COMS 4995: Introduction to Coding Theory.
Justin Cranshaw and Hila Becker
December 23, 2004

Expander Graphs and the zig-zag Product

1 Introduction

Informally, an expander is an undirected graph that has relatively sparse density, but whose vertices are nevertheless highly connected. Consequently, expanders have the property that any small subset of the vertices has a large set of neighbors outside of the set. This simple graph property has led to highly useful results in a number of branches of computer science. In addition, the study of expansion properties of graphs in and of itself has proven to be quite a rich field both in theoretical content, and in result applicability. Expander graphs have uses ranging from complexity theory and algorithm derandomization to coding theory and efficient network design. Although it has been proven that a random graph of constant degree at least 3 is an expander with high probability, many of the results in the fields above require an efficiently computable explicit method of construction of infinite families of growing size expanders.

One solution to this problem is based on the zig-zag graph product discovered by Wigderson *et al.* [**?**]. On a very informal level, the zig-zag product operates on two expander graphs, one large (in number of vertices), and one small (relative to the first). The output of the zig-zag product is a third graph which has a size equal to the product of the input sizes, and which has an expansion property based on the expansion properties of the input graphs. Specifically, if the input graphs are "good" expanders, then the output graphs will also be a "good" expander. This zig-zag product is then used in an iterative manner starting from a single seed expander, to create an entire family of expander graphs.

1.1 Overview

This study is motivated, ultimately from a coding theory perspective, although from the results presented here, this is not obvious. Expander graphs form the basis of frequently used concept in coding theory, *expander codes*. Expander codes appear in coding theory, both in their own right as a stand alone family of codes, and as a component of another code type, concatenated codes [**?**]. Thus having access to an infinite family of "good" expanders is essential in the design of expander codes, since the size of the graph is very much dependent on the coding problem at hand, and can sometimes be dictated by physical engineering constraints. For this reason, often there is not any flexibility in the choice of graph size.

The build up to the main proof of the zig-zag product depends on a variety of concepts which we try to present in at least enough detail so that the zig-zag result stands alone. The concepts include: algebraic eigenvalue analysis of graphs (the graph spectrum), random walks on graphs, and entropy of a probability distribution.

In addition, we since we are concerned with expanders from a coding theory perspective, we present a brief introduction into how the zig-zag product might be applied to construct expanders for use in coding theory. The main difference in this result from the zig-zag product in general is that expander codes require that the expander graph used be bipartite, whereas the zig-zag iterative method does not make this assumption.

2 Preliminaries

Before we can describe a way to explicitly construct expander graphs, we need to present some algebraic properties of graphs to enhance our understanding of expanders and their unique structure. In general, we define expanders to be sparse but highly connected graphs.

Let $G = (V, E)$ such that $|V| = N$. In this paper we are concerned with graphs G that are D-regular and assume that G may have self loops and parallel edges. For any $S \subseteq G$, let ∂S denote the *edge boundary* of S, which is defined as the set of edges connecting S to $V - S$. The *expansion parameter* $h(G)$ is a constant that measures how well connected a graph G is. A large expansion parameter h(G) implies a highly connected graph G. We define h(G) as

$$h(G) = min_{\{S||S|\leq \frac{n}{2}\}} \frac{|\partial S|}{|S|}$$

Note that we are only concerned with subsets S containing fewer than half of the vertices since $\partial S = \partial(V - S)$.

Since our goal is to show the existence of infinite families of expander graphs, we must first define what we mean by an infinite expander graph family. We say that the set of graphs $\{G_i\}$, $i \in \mathbb{N}$ is an *infinite family* of expanders with constant degree D if

- each G_i is a D-regular expander graph of size $\{N_i\}$.
- the sequence $\{N_i\}$ is monotonically increasing, yet it does not grow too rapidly.
- $h(G_i) \geq \epsilon > 0$ for all i.

A graph G can be described using an *adjacency matrix* $A(G)$ whose value on the *ith* row and *jth* column reflects the number of edges from i to j for $i, j \in V$. It is easy to see that $A(G)$ is symmetric if G is undirected, and the sum of every row and every column is D if G is D-regular.

Since we are only concerned with undirected graphs, the adjacency matrix A(G) is symmetric and has an orthonormal base $v_0, v_1, \ldots, v_{n-1}$ with eigenvalues $\mu_0, \mu_1, \ldots, \mu_{n-1}$ such that $Av_i = \mu_i v_i, \forall i$. Furthermore, we may assume without loss of generality that the eigenvalues are ordered with $\mu_0 \geq \mu_1 \geq \ldots \geq \mu_{n-1}$. The eigenvalues of A(G) are referred to as the *spectrum* of G.

