INF561: Using Randomness in algorithms	Winter 2013
Cours 4 — January, 30^{rd}	
Enseignant : David Xiao	*Rédacteur : Thierry* Deo *& Guillaume* Wenzek

4.1 Recalls and objectives

Définition 4.1. *$S = \{G_1, G_2, \ldots\}$ is a family of (d, λ)-expanders if $\forall G \in S$:*
- *G is d-regular*
- *$\lambda_2(G) \leq \lambda$ where $\lambda_2(G) = max\{|\lambda|, \lambda \neq 1$ eigenvalue of $G\}$*

We saw in last class how to construct algoriths with δ polynomially small, we will now study how to have δ exponentially small. We will as well study how to construct expander graphs.

4.2 Exponentially small error reduction

Théorème 4.2. *$\exists c > 0$ such that $\forall$ algorithm A deciding a language L in time T with error $1/3$ and randomness m, $\forall k$, $\exists$ algorithm A' deciding L in time kT^c with error 2^{-k} and randomness $m + O(k)$.*

For the proof, we will need next lemma :

Lemme 4.3. ***Expander Walk Lemma :*** *If G is a (d, λ)-expander and $B \subseteq V$, $\frac{|B|}{|V|} = \beta$. Let $v_1, v_2, \ldots, v_l$ denote a random walk of size l in G. Let $X_i = 1$ if $v_i \in B$, 0 else. Then $Pr\left(\frac{1}{l}\sum_{i=1}^{l} X_i > \frac{1}{2}\right) \leq (4\sqrt{\beta + \lambda^2})^{l/2}$*

Preuve: of theorem : Assume efficiently computable family of (d, λ)-expanders.

Claim : Without lost of generality, we can assume $\lambda \leq 1/10$, since G^l has degree d^l and $\lambda_2(G^l) = \lambda^l$.

Claim : We can assume as well that the error of A is less then $3/100$, since we can use algorithm from last class.

Let's say $|G_m| = 2^m$, and x is the input.

Let's define Algorithm A' :
1. Take a random walk $v_1, v_2, \ldots$ of length $l = O(k)$ in G_m
2. Run $A(x, v_i)$ $\forall i \in [l] = 1, 2, \ldots, l$ and return the output majority.

Randomness : m to choose v_1, $log(d)$ to compute a neighbour, a total of $m+log(d)*(l-1) = m+O(k)$.

Time : the time to compute a neighbour being $poly(log(|G_m|)) = poly(m) <= T^c$ for a certain c, the total time is in $O(lT^c) = O(kT^c)$.

Error : let's have $B = \{v \in G_m, A(x,v) \neq L(x)\}$. Using the Expander Walk Lemma, we get :

$$\begin{aligned}
Pr\left(A'(x) \neq L(x)\right) &= Pr\left(\frac{1}{l}\sum_{i=1}^{l} X_i > \frac{1}{2}\right) \\
&\leq \left(4\sqrt{\frac{3}{100} + \frac{1}{10}^2}\right)^{l/2} \\
&\leq \left(\frac{8}{10}\right)^{l/2} \\
&\leq 2^{-k} \text{ for } l \geq 8k
\end{aligned}$$

□

Preuve: of EW-Lemma :

Fix G, let $n = |V|$

Let $M_{u,v} = \frac{\#\text{ edges }(u,v)}{d}$

View $\vec{p} \in \mathbb{R}^n, p_i \geq 0, \sum p_i = 1$ as a probability distribution over V.

$M\vec{p}$ is the probability distribution of a random walk starting with $\vec{p}$ and taking one step in the graph.

Let $B \subseteq V$ be seen as a matrix $B_{u,v} = 1$ if $u = v \in B$, $B_{u,v} = 0$ else.
Then, $\forall$ distribution p over V,

$$\begin{aligned}
Pr_{v \leftarrow p}\left(v \in B\right) &= \sum_{u \in B} p_u \\
&= \sum_{u \in [n]} (B\vec{p})_u \\
&= (\vec{1}|B\vec{p})
\end{aligned}$$

Let $B_1, B_2, \ldots, B_l \subseteq V$, we have :

$$Pr_{v_1 \ldots v_l \text{ random walk}}\left(\forall i, v_i \in B_i\right) = (\vec{1}|B_l M B_{l-1} M \ldots B_2 M B_1 \vec{u})$$

We then have :

$$\begin{aligned}
Pr\left(\frac{1}{l}\sum X_i \geq \frac{1}{2}\right) &= Pr\left(\exists S \subseteq [l], |S| \geq l/2, \forall i \in S, v_i \in B\right) \\
&\leq \sum_{S\subseteq[l],|S|\geq l/2} Pr\left(\forall i \in S, v_i \in B\right) \\
&= \sum_{S\subseteq[l],|S|\geq l/2} \left(\vec{1}|\prod_{i=1}^{l}(B_i^S M)u\right) \\
&\leq \sum_{S\subseteq[l],|S|\geq l/2} \|\vec{1}\|.\|\prod_{i=1}^{l}(B_i^S M)u\|
\end{aligned}$$

