CS395T Pseudorandomness and Combinatorial Constructions
Course Project, April 24, 2001
Vladimir Trifonov

Gabber-Galil Expander Construction

In this lecture we will see a detailed proof of the expander construction due to Gabber and Galil. This construction was chosen, because it shows an interesting relation between analysis and combinatorial constructions. It is not the best existing today – Lubotzky, Phillips and Sarnak gave in 1986 an explicit construction of Ramanujan graphs, which have optimal second eigenvalue. Furthermore in 2000, Reingold, Vadhan and Wigderson gave an explicit combinatorial construction, which took a somewhat different path in constructing expanders; this construction was considered in Lecture 14. Nevertheless the extreme simplicity of the construction of Gabber and Galil and the relative simplicity of its proof make it an interesting object of study.

Let us remind what is the definition of expander.

Definition 1 *The bipartite graph $G = (V_I \cup V_O, E)$, V_I and V_O are the two parts of the graph, is (n,k,d)-expander if $|V_I| = |V_O| = n$, $|E| = kn$ (this is fulfilled if the graph is k-regular) and for every $X \subseteq V_I$, $|\Gamma(X)| \geq (1 + d\rho(\bar{X}))|X|$, where $\Gamma(X) \subseteq V_O$ are the neighbors of X, $\bar{X} = V_O - X$ and $\rho(\bar{X}) = |\bar{X}|/n$.*

The formal statement of the result of Gabber and Galil is

Theorem 1 *There is an explicit construction of $(n,5,d)$-expander, for $d = (2-\sqrt{3})/4$.*

1 Construction

Let $n = m^2$ and $A_m = \mathbb{Z}_m \times \mathbb{Z}_m$. The expander is constructed using the following five permutations of A_m.

- $\sigma_0(x,y) = (x,y)$,
- $\sigma_1(x,y) = (x,x+y)$,
- $\sigma_2(x,y) = (x,x+y+1)$,
- $\sigma_3(x,y) = (x+y,y)$, and
- $\sigma_4(x,y) = (x+y+1,y)$.

The vertex set of the expander G consists of two copies V_I and V_O of A_m. The neighbors of each vertex from V_I are its images in V_O under the five permutations defined above. We will show that the vertex expansion of G is exactly $(2-\sqrt{3})/4$, as stated in Theorem 1.

2 Proof of Theorem 1

The proof of Theorem 1 proceeds by several consecutive lemmata, which rephrase the expansion definition from its original combinatorial formulation, through a functional analysis formulation, to a formulation in terms of infinite series of complex numbers. The proof of Theorem 1 ends with a proof of the infinite series lemma.

We will start with a lemma from which Theorem 1 follows immediately.

Lemma 1 *For every* $X \subseteq A_m$, $\sum_{i=1}^{4} |\sigma_i(X) - X| \geq 4d|X||\bar{X}|/n$.

Proof (Theorem 1): From the conclusion of Lemma 1, for every $X \subseteq A_m$ there exits $i \in [4]$, such that $|\sigma_i(X) - X| \geq d|X||\bar{X}|/n$. We have that $\Gamma(X) \supseteq \sigma_0(X) \cup \sigma_i(X) = X \cup (\sigma_i(X) - X)$. Since $X \cap (\sigma_i(X) - X) = \emptyset$, $|\Gamma(X)| = |X| + |\sigma_i(X) - X| \geq (1 + d\rho(\bar{X}))|X|$ $\square$

Lemma 1 can be restated using permutations of the rectangle $A = [0,1) \times [0,1)$ instead of the five discrete permutation of A_m. Define the two permutations of A, $\tau_1(x,y) = (x, x+y)$ and $\tau_2(x,y) = (x+y, y)$ (the additions are performed modulo 1). Notice that τ_i is measure preserving, for $i \in [2]$ (take a rectangle in A with sides parallel to the axes and observe that its resulting parallelograms have the same area). Let $\mu(X)$ be the measure of $X \subseteq A$.

Lemma 2 *For every measurable* $X \subseteq A$, $\sum_{i=1}^{2} \mu(X - \tau_i^{-1}(X)) \geq 2d\mu(X)\mu(\bar{X})$

Proof (Lemma 1): Let $X \subseteq A_m$. For every $a = (x,y) \in A_m$, define

$$A_a = \left\{ \left(\frac{x+u}{m}, \frac{y+v}{m} \right) : 0 \leq u, v < 1 \right\}$$

A_a is the square with side $1/m$ and coordinates of the lower left corner $(x/m, y/m)$, i.e. A is partitioned into m^2 such squares. For every $p \in A$ there exist unique $a = (x,y) \in A_m$ and $0 \leq u, v < 1$, such that $p = ((x+u)/m, (y+v)/m)$; denote those with a_p, u_p and u_p. Let $X' = \bigcup_{a \in X} A_a$. By the definition of A_a, $\mu(X') = |X|/n$ and $\mu(\bar{X}') = |\bar{X}|/n$. Also, since X' is measurable, the conclusion of Lemma 2 holds for it.

