An Explicit Construction of Expander Graphs

January 29, 1999

1 Expander Graphs

Definition 1. An (n,k,d)-expander graph is a bipartite graph $G=(U,V;E)$ for which

- $|U|=|V|=n$,
- $|E|\leq kn$,
- $\forall X\subset U$, $|\Gamma(X)|\geq|X|\,(1+d\frac{|\overline{X}|}{n})$, where $\Gamma(X)=\{v\ :\ \exists u\in U,(u,v)\in E\}$ denotes the set of neighbors of X and $\overline{X}$ denotes the complement of X in U.

It is not difficult to demonstrate that $(n,O(1),\Omega(1))$-expanders exist by a counting argument (i.e., the probabilistic method). Our goal today is to give an *explicit* construction, due to Gabber and Galil [**?**].

Expanders have a wide variety of uses in theoretical computer science. Most notably, they have been used to create spectacular pseudorandom generators.

2 The Construction

Fix $n=m^2$ for a natural m and let $A_n=\mathbb{Z}_m\oplus\mathbb{Z}_m$, $\mathbb{Z}_m$ being the group of integers modulo m. A_n may be thought of a combinatorial torus. Consider the following 5 bijections on A_n:

1. $\sigma_0:(x,y)\mapsto(x,y)$,
2. $\sigma_1:(x,y)\mapsto(x,x+y)$,
3. $\sigma_2:(x,y)\mapsto(x,x+y+1)$,
4. $\sigma_3:(x,y)\mapsto(x+y,y)$, and
5. $\sigma_4:(x,y)\mapsto(x+y+1,y)$,

addition modulo m. Now define $G_n=(U_n,V_n;E_n)$ as follows:

- $U_n=V_n=A_n$, and
- $E_n=\{(u,\sigma(u))\ :\ u\in U_n,\sigma\in\{\sigma_i\}\}$.

Observe that, as defined, G_n is a multigraph.

Our goal is to prove the following theorem:

Theorem 1. G_n is an $(n,5,d_0)$-expander for $d_0=(2-\sqrt{3})/4$.

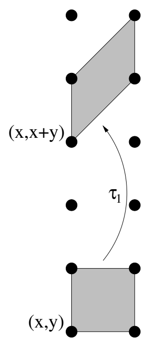

Figure 1: The action of τ_1 on $c_{x,y}$.

3 The Proof

The proof proceeds as a sequence of reductions. The first reduces Theorem 1 to Assumption 1, below.

Assumption 1. For every $X \subset A_n$, $\sum_{i=1}^{4} |\sigma_i(X) - X| \geq 4d_0 \frac{|X||\overline{X}|}{n}$.

Lemma 2. Assumption 1 implies Theorem 1.

Proof. Observe that for any $X \subset A_n$, there is some $i \in \{1,2,3,4\}$ for which $|\sigma_i(X) - X| \geq d_0 \frac{|X||\overline{X}|}{n}$. Considering that σ_0 is the identity map, this establishes the theorem. ☐

The proof, roughly, proceeds in two stages. The first is to reduce the combinatorial statement above to a continuous statement about sets on the 2-torus. Shifting our attention to the continuous problem, we then observe that the maps of interest (which shall be continuous versions of the σ_i above) act nicely on the standard Fourier basis functions. This will allow us to understand their behavior fully enough to prove the theorem.

The 2-torus, T_2, may be thought of as $[0,1) \times [0,1)$. Its topology is given by the quotient $\mathbb{R}^2/\mathbb{Z}^2$, where $\mathbb{R}^2$ is given its normal topology. This essentially means that you "wrap around" when you get to 0 or 1 in either dimension. For a simple discussion of quotient topology, see [**?**]. We adopt standard Lebesgue measure, denoted μ, on T_2 normalized so that $\mu(T_2) = 1$. For a discussion of Lebesgue measure, including its rather tedious construction, see [**?**]. No detailed knowledge of Lebesgue measure is necessary for this proof.

3.1 A Continuous Version

As advertised, the first phase of the proof allows us to shift our attention to a continuous version of the problem. Define two bijections on T_2 as follows:

1. $\tau_1 : (x,y) \mapsto (x, x+y)$, and
2. $\tau_2 : (x,y) \mapsto (x+y, y)$.

Specifically, we will reduce the combinatorial Assumption 1 to the following continuous assertion:

Assumption 2. For every measurable set $X \subset T_2$, $\sum_{i=1,2} \mu(X - \tau_i(X)) \geq 2d_0 \mu(X)\mu(\overline{X})$.

