{d-1}/d + f(N)$ is at least $1 - o(1)$.*

Another way to state this result is that *almost all* d-regular multigraphs have almost-optimal expansion, namely have $\lambda(G)$ close to $2\sqrt{d-1}/d$. The search for deterministic constructions of expander graphs can therefore be viewed as a derandomization problem.

2 Direct Constructions

An appealing approach to construct expanders is as *Cayley graphs of finite groups.*

Definition 1 (Cayley graph). *For any finite group H and any subset $S \subseteq H$, the Cayley graph $\mathrm{C}(H, S)$ is the digraph with vertex set H, and (a, b) is an edge if $a^{-1}b \in S$. In other words, all neighbors of a vertex $a \in H$ are of the form as for some $s \in S$.*

Note that $\mathrm{C}(H, S)$ is a regular digraph of degree S. It is undirected iff $S^{-1} \subseteq S$. For $\mathrm{C}(H, S)$ to be an expander, S better be a generating set; otherwise, $\mathrm{C}(H, S)$ is not strongly connected and therefore its spectral gap vanishes.

The characters of H are always eigenvectors of the transition matrix $M_{\mathrm{C}(H,S)}$ for the random walk on $\mathrm{C}(H, S)$, irrespective of the choice of S. The corresponding eigenvalues depend on S, as given in the next proposition.

Proposition 3. *Let H be a finite group, $S \subseteq H$, and $\chi : H \mapsto \mathbb{C}$ a character of H. Let M denote the transition matrix $M_{\mathrm{C}(H,S)}$, and $x \in \mathbb{C}^{|H|}$ be the vector with $x_a = \chi(a)$ for $a \in H$. Then x is an eigenvector of G with eigenvalue*

$$\frac{1}{|S|} \sum_{s \in S} \chi(s^{-1}) \,. \tag{1}$$

Proof. For $a, b \in H$, we have $M_{ab} = \frac{1}{|S|} I[(\exists s \in S)\, a = bs] = \frac{1}{|S|} I[b^{-1}a \in S]$, so

$$\begin{aligned} (Mx)_a = \sum_{b \in H} M_{ab} x_b &= \sum_{b \in H} \frac{1}{|S|} I[b^{-1}a \in S] \cdot \chi(b) \\ &= \frac{1}{|S|} \sum_{s \in S} \chi(as^{-1}) \\ &= \frac{1}{|S|} \sum_{s \in S} \chi(a)\chi(s^{-1}) \\ &= \left(\frac{1}{|S|} \sum_{s \in S} \chi(s^{-1}) \right) x_a. \end{aligned}$$

This shows that x is an eigenvector of M with the stated eigenvalue. □

Note that the trivial characters $\chi \equiv 1$ corresponds to the eigenvector $\vec{1}$ with eigenvalue 1.

In the case that H is Abelian, the characters of H form a full orthogonal basis for $\mathbb{C}^N$. It follows from Proposition 2 from Lecture 9 that

$$\lambda(C(H,S)) = \max_{\chi \not\equiv 1} \left| \frac{1}{|S|} \sum_{s \in S} \chi(s^{-1}) \right| = \max_{\chi \not\equiv 1} \left| \frac{1}{|S|} \sum_{s \in S} \chi(s) \right|, \tag{1}$$

where the last equality follows because $\chi(s^{-1}) = 1/\chi(s)$ and $1/\chi$ is a character whenever χ is.

For the Boolean cube, i.e., for $H = (\{0,1\}^n, +)$, the characters are of the form $\chi_a : x \mapsto (-1)^{\langle x,a \rangle}$ where $a \in \{0,1\}^n$, and the right-hand side of (1) is exactly the bias of U_S, the uniform distribution on S:

$$\frac{1}{|S|} \sum_{s \in S} \chi_a(s) = \frac{1}{|S|} \sum_{s \in S} (-1)^{\langle s,a \rangle} = \mathrm{E}_{s \leftarrow U_S}[(-1)^{\langle s,a \rangle}] = \mathrm{bias}_a(U_S).$$

This generalizes to every finite Abelian group with a natural generalization of the notion of bias. Thus, for finite Abelian groups, the goal of constructing a good Cayley expander of low degree is equivalent to the construction of a small set with small bias.

However, it turns out that Cayley graphs of Abelian groups cannot be good expanders of small degree – in order to have a spectral gap bounded below by some positive constant their degree needs to be $\Omega(N/\log\log(n))$. The argument hinges on the fact that the diameter of such expanders is logarithmic. This means that every group element can be written as a sum of $\Delta = O(\log N)$ terms, each from the set S. Since the group is Abelian, terms in this sum can be rearranged, and the element can be fully described by the number of times each element of S appears in the sum. As there are at most $\Delta^{|S|}$ such descriptions, we need that $\Delta^{|S|} \geq N$. This implies that $|S| = \Omega(N/\log(\Delta)) = \Omega(N/\log\log(N))$.

Thus, we need to consider non-Abelian finite groups and their Cayley graphs. More generally, we make use of *group actions* and their *Schreier graphs*, which we define next.