We can observe that the first eigenvalue μ_0, which is also the largest eigenvalue is equal to D, the degree of G. This is the case since G is D-regular and the all 1's vector $(1, 1, \ldots, 1)$ is an eigenvector of $A(G)$ of eigenvalue D. It was shown in [**?**] that all of the other eigenvalues have absolute value of at most D, and the second largest eigenvalue μ_1 is a good measure of the expansion properties of G.

Theorem 1 (?)

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

$D - \mu_1$ is a quantity known as the *spectral gap*, which is shown by this theorem to be a good estimate of the expansion properties of a graph. If G is an expander, $h(G) > \epsilon$ and therefore the spectral gap $D - \mu_1 > \epsilon'$.

We refer to a graph G is an (N,D,λ)-graph if it has N vertices, degree D and a second largest (absolute value) eigenvalue of $A(G)$ at most λD.

3 Expander Construction - The Zig-zag Product

We would like to introduce a combinatoric construction of expander graphs known as the zig-zag product. The zig-zag product, first discovered by [**?**], is an operation on two expander graphs G and H, which yields a third expander $G \textcircled{z} H$. The idea behind this operation is to take a small expander H and a large expander G and create a new expander that roughly inherits its size from G, degree from H, and expansion properties from both. In this section we define the zig-zag product and use it to show a construction that yields an infinite family of expanders with a bounded degree.

3.1 The Zig-zag Product: Definition

Consider two expander graphs G and H. Furthermore, assume that H is D-regular and the edges of G are D-colorable. For a color $i \in [D]$ and a vertex v, define v[i] as the neighbor of v along the edge colored i.

Definition 2 *Let G be a D_1-regular graph on N_1 vertices and H be a D_2-regular graph on D_1 vertices. The zig-zag product $G \textcircled{z} H$ is a D_2^2-regular graph on $N_1 D_1$ vertices such that for all $v \in V_1, k \in D_1$, an edge (i,j) connects the vertex (v,k) to the vertex (v[k[i]],k[i][j])*

Note that every vertex in the product $G \textcircled{z} H$ is a tuple (v,k) where the first component corresponds to a vertex from the large graph G and the second component can be viewed both as a vertex of the small graph H and as an edge color of G. For this reason, it is required that the size of the small graph corresponds to the degree of the large graph. In order to see how to connect an edge (i,j) from starting vertex (v,k) in the product graph, we can consider the following steps:

1 $(v, k) \rightarrow (v, k[i])$ - A step in the small graph, changing the second component from k to k[i] while the first component remains unchanged. This step is determined by the choice of the edge label i.

2 $(v, k[i]) \rightarrow (v[k[i]], k[i])$ - A step in the large graph, changing the first component according to the edge color represented by the second component, per the vertex color we land on after step 1.

3 $(v[k[i]], k[i]) \rightarrow (v[k[i]], k[i][j])$ - A step in the small graph, changing the second component from k[i] to k[i][j] while the first component remains unchanged. This step is determined by the choice of the edge label j.

More intuitively, we can think of the zig-zag product as taking an (N_1, D_1, λ_1)-expander G and an (D_1, D_2, β)-expander H and replacing every vertex in the large expander G with a "cloud" of vertices from the small expander H. Each vertex in the product graph has two components, the first comes from a vertex label v of G and the second from a vertex label k in the "cloud" H that replaced v. It is easy to see that there are N_1 choices for the first component and D_1 choices for the second component so the number of vertices in $G \textcircled{z} H$ is $N_1 D_1$.

In order to see how the edges in the product graph are formed, we must first assume that there is a way to D_1-color G. Consider a starting vertex (v, k). We follow the 3-step breakdown of the definition in order to discover all edges out of (v, k) in the product graph. The first step is a nondeterministic step from a (v, k) onto any vertex in the cloud that shares an edge with k in H. There are D_2 possible choices where D_2 is the degree of H. The second step is determined by the choice made in the first step; if vertex i was chosen, then we move along the edge of G that is colored i. This is a move between clouds. The third step is again nondeterministic, connecting the current vertex to any one of the d vertices in the cloud that share an edge with this vertex in H. Again, there are D_2 choices for the path taken in the third step. The final vertex that we land on is connected to our starting vertex to form an edge in $G \textcircled{z} H$. Since the first and third steps are nondeterministic, and each present D_2 path options, the total number of edges in the product graph is D_2^2.

