GRAPHES À TAUX D'EXPANSION OPTIMAL

F. JOUVE

Introduction

Dans ces notes, on donne la définition de ce qu'est un *graphe expanseur* et on montre en détails comment relier les propriétés d'expansion d'un graphe X à l'écart existant éventuellement entre les 2 valeurs propres de module (distinct) maximal de la matrice d'adjacence de X. Dans le cas où X est un graphe de Cayley sur un groupe abélien G, on exprime le spectre de X en fonction des caractères de G et on montre comment l'évaluation de sommes de caractères peut alors conduire à la preuve du fait qu'un graphe est expanseur.

1. Graphes

On rappelle qu'un *graphe* est la donnée d'un couple (V, E) où V est appelé ensemble des sommets et où E (ensemble des arêtes) est une partie de l'ensemble des couples d'éléments de V. Un graphe est *non-orienté* si l'ensemble des arêtes est globalement invariant par permutation (transposition) des coordonnées de ses éléments. Dans le cas contraire, le graphe sera dit *orienté*. Deux sommets x, y sont dits voisins si (x, y) (ou (y, x)) est une arête

Définition 1. *Soit $X = (V, E)$ un graphe. La* matrice d'adjacence *de X est la matrice A de taille $|V| \times |V|$ telle que $A_{x,y} = 1$ si (x, y) est une arête et $A_{x,y} = 0$ sinon.*

On remarque que si X est non orienté, sa matrice d'adjacence A est symétrique (et ses valeurs propres sont par conséquent réelles).

Certaines propriétés intéressantes que peut éventuellement vérifier un graphe sont codées dans sa matrice d'adjacence. Considérons par exemple

Définition 2. *Soit X un graphe ; X est dit* k-régulier *si tous ses sommets sont de* degré k *i.e. si chacun de ses sommets possède k voisins dans le sens sortant.*

Proposition 1. *Soit X un graphe k-régulier. k est la valeur propre de module maximal de la matrice d'adjacence A de X.*

Démonstration. Il est clair que le vecteur $(1, \dots, 1)$ est vecteur propre associé à la valeur propre k, puisque X est k-régulier.

Soit λ une valeur propre de la matrice d'adjacence A de X et $(x_1, \dots, x_n)$ un vecteur propre non-nul associé (on peut supposer $x_1 = \max_i |x_i|$ strictement positif (voir la preuve de la proposition suivante)). On a alors

$$|\lambda||x_1| = |\sum_j a_{1,j} x_j| \leqslant \Big|\sum_j a_{1,j}\Big||x_1| = k|x_1|, \quad \text{d'où } |\lambda| \leqslant k.$$

□

Définition 3. *Un graphe $X = (V, E)$ est dit connexe si, pour tout couple de sommets (x, y), il existe une suite finie de sommets (appelée* chemin*) $x = x_1, \dots, x_n = y$ telle que pour tout i, le couple (x_i, x_{i+1}) soit une arête.*

Il est alors clair que l'on peut définir, pour tout graphe, la notion de *composante connexe* d'un sommet v : ce sont tous les sommets du graphe reliés à v par un chemin. Les composantes connexes de X partitionnent l'ensemble V de ses sommets.

Proposition 2. *Soit X un graphe k-régulier non orienté. La multiplicité de k en tant que valeur propre de la matrice d'adjacence de X est le nombre de composantes connexes de X.*

Date: 16/05/07. GdT doctorants en théorie des nombres, Bordeaux 1.

Démonstration. D'après la proposition précédente, on sait que k est valeur propre de module maximal de X (on parlera dorénavant des valeurs propres de X pour désigner les valeurs propres de sa matrice d'adjacence).

