Introduction aux expandeurs

Omid Amini* Frédéric Havet*

JCALM Octobre 2006

Avant-propos

Cette introduction aux graphes expandeurs a été rédigée pour la première Journée Combinatoire du Littoral Méditerranéen le 20 octobre 2006 à Sophia-Antipolis. Les principales sources qui l'ont inspirée sont le survey de Hoory, Linial et Widgerson [10] sur les expandeurs, celui de Ram Murty [20] sur les graphes de Ramanujan, le mémoire de David Y. Xiao [23], **completer**.

1 Introduction

Soit $G = (V, E)$ un graphe. Son nombre de sommets $|V|$ sera également noté n. Ses sommets seront dénotés $v_1, v_2, \ldots, v_n$.

Soit $S, T \subset V$. L'ensemble des arêtes internes à S est dénoté $E(S) = \{uv \mid u \in S, v \in S, uv \in E\}$ et sa cardinalité $e(S)$. L'ensemble d'arêtes entre S et T est dénoté $E(S,T) = \{uv \mid u \in S, v \in T, uv \in E\}$ et sa cardinalité $e(S,T)$.

Le *bord* d'un ensemble de sommets S est l'ensemble $B(S) = E(S, \overline{S})$ d'arêtes ayant exactement une extrémité dans S. On note $b(S) = |B(S)| = e(S, \overline{S})$.

Le *degré* d'un sommet v, noté $d(v)$, est le nombre d'arêtes incidentes à v. Ainsi s'il n'y a pas de boucle en v, $d(v) = b(\{v\})$. Le *degré maximal* de G, noté $\Delta(G)$, est défini par $\Delta(G) = \max_{v \in V} d(v)$. Le *degré minimal* de G, noté $\delta(G)$, est défini par $\delta(G) = \min_{v \in V} d(v)$.

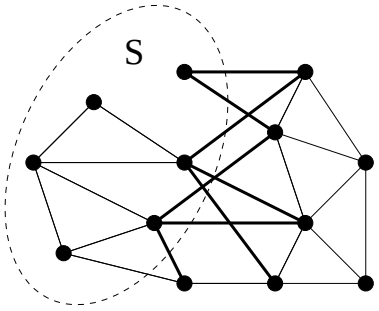

Figure 1: Le bord d'un ensemble de sommets S (arêtes en gras).

*Projet Mascotte, CNRS/INRIA/UNSA, INRIA Sophia-Antipolis, 2004 route des Lucioles BP 93, 06902 Sophia-Antipolis Cedex, France oamini,fhavet@sophia.inria.fr

L'*arête-expansion* ou *expansion* d'un ensemble S dans G, dénotée $exp_G(S)$ ou $exp(S)$, est $\frac{b(S)}{|S|}$. L'*arête-expansion* ou *expansion* du graphe G notée $exp(G)$ est définie par:

$$exp(G) = \min_{\{S \mid |S| \leq n/2\}} exp(S).$$

Un graphe G est dit *c-expandeur* si son expansion est au moins c, i.e. $exp(G) \geq c$.

Par définition, l'expansion est inférieure où égale au degré minimum, $exp(G) \leq \delta(G)$, mais elle peut être beaucoup plus petite.

1.1 Expansion de quelques graphes particuliers

Graphes complets L'expansion du graphe complet K_n à n sommets est $\lceil n/2 \rceil$. En effet, pour tout ensemble $S \subset V(K_n)$, on a $b(S) = |S|(n - |S|)$. Donc $exp(K_n) = \lceil n/2 \rceil$.

Cycles L'expansion du cycle à n sommets est $\frac{2}{\lfloor n/2 \rfloor}$, car le bord d'un sous-chemin est consitué de deux arêtes.

Bipartis complets Pour $n = 4p$, l'expansion d'un graphe biparti complet $K_{2p,2p}$ est $p = n/4$. En effet, si S a k sommets dans une partie de la bipartition et l dans l'autre partie, $b(S) = k(2p-l)+l(2p-k) = 2p(k+l) - 2kl$.

Hypercubes L'*hypercube de dimension d* ou *d-cube* est le graphe Q_d ayant pour ensemble de sommets $V(Q_d) = \{0,1\}^d$ tels que deux sommets v_1 et v_2 sont adjacents si et seulement si ces deux vecteurs différent d'une coordonnée exactement. Si $S \subset V(Q_d)$ est de taille k alors $b(S) \geq k(d - \log_2 k)$ avec égalité si et seulement si k est une puissance de 2, disons $k = 2^l$ et S induit un l-cube. Ainsi $exp(Q_d) = 1$.

Grille torique Supposons que G soit la grille torique à deux dimension $p \times p$. Elle a $n = p^2$ sommets. Un ensemble S à k sommets de plus faible bord, ressemble le plus possible à un sous-carré de la grille. De plus, son bord est de taille $b(S) \approx 4\sqrt{k}$. Ainsi l'expansion de la grille est $\approx \frac{4\sqrt{2}}{\sqrt{n}}$.

1.2 Importance des graphes expandeurs

Les expandeurs jouent un rôle important dans de nombreux domaines des mathématiques, de l'informatique ou de la physique. En informatique, s'il n'est pas surprenant que les expandeurs soient utiles à la conception de réseaux de communication [3, 9], ils apparaissent dans bien d'autres domaines de manière a priori moins évidente. On les retrouve ainsi dans la théorie des codes correcteurs d'erreurs [21] et la théorie du pseudo-aléatoire [12]. En mathématiques, ils jouent un rôle dans l'étude des plongements métriques (voir [13] ou les chaptitres de livres [16] et [11]) et en particulier sur les travaux autour de la Conjecture de Baum-Connes [22]. L'expansion est également fortement liée à la vitesse de convergence des chaines de Markov, et donc joue un role dans l'étude des algorithmes Monte-Carlo en physique statistique. Cette liste d'applications des expandeurs est non exhaustive et continue à croitre. Dans ce papier, nous ne détaillerons que l'application des expandeurs à la diminution de la probabilité d'erreur dans les algorithmes BBP (Voir Partie 3). Nous renvoyons ceux qui désirent en savoir plus sur les autres liens des expandeurs aux références ci-dessus ou au survey de Hoory, Linial et Widgerson [10].

Les graphes complets montrent que l'expansion peut être de l'ordre de n. Cependant, dans toutes les applications, on cherche des graphes de taille n très grande et de degré borné. Comme l'expansion est borné par le degré minimum, on cherche donc très des graphes d-réguliers d'ordre arbitrairement grand et d'expansion la plus grande possible.

Dans toute la suite de cette partie, nous considérerons presque uniquement des graphes d-réguliers.

Théorème 1 (Blum et al. [5]) *Le problème suivant est co-NP-difficile:*

Donnée: *Un graphe G et $c > 0$.*
Question: *G est-il un c-expandeur?*

1.3 Première borne supérieure pour l'expansion

Considérons un graphe $G = (V, E)$ avec $V = \{v_1, v_2, \dots v_n\}$.

Pour $S \subset V$, le *vecteur caractéritique* de S est $\mathbf{1}_S = (z_1, z_2, \dots, z_n)^T$, avec $z_i = 1$ si $v_i \in S$ et $z_i = 0$ sinon.

Soit S un ensemble de sommets. Nous pouvons facilement exprimer son expansion $exp(S)$ en fonction de $\mathbf{1}_S$. En effet, $|S| = \sum_{i=1}^{n} z_i$ et $b(S) = \sum_{v_iv_j \in E,\ i<j} |z_i - z_j|$.

Par définition, $exp(G) \leq exp(S)$ pour tout S tel que $|S| \leq n/2$. Ainsi pour tout vecteur $z = (z_1, z_2, \dots, z_n)^T$ de $\{0,1\}^n$ dont au moins la moitié des coordonnées sont nulles, nous avons $exp(G) \leq \dfrac{\sum_{v_iv_j \in E,\ i<j} |z_i - z_j|}{\sum_{i=1}^{n} z_i}$.

Nous allons maintenant montrer que cette inégalité est également vérifiée pour les vecteurs à valeur dans $\mathbb{R}^+$ dont au moins la moitié des coordonnées sont nulles. Pour cela, nous allons majorer l'expansion par la moyenne pondérée des expansions de certains ensembles emboités.