Lemma 3. Assumption 2 implies Assumption 1.

Proof. Fix a set $X \subset A_n$. Defining $c_{x,y} = \left[\frac{x}{m}, \frac{x+1}{m}\right) \times \left[\frac{y}{m}, \frac{y+1}{m}\right) \subset T_2$ for each $(x,y) \in A_n$, set

$$X' = \bigcup_{(x,y) \in X} c_{x,y}.$$

X' is a continuous analogue of X. Observe that $\mu(X') = |X|/n$. Naturally, we would like to see that there is a satisfactory connection between the maps σ_i on A_n and the maps τ_i on T_2. So consider the action of τ_1 on $c_{x,y}$. (See Figure 3.1.) Evidently, the top "triangle" of $\tau_1(c_{x,y})$ lies inside X' exactly when $\sigma_2(x,y) \in X$. Similarly, the bottom "triangle" of $\tau_1(c_{x,y})$ lies in X' exactly when $\sigma_1(x,y) \in X$. Hence

$$\mu(X' - \tau_1(X')) = \frac{1}{2n} \sum_{i=1,2} |X - \sigma_i(X)|.$$

A similar relationship holds between τ_2 and σ_3 and σ_4. Then $\sum_{i=1,2} \mu(X' - \tau_i(X')) = \frac{1}{2n} \sum_{i=1}^{4} |X - \sigma_i(X)|$, and applying the inequality in Assumption 2 finishes the proof. □

This completes the first phase of the proof; we now focus our attention on the continuous problem (Assumption 2). For purely technical reasons which manifest themselves in the final analysis, it will be more convenient for us to work with the maps τ_1^{-2} and τ_2^{-2}. With (considerable) foresight, we reduce to the following:

Assumption 3. For every measurable $X \subset T_2$, $\sum_{i=1,2} \mu(X - \tau_i^{-2}(X)) \geq 4d_0\mu(X)\mu(\overline{X})$.

Lemma 4. Assumption 3 implies Assumption 2.

Proof. Observe that both maps τ_1 and τ_2 are *measure preserving* bijections. Specifically, for any measurable set X, $\mu(X) = \mu(\tau_i(X))$. Observe, then, that for both $\tau \in \{\tau_1, \tau_2\}$, $\mu(\tau(X) - X) = \mu(X - \tau^{-1}(X))$. Now, for any three sets A, B, and C, one has $A - B \subset (A - C) \cup (C - B)$ so that for each $\tau \in \{\tau_1, \tau_2\}$,

$$X - \tau^{-2}(X) \subset (X - \tau^{-1}(X)) \cup (\tau^{-1}(X) - \tau^{-2}(X))$$

and

$$\mu(X - \tau^{-2}(X)) \leq \mu(X - \tau^{-1}(X)) + \mu(\tau^{-1}(X) - \tau^{-2}(X)).$$

From the comment above, $\mu(X - \tau^{-1}(X)) = \mu(\tau^{-1}(X) - \tau^{-2}(X))$, so $\mu(X - \tau^{-2}(X)) \leq 2\mu(X - \tau^{-1}(X)) = 2\mu(\tau(X) - X)$. This last inequality, combined with Assumption 3, implies Assumption 2, as desired. □

We pause now to review some material from Fourier analysis.

3.2 Fourier Analysis of Square Summable Functions on the Torus

Our primary focus shall be the $\mathbb{C}$-vector space of functions

$$L_2(T_2) = \left\{ f : T_2 \to \mathbb{C} \ : \ f \text{ measurable}, \int_{T_2} |f|^2 \, d\mu < \infty \right\}.$$

There is a natural inner product on this space: for $f, g \in L_2(T_2)$, $\langle f, g \rangle = \int_{T_2} f g^* \, d\mu$, where $*$ denotes complex conjugation. This inner product naturally gives rise to a *norm* given by $||f||^2 = \langle f, f \rangle = \int_{T_2} |f|^2 \, d\mu$. With respect to this norm, the space $L_2(T_2)$ is a metric space. This is, in fact, a *Hilbert space*, and hence enjoys all of the properties outlined in the last lecture:

- $L_2(T_2)$ is *complete* with respect to the metric $d(f,g) = ||f - g||$. (This means that for any sequence of functions f_n satisfying
$$\forall \varepsilon > 0, \exists n_0, \forall n, m > n_0, \, d(f_n, f_m) < \varepsilon,$$
there is actually a function $f \in L_2(T_2)$ so that $\lim_{n \to \infty} d(f_n, f) = 0$.
- There is a countable dense set in $L_2(T_2)$. (This means that there is a countable set $F \subset L_2(T_2)$ so that for any $f \in L_2(T_2)$ and any $\varepsilon > 0$, there is an $f' \in F$ for which $d(f, f') < \varepsilon$.) This condition is called *separability*.