Theorem 3 (The zig-zag theorem) *Let G be a (N_1, D_1, λ_1)-expander and H be a (D_1, D_2, λ_2)-expander then $G \textcircled{z} H$ is a $(N_1 D_1, D_2^2, f(\lambda_1, \lambda_2))$-expander where $f(\lambda_1, \lambda_2) = \lambda_1 + \lambda_2 + \lambda_2^2$*

We have already shown above that the degree of $G \textcircled{z} H$ is D_2^2 on $N_1 D_1$ vertices. We will prove an upper bound on the expansion parameter in a later section. For now, assuming that this holds true, we can use the zig-zag product to iteratively construct expander families.

3.2 Iterative Construction

We would like to show how the zig-zag product can be used to construct an infinite family of constant degree expanders. Let H be a $(D^4, D, \frac{1}{4})$-expander for a constant D. It has been shown [**?**] that such an expander exist with high probability, and since D is constant we can find a graph H in constant time using an exhaustive search.

The family of expanders is defined recursively as

- $G_1 = H^2$
- $G_{i+1} = G_i^2 \textcircled{z} H$

Note that for a graph G, G^2 is simply the square of the adjacency matrix $A(G)$.

Claim 4 *G_i is a $(D^{4i}, D^2, \frac{1}{2})$-expander*

Proof We prove this claim by induction. The base case $i = 1$ is implied by the definition. We assume the claim and let G_i be a $(D^{4i}, D^2, \frac{1}{2})$-expander. Therefore G_i^2 is a $(D^{4i}, D^4, \frac{1}{4})$-expander. From the zig-zag theorem, we can see that G_{i+1} is a $(D^{4i}, D^2, \frac{1}{2})$-expander. ■

We claim that if G and H are good expanders, so is their zig-zag product $G \textcircled{z} H$. We go on to prove this claim in the following section.

4 Entropy Waves

The proof of the zig-zag theorem relies intuitively on the concept of *entropy waves*, or how randomness propagates through the vertices and edges of expanders. The precise formulation of this concept is based on the linear algebra of random walks.

4.1 Random Walks on Expanders

A random walk on a graph is an iterative process through which, starting from an initial random vertex, we move a token from vertex to vertex by choosing an edge based on a probability distribution on the outgoing edges of the the current vertex. Since we are dealing with constant degree D, unweighted graphs, from a vertex v, the probability the we move from v to its neighbor v_i is uniformly $1/D$. This process can be completely described using linear algebra. If A is the adjacency matrix of our constant degree graph, then we will conduct a random walk on the graph with transition probabilities based on the weights on the edges of $\hat{A} = A/D$, where the matrix $\hat{A}$ is called the normalized adjacency matrix of A.

One of the central concerns in the study of random walks, is their convergence to the stationary probability. Let $x_j = (p_0^j, p_1^j, \ldots, p_{n-1}^j)$ be the probability distribution of the vertices at step j in the random walk. Thus p_i^j gives the probability of being at vertex i at step j in the random walk. The stationary distribution of a random walk is the probability distribution on the vertices x_k such that taking a step in the random walk results in the same distribution. That is $x_{k+1} = x_k$. It is easy to see that for a graph with uniform transition probabilities, the stationary distribution is just the uniform distribution $u = \frac{1}{n}(1, 1, \ldots, 1)$ [**?**]. However there is a convenient way to formalize the evolution of the probability distribution during random walks using linear algebra and the normalized adjacency matrix.

Claim 5 *Given an initial probability distribution $\pi_0 = (p_0^0, p_1^0, \ldots, p_{n-1}^0)$ over the n vertices of a constant degree graph G with normalized adjacency matrix $\hat{A}$, select vertex X at random over this distribution. Now, let Y be the uniformly chosen neighbor of X. Then the random variable Y is given by the matrix product $\hat{A}\pi_0$. Also, since Y represents the probability that a given vertex will be chosen after 1 step, $Y = \pi_1$.*

Proof We are looking for the probability $\Pr[Y = i]$ that Y is vertex i. This is of course conditioned on the initial probabilistic choice of X. Thus we have

$$\begin{aligned} \Pr[Y = i] &= \sum_j \Pr[Y = i | X = j] \Pr[X = j] \\ &= \sum_j \hat{A}_{ij} p_j^0 \\ &= (\hat{A}\pi_0)_i \end{aligned}$$

where the second to last step follows since $\hat{A}$ gives the transition probability of each edge, thus if we are at node j, the probability of selecting node i is $\hat{A}_{ij}$. Thus the full vector $\hat{A}\pi_0$ gives the value of the random variable Y, where the i^{th} component is the probability of being at node i after one step. Thus $\hat{A}\pi_0 = \pi_1$. ■

This process repeats iteratively. Thus the probability distribution at step 2 is $\pi_2 = \hat{A}\pi_1 = \hat{A}\hat{A}\pi_0 = \hat{A}^2\pi_0$. Generally, the probability over the vertices at step t is $\pi_t = \hat{A}^t\pi_0$.