Lemme 2 *Soit G un graphe sur les sommets $v_1, v_2, \dots, v_n$ et $z = (z_1, z_2, \dots, z_n)^T$ un vecteur de $(\mathbb{R}^+)^n$. Si au moins $n/2$ des z_i sont nuls alors*

$$exp(G) \leq \frac{\sum_{v_iv_j \in E,\ i<j} |z_i - z_j|}{\sum_{i=1}^{n} z_i}.$$

Preuve. Quitte à réindexer les sommets, on peut supposer $z_1 \geq z_2 \geq \cdots \geq z_n$. Mettons chaque sommet v_i sur l'intervalle $[0, z_1]$ avec coordonnée z_i. Considérons la fonction f, définie sur $[0, z_1]$, qui associe à chaque réel $t \in [0, z_1]$ le nombre d'arcs v_iv_j de G tel que $v_i < t \leq v_j$. C'est une fonction constante par morceaux qui vaut $b(V_i)$ sur $]z_{i+1}, z_i]$ avec $V_i = \{v_1, v_2, \dots, v_i\}$. Ainsi

$$\int_0^{z_1} f(t)dt = \sum_{i=1}^{n-1} (z_i - z_{i+1}) b(V_i).$$

Comme $z_i = 0$ si $i \geq n/2$ et chaque V_i, $1 \leq i \leq n/2$, est de taille i, $b(V_i) \leq exp(G)i$, on obtient

$$\int_0^{z_1} f(t)dt \leq exp(G) \sum_{i=1}^{n-1} i.(z_i - z_{i+1}) = exp(G) \left(\sum_{i=1}^{n-1} i.z_i - \sum_{i=2}^{n} (i-1) z_i \right) = exp(G) \sum_{i=1}^{n} z_i.$$

D'autre part, une arête v_iv_j, avec $i < j$ compte 1 pour f sur $]z_j, z_i]$ et 0 sinon. Ainsi

$$\int_0^{z_1} f(t)dt = \sum_{v_iv_j \in E,\ i<j} (z_i - z_j).$$

□

Remarque 3 Si $exp(S) = exp(G)$, alors posant $z = \mathbf{1}_S$, on a $exp(G) = \dfrac{\sum_{v_iv_j \in E,\ i<j} |z_i - z_j|}{\sum_{i=1}^{n} z_i}$.

2 Spectre du graphe et expansion

La *matrice d'adjacence* d'un graphe G à n sommets $v_1, v_2, \ldots, v_n$ est la matrice $n \times n$, dénotée $A(G)$ (ou A si G est explicite dans le contexte), dont l'entrée $a_{i,j}$ est le nombre d'arêtes entre v_i et v_j. Remarquons que si le graphe est sans boucle alors la diagonale est nulle. Comme la matrice $A(G)$ est réelle et symétrique, elle possède n valeurs propres réelles $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. L'ensemble des valeurs propres de $A(G)$ est appelé *spectre* de G.

Le spectre d'un graphe est fortement relié à certaines propriétés du graphe. Nous allons voir que la première valeur propre λ_1 est reliée au degré maximal du graphe et que l'*écart spectral*, i.e. la différence entre la première et la seconde valeur propre $(\lambda_1 - \lambda_2)$, est une estimation de son expansion.

2.1 Première valeur propre et degré maximum

Théorème 4 *Soit A la matrice d'adjacence d'un graphe G. Si λ est une valeur propre de A alors $|\lambda| \leq \Delta(G)$.*

Preuve. Soit $x = (x_1, \ldots, x_n)^T$ un vecteur propre de A associé à la valeur propre λ. Alors $Ax = \lambda x$. Soit i tel que $|x_i| = \max_{1 \leq j \leq n} |x_j|$. Alors,

$$|\lambda||x_i| = \left| \sum_{j=1}^{n} a_{i,j} x_j \right| \leq |x_i| \sum_{j=1}^{n} a_{i,j} = |x_i| d(v_i) \leq |x_i| \Delta(G).$$

Ainsi $|\lambda| \leq \Delta(G)$. □

Pour les graphes d-réguliers, $\Delta(G) = d$ est trivialement une valeur propre. En effet, la somme sur chaque ligne vaut d et donc $\mathbf{1} = (1, 1, \ldots, 1)^T$ est un vecteur propre asscocié à la valeur propre d. Si C est une composante connexe, son vecteur caractéristique est également un vecteur propre associé à λ_1.

Théorème 5 *Si G est un graphe d-régulier alors d est une valeur propre de $A(G)$ avec multiplicité le nombre de composantes connexes de G.*

Preuve. Soit C_1, C_2, …, C_p les composantes connexes de G. Considérons les vecteurs caractéristiques $\mathbf{1}_{C_l}$ des C_l. Clairement, ces vecteurs sont des vecteurs propres orthogonaux et associés à d.

Considérons maintenant un vecteur propre $x = (x_1, \ldots, x_n)^T$ associé à d. Soit $|x_i| = \max_{1 \leq j \leq n} |x_j|$. Sans perte de généralité, on peut supposer $x_i > 0$. Alors $dx_i = \sum_{j=1}^{n} a_{i,j} x_j \leq \sum_{j=1}^{n} a_{i,j} x_i = dx_i$. Ainsi pour tout j pour lequel $a_{i,j} \neq 0$, nous avons $x_i = x_j$. C'est le cas pour tous les j tels que $v_i v_j$ soit une arête. Répètant l'argument de proche en proche, pour tous les sommets v_j de la même composante connexe que v_i, on a $x_i = x_j$.

Appliquant cet argument pour chaque composante connexe, on montre que x est une combinaison linéaire des $\mathbf{1}_{C_l}$. □

2.2 Ecart spectral et expansion

Nous venons de voir que le degré maximum d'un graphe est relié à sa première valeur propre. Le théorème suivant, montré par Dodziuk [6] et indépendamment par Alon et Milman [2] et Alon [1], montre que l'expansion d'un graphe d-régulier est fortement reliée à l'*écart spectral*, c'est-à-dire à la différence $\lambda_1 - \lambda_2 = d - \lambda_2$ entre sa première et sa deuxième valeur propre.

Théorème 6 *Soit G un graphe d-régulier de spectre $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Alors*

$$\frac{d - \lambda_2}{2} \leq exp(G) \leq \sqrt{2d(d - \lambda_2)}.$$

Les bornes inférieures et supérieures de ce théorème sont serrées. En effet, nous avons vu Sous-partie1.1 que le d-cube a expansion 1. D'autre part son écart spectral vaut 2. Le cycle C_n a expansion $\Theta(1/n)$ alors que son écart spectral vaut $\Theta(1/n^2)$. Pour une preuve des estimations de ces écarts spectraux, voir partie 11.1 de [10] ou le livre de Lovász [19].

Preuve du Théorème 6.

Pour prouver ce théorème, nous devons prouver deux inégalités.

• $\frac{d-\lambda_2}{2} \leq exp(G)$**:** Pour prouver cette inégalité, nous avons besoin du Théorème de Rayleigh-Ritz ou plus précisément d'un de ces corollaires. Ce théorème affirme que $\lambda_1 = \max_{x \neq 0} \frac{x^T A x}{||x||^2}$. Rappelons que $||x||^2 = x^T x$. Comme dans un graphe d-régulier, $\mathbf{1} = (1, 1, \ldots, 1)^T$ est un vecteur propre associé à $\lambda_1 = d$, un corollaire immédiat est $\lambda_2 = \max_{x \neq 0, x^T \mathbf{1} = 0} \frac{x^T A x}{||x||^2}$. Il nous faut donc exhiber un vecteur x orthogonal à $\mathbf{1}$ tel que $\frac{x^T A x}{||x||^2} \geq d - 2exp(G)$.

Soit S un ensemble de taille au plus $n/2$ tel que $exp(G) = exp(S)$. Considérons le vecteur $x = |\overline{S}|\mathbf{1}_S - |S|\mathbf{1}_{\overline{S}}$. On a:

$$\begin{aligned} ||x||^2 &= |\overline{S}|^2|S| + |S|^2|\overline{S}| = |S||\overline{S}|(|S| + |\overline{S}|) = n|S||\overline{S}|, \\ x^t A x &= 2(\ |\overline{S}|^2 e(S) + |S|^2 |e(\overline{S}) - |S||\overline{S}|b(S)\ ). \end{aligned}$$

Comme G est d-régulier, nous avons

$$\begin{aligned} 2e(S) &= d|S| - b(S) \\ 2e(\overline{S}) &= d|\overline{S}| - b(S) \end{aligned}$$

Introduisant ces égalités dans les équations précédentes, il vient:

$$\frac{x^T A x}{||x||^2} = \frac{nd|S||\overline{S}| - n^2 b(S)}{n|S||\overline{S}|} = d - \frac{nb(s)}{|S||\overline{S}|}.$$

Comme $|\overline{S}| \geq n/2$, il vient $\frac{x^T A x}{||x||^2} \geq d - 2exp(G)$. De plus, il est facile de vérifier que $x^T \mathbf{1} = 0$. On a donc bien $\lambda_2 \geq d - 2exp(G)$.

• $exp(G) \leq \sqrt{2d(d-\lambda_2)}$**:** D'après le Lemme 2, pour tout vecteur $z = (z_1, z_2, \ldots, z_n)$ tel que la moitié au moins de ses coordonnées sont nulles, $\sigma(z) = (\sum_{u_i u_j \in E,\ i<j} |z_i - z_j|)/(\sum_{i=1}^n z_i)$ est une borne supérieure de l'expansion de G. Nous allons donc trouver un vecteur z tel que $\sigma(z) \leq \sqrt{2d(d-\lambda_2)}$.

Pour cela, considérons un vecteur propre x associé à λ_2. Notons que x est orthogonal à $\mathbf{1}$ donc il a des coordonnées à la fois positives et négatives. Soit $I^+ = \{i \mid x_i > 0\}$ et y le vecteur défini par $y_i = \max\{x_i, 0\}$. Quitte à considérer $-x$ (qui est également vecteur propre associé à λ_2) à la place de x, on peut supposer que $|I^+| \leq n/2$. Soit z le vecteur défini par $z_i = y_i^2$.