We shall be interested in the basis for $L_2(T_2)$ consisting of all functions $\chi_{m,n} : (x,y) \mapsto \exp(2\pi i(mx + ny))$. It is easy to check that

$$\langle \chi_{m,n}, \chi_{m',n'} \rangle = \begin{cases} 1 & \text{if } (m,n) = (m',n') \\ 0 & \text{if } (m,n) \neq (m',n') \end{cases},$$

proving that they are indeed orthonormal. Though it is not obvious, these functions do span $L_2(T_2)$ in the sense that for any $f \in L_2(T_2)$, there is a series $\sum_{m,n} \hat{f}_{m,n}\chi_{m,n}$ which converges to f in the metric given above. Since the functions $\chi_{m,n}$ are orthogonal, the coefficients $\hat{f}_{m,n}$ are unique and may be expressed in terms of the inner product

$$\hat{f}_{m,n} = \langle f, \chi_{m,n} \rangle.$$

The *Fourier transform* of a function $f \in L_2(T_2)$ is precisely this family of coefficients $f_{m,n}$. By expressing a function f in terms of its Fourier coefficients, it is easy to show the *Plancherel equality*: $||f||^2 = \sum_{m,n} \left|\hat{f}_{m,n}\right|^2$.

It will be convenient for us now to define another Hilbert space, the space of all square summable functions on a set $S \subset \mathbb{Z} \times \mathbb{Z}$. Formally,

$$\ell_2(S) = \left\{ f : S \to \mathbb{C} \;:\; \sum_S |f|^2 < \infty \right\}.$$

Inner products on $\ell_2(S)$ are given by $\langle f, g \rangle = \sum_{s \in S} f(s)g(s)^*$. The reason for introducing the above space is that the Plancherel equality (for functions $f \in L_2(T_2)$) shows us that the function $\hat{f} : (m,n) \mapsto \hat{f}_{m,n}$ is an element of $\ell_2(\mathbb{Z} \times \mathbb{Z})$. With this new language, we may consider the Fourier transform as a function

$$\mathfrak{F} : L_2(T_2) \to \ell_2(\mathbb{Z} \times \mathbb{Z})$$

which is, in fact, linear. To conserve brackets, we write $\mathfrak{F}f$ for the Fourier transform of a function f. The Plancherel equality shows that even more is true: we have $||\mathfrak{F}f|| = ||f||$, so that this linear map is an isometry.

For a beautifully written introduction to Fourier analysis, see [**?**].

3.3 The Transformed Problem

We are now in a position to complete the proof of Theorem 1. In preparation for applying the machinery of the last section, we begin by recasting the problem in terms of linear operators on $L_2(T_2)$. For a function $f \in L_2(T_2)$, let $\overline{\tau}_i(f) = f \circ \tau_i^{-1}$. Observe that $\overline{\tau}_i : L_2(T_2) \to L_2(T_2)$ is a linear operator (it is in fact an isometry).

Assumption 4. Let $f \in L_2(T_2)$ satisfy $\int_{T_2} f \, d\mu = 0$. Then $\sum_{i=1,2} \left\|\overline{\tau}_i^2(f) - f\right\|^2 \geq 8d_0 ||f||^2$.

Lemma 5. Assumption 4 implies Assumption 3.

Proof. Fix a measurable set $X \subset T_2$ and define $\phi_X = \chi_X - \mu(X)$ so that

$$\phi_X(p) = \begin{cases} 1 - \mu(X) & \text{if } p \in X \\ -\mu(X) & \text{if } p \in \overline{X}. \end{cases}$$

Observe that $\int_{T_2} \phi_X \, d\mu = 0$ and $||\phi_X||^2 = \mu(X)\mu(\overline{X})$, so that we may apply Assumption 4 to this function. The rest of the proof is computation. Note that for any $Y \subset T_2$, $\overline{\tau}_i(\chi_Y) = \chi_{\tau(Y)}$. Hence $\overline{\tau}_i^2(\phi_X) = \chi_{\tau_i^2(X)} - \chi_X$ and

$$\left|\overline{\tau}_i^2(\phi_X)(p) - \phi_X(p)\right| = \begin{cases} 1 & \text{if } p \in (\tau_i^2(X) - X) \cup (X - \tau_i^2(X)), \\ 0 & \text{otherwise.} \end{cases}$$