Definition 2 (Group action and Schreier graph). *Given a set X and a group H, an action of H on X is a mapping $\cdot : X \times H \to X$ such that the following conditions are satisfied:*

- ○ $(\forall x \in X)\, x \cdot 1 = x$.
- ○ $(\forall x \in X)\, (\forall g,h \in H)\, x \cdot (gh) = (x \cdot g) \cdot h$,

The action of H on X defines a group itself, which we also denote by H. Given a set $S \subseteq H$, we define the Schreier graph $\mathrm{S}(X,H,S)$ *to be the digraph with vertex set X and edges of the form $(x, x \cdot s)$ where $s \in S$.*

Note that Cayley graphs are Schreier graphs where G acts on itself by right multiplication.

The approach using Schreier graphs has been very effective, in particular when the group H is non-Abelian (needed by the above argument) and X itself has an Abelian group structure (so that harmonic analysis can still be applied). We describe two particularly interesting constructions along these lines.

Simple fully explicit constructions. We begin with a construction that acts on a discrete torus.

Construction 1. *Let M be a positive integer. The vertex set of G_{M^2} is $V \doteq \mathbb{Z}_M \times \mathbb{Z}_M$, where $\mathbb{Z}_M$ denotes the additive group of the integers modulo M. For each vertex $(x,y) \in V$, we define 8 neighbors (with multiplicity) as*

$$(x \pm y, y), (x \pm (y+1), y), (x, y \pm x), (x, y \pm (x+1)).$$

The graph G_{M^2} in Construction 1 can be viewed as the Schreier graph $\mathrm{S}(X,H,S)$ where $X = \mathbb{Z}_M \times \mathbb{Z}_{\mathbb{M}}$, H denotes (the action of) the unimodular affine transformations on X, i.e., mappings of the form $z \mapsto Az + b$ with $|\det(A)| = 1$, and S consists of the transformations $L_{b,s}$ and $L_{b,s} + s \cdot e_b$ for $b \in \{0,1\}$ and $s \in \{-1,1\}$, where $L_{0,s}$ and $L_{1,s}$ denote the linear transformations defined by

$$\begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 1 & 0 \\ s & 1 \end{bmatrix},$$

respectively, and where

$$e_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{and} \qquad e_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

As there are 8 transformations in total, the degree of G is 8. The determinant of each $L_{b,s}$ is 1, so all transformations are unimodular and therefore invertible over $\mathbb{Z}_M$. In fact, $L_{b,s}^{-1} = L_{b,-s}$, which implies that G is undirected.

Note that, given $z \in \mathbb{Z}_M \times \mathbb{Z}_M$, we can compute the neighbors of z in G_{M^2} in time and space $O(\log N)$, where $N = M^2$ denotes the number of vertices. Thus, Construction 1 is fully explicit.

Construction 1 yields a family of graphs that is fairly dense. It contains a graph for every number of vertices that is a positive square.

Finally, we have the following theorem about the spectral expansion of this construction.

Theorem 4. *There exists a constant $\lambda < 1$ such that every graph G_{M^2} from Construction 1 satisfies $\lambda(G_{M^2}) \leq \lambda$.*

We refer to [GG81] for a proof.

A construction that is even simpler to describe but only mildly explicit, acts on a cycle.

Construction 2. *Let p be a prime. The vertex set of G_p is $V \doteq \mathbb{Z}_p$, where $\mathbb{Z}_p$ denotes the field of the integers modulo p. For each vertex $x \in V$, we define 3 neighbors as*

$$x+1, x-1, \text{ and } x^{-1},$$

where 0^{-1} is defined as 0.

The graph G_p is the Schreier graph $\mathrm{S}(X,H,S)$, where $X = \mathbb{Z}_p$, H denotes (the action of) the unimodular linear fractional transformations on X, i.e., mappings of the form

$$x \mapsto \frac{ax+b}{cx+d} \qquad \text{with} \qquad \left| \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right| = 1,$$

and S consists of the transformations corresponding to the matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \text{ and } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The graph G_p has degree 3 and is undirected. When p is given, the neighbors in G_p can be computed in time $\operatorname{poly}\log(p)$, which is very efficient but somewhat more complex than Construction 1 due to the need to compute an inverse modulo p. There exists such a graph for every prime p, thus the family is fairly dense by the prime number theorem. However, we do not know how to find a prime p that is close to a target number of vertices N in deterministic time $\operatorname{poly}\log(N)$. Exhaustive search finds one in time $\operatorname{poly}(N)$. As such, Construction 2 is mildly explicit but not fully explicit.

The spectral gap of G_p is constant, as stated in the next result.

Theorem 5. *There exists a constant $\lambda < 1$ such that every graph G_p from Construction 2 satisfies $\lambda(G_p) \leq \lambda$.*

We refer to [Lub94, Theorem 4.42] for a proof.

