Lectures 16: Constructions of Expanders via the Zig-Zag Graph Product

In which we give an explicit construction of expander graphs of polylogarithmic degree, state the properties of the zig-zag product of graphs, and provide an explicit construction of a family of constant-degree expanders using the zig-zag product and the polylogarithmic-degree construction.

A *family of expanders* is a family of graphs $G_n = (V_n, E_n)$, $|V_n| = n$, such that each graph is d_n-regular, and the edge-expansion of each graph is at least h, for an absolute constant h independent of n. Ideally, we would like to have such a construction for each n, although it is usually enough for most applications that, for some constant c and every k, there is an n for which the construction applies in the interval $\{k, k+1, \ldots, ck\}$, or even the interval $\{k, \ldots, ck^c\}$. We would also like the degree d_n to be slowly growing in n and, ideally, to be bounded above by an explicit constant. Today we will see a simple construction in which $d_n = O(\log^2 n)$ and a more complicated one in which $d_n = O(1)$.

An *explicit construction* of a family of expanders is a construction in which G_n is "efficiently computable" given n. The weakest sense in which a construction is said to be explicit is when, given n, the (adjacency matrix of the) graph G_n can be constructed in time polynomial in n. A stronger requirement, which is necessary for several applications, is that given n and $i \in \{1, \ldots, n\}$, the list of neighbors of the i-th vertex of G_n can be computed in time polynomial in $\log n$.

In many explicit constructions of constant-degree expanders, the construction is extremely simple, and besides satisfying the stricter definition of "explicit" above, it is also such that the adjacency list of a vertex is given by a "closed-form formula." The analysis of such constructions, however, usually requires very sophisticated mathematical tools.

Example 1 *Let p be a prime, and define the graph $G_p = (V_p, E_p)$ in which $V_p = \{0, \ldots, p-1\}$, and, for $a \in V_p - \{0\}$, the vertex a is connected to $a+1 \bmod p$, to $a-1 \bmod p$ and to its multiplicative inverse $a^{-1} \bmod p$. The vertex 0 is connected to 1, to $p-1$, and has a self-loop. Counting self-loops, the graph is 3-regular: it is the*

union of a cycle over V_p and of a matching over the $p - 3$ vertices $V_p - \{0, 1, p - 1\}$; the vertices 0, 1, $p - 1$ have a self-loop each. There is a constant $h > 0$ such that, for each p, the graph G_p has edge expansion at least h. Unfortunately, no elementary proof of this fact is known. The graph G_{59} is shown in the picture below.
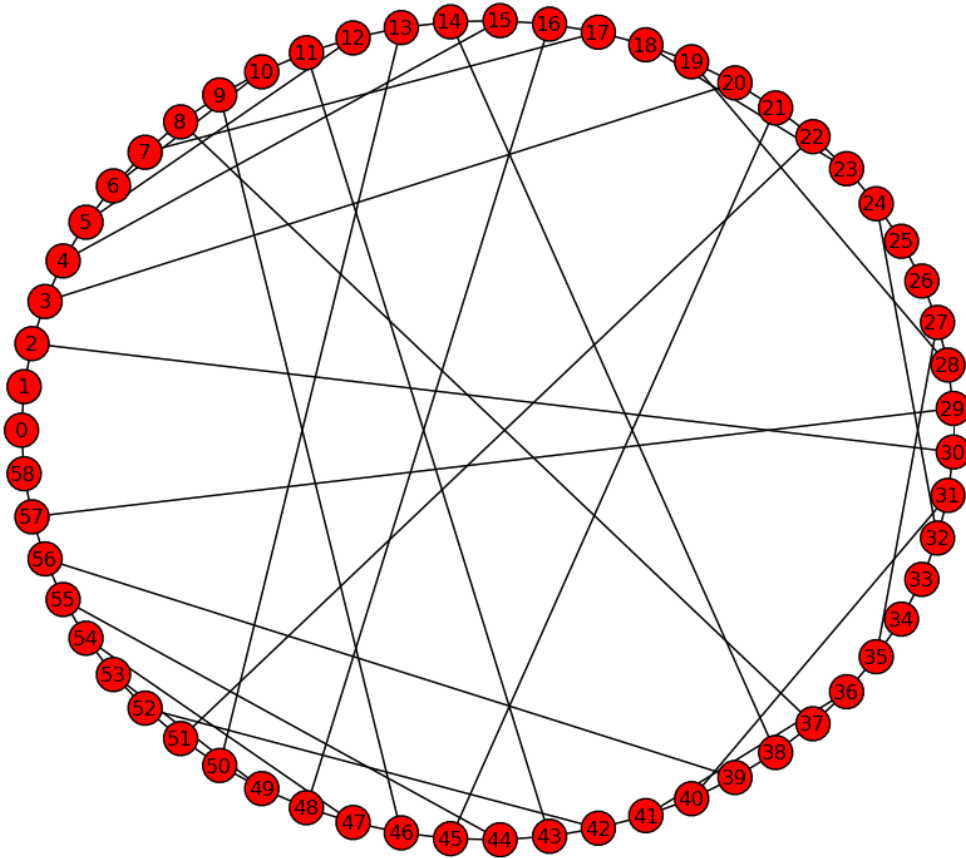
Constructions based on the *zig-zag graph product*, which we shall see next, are more complicated to describe, but much simpler to analyze.