Soit $(x_1, \dots, x_n)$ un vecteur propre non-nul associé à la valeur propre k. Sans perte de généralité, on peut supposer $x_1 = \max_i |x_i|$ strictement positif (on note que les x_i sont réels puisque l'on a supposé X non orienté). Si $A = (a_{i,j})_{i,j}$ est la matrice d'adjacence de X, on a alors

$$kx_1 = \sum_j a_{1,j}x_j \leqslant \Big(\sum_j a_{1,j}\Big)x_1 = kx_1\,,$$

ainsi

$$\sum_j a_{1,j}(x_1 - x_j) = 0\,,$$

d'où $x_1 = x_j$ dès que $a_{1,j} = 1$. On recommence le raisonnement avec x_j et on parcourt ainsi toute la composante connexe du sommet numéroté 1. Le nombre maximal de vecteurs libres du sous espace propre associé à k que l'on obtient ainsi est bien égal au nombre de composantes connexes de X. □

Il sera utile, dans la suite de l'exposé, de donner l'interprétation suivante de la matrice d'adjacence d'un graphe : si X est un graphe fini, on considère le $\mathbb{C}$-espace vectoriel des fonctions définies sur l'ensemble V des sommets de X et à valeurs complexes, on définit sur cet espace l'opérateur (appelé *opérateur de Hecke*)

$$\mathcal{A} : f \mapsto \Big(x \mapsto \sum_{\{y \in V \mid (x,y) \in E\}} f(y)\Big)\,.$$

Il est clair que l'ensemble des indicatrices des sommets de X forme une $\mathbb{C}$-base de l'espace de fonctions considéré. On voit alors facilement que la matrice de $\mathcal{A}$ relativement à cette base est la matrice d'adjacence de X.

2. Graphes expanseurs

La notion de graphe expanseur a été introduite dans les années 70 dans la but de résoudre des problèmes liés aux réseaux et aux télécommunications. Cette propriété traduit le fait qu'un graphe est "hautement connecté" dans le sens où, à partir d'un petit nombre de sommets (correspondant part exemples à des relais) on peut atteindre en un "pas" un grand nombre de sommets du graphe (par exemple des "récepteurs").

Soit $X = (V, E)$ un graphe fini. Pour S et T deux parties de V, on définit

$$E(S,T) = \{(u,v) \mid u \in S, v \in T, (u,v) \in E\}\,.$$

La *frontière* d'une partie S est par définition $\partial S = E(S, V \setminus S)$.

Définition 4. *Le* taux d'expansion *d'un graphe $X = (V, E)$ est le quotient*

$$h(X) = \min_{2|S| \leqslant |V|} \frac{|\partial S|}{|S|}\,,$$

où le minimum est pris sur les parties de V ne contenant pas plus de la moitié des sommets de X.

Pour ϵ strictement positif, X est dit ϵ-expanseur si $h(X) \geqslant \epsilon$.

Il est facile de voir que, pour peu que l'on prenne ϵ suffisament petit, tout graphe fini est ϵ-expanseur pour un certain ϵ dépendant du graphe considéré. Mais l'intérêt essentiel de la notion d'expansion réside dans la possibilité de construire des familles infinies $(X_n)_n$ de graphes (tel que le nombre de sommets de X_n tende vers l'infini lorsque n tend vers l'infini) qui soient ϵ-expanseurs pour un ϵ indépendant de n. On demande en outre que le nombre de voisins de chaque sommet "n'explose pas" lorsque n devient grand. Idéalement, on cherche donc à construire une famille infinie (X_n) (au sens ci-dessus) de graphes d-réguliers, ϵ-expanseurs où d et ϵ sont indépendants de n. Comme on peut s'y attendre, ces conditions fortes vont imposer des contraintes au taux d'expansion.

Dans un premier temps, on relie le taux d'expansion d'un graphe d régulier à l'écart existant entre les deux valeurs propres de module (distinct) maximal : si X est un graphe d-régulier non-orienté (que l'on suppose non-biparti pour s'assurer que $-k$ n'est pas valeur propre) à n sommets, on peut, d'après les propositions précédentes, ordonner ses valeurs propres :

$$d \geqslant \lambda_1 \geqslant \dots \geqslant \lambda_{n-1}$$

Notons $\lambda = \max(|\lambda_1|, |\lambda_{n-1}|)$ la valeur propre de X de module maximal une fois d exclu. On a alors

Proposition 3. *Si* X *est un graphe* d *régulier, on a, avec les notations ci-dessus,*

$$\frac{|\partial A|}{|A|} \geqslant \frac{d-\lambda}{2},$$

pour toute partie A *de l'ensemble des sommets de* X *ne contenant pas plus de la moitié des sommets de* X.