Observe that these two sets are disjoint so that $\left\|\overline{\tau}_i^2(\phi_X) - \phi_X\right\|^2 = \mu(\tau_i^2(X) - X) + \mu(X - \tau_i^2(X)) = 2\mu(X - \tau_i^2(X))$. Furthermore,

$$\mu(X - \tau_i^2(X)) = \mu(X) - \mu(X \cap \tau_i^2(X)) = \mu(\tau_i^2(X)) - \mu(X \cap \tau_i^2(X)) = \mu(X - \tau_i^{-2}(X))$$

so that $\left\|\overline{\tau}_i^2(\phi_X) - \phi_X\right\|^2 = 2\mu(X - \tau_i^{-2}(X))$. Substituting this into the inequality of Assumption 4 completes the proof. □

Analyzing the linear maps $f \mapsto \overline{\tau}_i^2(f) - f$ in the standard basis (where we express a function by describing its value on every element of T_2) is made complicated by the "wrap-around" of the topology in T_2. This phenomenon disappears if we consider these linear maps in the Fourier basis. Specifically, note that

$$\begin{aligned}\overline{\tau}_1^2(\chi_{m,n}) &= \chi_{m-2n,n} \\ \overline{\tau}_2^2(\chi_{m,n}) &= \chi_{m,n-2m}\end{aligned}$$

and hence

$$\begin{aligned}\widehat{\overline{\tau}_1^2(\phi_X)}_{m,n} &= \widehat{\phi_X}_{m+2n,n} \\ \widehat{\overline{\tau}_2^2(\phi_X)}_{m,n} &= \widehat{\phi_X}_{m,n+2m}\end{aligned}$$

In light of the above, we consider Assumption 4 in the Fourier basis. Observe that

$$\left\|\overline{\tau}_i^2(f) - f\right\|^2 = \left\|\mathfrak{F}(\overline{\tau}_i^2(f) - f)\right\|^2 = \left\|\mathfrak{F}\overline{\tau}_i^2(f) - \mathfrak{F}f\right\|^2,$$

the first equality by the Plancherel equality, and the second by linearity of $\mathfrak{F}$. Defining $\omega_1, \omega_2 : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ so that $\omega_1 : (m,n) \mapsto (m, n+2m)$ and $\omega_2 : (m,n) \mapsto (m+2n, n)$, we write

$$\sum_{i=1,2} \|\overline{\tau}_i(f) - f\|^2 = \sum_{i=1,2} \|\omega_i(\mathfrak{F}f) - \mathfrak{F}f\|^2. \tag{7}$$

(Recall that $\mathfrak{F}f \in \ell_2(\mathbb{Z}\times\mathbb{Z})$.)

The above reduces Assumption 4 to the following:

Assumption 5. Let $f \in \ell_2(\mathbb{Z}\times\mathbb{Z})$ with $f(0,0) = 0$ and ω_i as above. Then

$$\sum_{i=1,2} \|f\circ\omega_i - f\|^2 \geq (4 - 2\sqrt{3})\,\|f\|^2.$$

Lemma 6. Assumption 5 implies Assumption 4.

Proof. Observe that the condition $\int_{T_2} f\,d\mu = 0$ is identical to $\mathfrak{F}f(0,0) = 0$. Appropriately substituting the equality of equation 7 and the equality $\|f\| = \|\mathfrak{F}f\|$ into Assumption 5 yields Assumption 4 (with $d_0 = (2-\sqrt{3})/4$, as desired). □

The remainder of the proof is a rather unenlightening brute-force demonstration of Assumption 5.

Let $S = \mathbb{Z}\times\mathbb{Z} - \{(0,0)\}$. The two maps ω_1 and ω_2 are permutations of S. Define $S_t = \{(m,n) \in S \;:\; \gcd(m,n) = t\}$, where $\gcd(0,a) = |a|$. Observe that the sets S_t are invariant under the maps ω_i and that S may be written as a disjoint union $S = \cup_t S_t$. It is not hard to show that we may restrict our attention to real-valued functions in $\ell_2(S_1)$. Specifically, we reduce to the following:

Assumption 6. Let $f \in \ell_2(S_1)$ be real-valued. Then

$$\sum_{i=1,2} \|f\circ\omega_i - f\| \geq (4 - 2\sqrt{3})\,\|f\|.$$

Lemma 7. Assumption 6 implies Assumption 5.