We begin by describing a building block in the construction, which is also an independently interesting construction: a family of expanders with polylogarithmic degree, which have both a very simple description and a very simple analysis.

1 Expanders of Logarithmic Degree

Let p be a prime and $t < p$. We'll construct a p^2-regular multigraph $LD_{p,t}$ with p^{t+1} vertices. The vertex set of the graph will be the $(t+1)$-dimensional vextor space $\mathbb{F}_p^{t+1}$ over $\mathbb{F}_p$.

For each vertex $x \in \mathbb{F}_p^{t+1}$, and every two scalars $a, b \in \mathbb{F}$, we have the edges $(x, x + (b, ab, a^2 b, \ldots, a^t b))$.

In other words, the graph $LD_{p,t}$ is a Cayley graph of the additive group of $\mathbb{F}_p^{t+1}$, constructed using the generating multiset

$$S := \{(b, ab, \ldots, a^t b) : a, b \in \mathbb{F}_p^{t+1}\}$$

Note that the generating set is symmetric, that is, if $s \in S$ then $-s \in S$ (with the same multiplicity), and so the resulting multigraph is undirected.

Let $A_{p,t}$ be the adjacency matrix of $LD_{p,t}$ and $L_{p,t} := I - p^{-2} A_{p,t}$ be the normalized Laplacian matrix. We will prove the following bound on the eigenvalues of $L_{p,t}$.

Theorem 2 *For every prime p and every $t < p$, if we let $0 = \lambda_1 \leq \lambda_2 \leq \cdots \lambda_n$ be the eigenvalues of M with multiplicities, then, for every $i \in \{2, \ldots, n\}$*

$$1 - \frac{t}{p} \leq \lambda_i \leq 1$$

For example, setting $t = \lfloor p/2 \rfloor$ gives us a family of graphs such that $\lambda_2 \geq 1/2$ for each graph in the family, and hence $\phi(G) \geq 1/4$, and the number of vertices is $p^{p/2}$, while the degree is p^2, meaning the degree is $O((\log n / \log \log n)^2)$.

PROOF: We will compute the eigenvalues of the adjacency matrix of $A_{p,t}$, and prove that, except the largest one which is p^2, all the others are non-negative and at most pt.

Recall our characterization of the eigenvalues of the adjacency matrix of a Cayley multigraph $Cay(\Gamma, S)$ of an abelian group Γ with generating multiset S: we have one eigenvector for each character χ of the group, and the corresponding eigenvalue is $\sum_{s \in S} \chi(s)$.

What are the characters of the additive group of $\mathbb{F}_p^{t+1}$? It is the product of $t+1$ copies of the additive group of $\mathbb{F}_p$, or, equivalently, the product of $t + 1$ copies of the cyclic group $\mathbb{Z}/p\mathbb{Z}$. Following our rules for constructing the character of the cyclic group and of products of groups, we see that the additive group of $\mathbb{F}_p^{t+1}$ has one character for each $(c_0, \ldots, c_t) \in \mathbb{F}_p^{t+1}$, and the corresponding character is

$$\chi_{c_0, \ldots, c_t}(x_0, \ldots, x_t) := \omega^{\sum_{i=0}^t c_i x_i}$$

where
$$\omega := e^{\frac{2\pi i}{p}}$$

Thus, for each $(c_0, \ldots, c_t) \in \mathbb{F}_t^p$, we have an eigenvalue

$$\lambda_{c_0,\ldots,c_t} := \sum_{a,b \in \mathbb{F}_p} \omega^{\sum_{i=0}^t c_i b a^i}$$

When $(c_0, \ldots, c_t) = (0, \ldots, 0)$ then the corresponding character is always equal to one, and the corresponding eigenvalue is p^2.