If the random walk happens to be on an expander graph G, with normalized adjacency matrix $\hat{A}$, then the evolution of π can be characterized in terms of the eigenvalues of $\hat{A}$.

Theorem 6 *Let $\hat{A}$ be the normalized adjacency matrix of G with eigenvectors $v_0, \ldots, v_{n-1}$ with corresponding ordered eigenvalues $\mu_0 = 1 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$. Also, let π be a probability distribution over the vertices of G such that $\pi \perp u$, where u is the uniform distribution. Then*

$$\|\hat{A}\pi\| \leq \mu_1\|\pi\|.$$

Proof First, assume that the eigenvectors are all normalized. Then, it is clear that $v_0 = u$, since v_0 has the corresponding eigenvalue $\mu_0 = 1$. Then we can decompose π such that $\pi = c_1v_1 + c_2v_2 + \cdots + c_{n-1}v_{n-1}$. Thus

$$\begin{aligned}
\pi &= c_1v_1 + c_2v_2 + \cdots + c_{n-1}v_{n-1} \\
\hat{A}\pi &= c_1\hat{A}v_1 + c_2\hat{A}v_2 + \cdots + c_{n-1}\hat{A}v_{n-1} \\
\hat{A}\pi &= c_1\mu_1v_1 + c_2\mu_2v_2 + \cdots + c_{n-1}\mu_{n-1}v_{n-1} \\
\|\hat{A}\pi\|^2 &= (c_1\lambda_1)^2 + (c_2\lambda_2)^2 + \cdots + (c_{n-1}\lambda_{n-1})^2 \\
\|\hat{A}\pi\|^2 &\leq \mu_1^2(c_1^2 + c_2^2 + \cdots + c_{n-1}^2) \\
&= \mu_1^2\|\pi\|^2 \\
\|\hat{A}\pi\| &\leq \mu_1\|\pi\|
\end{aligned}$$

■

Corollary 7 *The second largest eigenvalue is bounded by $\mu_1 \geq \frac{\|\hat{A}\pi\|}{\|\pi\|}$, or equivalently $\mu_1 \geq \frac{|\langle\hat{A}\pi,\pi\rangle|}{\langle\pi,\pi\rangle}$.*

Proof This follows from direct manipulation of the result of theorem **??**. ■

Thus taking a random step in an expander graph increases the randomness of the vertex distribution towards uniformity since the norm is multiplicatively decreasing. This will be more clear when we present the concepts of entropy.

4.2 Entropy of a Probability Distribution

The concept of entropy spans many disciplines, from its introduction in thermodynamics by Boltzman and others, to its reformulation as the basis of *information science* by Claude Shannon. There are literally dozens of mathematical variations on entropy. Two of the most important are, for a given probability distribution p, $H(p) = -\sum_{i=1}^{n} p_i \log(p_1)$, and $H_2(p) = -\log(\|p\|_2)$. However, more important than the precise mathematical form is the intuition of what entropy measures, and how it evolves as the probability distribution changes. Entropy of a state p measures the predictability of the state, equivalently from an information science perspective, it tells us how much information is given by the state. A higher entropy corresponds to a high level of randomness and unpredictability, hence a small amount of information content. From the perspective of p, the uniform distribution corresponds to the max-entropy state. Similarly, if the probability is concentrated entirely on one outcome, then there is no randomness, hence min-entropy. This level of understanding is sufficient for the results that follow, however, for a thorough presentation of entropy especially as it applies to information science, one of the best sources is still Shannon's original 1948 paper on the subject [**?**].

4.3 Entropy Waves: Intuition

Consider taking a random walk on $G \textcircled{z} H$ with normalized adjacency matrix $\hat{M}$. Since each edge in $G \textcircled{z} H$ is a composite of first, a step in the initial H cloud, then a deterministic step on an edge in G, followed by another step in the resulting H cloud, we can view a random step in $G \textcircled{z} H$ in this manner as well. Also, the probability distribution π on the vertices of $G \textcircled{z} H$ can be thought of as two separate distributions (π_G, π_H) on the vertices of G and H respectively, since the vertices of $G \textcircled{z} H$ are all order pairs with first component in G and second component in H.

If $G \textcircled{z} H$ is an expander, then it will increase the overall H_2 entropy of the probability distribution $\pi = (\pi_G, \pi_H)$ of vertices in the the random walk, unless of course, π is not already uniform [**?**]. The rate of convergence of this walk to the maximum entropy of $H_2(\pi)$ is roughly log of the second eigenvalue many steps. Thus if we can show that a random step in $G \textcircled{z} H$ increases the entropy of the distribution on the vertices, then we will have shown that $G \textcircled{z} H$ is an expander, with second eigenvalue relative to the rate of convergence.