Par l'inégalité de Cauchy-Schwarz, nous avons

$$\begin{aligned} \sum_{v_i v_j \in E,\ i<j} |y_i^2 - y_j^2| &= \sum_{v_i v_j \in E,\ i<j} |y_i + y_j|.|y_i - y_j| \\ &\leq \sqrt{\sum_{v_i v_j \in E,\ i<j} (y_i + y_j)^2}.\sqrt{\sum_{v_i v_j \in E,\ i<j} (y_i - y_j)^2} \qquad (1) \end{aligned}$$

Evaluons maintenant les deux facteurs du membre droit de cette inégalité.

$$\sqrt{\sum_{v_iv_j\in E,\ i<j}(y_i+y_j)^2} \le \sqrt{2\sum_{v_iv_j\in E,\ i<j}(y_i^2+y_j^2)} = \sqrt{2\sum_{i=1}^{n} y_i^2} = \sqrt{2d}.||y|| \tag{2}$$

Nous avons $\sum_{u_iu_j\in E,\ i<j}(y_i-y_j)^2 = y^TLy.$ où L est la matrice $L = dI - A$ (appelée *Laplacien* de G) avec I la matrice identité. Or pour tout $i \in I^+$,

$$\begin{aligned}(Ly)_i &= dy_i - \sum_{j=1}^{n} a_{i,j}y_j = dx_i - \sum_{j\in I^+} a_{i,j}x_j \\ &\le dx_i - \sum_{j=1}^{n} a_{i,j}x_j = (Lx)_i = (d-\lambda_2)x_i.\end{aligned}$$

Comme $y_i = 0$ pour $i \notin I^+$, on obtient:

$$y^TLy = \sum_{i=1}^{n} y_i.(Ly)_i \le (d-\lambda_2)\sum_{i\in I^+} x_i^2 = (d-\lambda_2)\sum_{i\in I^+} y_i^2 = (d-\lambda_2)||y||^2.$$

Donc

$$\sqrt{\sum_{u_iu_j\in E,\ i<j}(y_i-y_j)^2} \le \sqrt{d-\lambda_2}||y|| \tag{3}$$

En reportant, les inégalités (2) et (3) dans (1), on obtient $\sigma(z) \le \sqrt{2d(d-\lambda_2)}$.

□

Remarque 7 La preuve précédente permet de trouver un ensemble de petite expansion. Si on trie les sommets v_i par ordre décroissant de la coordonnée x_i du vecteur propre x associé à λ_2. Disons $x_1 \ge x_2 \ge \cdots \ge x_n$. Un des ensembles $S_i = \{v_1, v_2 \ldots, v_i\}$ $1 \le i \le n/2$ a une expansion au plus $\sqrt{2d(d-\lambda_2)}$.

2.3 Bornes sur la deuxième valeur propre

Au vu Théorème 6, il est intéressant de connaître la valeur maximum que peut prendre l'écart spectral et donc la valeur minimum que peut atteindre la deuxième valeur propre.

Si on regarde le graphe complet K_n, sa matrice d'adjacence est $J - I$ où J est la matrice ayant des 1 partout et I la matrice identité. Ainsi le spectre de K_n est $[n-1, -1, -1, \ldots, -1]$. En particulier $\lambda_2 = -1$.

Cependant, nous sommes intéressés par des graphes d-régulier d'ordre n avec d très petit par rapport à n. Dans ce cas, le théorème d'Alon-Boppana donne une borne inférieure sur λ_2. La preuve originale de ce théorème est parue dans [18]. Une preuve alternative a été donnée par Friedman [8].

Théorème 8 (Alon-Boppana) *Pour tout graphe d-régulier d'ordre n,*

$$\lambda_2 \ge 2\sqrt{d-1}\,(1-o(1))\,.$$

Ce théorème et le Théorème 6 donnent directement la borne supérieure suivante sur l'expansion d'un graphe d-régulier d'ordre n.

Corollaire 9 *Pour tout graphe d-régulier d'ordre n,*

$$exp(G) \leq \sqrt{2d\left(d - 2\sqrt{d-1}\right)} + o(1).$$

Afin de prouver le théorème d'Alon-Boppana, nous allons établir le lemme suivant:

Lemme 10 *Soit G un graphe d-régulier. Si son diamètre est au moins* $2a + 2 \geq 4$ *alors*

$$\lambda_2 \geq 2\sqrt{d-1} - \frac{2\sqrt{d-1} - 1}{a}.$$

Soit G un graphe d-régulier G d'ordre n. Le nombre de sommets de G à distance au plus k d'un sommet v est au plus $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$. Ainsi le diamètre d'un graphe d-régulier d'ordre n est $\Omega(\log_{d-1} n)$. Le Lemme 10 implique donc le Théorème 8.

Remarque 11 Cette preuve du Théorème d'Alon-Boppana donne un $o(1)$ qui est un $O\left(\frac{1}{\log n}\right)$. Par des preuve plus fines que celle-ci, nous pouvons obtenir un $o(1)$ de la forme $O\left(\frac{1}{\log^2 n}\right)$.

Preuve du Lemme 10.

Considérons le Laplacien $L = dI - A$. Il est facile de voir que les valeurs propres de L sont les $d - \lambda_i$, $1 \leq i \leq n$. Ainsi par le théorème de Rayleigh-Ritz,

$$d - \lambda_2 = \min_{x \neq 0, x^T \mathbf{1} = 0} \frac{x^T L x}{||x||^2}.$$

Notre but va donc être de trouver un vecteur x orthogonal à $\mathbf{1}$ pour lequel $\frac{x^T L x}{||x||^2}$ est petit.

Soient u et w deux sommets de G tels que $dist(u,w) \geq 2a + 2$. Pour $0 \leq k$, notons $U_k = \{z \in G \mid dist(u,z) = k\}$ et $W_k = \{z \in G \mid dist(w,z) = k\}$. Posons $U = \bigcup_{k=0}^{a} U_k$ et $W = \bigcup_{k=0}^{a} W_k$. Clairement, les ensembles $U_0, U_1, \ldots, U_a, W_0, W_1, \ldots, W_a$ sont disjoints et aucun sommet de U n'est adjacent à un sommet de W. De plus, pour tout $k \geq 1$, chaque sommet de U_k est adjacent à au moins un sommet de U_{k-1} et donc à au plus $d-1$ sommets de U_{k+1}. Ainsi $|U_{k+1}| \leq (d-1)|U_k|$ et, par récurrence, $|U_a| \leq (d-1)^{(a-k)}|U_k|$. De même, $|W_{k+1}| \leq (d-1)|W_k|$ et $|W_a| \leq (d-1)^{(a-k)}|W_k|$.

Nous allons maintenant considérer un vecteur x tel que $x_i = \alpha_k$ si $v_i \in U_k$, $x_i = \beta_k$ si $v_i \in W_k$ et $x_i = 0$ sinon. On prend α_k et β_k tels que $\alpha_0 = \alpha$, $\beta_0 = \beta$, $\alpha_k = \alpha(d-1)^{-(k-1)/2}$ et $\beta_k = \beta(d-1)^{-(k-1)/2}$ en choisissant α et β pour que $x^T \mathbf{1} = 0$. Notons en particulier que $\alpha_0 = \alpha_1$ et $\beta_0 = \beta_1$.

Nous avons $x^T x = S(U) + S(W)$ avec $S(U) = \sum_{k=0}^{a} \alpha_k^2 |U_k|$ et $S(W) \sum_{k=0}^{a} \beta_k^2 |W_k|$.

Etablissons maintenant une borne supérieure de $x^T L x = \sum_{v_i v_j \in E,\ i<j} (x_i - x_j)^2$. Cette somme peut se voir comme la somme de deux sous-sommes:

$$\Sigma(U) = \sum_{\substack{v_i v_j \in E\ i<j \\ v_i \in U \text{ou } v_j \in U}} (x_i - x_j)^2 \quad \text{et} \quad \Sigma(W) = \sum_{\substack{v_i v_j \in E,\ i<j \\ v_i \in W \text{ou } v_j \in W}} (x_i - x_j)^2.$$

Celles-ci correspondent respectivement à la contribution des arêtes incidentes aux sommets de U et à celle des arêtes incidentes aux sommets de W (les autres arêtes ont une contribution nulle).

Nous allons maintenant borner $\Sigma(U)$. Par définition des U_i, une arête incidente à un sommet de U est

- soit interne à un niveau U_k et sa contribution est nulle,

- soit entre U_k et U_{k+1} $(0 \leq k < a)$ et sa contribution est $(\alpha_k - \alpha_{k+1})^2$,

- soit entre U_a et un sommet hors de U et sa contribution est α_a^2.