Proof. Let $f \in \ell_2(S)$. Assumption 5 follows by applying Assumption 6 to the real functions

$$(m,n) \mapsto \Re f(tm,tn) \qquad (m,n) \mapsto \Im f(tm,tn)$$

defined on S_1 for every $t \geq 1$. ($\Re z$ and $\Im z$ denote the real and imaginary parts of z, respectively.) □

Recalling the definition of $||\cdot||$, we have

$$||f\circ\omega_i - f||^2 = \langle f\circ\omega_1 - f, f\circ\omega_1 - f\rangle = ||f||^2 - 2\langle f, f\circ\omega_1\rangle + ||f\circ\omega_1||^2 .$$

Of course, $||f|| = ||f\circ\omega_1||$, so that

$$\sum_{i=1,2} ||f\circ\omega_i - f||^2 = 4||f||^2 - 2\sum_{i=1,2}\langle f, f\circ\omega_i\rangle$$

and it is enough to establish the following:

Assumption 7. Let $f\in\ell_2(S_1)$ be real valued. Then $2\sum_{i=1,2}\langle f, f\circ\omega_i\rangle \leq 2\sqrt{3}||f||$.

Proof of Assumption 7. Observe that for $a,b\in\mathbb{R}$ and $\lambda>0$, $(a\sqrt{\lambda}-b/\sqrt{\lambda})^2\geq 0$ so that $2ab\leq a^2\lambda+b^2/\lambda$. So let $\lambda : S_1\times S_1\to\mathbb{R}$ be a positive function for which $\lambda(p,q)=[\lambda(q,p)]^{-1}$. Then, for a permutation $\sigma : S_1\to S_1$,

$$2f(x)f(\sigma(x)) \leq \lambda(x,\sigma(x))f(x)^2 + \lambda(\sigma(x),x)f(\sigma(x))^2 = \lambda(x,\sigma(x))f(x)^2 + \lambda(\sigma(x),\sigma^{-1}(\sigma(x)))f(\sigma(x))^2$$

and evidently

$$2\sum_{i=1,2}\langle f, f\circ\omega_i\rangle \leq \sum_{\sigma\in\Sigma}\sum_{x\in S_1}\lambda(x,\sigma(x))f(x)^2 = \sum_{x\in S_1}\left[\sum_{\sigma\in\Sigma}\lambda(x,\sigma(x))f(x)^2\right]. \tag{8}$$

where $\Sigma = \left\{\omega_1,\omega_1^{-1},\omega_2,\omega_2^{-1}\right\}$.

For $(m,n)\in S_1$, let $||(m,n)|| = \max(|m|,|n|)$. A routine case analysis shows that

- if $||x|| = 1$, then $||\sigma(x)|| = ||x||$ for two $\sigma\in\Sigma$ and $||\sigma(x)|| > ||x||$ for two $\sigma\in\Sigma$.
- if $||x|| > 1$, then $||\sigma(x)|| < ||x||$ for one $\sigma\in\Sigma$ and $||\sigma(x)|| > ||x||$ for three $\sigma\in\Sigma$.

Select $\lambda : S_1\times S_1\to\mathbb{R}$ to be the function

$$\lambda(x,y) = \begin{cases} 1/\sqrt{3} & \text{if } ||x|| < ||y||, \\ 1 & \text{if } ||x|| = ||y||, \\ \sqrt{3} & \text{if } ||x|| > ||y||. \end{cases}$$

Observe that for all $x,y\in S_1$, $\lambda(x,y) = [\lambda(y,x)]^{-1}$, so that we may apply inequality 8 above. Now, for any $x\in S_1$, $\sum_{\sigma\in\Sigma}\lambda(x,\sigma(x)) \leq \max(2+2/\sqrt{3},\sqrt{3}+3/\sqrt{3}) = 2\sqrt{3}$. Combining this last inequality with inequality 8 above, we have

$$2\sum_{i=1,2}\langle f, f\circ\omega_i\rangle \leq \sum_{x\in S_1}\sum_{\sigma\in\Sigma}\lambda(x,\sigma(x))f(x)^2 \leq 2\sqrt{3}||f||^2,$$

as desired. □

4 Comments

Surprisingly, the constant $d_0 = (2-\sqrt{3})/4$ is optimal (for these graphs). This proof was improved in 1987 by Jimbo and Maruoka [?]. Their proof bounds all of the eigenvalues of a related graph and does not rely on a passage to the continuous version of the problem.