We will express $\mu(X' - \tau_1^{-1}(X'))$ in terms of X, σ_1 and σ_2. We have that $p \in X' - \tau_1^{-1}(X')$ iff $p \in X'$ and $p \notin \tau_1^{-1}(X')$, i.e. $p \in X'$ and $\tau_1(p) \notin X'$. The last is possible iff $a_p \in X$ and $a_{\tau_1(p)} \notin X$. By the definition of τ_1, σ_1 and σ_2, we have that $a_{\tau_1(p)} \notin X$ iff $u_p + v_p < 1$ and $\sigma_1(a_p) \notin X$ or $u_p + v_p \geq 1$ and $\sigma_2(a_p) \notin X$. Therefore $p \in X' - \tau_1^{-1}(X')$ iff $u_p + v_p < 1$ and $a_p \in X - \sigma_1^{-1}(X)$ or $u_p + v_p \geq 1$ and $a_p \in X - \sigma_2^{-1}(X)$. Using that $\mu(A_a) = 1/n$, for every $a \in A_m$, we obtain that

$$\begin{aligned}
\mu(X' - \tau_1^{-1}(X')) &= \frac{1}{2n}(|X - \sigma_1^{-1}(X)| + |X - \sigma_2^{-1}(X)|) \\
&= \frac{1}{2n}(|\sigma_1(X) - X| + |\sigma_2(X) - X|).
\end{aligned}$$

The second equality is true because σ_1 and σ_2 are permutations.

Using analogous argument we obtain that

$$\mu(X' - \tau_2^{-1}(X')) = \frac{1}{2n}(|\sigma_3(X) - X| + |\sigma_3(X) - X|).$$

Plugging those in the conclusion of Lemma 2 gives us Lemma 1. $\square$

Before rephrasing Lemma 2 in functional analysis terms we will state a technical lemma, which substitutes τ_i^{-1} with τ_i^{-2} in Lemma 2; the necessity of this lemma will be justified in the proof of Lemma 5.

Lemma 3 *For every measurable* $X \subseteq A$, $\sum_{i=1}^{2} \mu(X - \tau_i^{-2}(X)) \geq 4d\mu(X)\mu(\bar{X})$.

Proof (Lemma 2): First notice that for every function f and every two subsets C and D of its domain, $f(C) - f(D) \subseteq f(C - D)$. We also have that for every three sets C, D and E, $C - D \subseteq (C - E) \cup (E - D)$. Using those facts,

$$\begin{aligned} X - \tau_i^{-2}(X) &\subseteq (X - \tau_i^{-1}(X)) \cup (\tau_i^{-1}(X) - \tau_i^{-2}(X)) \\ &\subseteq (X - \tau_i^{-1}(X)) \cup \tau_i^{-1}(X - \tau_i^{-1}(X)) \end{aligned}$$

Hence, since τ_i is measure preserving, $\mu(X - \tau_i^{-2}(X)) \leq 2\mu(X - \tau_i^{-1}(X))$ and Lemma 2 follows. $\square$

If τ is a permutation of A and f is a complex function on A, let $\tilde{\tau}(f) = f \circ \tau^{-1}$. Then Lemma 3 is phrased in functional analysis terms in the following way.

Lemma 4 *Let ϕ be a measurable complex function on A such that $\int \phi = 0$ and $\int |\phi|^2 < \infty$. Then*

$$\sum_{i=1}^{2} \int |\tilde{\tau}_i^2(\phi) - \phi|^2 \geq 8d \int |\phi|^2.$$

Proof (Lemma 3): Let $X \subseteq A$ be measurable. Define $\phi = \chi_X - \mu(X)$, where χ_X is the characteristic function of X. Obviously ϕ is $\mu(\bar{X})$ on X and $-\mu(X)$ on $\bar{X}$. Therefore on one hand $\int \phi = \mu(\bar{X})\mu(X) - \mu(X)\mu(\bar{X}) = 0$ and on the other $\int |\phi|^2 = \mu(\bar{X})^2\mu(X) + \mu(X)^2\mu(\bar{X}) = \mu(X)\mu(\bar{X}) < \infty$. Hence the conclusion of Lemma 4 holds for ϕ.

Notice that $\tilde{\tau}(\chi_X) = \chi_{\tau(X)}$ and $\tilde{\tau}$ is linear. Hence

$$\begin{aligned} |\tilde{\tau}_i^2(\phi) - \phi|^2 &= |\chi_X - \chi_{\tau_i^2(X)}|^2 \\ &= \chi_{(X - \tau_i^2(X)) \cup (\tau_i^2(X) - X)}. \end{aligned}$$

Therefore $\int |\tilde{\tau}_i^2(\phi) - \phi|^2 = \mu((X - \tau_i^2(X)) \cup (\tau_i^2(X) - X))$.

