Introduction à la géométrie des groupes discrets

Yann Ollivier

Séminaire des élèves de l'ENS, 25 avril 2001

Nous donnons ici une introduction à différents thèmes liés à la géométrie des groupes discrets. On s'intéressera en particulier à des propriétés asymptotiques des groupes discrets infinis. On commence par donner un aperçu des propriétés usuellement étudiées (par exemple la propriété de Kazhdan, l'hyperbolicité, la moyennabilité), avec des exemples, et l'on énonce quelques-uns des « grands » théorèmes de ce domaine, sans démonstration.

Puis nous montrons comment la propriété de Kazhdan mentionnée plus haut peut aider à résoudre un problème classique de géométrie algorithmique des groupes, celui de trouver une méthode pour obtenir un élément aléatoire dans un groupe fini donné par des générateurs et une boîte noire effectuant la multiplication. L'idée d'un algorithme couramment utilisé sans démonstration, le PRA, est d'effectuer une marche aléatoire sur le graphe des k-uplets générateurs du groupe (voir section 3.1 pour une définition précise). En définissant une action d'un certain groupe de Kazhdan sur ce graphe, on peut obtenir une évaluation du temps de convergence, qui fait l'objet du théorème final que nous démontrerons.

1 Les groupes discrets

1.1 Le cadre géométrique

On donne ci-dessous une définition des groupes discrets. Des extensions sont possibles (en particulier, certaines des notions mentionnées plus loin sont définies dans le cadre des groupes localement compacts), mais nous nous en tiendrons à ce cadre (relativement) simple. Cette présentation est inspirée de l'excellent [GH].

Définition 1 (Groupes discrets) – *Un* groupe discret *est un groupe dénombrable engendré par un nombre fini d'éléments, muni de la topologie discrète et de la mesure de comptage.*

De plus, pour dépasser un peu cette définition, on voudrait faire de la

géométrie sur ces groupes, et on voudrait donc introduire une notion de distance. C'est possible en choisissant un système de générateurs donné.

On dit qu'un système de générateurs est *symétrique* s'il contient les inverses de ses éléments.

Définition 2 (Distance dans les groupes discrets) – *Soient G un groupe discret, et $s_1, \dots, s_k$ un système générateur symétrique de G. On définit une géométrie sur G :*

- *la* longueur *d'un élément $x \in G$ est la plus petite longueur d'une suite $s_{i_1}, \dots, s_{i_\ell}$ de générateurs telle que $x = s_{i_1} \dots s_{i\ell}$;*
- *la* distance *entre deux éléments $x, y \in G$ est la longueur de xy^{-1}.*

Il est immédiat de vérifier que cette distance en est bien une : si on peut passer de x à y en multipliant par ℓ générateurs et de y à z par ℓ' générateurs, on peut passer de x à z par $\ell + \ell'$ générateurs.

Par construction, elle est invariante par multiplication à gauche.

Cette distance peut s'interpréter comme distance dans un graphe :

Définition 3 (Graphe de Cayley) – *Soient G un groupe discret, et $s_1, \dots, s_k$ un système générateur symétrique de G. Le* graphe de Cayley *de G par rapport à ce système générateur est le graphe dont les sommets sont les éléments de G, avec une arête entre x et y si et seulement s'il existe s_i tel que $y = s_i x$.*

Exemple – *Le graphe de Cayley d'un groupe libre à k générateurs est un arbre dont chaque sommet est de degré $2k$ (ce qui peut servir comme définition géométrique du groupe libre : l'absence de relation est l'absence de cycles dans le graphe).*

Un groupe agit naturellement par multiplication à gauche sur son graphe de Cayley.