Comme pour $k \geq 1$, il y a au plus $|U_k|(d-1)$ arcs entre U_k et U_{k+1}, et $\alpha_1 = \alpha_0$ (donc les arêtes entre u et ses voisins sont de contribution nulle), on a :

$$\Sigma(U) \leq \sum_{k=1}^{a-1} |U_k|(d-1)\left((d-1)^{-(k-1)/2} - (d-1)^{-k/2}\right)\alpha^2 + |U_a|(d-1)(d-1)^{-(a-1)}\alpha^2.$$

Un calcul facile nous montre que le membre droit de cette inégalité vaut:

$$(\sqrt{d-1}-1)^2 \sum_{k=1}^{a} |U_k|(d-1)^{-k+1}\alpha^2 + (2\sqrt{d-1}-1)|U_a|(d-1)^{-b+1}\alpha^2.$$

Comme $|U_a| \leq (d-1)^{(a-k)}|U_k|$, il vient

$$\begin{aligned} \Sigma(U) &\leq (\sqrt{d-1}-1)^2 \left(\sum_{k=1}^{a} \alpha_k^2 |U_k|\right) + \frac{2\sqrt{d-1}-1}{a}\left(\sum_{k=1}^{a} \alpha_k^2 |U_k|\right) \\ &\leq \left(d - 2\sqrt{d-1} + \frac{2\sqrt{d-1}-1}{a}\right) S(U) \end{aligned} \tag{4}$$

De la même manière, posant $S(W) = \sum_{k=0}^{a} \beta_k^2 |W_k|$ on prouve

$$\Sigma(W) \leq \left(d - 2\sqrt{d-1} + \frac{2\sqrt{d-1}-1}{a}\right) S(W) \tag{5}$$

D'où $d - \lambda_2 \leq \dfrac{\Sigma(U) + \Sigma(W)}{S(U) + S(W)} \leq d - 2\sqrt{d-1} + \dfrac{2\sqrt{d-1}-1}{a}$.

□

2.4 Quelques expandeurs

Si on veut des graphes d-réguliers qui soient de bons expandeurs, d'après le Théorème 6, il faut que leur deuxième valeur propre λ_2 soit petite. D'autre part, le théorème d'Alon-Boppana, nous dit que nous ne pouvons pas espérer avoir celle-ci plus petite que $\sqrt{2d-1}$. Ainsi, de bons candidats pour être de bons expandeurs sont les graphes d-réguliers pour lesquels $\lambda_2 \leq 2\sqrt{d-1}$. De tels graphes sont appelés *graphes de Ramanujan*. D'après le Théorème 6, les graphes de Ramanujan sont des c-expandeurs avec $c = \dfrac{d - 2\sqrt{d-1}}{2}$.

Lubotsky, Phillips et Sarnak[14] et Margulis [15] ont montré de manière indépendante qu'il existe des graphes Ramanujan d-réguliers aussi grands que l'on veut lorsque $d-1$ est premier. Ils ont de plus donné une construction explicite de tels expandeurs qui sont des graphes de Cayley particuliers. Cette construction est explicitée dans la Partie 5.

Théorème 12 (Morgenstern [17]) *Pour tout entier premier p et tout entier positif k, il existe une infinité de graphes Ramanujan (p^k+1)-réguliers.*

Conjecture 13 *Pour tout $d \geq 3$, il existe une infinité de graphes Ramanujan d-réguliers.*

Assez paradoxalement, alors qu'il est assez difficle de trouver des familles explicites d'expandeurs, Friedman[7] a montré que les graphes d-réguliers aléatoires sont de bons expandeurs car ils sont presque Ramanujan:

Théorème 14 (Friedman) *Soit G un graphe d-régulier d'ordre n. Pour tout $\epsilon > 0$,*

$$Prob\left(\lambda_2(G) \leq 2\sqrt{d-1} + \epsilon\right) = 1 - o(1).$$

Les meilleurs expandeurs d-réguliers pour une valeur quelconque de d ont été donnés par Bilu et Linial [4].

Théorème 15 (Bilu et Linial [4]) *Pour tout $d \geq 3$, il existe une famille infinie de graphes d-réguliers tels que avec $\lambda_2 \leq O(\sqrt{d \log^3 d})$.*

Leur construction est basée sur la notion de *relevé*. Soit G et H deux graphes. Une application $f : V(H) \to V(G)$ est *couvrante* si pour tout sommet $v \in V(H)$, f est une bijection entre $N_H(v)$ et $N_G(f(v))$. S'il existe une application couvrante de H sur G, on dit que H est un *relevé* de G et que G est un *quotient* de H. Si f est une application couvrante d'un graphe H (fini) sur un graphe connexe G, alors il est facile de voir que $f^-1(v)$ est une constante k ne dépendant pas de v. On dit alors que H est un *k-relevé* de G.

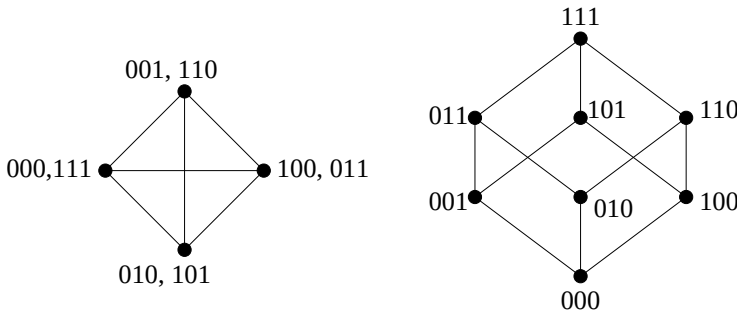

Figure 2: Le 3-cube est un 2-relevé de K_4. L'application couvrante identifie les sommets antipodaux du cube.

Il est facile de voir que si H est un relevé de G alors les valeurs propres de G sont des valeurs propres de H. En effet, si x est un vecteur propre de G alors $f(x)$ est un vecteur propre de H (avec f l'application couvrante de H sur G). L'idée de Bilu et Linial est de partir d'un graphe Ramanujan d-régulier (K_d par exemple) est de prendre une succession de relevés tels que les nouvelles valeurs propres soient petites. Dans le cas idéal, celles-ci vaudraient au plus $\sqrt{2d-1}$ et tous les graphes seraient Ramanujan.

Conjecture 16 (Bilu et Linial) *Tout graphe Ramanujan d-régulier G a un 2-relevé H tel que les valeurs propres de H et pas de G sont inférieures ou égales à $\sqrt{2d-1}$.*

Pour montrer le Théorème 15, Bilu et Linial ont montré un résultat plus faible que cette conjecture, à savoir qu'il existe un 2-relevé dont les nouvelles valeurs propres valent au plus $O\left(\sqrt{d \log^3 d}\right)$.

3 Marches aléatoires et expandeurs

3.1 Convergences des marches aléatoires

Soit D un digraphe sur les sommets $v_1, v_2, \ldots, v_n$. Une *marche aléatoire* sur D consiste à se balader sur les sommets de D en suivant ses arcs selon une probabilité de transition. Plus précisément, pour chaque sommet v_i de D, une fois qu'on est sur v_i, on suppose qu'avec une probabilité $p_{i,j}$ *strictement positive*, on se déplace vers le sommet v_j. Ainsi si $v_iv_j \notin E(D)$, la probabilité de transition $p_{i,j}$ est nulle.

Soit P la matrice de la marche aléatoire, dont les coordonnées sont $p_{i,j}$. Pour tout i, le vecteur $(p_{i,1}, \ldots, p_{i,n})$ est une loi de probabilité, i. e. $\sum_{j=1}^{n} p_{i,j} = 1$. On a donc

$$P\mathbf{1} = \mathbf{1}.$$

Ceci prouve que 1 est une valeur propre de P.

Le sommet de départ de la marche peut être fixé mais peut aussi être donné selon une loi de probabilité initiale. Dans tous les cas, on suppose que le vecteur π^0 désigne la loi de départ. Par π^k, on désigne la distribution des probabilités de présence sur les sommets de D à l'instant i, i.e.

$$\pi_i^k = Prob(\text{après } k \text{ étapes, on est en } v_i).$$

π^k peut se calculer facilement à partir de π^{k-1}. En effet, la probabilité de présence sur v_i à l'instant k est la somme sur j de la probabilité de présence sur v_j à l'instant $k-1$ multipliée par la probabilité de transition de v_j vers v_i. Formellement, $\pi_i^k = \sum_{j=1}^{n} \pi_j^{k-1} p_{j,i}$. Donc

$$\pi^k = \pi^{k-1} P.$$

On s'intéresse aux distributions *stationnaires* de notre marche aléatoire, c'est à dire les distributions qui restent inchangées d'une étape à l'autre. Ce sont les distributions π telles que $\pi = \pi P$. De telles distributions existent. En effet, nous avons vu que 1 est valeur propre de P et donc également de P^T. Ainsi un vecteur propre π associé à 1 et de norme 1 est une distribution stationnaire.

Nous allons montrer que pour un digraphe D fortement connexe, la distribution stationnaire est unique. De plus, nous verrons que sous certaines conditions d'*apériodicité*, toutes les marches aléatoires convergent vers cette distribution stationnaire à l'infini. De plus, nous bornerons la vitesse de convergence en fonction de la seconde valeur propre de D en valeur absolue. Cette estimation montre que les expandeurs sont les (di)graphes dont la vitesse de convergence est la plus grande.

Théorème 17 *Soit D un digraphe fortement connexe et P une matrice de transition sur D. Il existe une unique distribution stationnaire π^*.*

Preuve. La matrice P est une matrice positive ($p_{i,j} \geq 0$). De plus, comme D est fortement connexe, P est irréductible (P ne peut pas s'écrire sous la forme $\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$, avec A et B des matrices carrées, en changeant la position des lignes et des colonnes).

On est donc en mesure d'appliquer le théorème de Perron-Frobenius qui nous dit que P a une valeur propre réelle positive μ_1 telle que

- μ_1 est de multiplicité 1;
- le vecteur propre correspondant à μ_1 est positif;
- toutes les autres valeurs propres μ de P sont de valeur absolue strictement inférieure à μ_1, i.e. $|\mu| \leq \mu_1$.