We have that

$$\begin{aligned} \mu(\tau_i^2(X) - X) &= \mu(\tau_i^2(X)) - \mu(\tau_i^2(X) \cap X) \\ &= \mu(X) - \mu(\tau_i^2(X) \cap X) \\ &= \mu(X - \tau_i^2(X)) \\ &= \mu(\tau_i^{-2}(X) - X). \end{aligned}$$

In the second and the fourth equalities we use that τ_i is measure preserving. Thus we obtain that $\int |\tilde{\tau}_i^2(\phi) - \phi|^2 \leq 2\mu(\tau_i^{-2}(X) - X))$. Lemma 3 follows now immediately from the conclusion of Lemma 4. $\square$

We are ready to give a generalization of the definition of expander in terms of infinite sequences of complex numbers.

Lemma 5 *Let $\{a_{m,n}\}_{-\infty<m,n<+\infty} \subseteq \mathbb{C}$ be such that $a_{0,0} = 0$ and $\sum_{m,n} |a_{m,n}|^2 < \infty$. Then*

$$\sum_{m,n} |a_{m+2n,n} - a_{m,n}|^2 + \sum_{m,n} |a_{m,n+2m} - a_{m,n}| \geq 8d \sum_{m,n} |a_{m,n}|^2.$$

Proof (Lemma 4): Let ϕ be a measurable complex function on A, such that $\int \phi = 0$ and $\int |\phi|^2 < \infty$. The Fourier coefficients of ϕ are defined. Let $a_{m,n}(\phi) = \int_A \phi(p)\chi_{m,n}(p)d\mu(p)$, where $\chi_{m,n}(x,y) = e^{2\pi i(mx+ny)}$, be the (m,n)-th Fourier coefficient of ϕ. Then $a_{0,0} = \int \phi = 0$ and $\sum |a_{m,n}|^2 = \int |\phi|^2 < \infty$ (using Parseval's Equality), and the condition of Lemma 5 is fulfilled for the Fourier coefficient of ϕ.

Let us express the infinite sums in the left hand side of the inequality of the conclusion of Lemma 5 in terms of ϕ. We will need

$$\begin{aligned} a_{m,n}(\tilde{\tau}_1^2(\phi)) &= \int_A \phi(\tau_1^{-2}(p))\chi_{m,n}(p)d\mu(p) \\ &= \int_{\tau_1^2(A)} \phi(p)\chi_{m,n}(\tau_1^2(p))d\mu(\tau_1^2(p)) \\ &= \int_A \phi(p)\chi_{m,n+2m}(p)d\mu(p) \\ &= a_{m+2n,n}(\phi) \end{aligned}$$

In the second equality we change the variable of integration and in the third we use that τ_1 is a measure preserving permutation of A and that $\chi_{m,n}(\tau_1^2(x,y)) = \chi_{m,n}(x, 2x+y) = e^{2\pi i(mx+n(2x+y))} = e^{2\pi i((m+2n)x+ny)} = \chi_{m+2n,n}(x,y)$. Using that $a_{m,n}$ is linear, $a_{m,n}(\tilde{\tau}_1^2(\phi)-\phi) = a_{m+2n,n}(\phi) - a_{m,n}(\phi)$. Analogously $a_{m,n}(\tilde{\tau}_2^2(\phi)-\phi) = a_{m,n+2m}(\phi) - a_{m,n}(\phi)$. Plugging those in the conclusion of Lemma 5 for the Fourier coefficients of ϕ and using Parseval's Equality gives us Lemma 4. $\square$

Nothing is left now, but to prove Lemma 5. It will be easier to restate the lemma with complex functions defined on $S = \mathbb{Z} \times \mathbb{Z} - \{(0,0)\}$. For two such functions f and g and $T \subseteq S$, define $\langle f, g\rangle_T = \sum_{x\in T} f(x)g(x)$ (we will omit the subscript T when it is understood by the context). Denote with $l_2(T)$ those functions f for which $\|f\|_T^2 < \infty$. Define the two permutations of S $\omega_1(m,n) = (m+2n, n)$ and $\omega_2(m,n) = (m, n+2m)$. In this notation Lemma 5 becomes.

Claim 1 *For every* $f \in l_2(S), \sum_{i=1}^2 \|f\circ\omega_i - f\|^2 \geq (4-2\sqrt{3})\|f\|^2$

For every $m \geq 1$, define the invariant under ω_1 and ω_2 subsets of S, $S_m = \{(a,b) : \gcd(a,b) = m\}$, where for convenience $\gcd(0,a) = \gcd(a,0) = |a|$. Notice that $\{S_m\}_{m\geq 1}$ forms a partition of S. We will simplify Claim 1, by stating it for real functions defined on S_1.