Ramanujan graphs. Recall that d-regular graphs that achieve the bound $\lambda(G) \leq 2\sqrt{d-1}/d$ are called *Ramanujan graphs*, and Theorem 2 says that almost all d-regular graphs are almost Ramanujan. There are explicit constructions of Ramanujan graphs. We describe one such construction.

Construction 3. *Let p, q be distinct primes such that $p \equiv q \equiv 1 \bmod 4$ and p is a square modulo q. Let $i \in \mathbb{Z}_q$ be such that $i^2 \equiv -1 \bmod q$. We define the graph $G = (V, E)$ where $V \doteq \mathbb{Z}_q \cup \{\infty\}$ denotes the field of the integers modulo q plus one extra node representing infinity. For each vertex $x \in V$, we define its neighbors as all vertices of the form*

$$\frac{(a_0 + ia_1)x + (a_2 + ia_3)}{(-a_2 + ia_3)x + (a_0 - ia_1)}$$

for $a_0, a_1, a_2, a_3 \in \mathbb{Z}_p$ such that $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$, a_0 odd and positive, and a_1, a_2, a_3 are even.

The graph G is the Schreier graph $\mathrm{S}(X, H, S)$, where $X = \mathbb{Z}_q \cup \{\infty\}$, H denotes (the action of) the invertible linear fractional transformations on X, and S consists of those transformations corresponding to matrices of the form

$$\begin{bmatrix} a_0 + ia_1 & a_2 + ia_2 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix}, \tag{2}$$

where the a_j's and i are as stated in Construction 3.

Note that the determinant of (2) equals $a_0^2 + a_1^2 + a_2^2 + a_3^2 \equiv p \not\equiv 0 \bmod q$, so the transformations are invertible. In fact, the inverse of the transformation induced by (a_0, a_1, a_2, a_3) is induced by $(a_0, -a_1, -a_2, a_3)$. It follows that the graph G is undirected.

The condition that $q \equiv 1 \bmod 4$ guarantees that -1 is a square modulo q, i.e., that i in Construction 3 exists. The condition that p is a square modulo q guarantees that G is not bipartite (which is a necessary condition to be an expander). If p is not a square modulo q, the resulting graph G is a so-called bipartite expander. These facts as well as the following theorem can be proved using number theory, including results related to the "Ramanujan conjectures," from which the name "Ramanujan graphs" originates. We refer to [Sar90, Lub94] for more about the underlying mathematical machinery and the proofs.

Theorem 6. *The graph G in Construction 3 is a regular Ramanujan graph of degree $p+1$.*

Like Construction 2, Construction 3 is mildly explicit but not explicit. In fact, it is an open problem whether fully explicit Ramanujan graphs exist.

3 Iterative Constructions

We now develop and fully analyze an iterative combinatorial construction of expanders. The idea is to start with a good expander graph G_0 of constant size, and then use graph products to iteratively construct a sequence $G_1, G_2, \dots$ of multigraphs of increasing size, while keeping the degree of the graph and the expansion under control.

The multigraphs G that we construct will be undirected and d-regular, and may have parallel edges. We describe them via the notion of a *neighbor function* $\Gamma_G : V(G) \times [d] \to V(G)$, where $\Gamma(u, \ell)$ denotes the vertex we reach from u if we follow the ℓth edge out of u. Since G is undirected, for every edge between u and v there exist unique $\ell \in [d]$ and $\ell' \in [d]$ such that $\Gamma_G(u, \ell) = v$ and $\Gamma_G(v, \ell') = u$. This holds even in the presence of parallel edges, where the uniqueness property is interpreted as follows: The values for ℓ used for distinct edges incident with u are distinct, as are the values for ℓ' used for distinct edges incident with v, where distinct edges may go between the same end points u and v.

Note that ℓ and ℓ' may differ for a given undirected edge between u and v, i.e., the edge may be labeled differently at u and at v. A neighbor function Γ under which $\ell = \ell'$ for all edges is equivalent to a proper edge coloring of G with d colors, i.e., a mapping $c : E(G) \to [d]$ such that incident edges receive distinct colors. We point out that not every d-regular multigraph has a proper edge coloring with d colors. For example, an odd cycle does not have a proper edge coloring with two colors; it does have one with three colors. In general, Vizing's Theorem states that every d-regular multigraph has a proper edge coloring with d or $d+1$ colors, but deciding whether one exists with d colors is NP-complete.

3.1 The initial graph

There are several ways to pick the initial multigraph G_0. Since it has some constant size N_0 and constant degree d, we could use brute force to find one that has sufficiently small $\lambda(G_0)$ (e.g., is Ramanujan). Doing so will take constant time, although we would probably want to avoid this approach in practice. A simpler choice, and the one we are going to use, is to pick G_0 as the complete graph K_d on $N_0 = d$ vertices with all self-loops. Note that K_d has a proper edge coloring with d colors: for $u, v \in V(K_d) = [d]$, we set $c(\{u, v\}) = (u + v) \bmod d + 1$. Since $\lambda(K_d) = 0$, the expansion is perfect.

3.2 Tensor product: Squaring the size

One of the simplest graph products is the *tensor product*. Its role in our construction is to increase the size of the graph quickly.