Ces notions dépendent bien entendu du système générateur choisi. Pour étudier cette dépendance, on introduit la notion suivante :

Définition 4 (Quasi-isométries) – *Soient (X, d) et (X', d') deux espaces métriques. On dit qu'ils sont* quasi-isométriques *s'il existe des applications $f : X \to X'$ et $g : X' \to X$, ainsi que des constantes $\lambda > 0$ et $C \geqslant 0$ telles que pour tous $x, y \in X$, $x', y' \in X'$:*

$$\begin{aligned} d'(f(x), f(y)) &\leqslant \lambda\, d(x, y) + C \\ d(g(x'), g(y')) &\leqslant \lambda\, d'(x', y') + C \end{aligned}$$

et

$$\begin{aligned} d(g(f(x)), x) &\leqslant C \\ d'(f(g(x')), x') &\leqslant C \end{aligned}$$

Ainsi, excepté à petite distance, les fonctions f et g sont presque lipschitziennes et presque inverses.

La quasi-isométrie est une relation d'équivalence sur les espaces métriques.

Proposition 1 – *Les structures métriques d'un groupe selon deux systèmes générateurs sont quasi-isométriques.*

Démonstration (ébauche) – Il suffit de considérer les longueurs des éléments du deuxième système générateur dans le premier ; cela fournit une évaluation de la constante de quasi-isométrie. □

Nous considérerons donc les groupes discrets comme des espaces métriques à quasi-isométrie près. En particulier, nous définirons souvent des propriétés d'un groupe en regardant son graphe de Cayley pour un certain système générateur, et en vérifiant que la propriété est invariante par quasi-isométrie.

Exemples – *Tous les groupes finis sont quasi-isométriques entre eux. $\mathbb{Z}$ et $\mathbb{R}$ sont quasi-isométriques. Un sous-groupe d'indice fini dans un groupe discret lui est quasi-isométrique.*

Exemple – *Soit M une variété riemannienne compacte. Son groupe fondamental et son revêtement universel sont quasi-isométriques.*

1.2 Quelques classes de groupes discrets

Un théorème de M. Gromov affirme qu'un théorème valable pour tous les groupes est soit trivial soit faux. Par conséquent, pour démontrer des théorèmes vrais et intéressants, on doit se restreindre à des sous-classes de groupes possédant certaines propriétés. Nous en présentons ici trois : la moyennabilité, l'hyperbolicité et la propriété (T) de Kazhdan. C'est cette dernière qui nous servira de manière cruciale par la suite.

Ces notions reflètent véritablement des propriétés des groupes infinis. En effet, tous les groupes finis les vérifient.

Groupes moyennables. Les groupes moyennables sont ceux dans lesquels les effets de bord sont négligeables lorsqu'on considère des sous-parties assez grandes (cf. les problèmes de conditions aux limites en physique). Ainsi $\mathbb{R}^n$ ou $\mathbb{Z}^n$ sont moyennables, car le rapport de la mesure du bord d'une boule à la mesure de la boule tend vers 0 quand la boule devient grande.

Dans un graphe, le *bord* d'une partie A, noté ∂A, est défini comme l'ensemble des points du complémentaire de A joints par une arête à un point de A.

Définition 5 (Groupes moyennables) – *Un groupe discret G est dit* moyennable *si son graphe de Cayley est de constante isopérimétrique nulle i.e. si*

$$\inf\left\{\frac{|\partial A|}{|A|}, A \subset G \text{ fini non vide}\right\} = 0$$

On vérifie aisément que cette notion est invariante par quasi-isométrie, donc bien définie pour un groupe à partir d'un graphe de Cayley.

On peut montrer que :

Exemples – *Les groupes finis sont moyennables. Les groupes abéliens sont moyennables. Une extension de groupes moyennables est moyennable.*

Groupes hyperboliques. La notion de groupe hyperbolique est une invention de M. Gromov (cf. [Gr]), s'inspirant des variétés hyperboliques (à courbure négative).

Dans un graphe, on appelle *triangle* la donnée de trois sommets, et de trois chemins de longueur minimale (ces chemins ne sont pas forcément uniques) reliant ces sommets deux à deux, qu'on appelle *côtés* du triangle.

Dans un plan hyperbolique habituel, les côtés des triangles ont la propriété d'êtres courbés vers l'intérieur, au sens où la distance d'un point d'un côté à la réunion des deux autres côtés est toujours inférieure à ce qu'elle serait dans un triangle euclidien... en fait elle est même bornée. Ceci sert de base à une définition des groupes hyperboliques.