We will proove later that :

$$\|\prod_{i=1}^{l}(B_i^S M)u\| \leq (\sqrt{\beta+\lambda^2})^{l/2} * 1/\sqrt{n}$$

Which gives us :

$$\begin{aligned}
Pr\left(\frac{1}{l}\sum X_i \geq \frac{1}{2}\right) &\leq \sum_{S\subseteq[l],|S|\geq l/2} \|\vec{1}\|.\|\prod_{i=1}^{l}(B_i^S M)u\| \\
&\leq \sum_{S\subseteq[l],|S|\geq l/2} \sqrt{n} * (\sqrt{\beta+\lambda^2})^{l/2} * 1/\sqrt{n} \\
&\leq 2^l(\sqrt{\beta+\lambda^2})^{l/2} \\
&\leq (4\sqrt{\beta+\lambda^2})^{l/2}
\end{aligned}$$

□

Recall :

- $\|M\| = \max_{\vec{v}\in\mathbb{R}^n, \|\vec{v}\|=1} \|M\vec{v}\|$
- $\|MM'\| \leq \|M\|.\|M'\|$
- for real symmetric M, $\|M\| = \max\{|\lambda|, \lambda \in Spect(M)\}$
- $\lambda_2(M) = \max_{v\in\mathbb{R}^n,(\vec{v}|\vec{1})=0} \frac{\|M\vec{v}\|}{\|\vec{v}\|}$

Preuve: of the formula used before : We know already that $|S| \geq l/2$ and that $\|M\| = 1$, we thus have :

$$\begin{aligned}
\|\prod_{i=1}^{l}(B_i^S M)u\| &\leq \prod_{i=1}^{l}\|B_i^S M\|\|\vec{u}\| \\
&\leq \|BM\|^{l/2}\frac{1}{\sqrt{n}}
\end{aligned}$$

The only thing left to do know if to proove that $\|BM\| \leq \sqrt{\beta+\lambda^2}$

Let's fix $\vec{v} \in \mathbb{R}^n$, $\|\vec{v}\| = 1$

Since M is real symmetric, M has orthonormal basis of eigenvectors : $\frac{1}{\sqrt{n}}\vec{1} = \vec{X}_1, \vec{X}_2, \ldots, \vec{X}_n$ associated with $1 = \lambda_1 \geq \lambda = \lambda_2 \geq \ldots \geq \lambda_n$.

Let's write $\vec{v} = v^{\parallel} + v^{\perp}$ with $v^{\parallel} = (\vec{v}|\frac{1}{\sqrt{n}}\vec{1})\frac{1}{\sqrt{n}}\vec{1}$, we have $\|Mv^{\perp}\| \leq \lambda\|v^{\perp}\|$ since $(v^{\perp}|\vec{1} = 0$ and thanks to last recall.

Let's compute :

$$\begin{aligned}
\|BM\vec{v}\| &= \|BM(v^{\parallel} + v^{\perp})\| \\
&\leq \|BMv^{\parallel}\| + \|BMv^{\perp}\| \\
&\leq \sqrt{\sum_{u\in B}\left(\frac{(\vec{v}|\vec{1})}{n}\right)^2} + \|B\|.\|Mv^{\perp}\| \\
&\leq \sqrt{\frac{\beta n}{n}(\vec{v}|\frac{1}{\sqrt{n}}\vec{1})^2} + \lambda\|v^{\perp}\| \\
&\leq \sqrt{\beta}\left|(\vec{v}|\frac{1}{\sqrt{n}}\vec{1})\right| + \lambda\|v^{\perp}\| \\
&\leq \sqrt{\beta}\|v^{\parallel}\| + \lambda\|v^{\perp}\| \\
&\leq \sqrt{\beta + \lambda^2}\sqrt{\|v^{\parallel}\| + \|v^{\perp}\|} \text{ by Cauchy-Schwartz} \\
&\leq \sqrt{\beta + \lambda^2}\|\vec{v}\|
\end{aligned}$$

□

4.3 Constructing expander graphs

Combinatorial approach : compose small expanders to get bigger ones.

operation	size	degree	expansion	efficiency
squaring	=	$-(d^2)$	$+(\lambda^2)$	$(d+1)t)$
tensor	$++(\lvert V_1\rvert\lvert V_2\rvert)$	$-(d_1.d_2)$	=	$t_1 + t_2 + d_1d_2$
zig-zag	$+(\lvert V_1\rvert d_1)$	$+(d_1^2)$	$\approx$	$t_G + (d+1)t_H$

4.3.1 Graph tensor product :

Given $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, $G_1 \otimes G_2 = (V_1 \times V_2, E')$ where $E' = \{((u,a),(v,b))|(u,v) \in E_1, (a,b) \in E_2\}$.