Definition 3 (Tensor product). *The* tensor product *of a multigraph G of degree d_G and a multigraph G' of degree $d_{G'}$ is the multigraph $G \otimes G'$ whose vertex set is $V(G) \times V(G')$, whose degree is $d_G d_{G'}$, and whose edges are defined by the neighbor function*

$$\Gamma_{G\otimes G'} : \big(V(G) \times V(G')\big) \times \big([d_G] \times [d_{G'}]\big) \to \big(V(G) \times V(G')\big)$$
$$\Gamma_{G\otimes G'}\Big((u,u'),(\ell,\ell')\Big) = \big(\Gamma_G(u,\ell), \Gamma_{G'}(u',\ell')\big)\,.$$

Note that if G and G' are undirected, then so is $G \otimes G'$. Also, if Γ_G and $\Gamma_{G'}$ correspond to a proper edge coloring, then so does $\Gamma_{G\otimes G'}$.

In order to construct the desired sequence of expanders of increasing size, we could try to inductively define the sequence as $G_i = G_{i-1} \otimes G_{i-1}$. In each iteration, the number of vertices gets squared, so the number of vertices at step i is equal to $|V(G_0)|^{2^i}$, which quickly grows to the size we desire. The expansion of these graphs is very good, but this comes at a price. If G_0 is the complete graph, then all graphs G_i in the sequence are actually complete graphs. More generally, the problem is that next to the number of vertices, the degree gets squared in every iteration as well, which is no good if we want to construct expanders of constant degree.

Still, if we somehow manage to reduce the degree, the tensor product can be an important building block to make the graphs grow quickly in our construction. The sequence does not consist of complete graphs anymore, but we can still guarantee that the expansion of the tensor product is at least as good as the expansion of its components, as is formalized in the following lemma.

Lemma 7. $\lambda(G \otimes G') = \max(\lambda(G), \lambda(G'))$.

Proof. The transition matrix of the random walk on the graph tensor product corresponds to the usual tensor product of the transition matrices. Indeed, if A and A' are the transition matrices of G and G', respectively, then the matrix $A \otimes A' = (A_{vu}A'_{v'u'})_{v,u\in[N];\, v',u'\in[N']}$ is the transition matrix of $G \otimes G'$. Since A and A' are real symmetric matrices, they have orthonormal bases of eigenvectors, say $(w_1, \ldots, w_N)$ and $(w'_1, \ldots, w'_{N'})$, corresponding to eigenvalues $\lambda_1, \ldots, \lambda_N$ and $\lambda'_1, \ldots, \lambda'_{N'}$, respectively. Then we observe that $\{w_i \otimes w'_j\}_{i\in[N],j\in[N']}$ is an orthonormal basis of $\mathbb{R}^{NN'}$, and straightforward computation shows that $(A \otimes A')(w_i \otimes w'_j) = (Aw_i \otimes A'w'_j) = \lambda_i\lambda'_j(w_i \otimes w'_j)$, Therefore the set $\{\lambda_i\lambda'_j\}_{i\in[N],j\in[N']}$ is the set of all eigenvalues of $A \otimes A'$. Recall that the largest eigenvalue of a regular graph is 1. Therefore, the largest eigenvalue of $A\otimes A'$ is $1\cdot 1$, and the second-largest one (in absolute value) is either $1 \cdot \lambda(G')$ or $\lambda(G) \cdot 1$. Thus $\lambda(G \otimes G') = \max(\lambda(G), \lambda(G'))$.□

3.3 Replacement product: Reducing the degree

To counteract the tensor product's degree explosion, we use an operation that reduces the degree of a multigraph without deteriorating the spectral gap by too much. The simplest way to reduce the degree without loosing the connectivity or the overall structure is to replace every vertex u of degree d by a copy of d fresh vertices $u_1, \ldots, u_d$ that are connected in a cycle. We refer to those d vertices as the *cloud* of u. Furthermore, the d edges incident to u get distributed to the d vertices of the cycle in such a way that that the resulting graph remains undirected. Formally, for G of degree d_G, we define the graph G' with vertex set $V(G) \times [d_G]$ via the following neighbor function:

$$\Gamma_{G'}\big((u,\ell);1\big) = (u,\ell+1)$$
$$\Gamma_{G'}\big((u,\ell);2\big) = (u,\ell-1)$$
$$\Gamma_{G'}\big((u,\ell);3\big) = (v,\ell'),$$

where $\ell + 1$ denotes the successor and $\ell - 1$ the predecessor in the cycle of length d_G, $v \doteq \Gamma_G(u, \ell)$, and $\ell' \in [d_G]$ is such that $\Gamma(v, \ell') = u$. Note that ℓ' is well-defined because G is undirected.

Basically, label 1 means staying within the same cloud and moving one position in one direction, label 2 means the same but moving in the opposite direction, and label 3 means jumping to a neighboring cloud, namely the one corresponding to $v \doteq \Gamma(u, \ell)$. Note that v could coincide with u, in which case G' would have a self-loop at (u, ℓ) labeled 3.