We consider only distributions on the vertices, $\pi = (\pi_G, \pi_H)$ that are non-uniform, since expanders can not increase the entropy of the uniform distribution (the uniform distribution is the case of max entropy). There are thus two cases to consider in breaking the random step down into its three components. Case 1 considers all non-uniform distributions $\pi = (\pi_G, \pi_H)$ in which the component over vertices in H, π_H is also non-uniform. Case 2 considers all non-uniform distributions in which the component over H, π_H is uniform (since the total probability distribution π is non-uniform, we require that the distribution over G, π_G is non-uniform for case 2).

Case 1 (π_H *is non-uniform.*): If the probability distribution on vertices in H is non-uniform, then by virtue of the expansion properties of H, taking step 1 in the small graph will increase the entropy in the second component of π. The second step cannot increase the overall entropy of π since it is completely determined by the choice of vertex for step 1. A deterministic step cannot increase the randomness since it is just a permutation of the first component of the vertex label.

The third step is another random step in the H cloud that the between cloud edge in step 2 sent us. Since it is a random step in an expander, it cannot decrease the overall entropy of π, thus any increase in the entropy from step 1 is maintained. It follows that $H_2(\hat{M}\pi) > H_2(\pi)$.

Case 2 (π_H *is uniform.*): If the probability distribution on vertices in H is already uniform, then clearly the first step in the random walk cannot increase the overall entropy of π_0 since this step only acts on the second vertex component. The second step, again since it is a permutation on the first vertex component, cannot increase the overall entropy. However, although it is a deterministic choice of edge given the choice of vertex in step 1, since step 1 is random, we can view step 2 as a random choice from the edges of G. Since G is an expander, this increases the entropy $H_2(\pi_G)$ over choices of vertices in G. Since we already stated that the overall entropy cannot increase as a result of this step, this means that the entropy on the second component $H_2(\pi_H)$ must decrease proportionally. This means that the probability distribution of vertices in H can no longer be uniform. Thus when a random step is taken in step 3, since H is an expander, and since the distribution over vertices in H is no longer uniform, step 3 increase the entropy on the second component, thus the overall entropy on vertices in the zig-zag graph is increased, that is $H_2(\hat{M}\pi) > H_2(\pi)$.

The formal proof of the zig-zag theorem involves describing the random walk process precisely with linear algebra, then tying in the random walk with μ_1, and the corresponding expansion properties of $G \textcircled{z} H$. This is done in the following section.

4.4 Formal Analysis

For the formal analysis, we again consider a random walk on $G \textcircled{z} H$ with normalized adjacency matrix $\hat{M}$. Let $\pi \in \mathbb{R}^{N_1 D_1}$ be any initial probability distribution on the vertices of $G \textcircled{z} H$, which we assume is non-uniform. It is well known from linear algebra, that π can be decomposed into a sum of vectors $\pi = \alpha^{\|} + \alpha^{\perp}$, where $\alpha^{\|}$ is constant over vertices within each of the N_1 clouds of vertices in H , and $\alpha^{\perp}$ is orthogonal to the uniform distribution over vertices within each H cloud. In other words, $\alpha^{\|}$ represents the the distribution over vertices in G, and $\alpha^{\perp}$ represents the distribution over vertices in H.

Since in the proof intuition, we decomposed a random step in $G \textcircled{z} H$ into its three component steps, we need to formalize this using the linear algebra of random walks. Let B be the $N_1 D_1 \times N_1 D_1$ matrix of the transition probabilities of random steps in each of the H clouds, and let A be the $N_1 D_1 \times N_1 D_1$ permutation matrix of all the *between cloud* edges corresponding to edges from G. Then $\hat{M} = BAB$. Each of these matrices can be constructed formally using G, H and the standard tensor product. However, the intuition above suffices for our purposes. For the construction of A and B, see Wigderson *et al.* [**?**].

Claim 8 *Given M, the normalized adjacency matrix of $G \textcircled{z} H$, and π, any non-uniform probability distribution over vertices of $G \textcircled{z} H$, then*

$$|\langle M\pi, \pi\rangle| \leq (\lambda_1 + \lambda_2 + \lambda_2^2) \cdot \langle \pi, \pi\rangle \tag{1}$$

where λ_1 and λ_2 are the expansion parameters of G and H respectively.