On a vu que pour la matrice P, la valeur propre μ_1 correspondante est 1. Comme P^T et P ont les mêmes valeurs propres, 1 est également l'unique valeur propre maximum de P^T. Il existe alors un unique vecteur propre positif π^* (de norme $\ell_1 = 1$) correspondant à la valeur propre 1 de P^t, i.e. tel que $\pi^* P = \pi^*$. Le vecteur π^* est l'unique distribution stationnaire de P. □

Remarque 18 Pour un digraphe non fortement connexe, il peut y a avoir plusieurs distributions stationnaires. En effet, si un digraphe D possède plusieurs composantes fortement connexes *terminales* (i.e. desquelles aucun arc ne sorte), les distributions stationnaires de chacune de ces composantes sont des distributions stationnaires de tout le digraphe. Plus généralement, les distributions stationnaires de D sont les combinaisons convexes des distributions stationnaires de ses composantes fortement connexes *terminales*.

Une marche aléatoire est dite

- *ergodique* si elle admet une unique distribution stationnaire π^*, et que pour toute distribution de départ π^0, on a $\lim_{i\to\infty} \pi^k = \pi^*$.
- *apériodique* si $\mathrm{PGCD}(\{s : P^s_{i,i} > 0\}) = 1$.

Théorème 19 *Une marche aléatoire sur un digraphe D est ergodique si et seulement si elle est apériodique et D est fortement connexe.*

Afin de ne pas alourdir cette présentation, nous nous contenterons de montrer le théorème suivant qui correspond au Théorème 19 dans le cas symétrique qui correspond au cas des graphes non orientés qui nous intéressent plus particulièrement.

Théorème 20 *Soit D un digraphe symétrique (fortement) connexe, P une matrice de transition symétrique sur D et π^* la distribution stationnaire de P.*

Si $p_{i,i} > 0$ pour tout $1 \le i \le n$, (i.e. D a une boucle sur tous les sommets) alors quelle que soit la distribution de départ π^0, on a $\lim_{i\to\infty} \pi^k = \pi^*$.

Preuve. Soit $1 \ge \mu_2 \ge \mu_3 \ge \cdots \ge \mu_n$ les valeurs propres de P. Posons $\mu = \max_{2\le j\le n} |\mu_j|$. Par le théorème de Perron-Frobenius, $\mu < 1$.

Nous allons montrer

$$|\pi^k - \pi^*| \le C.\mu^k$$

pour une constante C. Comme $\mu < 1$ ceci démontrera la convergence cherchée.

On sait que $\pi^k = \pi^0 P^k$ et $\pi^* = \pi^* P^k$, donc $\pi^k - \pi^* = (\pi^0 - \pi^*)P^k$. Comme P est symétrique, on a

$$\pi^k - \pi^* = P^k(\pi^0 - \pi^*)^T.$$

D'autre part, $\pi^0 - \pi^*$ est orthogonal à $\mathbf{1}$. En effet,

$$(\pi^0 - \pi^*)\mathbf{1}^T = \sum_{j=1}^{n}(\pi^0_j - \pi^*_j) = \sum_{j=1}^{n}\pi^0_j - \sum_{j=1}^{n}\pi^*_j = 1 - 1 = 0.$$

Donc $\pi^0 - \pi^*$ est dans l'espace vectoriel engendré par des vecteurs propres $z_2, z_3, \ldots, z_n$ associés aux valeurs propres $\mu_2, \mu_3, \ldots, \mu_n$ Ainsi $\pi^0 - \pi^*$ s'écrit comme combinaison linéaire de ces vecteurs: $\pi^0 - \pi^* = \sum_{j\ge 2} \alpha_j z_j$. On a donc

$$\pi^k - \pi^* = P^k(\pi^0 - \pi^*)^T = \sum_{j=2}^{n} \alpha_j \mu_j^k z_j.$$

Comme $|\mu_j| \leq \mu$ pour tout $2 \leq j \leq n$, il vient

$$|\pi^k - \pi^*| \leq \mu^k \ (\alpha_2|z_2| + \cdots + \alpha_n|z_n|) = C.\mu^k.$$

□

3.2 Algorithmes BPP et marches alétoires sur les expandeurs

3.2.1 Algorithmes BPP

Un *algorithme probabiliste* est un algorithme déterministe qui prend en entrée, l'entrée proprement dite x que l'on étudie, et une chaine A de bits aléatoires de longeur m , i.e. un élément uniformément choisi dans $\{0,1\}^m$.

La classe **RP** pour *Randomized Polynomial* est la classe des langages $\mathcal{L}$ pour lesquels il existe un algorithme probabiliste tel que :

- lorsque $x \in \mathcal{L}$, alors l'algorithme rejette α avec probabilité $\alpha < 1$ et donc l'accepte comme élément de L avec probabilité $1 - \alpha > 0$;
- lorsque $x \notin \mathcal{L}$, l'algorithme rejette la chaine avec une probabilité 1.

L'algorithme reconnait $\mathcal{L}$ avec probabilité d'erreur α. Cependant une erreur ne peut arriver que lorsque l'entrée est acceptée. Si on veut diminuer la probabilité d'erreur, il suffit de faire tourner l'algorithme plusieurs fois consécutives avec des chaines de bits aléatoires indépendantes. En effet, en faisant n fois le test (et donc en utilisant $m \times n$ bits aléatoires), un mot $x \in \mathcal{L}$ est rejeté avec probabilité α^n.

Il existe une classe plus générale de langages pour lesquels une erreur est possible lorsque l'entrée est rejetée et lorsque elle est acceptée : la classe **BPP** pour *Bounded-error Probabilistic Polynomial* est la classe des langages $\mathcal{L}$ pour lesquels il existe un algorithme probabiliste tel que:

- lorsque $x \in \mathcal{L}$, alors l'algorithme rejette x avec une probabilité au plus $\alpha < \frac{1}{2}$;
- lorsque $x \notin \mathcal{L}$, l'algorithme accepte x avec probabilité au plus $\alpha < \frac{1}{2}$.

De même que pour les langages **RP**, on peut diminuer la probabilité d'erreur en effectuant n fois l'algorithme avec des chaines de bits aléatoires indépendantes. Pour cela, il suffit de considérer le vote à la majorité. En effet, soient $A_1, A_2, \ldots, A_n$ des chaines aléatoires indépendantes de longeur m et pour chaque A_i, soit R_i la variable aléatoire des réponses de l'algorithme, i.e. $R_i = 1$ si l'agorithme accepte x comme un élément de $\mathcal{L}$, et $R_i = 0$ si la chaine x est rejetée. Comme les chaines A_i sont indépendantes, les variables R_i sont indépendantes. Soit R la variable aléatoire obtenue à partir des R_i en faisant un vote de majorité.

Estimons la probabilité que R soit une mauvaise réponse. On a

$$Prob(\ R = 1 \mid x \notin \mathcal{L}\ ) = Prob\Big(\ \sum R_i \geq \frac{n}{2} \mid x \notin \mathcal{L}\Big) = Prob\Big(\ \sum (R_i | x \notin \mathcal{L}) \leq \frac{n}{2}\Big).$$

Or $Prob(\ R_i = 1 \mid x \notin \mathcal{L}\ ) = \alpha$, donc $E(R_i|x \notin \mathcal{L}) = \alpha < \frac{1}{2}$. D'après la borne de Chernoff,

$$Prob\Big(\ \sum (R_i|x \notin \mathcal{L}) \leq \frac{n}{2}\Big) = Prob\Big(\ \sum (R_i|x \notin \mathcal{L}) - \alpha.n \leq\ (\frac{1}{2} - \alpha).n\Big) < e^{-(\frac{1}{4\alpha}n)/2} = 2^{-\Omega(n)}.$$

Ainsi $Prob(\ R = 1 \mid x \notin \mathcal{L}\ ) = 2^{-\Omega(n)}$. Un raisonnement identique nous donne $Prob(\ R = 0 \mid x \in \mathcal{L}\ ) = 2^{-\Omega(n)}$.

Exemple de langage RP: test de non-primalité. Soit $\mathcal{L}$ l'ensemble des entiers composés (i.e. non-premiers). Le Petit Théorème de Fermat nous dit que si p est premier alors pour tout $1 \leq a < p$ alors $a^{p-1} - 1$ est divisible par p.

Si p est notre entrée et que l'on trouve un entier a tel que p ne divise pas $a^{p-1}-1$ alors a est un *témoin* du fait que p n'est pas premier. Habituellement (attention c'est une simplification), si p est composé alors au moins la moitié des entiers $1 \leq a < p$ sont des témoins.

Ainsi si l'on prend un a au hasard dans $\{1, \ldots, p-1\}$ et que l'on accepte p si $a^{p-1} - 1$ n'est pas divisible par p, si p est composé, on l'accepte avec probabilité au moins $\frac{1}{2}$ et si p est premier on le rejette tout le temps.