By replacing every vertex by a cycle, we thus obtain a multigraph G' that is undirected and 3-regular. We still need to check how our construction fares with respect to the spectral expansion. It turns out that the cycle does not do so well in this respect.

Exercise 1. *Let $\tilde{H}$ denote the d-cycle H with self-loops added at every vertex for even d.*

(a) Show that if Γ_G corresponds to a proper edge coloring of G, then $\lambda(G') \geq \lambda(\tilde{H})$.
Hint: Use the characterization given in Proposition 1 from Lecture 9, consider the same optimal vector in each copy of H, and match up the components of different copies according to the proper edge coloring.

(b) Show that $\lambda(\tilde{H}) \geq \sqrt{1 - \frac{32}{9d}}$.
Hint: Again use the characterization given in Proposition 1 from Lecture 9, and consider the vector $x \in \{-1, 1\}^d$ representing a cut of the cycle into two equal connected halves.

By combining parts (a) and (b) from Exercise 1, we have that $\lambda(G') \geq \sqrt{1 - \frac{32}{9d}}$, which is too close to 1 for our purposes.

The reason the cycle fails to maintain a good spectral gap in the construction is because its own spectral gap (or that of the closely related variant that has a self-loop at every vertex) is not good. Instead of replacing each vertex with a cycle, we can replace it with some other multigraph H on the vertex set $V(H) = [d_G]$ that has a good spectral gap and some constant degree d_H. We also duplicate each original edge from G into d_H parallel edges that cross between clouds in the replacement product in order to make the event that a random walk moves between clouds and the event that it moves within a cloud equally probable. This leads to the following definition of the replacement product.

Definition 4 (Replacement product). *The* replacement product *of a multigraph G of degree d_G and a multigraph H of degree d_H with vertex set $V(H) = [d_G]$ is the multigraph $G \textcircled{r} H$ whose vertex set is $V(G) \times [d]$, whose degree is $2d_H$, and whose edges are defined by the neighbor function*

$$
\begin{aligned}
&\Gamma_{G \textcircled{r} H} : \big(V(G) \times V(H)\big) \times [2d_H] \to \big(V(G) \times V(H)\big) \\
&\Gamma_{G \textcircled{r} H}\big((u, \ell); 1\big) = (u, \Gamma_H(\ell, 1)) \\
&\qquad \vdots \\
&\Gamma_{G \textcircled{r} H}\big((u, \ell); d_H\big) = (u, \Gamma_H(\ell, d_H)) \\
&\Gamma_{G \textcircled{r} H}\big((u, \ell); d_H + 1\big) = (v, \ell') \\
&\qquad \vdots \\
&\Gamma_{G \textcircled{r} H}\big((u, \ell); 2d_H\big) = (v, \ell'),
\end{aligned}
$$

where $v \doteq \Gamma_G(u, \ell)$, and $\ell' \in [d_G]$ is such that $\Gamma(v, \ell') = u$.

Note that the replacement product is only defined if H has the same number of vertices as the degree of G, and that ℓ' in the above definition is well-defined because G is undirected. Also, $G \textcircled{r} H$ is undirected, and if both Γ_G and Γ_H correspond to proper edge colorings then so does $\Gamma_{G \textcircled{r} H}$.

We will prove that the spectral expansion of $G \textcircled{r} H$ is not much worse than the spectral expansions of G and H. For this, we consider random walks in $G \textcircled{r} H$ of length 3 and focus on the case where the first edge stays within a cloud, the second edge crosses to another cloud, and the third edge again stays within a cloud. Instead of performing the 3-step approach in the *analysis* of the replacement product, it is also possible to directly consider the graph that is defined by those walks on the same vertex set as $G \textcircled{r} H$. We refer to this multigraph as the *zig-zag product* $G \textcircled{z} H$, and formally define it as follows.

Definition 5 (Zig-Zag product). *The* zig-zag product *of a multigraph G of degree d_G and a multigraph H of degree d_H with vertex set $V(H) = [d_G]$ is the multigraph $G \textcircled{z} H$ whose vertex set is $V(G) \times [d_G]$, whose degree is d_H^2, and whose edges are defined by the neighbor function*

$$\begin{aligned}
&\Gamma_{G \textcircled{z} H} : \big(V(G) \times V(H)\big) \times [d_H]^2 \to \big(V(G) \times V(H)\big) \\
&\Gamma_{G \textcircled{z} H}\big((u,\ell);(a,b)\big) = \Gamma_{G \textcircled{r} H}(\Gamma_{G \textcircled{r} H}(\Gamma_{G \textcircled{r} H}((u,\ell);a);d_H+1);b).
\end{aligned}$$

Note that in $G \textcircled{z} H$ we do not duplicate edges that cross between clouds, as we did in $G \textcircled{r} H$. An edge label $(a,b) \in [d_H] \times [d_H]$ specifies the walk a, d_H+1, b in $G \textcircled{r} H$.