First note that this give us the desired result, specifically, that the H_2 entropy increases with a random step in $G \textcircled{z} H$. Also, by corollary **??** this gives us an upper bound of $\lambda_1 + \lambda_2 + \lambda_2^2$ on the second eigenvalue of M. The proof of this claim follows quickly from three lemmas which break the affect of M on π into its affect on the components of π, $\pi^{\|}$ and $\pi^{\perp}$.

Lemma 9 $B\pi^{\|} = \pi^{\|}$.

Proof Since B represents all steps in the N_1 clouds of vertices in H, and since $\pi^{\|}$ is uniform over these steps, then $\pi^{\|}$ is an eigenvector of eigenvalue 1 since the matrix is stochastic. Thus $B\pi^{\|} = 1\pi^{\|} = \pi^{\|}$. ■

Lemma 10 $\|B\pi^{\perp}\| \leq \lambda_2 \cdot \|\pi^{\perp}\|$.

Proof Since H is an expander, and $\pi^{\perp}$ is the probability component over steps in H, this follows directly from theorem **??**. ■

The two above lemmas correspond to case 1 in the intuition above. If the probability over the H components is non-uniform, then step 1 increases the entropy.

Lemma 11 $|\langle A\pi^{\|}, \pi^{\|}\rangle| \leq \lambda_1 \cdot \langle \pi^{\|}, \pi^{\|}\rangle$.

Proof Since $\pi^{\|}$ is constant over vertices in H, it corresponds to the transition probabilities for moving between clouds, hence $A\pi^{\|}$ is a step in the random walk over G edges. Since G is an expander, this also follows directly from corollary **??**. ■

This corresponds to case 2 in the intuition above, since the entropy over the first component π_G is increased.

Applying these lemmas to $\hat{M}\pi = BABA\pi$ yields a bound on the second largest eigenvalue of $\hat{M}$.

Proof of claim ?? [?]: We'd like to find a measure of $\langle M\pi, \pi\rangle$ in terms of λ_1 and λ_2. Simple algebraic manipulation yields

$$\langle M\pi, \pi\rangle = \langle BABA\pi, \pi\rangle = \langle ABA\pi, B\pi\rangle. \tag{2}$$

Now we break π into its components $\pi^{\|}$ and $\pi^{\perp}$.

$$\begin{aligned} \langle M\pi, \pi\rangle &= \langle AB(\pi^{\|} + \pi^{\perp}), B(\pi^{\|} + \pi^{\perp})\rangle \\ &= \langle AB\pi^{\|} + AB\pi^{\perp}, B\pi^{\|} + B\pi^{\perp}\rangle \end{aligned}$$

which because A is a length preserving expander is bounded by

$$\langle M\pi, \pi\rangle \leq |\langle A\pi^{\|}, \pi^{\|}\rangle| + 2\|\pi^{\|}\| \cdot \|B\pi^{\perp}\| + \|B\pi^{\perp}\|^2. \tag{3}$$

Now, using the above lemmas on the form above, we get

$$\begin{aligned}\langle M\pi,\pi\rangle &\leq \lambda_1\langle\pi^{\|},\pi^{\|}\rangle + 2\lambda_2\|\pi^{\|}\|\cdot\|\pi^{\perp}\| + \lambda_2^2\|\pi^{\perp}\| \\ &\leq \lambda_1\cdot\|\pi^{\|}\|^2 + 2\lambda_2\|\pi^{\|}\|\cdot\|\pi^{\perp}\| + \lambda_2^2\|\pi^{\perp}\|.\end{aligned}$$

Using a simple substitution, we can get this into the desired form. Let $p = \|\pi^{\|}\|/\|\pi\|$ and $q = \|\pi^{\perp}\|/\|\pi\|$, with $p^2 + q^2 = 1$. Then the above expression becomes

$$\begin{aligned}\frac{|\langle M\pi,\pi\rangle|}{\langle\pi,\pi\rangle} &\leq \lambda_1\cdot p^2 + 2\lambda_2\cdot pq + \lambda_2^2\cdot q^2 \\ &\leq \lambda_1 + \lambda_2 + \lambda_2^2.\end{aligned}$$

Hence the second eigenvalue of M is bounded by $\lambda_1 + \lambda_2 + \lambda_2^2$.

■

5 Lossless Expanders and Coding Theory Applications

Expander graphs have vast applications in the field of coding theory and error correcting codes. In particular, expander codes, introduced by Sipser and Spielman in 1996 [**?**] use bipartite expander graphs as their underlying structure. In coding theory, we are interested in the optimization of code parameters such as rate and distance. It is therefore important to show the existence of code families with increasing size and asymptotically good distance.