3.2.2 Marche aléatoires sur les expandeurs et les algorithmes BPP

Nous avons vu qu'en utilisant $m \times n$ bits alétoires, on peut réduire la probabilité d'erreur à $2^{-\Omega(n)}$. On peut cependant se demander si une telle quantité de bits aléatoires est bien nécessaire pour faire cela. La réponse est non:

Théorème 21 *On peut réduire la probabilité d'erreur à 2^{-n}, en utilisant au plus $O(m+n)$ bits aléatoires et en faisant tourner l'algorithme au plus $O(n)$ fois.*

Preuve. Afin de prouver le Théorème 21, nous allons effectuer une marche aléatoire sur un expandeur G d-régulier (auquel on rajoute les boucles) d'ensemble de sommets $\{0,1\}^{c_1 m}$ afin de générer une suite pseudo-aléatoire de chaines de $c_1 m$ bits. La matrice de transition que nous allons utiliser est la suivante:

$$p_{ij} = \begin{cases} \frac{1}{2} & \text{si } i = j \\ \frac{1}{2d} & \text{si } i \neq j \text{ et } v_i v_j \in E(G) \end{cases}$$

On commence par la distribution aléatoire uniforme Π^u sur les sommets de G, ce qui nécessite $c_1 m$ bits. Nous allons ensuite trouver $l = n/k$ chaines de $c_1 m$ bits pour chacune desquelles nous faisons tourner l'algorithme. On prend ensuite le vote à la majorité pour décider ou non d'accepter l'entrée. Pour passer d'une chaine à une autre, on effectue k pas dans la marche aléatoire. Pour chaque pas de la marche aléatoire, nous avons besoin d'au plus $c_2 = \lceil \log d + 1 \rceil$ bits. Ainsi, comme nous effectuons n pas nous aurons besoin de $c_2 n$ bits. Au total, nous aurons donc besoin de $c_1 m + c_2 n$ bits.

Il nous reste donc à montrer que pour c_1 et k des constantes bien choisies, la probabilité d'erreur est $2^{-\Omega(n)}$.

Choisissons d'abord les constantes c_1 et k.

La probabilité d'erreur de l'algorithme est petite ($< 1/2$). Cependant, avant de démarrer notre marche aléatoire, nous avons besoin qu'elle soit très petite i.e. $< 1/100$. Pour cela nous faisons tourner notre algorithme un nombre c_1 constant de fois. Ainsi l'ensemble F des mots de $c_1 m$ bits qui empêchent l'algorithme **BPP** de donner une bonne réponse pour l'entrée x est de taille au plus $2^{c_1 m}/100$.

Soit $\lambda_1 \geq \cdots \geq \lambda_n$ les valeurs propres de la matrice d'adjacence de G. Alors les valeurs propres de P sont les $\mu_i = \frac{1}{2} + \frac{\lambda_i}{2d}$). Ainsi $\mu_1 = 1 > \mu_2 \geq \ldots \mu_n \geq 0$. Le fait que G soit un expandeur nous garantit que μ_2 est petit, et ceci indépendamment de la valeur de m. Soit k le plus petit entier tel que $\mu_2^k \leq \frac{1}{10}$. Soit la suite $v_0, v_1, \ldots, v_l$, la suite de sommets visités durant les n premiers pas de la marche aléatoires, v_0 ayant été choisi de manière uniforme sur $V(G)$.

Nous allons montrer que la probabilité que la marche aléatoire ait plus de la moitié de ses sommets dans F est au plus $2^{-\Omega(n)}$, ce qui prouvera le théorème.

Pour une distribution donnée π, la probabilité de présence dans F pour une distribution donnée π est tout simplement $\pi \mathbf{1}_{\mathbf{F}}$. On peut aussi voir cela comme la norme ℓ_1 de $\pi.T$ où T est la matrice carré, l'identité sur F, et nulle sur F^c. En d'autres termes, toutes les coordonnées de T sont nulles à part les

coordonnées $T_{i,i}$ pour $v_i \in F$. On introduit les variables aléatoires de passage en F à l'étape i; X_i. Plus formelement:

$$X_i = \begin{cases} 1 & \text{si à l'étape } i, \text{ on est dans } F \\ 0 & \text{sinon} \end{cases}$$

Soit $a_0, \ldots, a_l$ une suite données dans $\{0,1\}$. Pour la suite des variables aléatoires X_i, on s'intéresse maintenant à calculer $Prob(X_0 = a_0, \ldots, X_l = a_l)$. Pour cela considérons la suite de matrices carrées T_i définie à partir de a_i de la façon suivante: $T_i = T$ si $a_i = 1$, et sinon $T_i = 1 - T$. Une simple récurrence, nous donne

$$Prob(X_0 = a_0, \ldots, X_l = a_l) = |\pi^u T_0 P^k T_1 P^k \ldots P^k T_l| = \sum (\pi^u T_0 P^k T_1 P^k \ldots P^k T_l)_i$$

Estimons maintenant la probabilité p de passage par F un nombre de fois plus grand que la moitié. On a

$$\begin{aligned} p = Prob(\sum_{i=0}^{i=l} X_i > \frac{l}{2}) &= \sum_{\{(a_0,a_1,\ldots,a_l)\in\{0,1\}^l \mid \sum a_i > \frac{l}{2}\}} Prob(X_0 = 0, \ldots, X_l = a_l) \\ &\leq 2^l \max_{\{(a_0,a_1,\ldots,a_l)\in\{0,1\}^l \mid \sum a_i > \frac{l}{2}\}} Prob(X_0 = 0, \ldots, X_l = a_l) \end{aligned}$$

Nous allons maintenant majorer le membre droit de cette inégalité.

Lemme 22 *Soit x un vecteur non négatif.*

- $||xP^k(1-T)|| \leq ||x||$
- $||xP^kT||_2 \leq \frac{1}{5}||x||$

Preuve. La première inégalité est triviale, étant donné que $||xP|| \leq ||x||$.

Pour démontrer la deuxième, après la normalisation, on peut supposer que x est une distribution de probabilité sur G.

Maintenant

$$||xP^kT|| \leq ||\pi^u T|| + ||(xP^k - \pi^u)T||.$$

Or $\pi^u T = \frac{1}{2^{c_1 m}}\mathbf{1}_F$. Puisque $|F| \leq 2^{c_1 m}/100$, il vient $||\pi^u T|| \leq \frac{1}{10\sqrt{2^{c_1 m}}}$. De plus, par Cauchy-Schwarz, $1 = \sum x_i \leq ||x|| \times ||\mathbf{1}|| = ||x||\sqrt{2^{c_1 m}}$. Ainsi

$$||\pi^u T|| \leq \frac{||x||}{10}.$$

La distribution uniforme π^u est stationnaire pour P. Donc $x - \pi^u$ est une combinaison linéaire des vecteurs propres $z_2, \ldots, z_{c_1 m}$ correspondant aux valeurs propres de P $\mu_2, \ldots, \mu_{c_1 m}$. Ainsi il existe des α_i tels que $x - \pi^u = \sum \alpha_i z_i$. On a alors

$$||(xP^k - \pi^u)T|| \leq ||(xP^k - \pi^u)|| = ||(x - \pi^u)P^k|| = ||\sum \mu_i^k \alpha_i z_i|| \leq \mu_2^k ||\sum \alpha_i z_i|| = \mu_2^k ||x|| \leq \frac{||x||}{10}.$$

Les trois inégalités nous donnent

$$||xP^kT|| \leq \frac{||x||}{10} + \frac{||x||}{10} \leq \frac{||x||}{5}.$$

□

En itérant l fois le lemme, on obtient

$$Prob(X_0 = a_0, \ldots, X_l = a_l) \leq (\frac{1}{5})^N ||\pi^u T_0||$$

où N désigne le nombre de $a_i = 1$. Donc

$$Prob\left(\sum_{i=0}^{i=l} X_i > \frac{l}{2}\right) \leq 2^l (\frac{1}{5})^{\frac{l}{2}} ||\pi^u T_0|| = 2^{-\Omega(n)}.$$

□

4 Sommet-expansion

Le *voisinage* d'un sommet u est l'ensemble $N(u) = \{v \mid uv \in E\}$ des sommets reliés à u par une arêtes. Le *voisinage* d'un ensemble de sommets S est l'ensemble $N(S) = \bigcup_{u \in S} N(u) \setminus S$ des sommets du complémentaire de S qui sont voisins d'au moins un sommet de S. Le *voisinage complet* de S est l'union des voisinages des sommets de S: $\Gamma(S) = \bigcup_{u \in S} N(u)$. Ainsi $N(S) = \Gamma(S) \setminus S$.

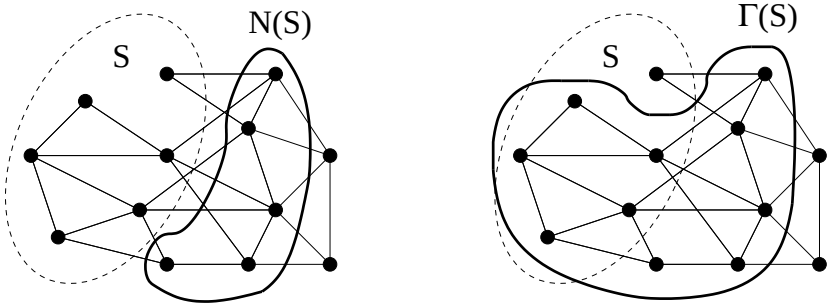

Figure 3: Le voisinage $N(S)$ et le voisinage complet $\Gamma(S)$ d'un ensemble S.