Like the replacement product, the zig-zag product is only defined if H has the same number of vertices as the degree of G, and $G \textcircled{z} H$ is undirected. Unlike $G \textcircled{r} H$, it does not hold in general that if both Γ_G and Γ_H correspond to proper edge colorings then so does $\Gamma_{G \textcircled{z} H}$. Indeed, in general, the following will not hold: $(u,\ell) = \Gamma_{G \textcircled{z} H}\big(\Gamma_{G \textcircled{z} H}((u,\ell);(a,b));(a,b)\big)$.

We now analyze $\lambda(G \textcircled{z} H)$, which we will then use to upper bound $\lambda(G \textcircled{r} H)$. Intuitively, since H is a good expander, the first step in the above walk of length 3 is close to choosing a uniform vertex in the same cloud, the second step then deterministically moves to a neighboring cloud depending on where we moved to in the first step, and the third step is again close to choosing a uniform vertex within the new cloud. Thus the whole "zig-zag" process is close to a single random step in G and a single independent random step in H.

Before formalizing this intuition, let us introduce some notation for various relevant transition matrices:

1. A denotes the adjacency matrix of G.

2. $B \doteq M_H$ denotes the transition matrix of a random walk on H.

3. $\hat{A}$ denotes the adjacency matrix corresponding to edges *between* the clouds of $G \textcircled{r} H$, that is, we have $\hat{A}_{(v,\ell'),(u,\ell)} = 1$ if $\Gamma_G(u,\ell) = v$ and $\Gamma_G(v,\ell') = u$; otherwise $\hat{A}_{(v,\ell'),(u,\ell)} = 0$.

4. $\hat{B} = I_N \otimes B$ denotes the transition matrix for a random walk *within* any cloud of $G \textcircled{r} H$, that is, $\hat{B}_{(u,\ell'),(u,\ell)} = B_{\ell',\ell}$ and $\hat{B}_{(v,\ell'),(u,\ell)} = 0$ for distinct $u, v \in V(G)$.

Then the transition matrix for a random walk on the replacement product and on the zig-zag-product can be written as

$$\begin{aligned} M_{G \textcircled{r} H} &= \frac{1}{2}\hat{B} + \frac{1}{2}\hat{A}, && (3) \\ M_{G \textcircled{z} H} &= \hat{B}\hat{A}\hat{B}. && (4) \end{aligned}$$

With those expressions in hand, we first upper bound $\lambda(G \textcircled{z} H)$ and then $\lambda(G \textcircled{r} H)$.

Lemma 8. $\lambda(G \textcircled{z} H) \leq 1 - (1 - \lambda(H))^2 \cdot (1 - \lambda(G))$.

Proof. Let $\lambda \doteq \lambda(G)$ and $\mu \doteq \lambda(H)$. We decompose the matrix B using Proposition 3 from Lecture 9:

$$B \doteq M_H = (1-\mu)M_K + \mu\Delta,$$

where K denotes the complete graph with self-loops on d vertices, and Δ is an error term with matrix norm $\|\Delta\|_2 \leq 1$. Plugging this decomposition into (4) and using the linearity of the matrix tensor product, we can write

$$\begin{aligned} M_{G \textcircled{z} H} &= (1-\mu)^2 \cdot (I \otimes M_K)\hat{A}(I \otimes M_K) + (1-\mu)\mu \cdot (I \otimes M_K)\hat{A}(I \otimes \Delta) \\ &\quad + \mu(1-\mu) \cdot (I \otimes \Delta)\hat{A}(I \otimes M_K) + \mu^2 \cdot (I \otimes \Delta)\hat{A}(I \otimes \Delta) \\ &= (1-\mu)^2 A \otimes M_K + \big(1 - (1-\mu)^2\big)\Delta', \end{aligned}$$

where Δ' is defined so that the last equality holds, and we note that $(I \otimes M_K)\hat{A}(I \otimes M_K) = A \otimes M_K$ holds because both correspond to the transition matrix of a random walk on the graph $G \otimes K$, where we pick a random neighbor in G and a random vertex in the corresponding cloud independently. We further note that Δ' is a convex combination of the matrices $(I \otimes M_K)\hat{A}(I \otimes \Delta)$, $(I \otimes \Delta)\hat{A}(I \otimes M_K)$, and $(I \otimes \Delta)\hat{A}(I \otimes \Delta)$. The matrix $\hat{A}$ is a permutation matrix and therefore has 2-norm 1. As $\|M_K\|_2 = 1$ and $\|\Delta\|_2 \leq 1$, the other factors also have 2-norm at most 1. If follows that each of the three component matrices of Δ' have 2-norm at most 1, and therefore so does their convex combination Δ'. By Proposition 3 from Lecture 9 we conclude that

$$\lambda(G \textcircled{z} H) \leq (1-\mu)^2 \cdot \lambda + \big(1 - (1-\mu)^2\big) = 1 - (1-\mu)^2 cdot(1-\lambda). \qquad \square$$

We next transfer the bound on $\lambda(G \textcircled{z} H)$ to $\lambda(G \textcircled{r} H)$ and show that the degree reduction using the replacement product does not hurt the expansion too much. In particular, we show that if $\lambda(G)$ and $\lambda(H)$ are bounded by constants smaller than one, then so is $\lambda(G \textcircled{r} H)$.