Since we are interested in maximizing the expansion parameter, we would like to look at a special type of expander graphs known as *lossless expanders*. Lossless expanders are graphs with an expansion factor $(1-\epsilon)D$ for an arbitrarily small constant ϵ and degree D, which is close to the best attainable expansion parameter. Before it has been proven that lossless expanders exist, the best known bound on the expansion parameter was $D/2$ by the eigenvalue bound, due to expanders with an optimal second eigenvalue known as Ramanujan graphs. Therefore, using lossless expander graphs to construct expander codes would yield optimal results.

In this section we also introduce randomness enhancing functions called conductors. We discuss how the zig-zag product can be used on conductors to obtain an explicit construction of constant degree lossless expanders. Thus we can conclude that there exist constructible good expander code families.

5.1 Conductors

Intuitively, conductors are functions that transfer entropy from their inputs to their outputs according to an input distribution. The similar notions of extractors from [**?**] and condensers from [**?**] are also randomness enhancing functions that are a special case of conductors. We will show how conductors can be represented as bipartite graphs that can be used in Sipser and Spielman's

expander codes.

Before we can formally define conductors we need to find a suitable way to measure randomness. It turns out that the preferred way to measure the randomness distributed by conductors is using the notion of min-entropy [**?**] combined with a statistical difference. Let X,Y be random variables over a set S.

Definition 12 *The min-entropy of X is:*

$$H_\infty(X) \stackrel{\text{def}}{=} log_2(1/max_{x \in S} Pr[X = x])$$

X is a *k-source* if $H_\infty(x) \geq k$. For instance, the uniform distribution on a set of size 2^k is a k-source.

Definition 13 *The statistical difference between X and Y is defined to be*

$$max_{P \subseteq S} |Pr[X \in P] - Pr[Y \in P]| = \frac{1}{2} \sum_{a \in S} |Pr[X = a] - Pr[Y = a]|$$

X and Y are said to be ϵ-close if the statistical difference between them is at leat ϵ. X is a (k, ϵ)-source if it is ϵ-close to some k-source.

Now that we have a way to measure randomness, we can define randomness conductors. Let U_n denote the uniform distribution over $\{0,1\}^n$.

Definition 14 *A function $E : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ is a (k_{max}, a, ϵ)-conductor if for any distribution X on $\{0,1\}^n$ satisfying $H_\infty(X) = k \leq k_{max}$ the distribution $E(X, U_d)$ is a $(k + a, \epsilon)$-source.*

We are interested in a special case of conductors known as lossless conductors. For a conductor to be considered lossless, we require that the min-entropy of the output is equivalent to the min-entropy of the input added to the randomness from true random bits. This creates the requirement $a = d$.

Definition 15 *A function $E : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ is a $(k_{max}\epsilon)$-lossless conductor if for any distribution X on $\{0,1\}^n$ satisfying $H_\infty(X) = k \leq k_{max}$ the distribution $E(X, U_d)$ is a $(k + d, \epsilon)$-source.*

Lossless conductors were also referred to as lossless condensers by [**?**], where it was observed that lossless condensers are equivalent to bipartite graphs of left degree $D = 2^d$ such that every subset of the left vertices of size at most 2^k expands by a factor of $(1 - \epsilon)D$.

We now define lossless expanders and show that they are a special case of lossless conductors.

Definition 16 *A D-regular bipartite graph is a (k_{max}, ϵ)-lossless expander if every subset of size $k \leq k_{max}$ of the left vertices expands by a factor of $(1 - \epsilon)D$.*

It is easy to see from this definition that a lossless conductor, which is just a bipartite graph with left degree $D = 2^d$ such that every subset of the left vertices of size at most 2^k expands by a factor of $(1 - \epsilon)D$, is equivalent to a $(2^{k_{max}}, \epsilon)$-lossless expander.

It is only left to show that an infinite family of lossless expanders can be constructed efficiently. This is done by using the zig-zag product on conductors.

5.2 The zig-zag product and lossless conductors

We would like to extend the zig-zag product to apply to bipartite graphs and then discuss its use on lossless conductors.

Definition 17 (zig-zag product for bipartite graphs) *Let H be a d-regular bipartite graph with m vertices on each side. Let G be an m-regular bipartite graph with n vertices on each side. The zig-zag product $G \textcircled{z} H$ is d^2-regular with mn vertices on each side. The 3-step process determining the edges from a starting vertex (v, k) on the left side changes to:*

1. *take a nondeterministic left to right step in the "cloud" H.*
2. *take a left to right step between clouds along the edge color of G determined by the choice from step1.*
3. *take another nondeterministic left to right step in the "cloud" H*

Capalbo et al. [**?**] present a construction of infinite families of conductors and show that with specific parameters these conductors reduce to constant degree lossless expanders. These results were obtained in part using a modified version of the zig-zag product for conductors. Since the modified product uses different types of conductors such as buffer conductors and permutation conductors, it is difficult to present the details of the construction without providing a deeper insight into the area of randomness enhancing functions, which is beyond the scope of this paper. Instead we give an intuition for the construction and the motivation behind it.