De même, que pour l'arête-expansion, on peut définir la *sommet-expansion* d'un ensemble S comme $vexp(S) = \frac{|\Gamma(S)|}{|S|}$ et la *sommet-expansion* de G comme $vexp(G) \max_{\{S \mid |S| \leq n/2\}} vexp(S)$.

Remarque 23 On regarde parfois une autre sorte de sommet-expansion $wexp(G) = \max_{\{S \mid |S| \leq n/2\}} \frac{|N(S)|}{|S|}$. Les deux définitions de sommet-expansion sont très proches: en effet, comme $N(S) = \Gamma(S) \setminus S$, on a $vexp - 1 \leq wexp \leq vexp$. La seule sommet-expansion que nous considérerons ici sera donc $vexp$.

Clairement la sommet-expansion d'un graphe est au plus 2 si n est pair et $2 + \frac{2}{n-1}$ si n est impair.. En effet, pour tout ensemble S de taille $\lfloor n/2 \rfloor$, $vexp(S) = \frac{|\Gamma(S)|}{|S|} \leq \frac{n}{\lfloor n/2 \rfloor}$.

4.1 Sommet-expansion de quelques graphes particuliers

Graphes complets La sommet-expansion du graphe complet K_n à n sommets est 2 si n est pair et $2 + \frac{2}{n-1}$ si n est impair. En effet, pour tout ensemble $S \subset V(K_n)$, on a $\Gamma(S) = V(K_n)$.

Graphes réguliers La sommet-expansion d'un graphe d-régulier est au moins 1. En effet, soit S un ensemble de sommets. Chaque sommet de S à d voisins, il y a donc $d|S|$ voisins comptés avec multiplicité. Mais chaque sommet de $\Gamma(S)$ est compté au plus d fois. Donc $|\Gamma(S)| \geq |S|$. Cette borne de 1 est atteinte pour les graphes bipartis réguliers. En effet, si on prend une des deux parties de la bipartition, elle est de taille $n/2$ et son voisinage complet est l'autre partie elle aussi de taille $n/2$.

Grille torique Supposons que G soit la grille torique à deux dimension $p \times p$. Elle a $n = p^2$ sommets. Un ensemble S à k sommets de plus faible voisinage complet, ressemble le plus possible à un sous-carré de la grille. De plus, son bord est de taille $b(S) \approx k + 4\sqrt{k}$. Ainsi l'expansion de la grille est $\approx 1 + \frac{4\sqrt{2}}{\sqrt{n}}$.

4.2 Sommet-expansion et valeurs propres

Les notions d'arête et sommet-expansion sont très fortement reliées. En effet, pour tout ensemble S, $b(S) \geq |N(S)| \geq |\Gamma(S)| - |S|$ et $|\Gamma(S)| \geq |N(S)| \geq b(S)/\Delta(G)$.

Ainsi $\frac{exp}{\Delta} \leq vexp \leq exp + 1$. Nous allons voir que ces deux facteurs sont cependant beaucoup plus proches. Pour cela, nous allons relier la sommet-expansion aux valeurs propres de la matrice d'adjacence dans le cas des graphes d-réguliers.

On dénote par λ la seconde plus grande valeur propre en valeur absolue:

$$\lambda = \max_{2 \leq i \leq n} |\lambda_i|$$

Par le théorème de Rayleigh-Ritz:

$$\lambda = \max_{||x||=1, x^T \mathbf{1}=0} ||Ax||$$

Alors que l'expansion peut être estimée avec la seconde valeur propre λ_2, nous allons relier la sommet adjacence avec λ.

Pour des raisons de simplicité, plutot que de travailler, avec le matrice d'adjacence, nous allons travailler avec la matrice d'adjacence normalisée. Pour un graphe d-régulier, sa *matrice d'adjacence normalisée* est $\bar{A} = \frac{1}{d}A$. Les valeurs propres de $\bar{A}$ sont les $\bar{\lambda}_i = \frac{1}{d}\lambda_i$. De plus, on définit $\bar{\lambda} = \max_{2 \leq i \leq n} |\bar{\lambda}_i| = \frac{1}{d}\lambda$.

Théorème 24 *Soit G un graphe d-régulier.*

$$vexp(G) \geq \frac{2}{1 + \bar{\lambda}^2} = \frac{2}{1 + \frac{\lambda^2}{d^2}}$$

Afin de prouver ce théorème, nous allons d'abord établir un lemme sur les *distributions* (de probabilités), c'est à dire les vecteurs[1] π à coordonnées positives de somme 1 ($\pi_i \geq 0$ et $\sum_{i=1}^{n} \pi_i = 1$). Le *support* d'une distribution π est $support(\pi) = \{i \mid \pi_i > 0\}$.

On désigne par $\pi^u = \frac{1}{n}\mathbf{1}$, la probabilité uniforme sur V.

Lemme 25 *Soit π une distribution.*

$$||\pi||^2 = ||\pi - \pi^u||^2 + 1/n \geq \frac{1}{|support(\pi)|}$$

[1] Dans la Partie 3, les distributions que nous considérions étaient des vecteurs lignes. Ici ce sont des vecteurs colonnes.

Preuve. On voit facilement que $\pi - \pi^u$ est orthogonal à π^u. Donc $||\pi||^2 = ||\pi - \pi^u||^2 + ||\pi^u||^2 = ||\pi - \pi^u||^2 + 1/n$.

Posons $m = |support(\pi)|$. Si $x_1 + x_2 + \cdots + x_m = 1$ alors $x_1^2 + x_2^2 + \cdots + x_m^2$ est minimisée lorsque $x_1 = \cdots = x_m = 1/m$. Ainsi $||\pi||^2 \geq 1/m$. □

Preuve du Lemme 24. Soit S tel que $|S| \leq n/2$. Soit $\pi^S = \frac{1}{S}\mathbf{1}_S$ la distribution uniforme sur S et nulle ailleurs.

On a $||\pi_S|| = 1/|S|$.

D'autre part, $\bar{A}\pi^S$ est une distribution donc, par le Lemme 25, $||\bar{A}\pi^S - \pi^u||^2 + 1/n = ||\bar{A}\pi^S|| \geq 1/|support(\pi^S)| \geq 1/|\Gamma(S)|$. Or

$$\bar{A}\pi^S - \pi^u = \bar{A}(\pi^S - \pi^u + \pi^u) - u = \bar{A}\pi^u - \pi^u + \bar{A}(\pi^S - \pi^u) = \bar{A}(\pi^S - \pi^u).$$

Donc
$$||\bar{A}\pi^S - \pi^u||^2 = ||\bar{A}(\pi^S - \pi^u)||^2 \leq \bar{\lambda}^2||\pi^S - \pi^u||^2 = \bar{\lambda}^2(||\pi^S||^2 - 1/n).$$

D'où
$$1/|\Gamma(S)| - 1/n \leq \bar{\lambda}^2(1/|S| - 1/n).$$

Comme $n \geq 2|S|$, on a $|\Gamma(S)| \geq \frac{2|S|}{1+\lambda^2}$.

□

Théorème 26 (Alon [1]) *Soit G un graphe d-régulier de sommet-expansion $1+\alpha$. Si les valeurs propres de $A(G)$ la matrice d'adjacence de G sont toutes positives alors $\lambda(G) \leq d - \frac{\alpha^2}{8+4\alpha^2}$.*

Preuve.

Soit x un vecteur associé à λ ou $-\lambda$. Comme x est orthogonal à $\mathbf{1}$, il a des coordonnées négatives et positives. Soit $I^+ = \{i \mid x_i > 0\}$ et $I^- = \{i \mid x_i \leq 0\}$. Sans perte de généralité, on peut supposer que $|I^+| \leq n/2$. Soit y le vecteur définit par $y_i = x_i$ si $i \in I^+$ et $y_i = 0$ sinon.

On a $||y||^2 = y^T y = y^T x$. Donc

$$\lambda = \frac{\lambda y^T x}{y^T x} = \frac{y^T A x}{||y||^2}.$$

Ainsi

$$\begin{aligned}
\lambda||y||^2 &= y^T A x \\
&= \sum_{i,j} a_{i,j}x_j y_i = \sum_{i\in I^+, v_iv_j\in E} x_j y_i = d||x||^2 - \left(d||x||^2 - \sum_{i\in I^+, v_iv_j\in E} x_j y_i\right) \\
&\leq d||x||^2 - \left(d||x||^2 - \sum_{i,j\in I^+, v_iv_j\in E} x_j y_i\right) = d||x||^2 - \left(d||x||^2 - \sum_{v_iv_j\in E} y_j y_i\right) \\
&= d||x||^2 - \frac{1}{2}\sum_{v_iv_j\in E}(y_i - y_j)^2
\end{aligned}$$

Donc
$$\lambda \leq d - \frac{\sum_{v_iv_j\in E}(y_i - y_j)^2}{2||y||^2} \tag{6}$$

Construisons un digraphe D comme suit: $V(D) = \{s,t\} \cup \{v_i \mid i \in I^+\} \cup \{w_j \mid 1 \leq i \leq n\}$. Pour tout $i \in I^+$, on met l'arc sv_i avec capacité $1+\alpha$. Pour tout $1 \leq j \leq n$, on met l'arc $w_j t$ avec capacité 1. Enfin pour tout $i \in I^+$ et $1 \leq j \leq n$ tels que $v_iv_j \in E(G)$ alors on met l'arc v_iw_j avec capacité 1.