Lemma 9. $\lambda(G \textcircled{r} H) \leq \left(\frac{\lambda'+7}{8}\right)^{1/3}$, *where* $\lambda' \doteq 1 - (1-\lambda(H))^2(1-\lambda(G))$.

Proof. Let M denote $M_{G \textcircled{r} H}$. In order to apply Lemma 8, we consider the multigraph on $V(G \textcircled{r} H)$ where every edge corresponds to a walk of length 3 in $G \textcircled{r} H$. We have that $M_{G'} = M^3$. The eigenvalues of M^3 are the cubes of the eigenvalues of M. This holds in general but easily follows for M as M has a full basis of eigenvectors. In particular,

$$\lambda(G') = \lambda(G \textcircled{r} H)^3. \tag{5}$$

By (3) we can write $M = \frac{1}{2}(\hat{A}+\hat{B})$. Multiplying out M^3 leads to a sum of 8 terms, one of which is $\frac{1}{8} \cdot M_{G \textcircled{z} H}$ by (4). We collect the remaining 7 terms of M^3 into a matrix $M' \doteq M^3 - \frac{1}{8} M_{G \textcircled{z} H}$. The 2-norm of M' is bounded by $\frac{7}{8}$ because all of the 7 terms have a coefficient of $\frac{1}{8}$, and the matrices involved have 2-norm at most one each. Thus, we can write $M_{G'} = \frac{1}{8} M_{G \textcircled{z} H} + M'$ where $\|M'\|_2 \leq \frac{7}{8}$. By Proposition 3 from Lecture 9 this means that $\lambda(G') \leq \frac{1}{8}\lambda(G \textcircled{z} H) + \frac{7}{8}$. By Lemma 8, $\lambda(G \textcircled{z} H) \leq \lambda'$, so $\lambda(G') \leq \frac{\lambda'+7}{8}$. The result then follows from (5) by taking cube roots. □

3.4 Attempted construction

Recall that our plan is to start from a constant-size complete graph G_0 with self-loops, increase the size of the graph using the tensor product, and reduce the degree back to a fixed constant without loosing too much in expansion. For the latter we use the replacement product with a suitable fixed graph H of degree d_H. The attempted iterative procedure is therefore

$$G_i = (G_{i-1} \otimes G_{i-1}) \textcircled{r} H \,. \tag{6}$$

We need to make sure that the degree of $G_{i-1} \otimes G_{i-1}$ and the number of vertices of H work out to be the same. The degree of G_i is, by definition of the replacement product, equal to $2d_H$. Therefore, if we choose G_0 to have degree $2d_H$ as well, and the number of vertices of H to be $(2d_H)^2$, the construction is indeed well-defined. We still need to argue the existence of a regular multigraph H with degree d_H, $(2d_H)^2$ vertices, and good expansion. However, there is a more pressing issue – the resulting spectral expansion deteriorates by too much.

Let $\lambda_i \doteq \lambda(G_i)$ and $\mu \doteq \lambda(H)$. We have $\lambda_0 = 0$ because G_0 is a complete graph with self-loops. By combining Lemma 7 and Lemma 9, we obtain the bound

$$\lambda_i \leq \left(1 - \frac{(1-\mu)^2}{8}(1-\lambda_{i-1})\right)^{1/3}. \tag{7}$$

Note that for λ_{i-1} close to 1, the right-hand side of (7) is asymptotically $1 - \frac{(1-\mu)^2}{24}(1-\lambda_{i-1})$, which means that our bound on λ_i converges to 1 once it gets close to 1. In fact, no matter how small a positive value μ is, the bound on λ_i converges to 1 as $i \to \infty$. Thus, the expansion guarantee vanishes as the graphs get larger, and we are not done yet. In each iteration, we need to do something to slightly boost the expansion without loosing too much in the degree and the size of the graph.

3.5 Squaring: Increasing the expansion

Perhaps the simplest operation we can perform to boost the expansion is *squaring*. Given a multigraph G, the square G^2 of G has edges for each walk of length 2 in G. This operation squares the degree, and leaves the number of vertices the same. The edge labels transfer from G to G^2 in a natural way, which we make formal in the definition below.

Definition 6 (Squaring). *The* square *of a multigraph G of degree d is the multigraph G^2 whose vertex set is $V(G)$, whose degree is d^2, and whose edges are defined by the neighbor function*

$$\begin{aligned} &\Gamma_{G^2} : V(G) \times [d]^2 \to V(G) \\ &\Gamma_{G^2}\big(u; (a,b)\big) = \Gamma_G(\Gamma_G(u;a);b). \end{aligned}$$

Note that G^2 is undirected. For similar reasons as the zig-zag product, squaring does not preserve proper edge colorings: $u = \Gamma_{G^2}(\Gamma_{G^2}(u, (a, b)), (a, b))$ does not need to hold in general.