Now consider any $(c_0, \ldots, c_t) \neq (0, \ldots, 0)$, and define the polynomial $q(x) = \sum_{i=0}^t c_i x^i \in \mathbb{F}_p[x]$. Note that it is a non-zero polynomial of degree at most t, and so it has at most t roots. The eigenvalue corresponding to $(c_0, \ldots, c_t)$ is

$$\lambda_{c_0,\ldots,c_t} = \sum_{a,b \in \mathbb{F}_p} \omega^{\sum_{i=0}^t b \cdot q(a)}$$

$$= \sum_{a : q(a)=0} \sum_b \omega^0 + \sum_{a : q(a)\neq 0} \sum_b \omega^{b \cdot q(a)}$$

$$= p \cdot |\{a \in \mathbb{F}_p : q(a) = 0\}|$$

where we use the fact that, for every $q \neq 0$, the sum $\sum_b \omega^{b \cdot q}$ equals zero, since it is the sum of the values of the non-trivial character $x \to \omega^{x \cdot q}$, and we proved that, for every non-trivial character, the sum is zero.

In conclusion, we have

$$0 \leq \lambda_{c_0,\ldots,c_t} \leq pt$$

$\square$

2 The Zig-Zag Graph Product

Given a d-regular graph G with adjacency matrix A, if $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ are the eigenvalues of A with multiplicities we define

$$\lambda(G) := \max_{i=2,\ldots,n} \{|\lambda_i|\}$$

In particular, $\lambda(G) \geq \lambda_2$, and if we are able to construct a family of graphs such that $\lambda(G)$ is at most a fixed constant bounded away from one times d, then we have a family of expanders. (Our construction will be inductive and, as often happens with

inductive proofs, it will be easier to maintain this stronger property than the property that λ_2 is bounded away from one.)

Given graphs G and H of compatible sizes, with small degree and large edge expansion, the zig zag product $G\textcircled{z}H$ is a method of constructing a larger graph also with small degree and large edge expansion.

If:

- G a D-regular graph on n vertices, with $\lambda(G) \leq \alpha D$

- H a d-regular graph on D vertices, with $\lambda(H) \leq \beta d$

Then:

- $G\textcircled{z}H$ a d^2-regular graph on nD vertices, with $\lambda(G\textcircled{z}H) \leq (\alpha + \beta + \beta^2)d^2$.

We will see the construction and analysis of the zig zag product in the next lecture.

For the remainder of today, we'll see how to use the zig zag product to construct arbitrarily large graphs of fixed degree with large edge expansion.

Fix a large enough constant d. ($1369 = 37^2$ will do.) Construct a d-regular graph H on d^4 vertices with $\lambda_2(H) \leq d/5$. (For example $LD_{37,7}$ is a degree 37^2 graph on $37^{(7+1)} = (37^2)^4$ vertices with $\lambda_2 \leq 37 \times 7 < 37^2/5$.)

For any graph G, let G^2 represent the graph on the same vertex set whose edges are the paths of length two in G. Thus G^2 is the graph whose adjacency matrix is the square of the adjacency matrix of G. Note that if G is r-regular then G^2 is r^2-regular

Using the H from above we'll construct inductively, a family of progressively larger graphs, all of which are d^2-regular and have $\lambda \leq d^2/2$.

Let $G_1 = H^2$. For $k \geq 1$ let $G_{k+1} = (G_k^2)\textcircled{z}H$.

Theorem 3 *For each $k \geq 1$, G_k has degree d^2 and $\lambda(G_k) \leq d^2/2$.*

PROOF: We'll prove this by induction.
Base case: $G_1 = H^2$ is d^2-regular. Also, $\lambda(H^2) = (\lambda(H))^2 \leq d^2/25$.

Inductive step: Assume the statement for k, that is, G_k has degree d^2 and $\lambda(G_k) \leq d^2/2$. Then G_k^2 has degree $d^4 = |V(H)|$, so that the product $(G_k^2)\textcircled{z}H$ is defined. Moreover, $\lambda(G_k^2) \leq d^4/4$. Applying the construction, we get that G_{k+1} has degree d^2 and $\lambda(G_{k+1}) \leq (\frac{1}{4} + \frac{1}{5} + \frac{1}{25})d^2 = \frac{46}{100}d^2$ This completes the proof. $\square$

Finally note that G_k has d^{4k} vertices.