Minimiser λ peut ainsi paraître une bonne stratégie pour construire de bons expanders. Dans l'optique de la construction d'une famille infinie de graphes expanseurs, on a cependant le théorème limitatif suivant

Théorème 1 (Alon-Boppana, 1985). *Soit* $(X_n = (V_n, E_n))_n$ *une famille de graphes* d *réguliers telle que* $|V_n| \to \infty$ *lorsque* $n \to \infty$, *alors*

$$\liminf_{n\to\infty} \lambda(X_n) \geqslant 2\sqrt{d-1}.$$

Ainsi, la meilleurs borne supérieure uniforme que l'on peut espérer concernant les $\lambda(X_n)$ est $2\sqrt{d-1}$.

Définition 5. *Un graphe* X *connexe* d*-régulier est appelé* graphe de Ramanujan *si* $\lambda \leqslant 2\sqrt{d-1}$.

Les graphes de Ramanujan sont donc des graphes expanseurs optimaux si on les considère en tant qu'éléments de familles infinies de graphes.

3. Graphes de Cayley

C'est à partir de cette classe particulière de graphes que les premiers exemples explicites de familles d'expanders ont été construites.

Définition 6. *Soient* G *un groupe fini et* S *une partie de* G. *Le graphe noté* $\mathcal{C}(G,S)$ *dont les sommets sont les éléments de* G *et tel que* (g,h) *est une arête si et seulement si* $g^{-1}h \in S$ *est appelé* graphe de Cayley *sur* G *relativement à* S.

Il est clair qu'un graphe de Cayley est non orienté si et seulement si $s \in S \Rightarrow s^{-1} \in S$ et que $\mathcal{C}(G,S)$ est connexe si et seulement si S engendre G. Revenant à l'interprétation de la matrice d'adjacence d'un graphe en terme d'opérateur de Hecke, on peut donner une expression simple des valeurs propres de $\mathcal{C}(G,S)$ dans le cas où G est abélien.

Soit en effet ψ un caractère de G (supposé abélien fini), i.e. un morphisme $G \to \mathbb{C}^\times$. Avec les mêmes notations que dans la section précédente, on a, pour tout $g \in G$,

$$\mathcal{A}(\psi)(g) = \sum_{\{h \mid g^{-1}h \in S\}} \psi(h) = \sum_{s\in S} \psi(gs) = \Big(\sum_{s\in S} \psi(s)\Big)\psi(g).$$

$\{\psi \text{ caractère de } G\}$ est donc une base de diagonalisation de l'opérateur $\mathcal{A}$; la valeur propre associée au vecteur propre ψ étant $\sum_{s\in S} \psi(s)$.

Dans le cas particulier d'un graphe de Cayley sur un groupe abélien fini $\mathcal{C}(G,S)$, l'estimation des valeurs propres (et par conséquent l'évaluation du taux d'expansion du graphe considéré) se réduit donc au calcul des sommes d'exponentielles du type $\sum_{\{s\in S\}} \psi(s)$. On note que si ψ est le caractère trivial, on retrouve le fait que $|S|$ (degré commun à tous les sommets) est valeur propre de $\mathcal{C}(G,S)$. La proposition (facile) suivante précise cette idée

Proposition 4. *Si* G *est un groupe abélien fini et* $\mathcal{S} \subset G$, *le graphe* $\mathcal{C}(G,S)$ *est connexe si et seulement si aucun caractère non trivial de* G *ne se restreint trivialement à* S.