Similar to the argument in the first part of the proof of Lemma 9, the transition matrix M_{G^2} for the random walk on G^2 equals M_G^2 (the square of the transition matrix for G), and the eigenvalues of M_{G^2} are the squares of the eigenvalues of M_G. In particular, we have the following.

Lemma 10. *$\lambda(G^2) = \lambda(G)^2$.*

3.6 The final construction

Our next attempt is a construction of the form

$$G_i = \left((G_{i-1} \otimes G_{i-1}) \textcircled{r}\, H\right)^a, \tag{8}$$

where a is some large constant to be specified later. If d denotes the degree of H, then the degree of G_i now equals $(2d)^a$, so choosing G_0 as the complete graphs with self-loops on $(2d)^a$ vertices and H with $(2d)^a$ vertices yields a well-defined construction. Moreover, for every $d \geq 3$ Theorem 2 guarantees the existence of such a multigraph H with $\mu \doteq \lambda(H) < 1$ and a sufficiently large (depending on d). In fact, by choosing d large enough, we can make μ an arbitrarily small positive real.

Our bound on λ_i now becomes

$$\lambda_i \leq \left(1 - \frac{(1-\mu)^2}{8}(1 - \lambda_{i-1})\right)^{a/3},$$

which for λ_{i-1} close to 1 asymptotically equals $1 - \frac{a(1-\mu)^2}{24}(1 - \lambda_{i-1})$. This implies that for $a > \frac{24}{(1-\mu)^2}$, the value 1 is a repelling fixed point of our bound, and since $\lambda_0 = 0$, λ_i remains bounded away from 1, i.e., there exists $\lambda < 1$ such that $\lambda_i \leq \lambda$ for every i.

There is one remaining issue with the construction – the resulting family of expanders is too sparse. This is because the number of vertices grows doubly exponential: $|V(G_i)| = (2d)^a \cdot |V(G_{i-1})|^2$, so $|V(G_i)| \geq |V(G_0)|^{2^i}$. To remedy this issue, we modify the construction as follows:

$$G_i = \left((G_{i/2} \otimes G_{i/2}) \textcircled{r}\, H\right)^a.$$

Now the number of vertices grows more mildly. More precisely, $|V(G_{2^k})| = (2d)^a \cdot |V(G_{2^{k-1}})|)^2 = O\left(((2d)^a \cdot |V(G_1)|)^{2^k}\right)$. This yields a family with inverse quadratic density: For every target value N there exists some G_i satisfying $N \leq |V(G_i)| \leq (2d)^a \cdot N^2$.

We still need to argue that the family is fully explicit. Let $T(i)$ denote the running time required to evaluate Γ_{G_i}. In order to compute a neighbor in G_i, we need to make at most $2a$ queries to $\Gamma_{G_{i/2}}$, which are combined in time that is polylogarithmic in the size of G_i. This leads to the recurrence $T(i) \leq 2a \cdot T(i/2) + \operatorname{poly}\log(|V(G_i)|)$, which solves to $T(i) \leq (\operatorname{poly}\log(|V(G_i)|))^{\log(2a)} = \operatorname{poly}\log(|V(G_i)|)$, so the family is indeed fully explicit.

To summarize, we have established the following theorem.

Theorem 11 (Iterative Construction of Expanders). *There exists a fully explicit family of inverse quadratic density consisting of multigraphs G_i with constant degree and $\lambda(G_i) \leq \lambda$ for some constant $\lambda < 1$ that can be constructed using tensor products, replacement products, and squaring starting from two fixed multigraphs.*

Finally, we point out an alternate construction that uses the zig-zag product instead of the replacement product:

$$\begin{aligned} G_0 &= K_{d^2} \\ G_i &= (G_{i/2} \otimes G_{i/2})^2 \textcircled{z} H. \end{aligned}$$

The construction is well-defined if H has d^8 vertices and degree d. All graphs G_i have degree d^2, and for $\lambda(H)$ sufficiently small, a similar analysis based on Lemma 7 and Lemma 8 shows that $\lambda(G_i) \leq \lambda$ for some constant $\lambda < 1$.

References

[Alo86] Noga Alon. Eigenvalues and expanders. *Combinatorica*, 6:83–96, 1986.

[Fri08] Joel Friedman. *A proof of Alon's second eigenvalue conjecture and related problems*, volume 195 of *Memoirs of the American Mathematical Society.* American Mathematical Society, 2008.

[GG81] O. Gabber and Z. Galil. Explicit constructions of linear-sized superconcentrators. *Journal of Computer and System Sciences*, 22:407–420, 1981.

[Lub94] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125 of *Progress in Mathematics.* Birkhäuser Verlag, 1994.

[Sar90] Peter Sarnak. *Some applications of modular forms*, volume 99 of *Cambridge Tracts in Mathematics.* Cambridge University Press, 1990.

[Yeh12] Amir Yehudayoff. Proving expansion in three steps. *SIGACT News*, 43(3):67–84, 2012.