$M(G_1 \otimes G_2) = M(G_1) \otimes M(G_2)$

where

$$A \otimes B = \left(\begin{array}{c|c|c|c} A_{1,1}B & A_{1,2}B & \dots & A_{1,n}B \\ \hline A_{2,1}B & A_{2,2}B & \dots & A_{2,n}B \\ \hline \dots & \dots & & \dots \\ \hline A_{n,1}B & A_{n,2}B & \dots & A_{1,n}B \end{array}\right) \tag{4.1}$$

and

$$\vec{v} \in \mathbb{R}^n, \vec{w} \in \mathbb{R}^m, \vec{v} \otimes \vec{w} = \left(\begin{array}{c} v_1\vec{w} \\ \hline v_2\vec{w} \\ \hline \\ \hline v_n\vec{w} \end{array}\right) \tag{4.2}$$

Facts :
- $(A \otimes B)(\vec{v} \otimes \vec{w}) = A\vec{v} \otimes B\vec{w}$
- $Spec(A \otimes B) = \{\lambda\mu, \lambda \in Spec(A), \mu \in Spec(B)\}$
- $(\vec{v} \otimes \vec{w}|\vec{x} \otimes \vec{y}) = (\vec{v}|\vec{x})(\vec{w}|\vec{y}))$

Fact : if G_1 is a (d_1, λ)-expander and G_2 is a (d_2, μ)-expander, $G_1 \otimes G_2$ is a $(d_1 d_2, \max(\lambda, \mu))$-expander of size $|V_1||V_2|$

4.3.2 Zig-zag product

Let $G = (V, E)$ be a (D, λ)-expander with n vertices, H be a (d, μ)-expander with D vertices.

$G \circledz H = (V \times [D], E')$

We need to imagine an arbitrary labeling with $[D]$ on the edges at each vertex of G, and we can define the rotation map of G, the bijective function :

$$\begin{array}{rcl} Rot_G : V \times [D] & \longrightarrow & V \times [D] \\ (u, i) & \longrightarrow & (v, j) \end{array}$$

where v is the i^{th} neighbour of u and u is the j^{th} neighbour of v.

$E' = \{((u, i), (v, j)) \,|\exists k, l \in [D], (i, k) \in H, Rot_G(u, k) = (v, l), (v, l) \in H\}$

That zig-zag product is of size $D \times n$ and degree d^2.

Théorème 4.4. *$G \circledz H$ is a $(d^2, \lambda + \mu + \mu^2)$-expander*

Preuve: Let's denote $X = M(H)$ and $M = M(G)$, then $M(G ⓩ H)$ can be written $\tilde{X}\tilde{M}\tilde{X}$ with $\tilde{X} = Id_n \otimes X$ and $\tilde{M}_{(u,i),(v,j)} = 1$ if $Rot_G(u,i) = (v,j)$, 0 else.

We know that $\lambda_2(M(G ⓩ H)) = \max_{(\vec{v}|\vec{1})=1, \|\vec{v}\|=1} (\vec{v}|\tilde{X}\tilde{M}\tilde{X}\vec{v})$
Let's write $J_D = (1)_{1 \le i,j \le D} \in M_D(\mathbb{R})$ and $v^{\parallel} = \left(Id_n \otimes \frac{J_D}{D}\right)\vec{v}$

Facts :
- $v^{\parallel} = \vec{y} \otimes \frac{\vec{1_D}}{D}$ where $y_u = \sum_{i=1} v_{u,i}$
- $\forall u \in [n], \sum_{i=1} v^{\perp}_{u,i} = 0$

$$\begin{aligned}(\vec{v}|\tilde{X}\tilde{M}\tilde{X}\vec{v}) &= (v^{\parallel} + v^{\perp}|\tilde{X}\tilde{M}\tilde{X}(v^{\parallel} + v^{\perp})) \\ &= (v^{\parallel}|\tilde{X}\tilde{M}\tilde{X}v^{\parallel}) + 2(v^{\parallel}|\tilde{X}\tilde{M}\tilde{X}v^{\perp}) + (v^{\perp}|\tilde{X}\tilde{M}\tilde{X}v^{\perp})\end{aligned}$$

Let's denote $(1), (2)$ and (3) the three terms of this sum.