Nous affirmons que la (s,t)-coupe minimum de de ce graphe vaut $(1+\alpha)|I^+|$. Une coupe de cette valeur est donné par le bord de $\{s\}$. Considérons maintenant une autre (s,t)-coupe C. Soit $S = \{v_i \in V(G) \mid sv_i \notin C\}$. Pour tout $v_j \in N_G(S)$, dans D, il doit y avoir un arc de C incident à w_j. Comme $|S| \leq |I^+| \leq n/2$, on a $|N_D(S)| = |\Gamma_G(S)| \geq (1+\alpha)|S|$. Ainsi en ajoutant les arcs $sv_i \in C$ on obtient que C a capacité au moins $(1+\alpha)|I^+|$.

Par le théorème "coupe-min=flot-max"de Ford et Fulkerson, il existe un flot sur D de valeur $(1+\alpha)|I^+|$. Notons que le flot qui passe à travers chaque v_i doit donc être de $1+\alpha$. En lisant ce flot sur les arcs v_iw_j, on obtient une fonction $f : \{1,\ldots,n\}^2 \to \mathbb{R}$ telle que:

- $0 \leq f(i,j) \leq 1$ pour tout (i,j) dans $\{1,\ldots,n\}^2$;
- $f(i,j) = 0$ si $i \notin I^+$ ou $v_iv_j \notin E$;
- $\sum_{j \mid v_iv_j \in E} f(i,j) = 1+\alpha$ pour tout $i \in I^+$;
- $\sum_{i \mid v_iv_j \in E} f(i,j) \leq 1$ pour tout $1 \leq i \leq n$.

Nous allons maintenant donner des bornes sur f.

$$\begin{aligned}\sum_{v_iv_j \in E} f^2(i,j)(y_i+y_j)^2 &\leq 2\sum_{v_iv_j \in E} f^2(i,j)(y_i^2+y_j^2) \\ &= 2\sum_{i=1}^{n} y_i^2 \left(\sum_{v_iv_j \in E} f^2(i,j) + \sum_{v_iv_j \in E} f^2(j,i) \right)\end{aligned}$$

Si $\sum_{i=1}^n a_i = 1+\alpha$ et $0 \leq a_i \leq 1$ alors $\sum_{i=1}^n a_i^2 \leq 1+\alpha^2$ donc $\sum_{v_iv_j \in E} f^2(i,j) + \sum_{v_iv_j \in E} f^2(j,i) \leq 2+2\alpha^2$, d'où

$$\sum_{v_iv_j \in E} f^2(i,j)(y_i+y_j)^2 \leq (4+2\alpha^2)\sum_{i=1}^{n} y_i^2.$$

D'autre part,

$$\begin{aligned}\sum_{v_iv_j \in E} f(i,j)(y_i^2-y_j^2) &= \sum_{i=1}^{n} y_i^2 \left(\sum_{v_iv_j \in E} f(i,j) - \sum_{v_iv_j \in E} f(j,i) \right) \\ &\leq \alpha \sum_{v_iv_j \in E} f(i,j)\end{aligned}$$

Multiplions l'Equation (6) par $1 = \frac{\sum_{v_iv_j \in E} f^2(i,j)(y_i+y_j)^2}{\sum_{v_iv_j \in E} f^2(i,j)(y_i+y_j)^2}$ et utilisons l'inégalité de Cauchy-Schwarz. On obtient:

$$\begin{aligned}\lambda &\leq d - \frac{\sum_{v_iv_j \in E}(y_i-y_j)^2 . \sum_{v_iv_j \in E} f^2(i,j)(y_i+y_j)^2}{2||y||^2 . \sum_{v_iv_j \in E} f^2(i,j)(y_i+y_j)^2} \\ &\leq d - \frac{\left(\sum_{v_iv_j \in E} f(i,j)(y_i^2-y_j^2)\right)^2}{2(4+2\alpha^2)||y||^2} \\ &\leq d - \frac{\alpha^2}{8+4\alpha^2}\end{aligned}$$

□

Corollaire 27 *Soit G un graphe d-régulier de sommet-expansion $vexp(G) = 1 + \alpha$. Alors*

$$\lambda \leq \sqrt{d^2 - \frac{\alpha^2}{8 + 4\alpha^2}}.$$

Preuve. Considérons le graphe G^2. Sa matrice d'adjacence est A^2. Ainsi G est d^2-régulier et ses valeurs propres sont les carrés de celles de A et donc toutes positives. En particulier, $\lambda(G^2) = \lambda(G)^2$.

Montrons que G^2 est un $(1 + \alpha)$-expandeur. Soit S un ensemble de sommets de taille au plus $n/2$. Alors $|\Gamma_G(S)| \geq (1 + \alpha)|S| \geq |S|$. Soit S' un sous-ensemble de $\Gamma_G(S)$ tel que $|S| = |S'| \leq n/2$. Alors

$$|\Gamma_{G^2}(S)| = |\Gamma_G(\Gamma_G(S))| \geq |\Gamma_G(S')| \geq (1 + \alpha)|S| = (1 + \alpha)|S'|.$$

Donc par le théorème précédent,

$$\lambda(G)^2 = \lambda(G^2) \leq d^2 - \frac{\alpha^2}{8 + 4\alpha^2}.$$

□

Comme $\lambda_2 \leq \lambda$, le Corollaire 27 et le Théoreme 6 entrainent immédiatement:

Corollaire 28 *Soit G un graphe d-régulier de sommet-expansion $vexp(G) = 1 + \alpha$. Alors*

$$exp(G) \geq \frac{1}{2}\left(d - \sqrt{d^2 - \frac{\alpha^2}{8 + 4\alpha^2}}\right).$$

5 Graphes de Cayley

References

[1] N. Alon. Eigenvalues and expanders, *Combinatorica*, 6(2):83–96, 1986.

[2] N. Alon and V. D. Milman. λ_1, isoperimetric inequalities for graphs, and superconcentrators. *J. Combin. Theory Ser. B*, 38(1):73–88, 1985.

[3] O. Amini, F. Giroire, F. Huc and S. Pérennes, Minimal selectors and fault tolerant networks, *INRIA Research Report*, 2006.

[4] Y. Bilu and N. Linial. Lifts, discrepancy and nearly optimal spectral gaps, *Combinatorica*, to appear.

[5] M. Blum, R. M. Karp, O. Vornberger, C. H. Papadimitriou, and M. Yannakakis. The complexity of testing whether a graph is a superconcentrator. *Inform. Process. Lett.*, 13(4-5):164–167, 1981.

[6] J. Dodziuk. Difference equations, isoperimetric inequality and transience of certain random walks. *Trans. Amer. Math. Soc.*, 284(2):787–794, 1984.

[7] J. Friedman. A proof of Alon's second eigenvalue conjecture, *Memoirs of the A. M. S.*, to appear.

[8] J. Friedman. Some geometric aspects of graphs and their eigenfunctions, *Duke Math. J.*, 69(3):487–525, 1993.

[9] F. Havet. Repartitors, selectors and superselectors, *J. of Interconnexion Networks*, September 2006, to appear.

[10] S.Hoory, N. Linial and A. Widgerson. Expander Graphs and their Applications, *Bull. A. M. S.*, 43:439–561, 2006.

[11] P. Indyk and J. Matoušek. Low-distorsion embeddings of finite metrics spaces. In Jacob E. Goodman and Joseph O'Rourke, editors, *Handbook of discrete and computationnal geometry*, Discrete Mathematics and its Applications (Boca Raton), pages 177-196, Chapman & Hall/CRS, Boca Raton, FL, second edition, 2004.

[12] M. Krivelevich and B. Sudakov. Pseudo-random graphs, In: *More Sets, Graphs and Numbers*, *Bolyai Society Mathematical Studies* 15: 199–262, 2006. Springer.

[13] N. Linial. Finite metrics spaces –combinatorics, geometry and algorithms. In *Proceedings of the International Congress of Mathematicians*, Vol. III (Beijing, 2002), pages 573–586, Beijing, 2002. Higher Ed. Press.

[14] Lubotsky, Phillips et Sarnak. Ramanujan graphs, *Combinatorica*, 8(3):261–277, 1988.

[15] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators, *Problems of Information Transmision*, 24(1):39–46, 1988.

[16] J. Matoušek. *Lectures on discrete geometry*, volume 212 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[17] M. Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramnujan graphs for every prime power q, *J. Combin. Theory Ser. B*, 62(1):44–62, 1994.

[18] A. Nilli. On the second eigenvalue of a graph, *Discrete Math.*, 91(2):207–210, 1991.

[19] L. Lovász. *Combinatorial problems and exercises*. North-Holland Publishing Co. Amsterdam, second edition, 1993.

[20] M. Ram Murty. Ramanujan graphs, *J. Ramanujan Math. Soc.*, 18(1):1–20, 2003.

[21] T. Richardson and R. Urbanke. *Modern coding theory*, Draft of the book, `http://lthcwww.epfl.ch/papers/mct.ps`.

[22] A. Valette. On the Baum-Connes assembly map for discrete groups, In *Proper group actions and Baum-Connes conjecture*, Adv. Courses Math. CRM Barcelona, pages 79–124. Brikhäuser, Basel, 2003.

[23] D. Y. Xiao. The evolution of expander graphs, *Bachelor's thesis*, Harvard College, Cmabridge, Massachusetts.