In our discussion of the zig-zag product we have shown that the product graph $G \textcircled{z} H$ is a good expander if G and H are good expanders. In order to construct lossless expanders it is not enough to use the zig-zag product as we first defined it since the resulting expansion parameter of the product might be far from optimal. This is mainly due to the fact that the product graph inherits expansion properties from G and H, which was shown to be bounded above by the square root of the degree of $G \textcircled{z} H$. Since lossless expanders require an expansion parameter that is ϵ-close to the degree, they cannot be efficiently constructed using the zig-zag as we have defined it.

In the entropy analysis of the zig-zag product, we have shown that at least one of the nondeterministic steps in the construction (steps 1 and 3) increases the entropy of the product graph. Therefore it is the case that only D choices always contribute to the increase in entropy, where D is the degree of the small expander. In the improved zig-zag product for conductors, we preserve the entropy that would have otherwise been lost, by keeping a buffer of the random "unused" choices. The buffer is then used with a lossless conductor, which condenses this leftover entropy. Therefore, this new definition of the zig-zag product utilized the maximal amount of randomness to arrive at a

lossless conductor with an expansion parameter which is close to optimal. By [**?**] we may conclude that in selecting specific parameters (namely number of vertices on each side and degree) for the conductors used in the product, the resulting graph is a lossless expander.

6 Conclusion

We have shown that there exists an explicit construction of infinite families of constant degree expanders using the zig-zag product. This is a very important result in that it backs up theoretical assumptions that such expander graph families exist, and thus may be used in many applications. In particular, we have shown an application to coding theory and expander based codes that relies on the work in [**?**], where expanders are shown to be in instance of a larger set known as randomness enhancing functions.
Although there were other construction methods for expander graphs before the zig-zag product, it is easy to see why it became the method of choice for constructing constant degree expanders. With an intuitive definition that yields explicit results, a straight forward proof and flexibility in terms of its extension to different types of expanders, the zig-zag product proved to be a great tool for expander construction.

References

[1] O. Reingold, S. Vadhan, A. Wigderson. Entropy Waves, the zig-zag Graph Product, and New Constant-Degree Expanders. *Annals of Mathematics*, Vol. 155, No.1, pp. 157-187, 2002.

[2] O. Reingold, S. Vadhan, A. Wigderson. Entropy Waves, The zig-zag Graph Product, and New Constant-Degree Expanders and Extractors. *Proc. of the 41st FOCS*, pages 3-13, 2000.

[3] N. Linial, Wigderson. Expander Graphs and Their applications. *Course Notes: Hebrew University, Israel*. http://www.math.ias.edu/ boaz/ExpanderCourse/

[4] C.E. Shannon. A Mathematical Theory of Communication. *The Bell Systems Technical Journal*, Vol 27, pp. 379-423, 623-656, July, October, 1948.

[5] V. Kabanets. Pseudorandomness. *Course Notes: Simon Fraser University*, British Columbia, Canada. 2004. Lecture 6: Random Walks on Graphs and Spectral Graph Theory. http://www.cs.sfu.ca/ kabanets/cmpt881/

[6] R. Durrett. Random Graphs. *Course Notes: Cornell University*. Section 3.3: Eigenvalues and Expanders. http://www.math.cornell.edu/ durrett/math777/math777.html

[7] M. Sipser, D. Spielman. Expander codes. *IEEE Trans. Inform. Theory*. 42: 1710-1722, 1996. Codes and Complexity.

[8] G. Davidoff, P. Sarnak, A. Valette. *Elementary Number Theory, Group Theory, and Ramanujan Graphs*. Cambridge University Press. New York, NY. 2003.

[9] M. Capalbo, O. Reingold, S. Vadhan, A. Wigderson. Randomness Conductors and Constant-Degree Expansion Beyond the Degree / 2 Barrier. *Proceedings of the 34th STOC*, 659-668, 2002.

[10] N. Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):8396, 1986.

[11] Mark S. Pinsker. On the complexity of a concentrator. *In 7th Annual Teletraffic Conference*, pages 318/1318/4, Stockholm, 1973.

[12] A. Ta-Shma, C. Umans, and D. Zuckerman. Loss-less condensers, unbalanced expanders, and extractors. *In Proc. of the 33rd Annual ACM Symposium on the Theory of Computing*, pages 143152, 2001.