About (1), since $\tilde{X}v^{\parallel} = v^{\parallel}$:

$$\begin{aligned}(v^{\parallel}|\tilde{M}v^{\parallel}) &= \left((Id \otimes \frac{J_D}{D})v^{\parallel}|\tilde{M}(Id \otimes \frac{J_D}{D})v^{\parallel}\right) \\ &= (v^{\parallel}|(Id \otimes \frac{J_D}{D})\tilde{M}(Id \otimes \frac{J_D}{D})v^{\parallel})\end{aligned}$$

We can see that $(Id \otimes \frac{J_D}{D})\tilde{M}(Id \otimes \frac{J_D}{D}) = M \otimes \frac{J_D}{D}$ because during the multiplication on the left, each block in $\tilde{M}$ is multiplied by $\frac{J_D}{D}$ on the right and on the left, hence the blocks of the result are uniforms.

We can now compute :

$$\begin{aligned}(v^{\parallel}|\tilde{X}\tilde{M}\tilde{X}v^{\parallel}) &= (v^{\parallel}|(M \otimes \frac{J_D}{D})v^{\parallel}) \\ &= (\vec{y} \otimes \frac{\vec{1}}{D}|(M \otimes \frac{J_D}{D})(\vec{y} \otimes \frac{\vec{1}}{D})) \\ &= (\vec{y} \otimes \frac{\vec{1}}{D}|M\vec{y} \otimes \frac{\vec{1}}{D}) \\ &= (\vec{y}|M\vec{y})(\frac{\vec{1}}{D}|\frac{\vec{1}}{D}) \\ &\le \lambda\|\vec{y}\|^2\frac{1}{D} \\ &\le \lambda\|v^{\parallel}\|^2\end{aligned}$$

Let's now calculate a bound on (2) :

$$\begin{aligned}
(v^{\parallel}|\tilde{X}\tilde{M}\tilde{X}v^{\perp}) &\leq \|v^{\parallel}\|\|\tilde{X}\tilde{M}\tilde{X}v^{\perp}\| \\
&\leq \|v^{\parallel}\|\|\tilde{X}v^{\perp}\| \\
&\leq \|v^{\parallel}\|\|(I\otimes X)v^{\perp}\| \\
&\leq \|v^{\parallel}\|\|(I\otimes X)\sum_{u\in[n]} e_u\otimes v_u^{\perp}\| \text{ where } (e_u)_i=\delta_{iu} \\
&\leq \|v^{\parallel}\|\|\sum_{u\in[n]} e_u\otimes Xv_u^{\perp}\| \\
&\leq \|v^{\parallel}\|\sqrt{\sum_{u\in[n]}\|eu\otimes Xv_u^{\perp}\|^2} \text{ by orthogonality} \\
&\leq \|v^{\parallel}\|\sqrt{\sum_{u\in[n]}\|Xv_u^{\perp}\|^2} \\
&\leq \|v^{\parallel}\|\sqrt{\sum_{u\in[n]}\mu^2\|v_u^{\perp}\|^2} \\
&\leq \mu\|v^{\parallel}\|\sqrt{\sum_{u\in[n]}\|v_u^{\perp}\|^2} \\
&\leq \mu\|v^{\parallel}\|\|v^{\perp}\|
\end{aligned}$$

And finally, on (3) :

$$\begin{aligned}
(v^{\perp}|\tilde{X}\tilde{M}\tilde{X}v^{\perp}) &= (\tilde{X}v^{\perp}|\tilde{M}\tilde{X}v^{\perp}) \\
&\leq \|\tilde{X}v^{\perp}\|\|\tilde{M}\tilde{X}v^{\perp}\| \\
&\leq \|\tilde{X}v^{\perp}\|^2 \\
&\leq \mu^2\|v^{\perp}\|^2
\end{aligned}$$

If we notice that $2\|v^{\parallel}\|\|v^{\perp}\| \leq \|v^{\parallel}\|^2+\|v^{\perp}\|^2 \leq 1$, we finally have, combining those three bounds :

$$\begin{aligned}
\lambda_2(G \text{ⓩ} H) &\leq \max{(\vec{v}|\vec{1})=0,\|\vec{v}\|=1}\lambda\|v^{\parallel}\|^2+2\mu\|v^{\parallel}\|\|v^{\perp}\|+\mu^2\|v^{\perp}\|^2 \\
&\leq \lambda+\mu+\mu^2
\end{aligned}$$

□

4.4 Construction of family of $(d, 1/5)$-expanders

Take any $H = (d, 1/10)$-expander on d^8 vertices, we define :

$$\begin{aligned} G_1 &= H^2 \\ G_2 &= H \otimes H \\ G_i &= \left(G_{\lceil i-1/2 \rceil} \otimes G_{\lfloor i-1/2 \rfloor}\right)^2 \text{Ⓩ} H \end{aligned}$$

For all i, G_i is of size d^{8i}, degree d^2 and $\lambda_2(G_i) \leq \frac{1}{5}$
Running time to compute neighbours in G_i : $t_i \leq i^c$