D'après la proposition ci-dessus, pour construire un graphe de Cayley $\mathcal{C}(G,S)$ (sur G abélien), qui soit un graphe de Ramanujan $|S|$-régulier, il faut trouver $S \subset G$ tel que

$$\Big|\sum_{s\in S} \psi(s)\Big| \leqslant 2\sqrt{|S|-1},$$

pour tout caractère ψ non-trivial de G.

Ex1 Pour p premier, on prend $G = \mathbb{Z}/p\mathbb{Z}$ et $S = \{x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\}$. On voit rapidement que ce premier exemple pose des problèmes quant aux conventions prises pour dénombrer le degré de chaque sommet. Pour construire un graphe de Ramanujan dans le cas présent, il faut en fait voir S comme un multi-ensemble (chaque carré non-nul apparait 2 fois dans S, puisqu'il provient de 2 éléments différents de $\mathbb{Z}/p\mathbb{Z}$). Ainsi le graphe $\mathcal{C}(G,S)$ présente des arêtes multiples et des boucles en chacun de ses sommets (correspondant au fait que 0 est un carré). En théorie des graphes, on convient d'attribuer une contribution $+2$ à chaque sommet présentant une

boucle. Ainsi $\mathcal{C}(G,S)$ est $p+1$-régulier et possède p sommets. Soit alors ψ un caractère non-trivial de $\mathbb{Z}/p\mathbb{Z}$; en notant χ_p le caractère de Legendre de $\mathbb{Z}/p\mathbb{Z}$, on a

$$2\sum_{s\in\mathbb{Z}/p\mathbb{Z}}\psi(s^2)=\sum_{s\in\mathbb{Z}/p\mathbb{Z}}(1+\chi_p(s))\psi(s)=\sum_{s\in\mathbb{Z}/p\mathbb{Z}}\chi_p(s)\psi(s)\,.$$

À chaque caractère non-trivial de $\mathbb{Z}/p\mathbb{Z}$ correspond donc une valeur propre égale à une somme de Gauss quadratique et l'on sait que, pour ψ non-trivial

$$\Big|\sum_{s\in\mathbb{Z}/p\mathbb{Z}}\chi_p(s)\psi(s)\Big|=\sqrt{p}\leqslant 2\sqrt{p+1-1}=2\sqrt{p}\,.$$

Ainsi $\mathcal{C}(G,S)$ est un graphe de Ramanujan... si tant est que l'on accepte les graphes présentant des boucles ou des multi-arêtes.

Ex2 L'exemple qui suit (beaucoup moins ad hoc) est dû à W-C. W. Li. Soient q une puissance d'un nombre premier p et $\mathbb{F}_q$ le corps fini à q éléments. Pour $n\geqslant 1$, la norme

$$N=N_{\mathbb{F}_{q^n}/\mathbb{F}_q}:x\in\mathbb{F}_{q^n}^\times\mapsto x x^q\cdots x^{q^{n-1}}\in\mathbb{F}_q^\times\,,$$

est un morphisme surjectif de groupes. Son noyau N_n vérifie donc

$$|N_n|=\frac{q^n-1}{q-1}\,.$$

Posons alors $G=\mathbb{F}_{q^n}$ et $S=N_n$. Pour un caractère ψ non-trivial de $\mathbb{F}_{q^n}$, la valeur propre λ_ψ du graphe de Cayley $\mathcal{C}(G,S)$ est

$$\lambda_\psi=\sum_{x\in N_n}\psi(x)\,.$$

Tous les caractères additifs de $\mathbb{F}_{q^n}$ étant de la forme $x\mapsto\varphi(\mathrm{Tr}(ax))$, où φ est un caractère non-trivial de $\mathbb{F}_q$ et a décrit $\mathbb{F}_{q^n}$, on obtient que les valeurs propres de $\mathcal{C}(G,S)$ sont de la forme

$$\lambda_a=\sum_{x\in N_n}\varphi(\mathrm{Tr}(ax))=\sum_{N(y)=b}\varphi(\mathrm{Tr}(y))\,,$$