Claim 2 *For every real* $f \in l_2(S_1)$, $\sum_{i=1}^2 \langle f, f\circ\omega_i\rangle \leq 2\sqrt{3}\|f\|^2$.

Proof (Claim 1): First notice that for real $f \in l_2(S_1)$, $\sum_{i=1}^2 \|f\circ\omega_i - f\| = 4\|f\|^2 - \sum_{i=1}^2 \langle f, f\circ\omega_i\rangle$ (we use that for such functions the inner product is commutative, and that ω_i is a permutation of S_1 and hence $\|f\circ\omega_i\|^2 = \|f\|^2$). Therefore Claim 2 is exactly Claim 1 restricted to real functions from $l_2(S_1)$.

On the other hand Claim 1 follows from Claim 2 in the following way. For $f \in l_2(S)$, define $g_m(x,y) = \operatorname{Re} f(mx, my)$ and $h_m(x,y) = \operatorname{Im} f(mx, my)$, for every $m \geq 1$ and $(x,y) \in S_1$. Since $f \in l_2(S)$, $g_m, h_m \in l_2(S_1)$, for every $m \geq 1$. Now

$$\begin{aligned} \sum_{i=1}^2 \|f\circ\omega_i - f\|_S^2 &= \sum_{i=1}^2 \sum_{m=1}^\infty \|f\circ\omega_i - f\|_{S_m}^2 \\ &= \sum_{i=1}^2 \sum_{m=1}^\infty (\|g_m\circ\omega_i - g_m\|_{S_1}^2 + \|h_m\circ\omega_i - h_m\|_{S_1}^2) \end{aligned}$$

$$
\begin{aligned}
&\geq (4-2\sqrt{3}) \sum_{m=1}^{\infty} (\|g_m\|_{S_1}^2 + \|h_m\|_{S_1}^2) \\
&= (4-2\sqrt{3}) \sum_{m=1}^{\infty} \|f\|_{S_m}^2 \\
&= (4-2\sqrt{3})\|f\|_S^2
\end{aligned}
$$

□

For $x = (m, n) \in S_1$, define $\|x\| = max\{|m|, |n|\}$. Let $\Sigma = \{\omega_1^{\pm 1}, \omega_2^{\pm 1}\}$. By simple case analysis the following claim holds.

Claim 3 *Let $x \in S_1$. If $\|x\| = 1$, then $\|x\| = \|\sigma(x)\|$, for two $\sigma \in \Sigma$ and $\|x\| < \|\sigma(x)\|$, for the other two. If $\|x\| > 1$, then $\|x\| < \|\sigma(x)\|$, for three $\sigma \in \Sigma$ and $\|x\| > \|\sigma(x)\|$, for the other one.*

Define

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

By Claim 3, $\sum_{\sigma\in\Sigma} \lambda(x, \sigma(x)) \leq 2\sqrt{3}$. Notice also that $\lambda^{-1}(x, y) = \lambda(y, x)$.

We are ready to proof Claim 2 and thus to finish the proof of Theorem 1.

Proof (Claim 2): For every $a, b, \lambda \in \mathbb{R}$, $\lambda > 0$, we have that $2ab \leq a^2\lambda + b^2/\lambda$. For $x \in S_1$ and $\sigma \in \{\omega_1, \omega_2\}$, set $a = f(x)$, $b = f(\sigma(x))$ and $\lambda = \lambda(x, \sigma(x))$ in this inequality. Then

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

Summing this inequality over $x \in S_1$, we obtain that

$$
2\langle f, f \circ \sigma\rangle \leq \sum_{\sigma' \in\{\sigma,\sigma^{-1}\}} \sum_{x\in S_1} (f(x))^2\lambda(x, \sigma'(x))
$$

Summing the last inequality over σ, we have that

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

□

As a final word we justify Lemma 3 in the following way. If we did not take the double inverse of the permutations (and stay only with their single inverses), we would have to take $\omega_1(m, n) = (m+n, n)$ and $\omega_2(m, n) = (m, n+m)$. Unfortunately those two permutations does not give the nice properties stated in Claim 2, which justify the definition of $\lambda(x, y)$. For example in this case we will have elements of S_1 (e.g. $(1, 0)$) which have $\|x\| = \|\sigma(x)\|$, for all $\sigma \in \Sigma$. This does not say that we cannot stay with the single inverses, but the proof of Lemma 5 will possibly be more complicated in this case. Gabber and Galil also show that the constant d obtained for their construction is the best possible, i.e. that there is a family of sequences, for which the inequality in the conclusion of Lemma 5 is reversed and the factor d on the right hand side is replaced by a factor which is subconstant additive term away from d.