où $b=N(a)$. Cette dernière somme est une somme de Kloosterman multiple (on peut utiliser la relation de Hasse Davenport pour s'en convaincre). L'estimation de Deligne donne alors

$$|\lambda_a|\leqslant nq^{(n-1)/2}\,,$$

dès que $a\neq 0$. Pour $n=2$ on obtient d'une part

$$|\lambda_a|\leqslant 2\sqrt{q}\,,$$

et d'autre part

$$2\sqrt{|N_2|-1}=2\sqrt{q+1-1}=2\sqrt{q}\,.$$

Le graphe $\mathcal{C}(\mathbb{F}_{q^2},N_2)$ est donc un graphe de Ramanujan. Cette construction fournit par conséquent une famille infinie de graphes de Ramanujan, le seul affaiblissemnt par rapport aux contraintes que l'on s'était fixé initialemnt étant que le degré commun aux sommets $(q+1)$ dépend du nombre de sommets (q^2) du graphe.

Ex3 Dans ce dernier exemple, on décrit succintement une construction de Lubotzky, Phillips et Sarnak qui est à l'origine de la terminologie "graphe de Ramanujan" et qui fournit un exemple de famille infinie de graphes de Ramanujan d-réguliers, où d est fixé.

Soient p,q des nombres premiers distincts et congrus à 1 modulo 4. On fixe i une racine de $-1\pmod q$. D'après l'identité de Jacobi (voir à ce sujet les excellentes notes de Cécile Armana ([A])), on sait qu'il existe $8(p+1)$ solutions (a_0,a_1,a_2,a_3) à l'équation

$$a_0^2+a_1^2+a_2^2+a_3^2+a_4^2=p\,,$$

d'où l'on peut déduire qu'il existe $p+1$ telles solutions avec a_0 impair strictement positif et les a_i pairs pour $i\neq 0$. À une telle solution, on associe la matrice de $\mathrm{PGL}(2,\mathbb{Z}/q\mathbb{Z})$

$$\begin{pmatrix} a_0+ia_1 & -a_2+ia_3\\ a_2+ia_3 & a_0-ia_1\end{pmatrix}.$$

On considère alors le graphe de Cayley sur $\mathrm{PGL}(2,\mathbb{Z}/q\mathbb{Z})$ relativement aux $p+1$ éléments ci-dessus. Ce graphe est $p+1$-régulier sur $q(q^2-1)$ sommets. Pour que ce graphe ait une chance d'être un graphe de Ramanujan, il faut qu'il soit connexe ; or, si $\chi_q(p)=1$ (où χ_q désigne le symbole de Legendre relativement à q), tous les éléments ci-dessus sont dans le sous groupe $\mathrm{PSL}(2,\mathbb{Z}/q\mathbb{Z})$ d'indice 2 de $\mathrm{PGL}(2,\mathbb{Z}/q\mathbb{Z})$.

Dans le cas où $\chi_q(p) = -1$, on définit donc le graphe $X^{p,q}$ comme étant le graphe de Cayley décrit ci-dessus et, si $\chi_q(p) = 1$, le graphe $X^{p,q}$ est le graphe de Cayley sur $\mathrm{PSL}(2, \mathbb{Z}/q\mathbb{Z})$ relativement au même ensemble de cardinalité $p + 1$. On a alors le théorème suivant pour lequel on renvoie à [LPS] :

Théorème 2. *La famille de graphes $X^{p,q}$ est une famille de graphes de Ramanujan $p + 1$-réguliers.*

Références

[A] Armana, C. : *Les formes modulaires, «La cinquième opération de l'arithmétique»*, `http://www.math.u-bordeaux.fr/~pazuki/2007formesmodlambdabordeaux.pdf`

[LPS] Lubotzky, A., Phillips, R. and Sarnak, P. : *Ramanujan graphs*, Combinatorica 8, no 3, 261-277, (1988).