Définition 6 (Groupes hyperboliques) – *Un groupe est dit* hyperbolique *si, dans un certain graphe de Cayley, il existe une constante $C \geqslant 0$ telle que pour tout triangle, la distance d'un point d'un côté du triangle à la réunion des deux autres côtés est inférieure à C.*

Il est vrai, mais pas du tout trivial, que cette propriété ne dépend pas du graphe de Cayley choisi (elle est invariante par quasi-isométrie).

Exemples – *Un groupe fini est hyperbolique. Un groupe libre est hyperbolique (le graphe de Cayley étant un arbre, tout triangle y est complètement aplati...). Un produit libre de groupes hyperboliques est hyperbolique.*

Voici une autre justification du nom :

Exemple – *Le groupe fondamental d'une variété compacte à courbure (sectionnelle) négative est hyperbolique.*

Il existe de nombreuses définitions équivalentes de l'hyperbolicité d'un groupe, de nature géométrique ou combinatoire (cf. [GH]). Par exemple, l'une d'elles est obtenue en formalisant précisément l'intuition que vu de loin, le graphe de Cayley d'un groupe hyperbolique ressemble à un arbre.

Propriété (T) de Kazhdan. Une notion supplémentaire, d'apparence abstraite, s'est révélée extrêmement féconde dans des domaines très variés de l'étude des groupes, de la théorie des graphes, de la théorie de la mesure et même en informatique : c'est la propriété (T) de Kazhdan. Elle est très bien présentée dans [HV]. Elle est plus généralement définie pour des groupes localement compacts, et ci-dessous nous dirons souvent « compact » là où « fini » aurait le même sens dans le cadre des groupes discrets.

Une *représentation unitaire* d'un groupe discret G est une action de G par des isométries linéaires sur un espace de Hilbert $\mathcal{H}$, ou encore un morphisme de G vers les endomorphismes unitaires de $\mathcal{H}$.

Définition 7 (Vecteurs invariants, presque invariants) – *On dit qu'une représentation unitaire π de G sur un Hilbert $\mathcal{H}$ a des* vecteurs invariants *s'il existe $x \in \mathcal{H}$ non nul tel que pour tout $g \in G$, $\pi(g)x = x$.*

On dit que π a des vecteurs presque invariants si pour tout $\varepsilon > 0$, pour tout compact $K \subset G$, on peut trouver un $x \in H$ non nul tel que pour tout $g \in K$, $\|\pi(g)x - x\| \leqslant \varepsilon \ \|x\|$.

Définition 8 (Propriété (T) de Kazhdan) – *On dit qu'un groupe G est* de Kazhdan*, ou qu'il a la* propriété (T)*, si toute représentation unitaire de G ayant des vecteurs presque invariants a des vecteurs invariants.*

Cette condition porte sur toutes les représentations, et est donc extrêmement forte. En fait, selon la proposition ci-dessous, il suffit de la tester sur un compact générateur de G et sur les représentations irréductibles, puisque d'autres représentations et d'autres éléments du groupe peuvent être obtenus par construction sur ceux-là.

On rappelle qu'une représentation d'un groupe sur un espace $\mathcal{H}$ est *irréductible* si l'on ne peut pas trouver de décomposition $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ telle que $\mathcal{H}_1, \mathcal{H}_2$ sont stables par l'action de la représentation. Toute représentation peut se décomposer en une somme de représentations irréductibles.

Proposition 2 – *Soit K un compact engendrant le groupe G. On suppose qu'il existe ε tel que toute représentation unitaire irréductible de G possédant des vecteurs unitaires (K, ε)-invariants, possède des vecteurs invariants. Alors G est de Kazhdan.*

Le couple (K, ε) est appelé une constante de Kazhdan *de G.*

On peut montrer :

Exemples – *Un groupe compact est de Kazhdan. Une extension de groupes de Kazhdan est de Kazhdan. L'(adhérence de l')image d'un groupe de Kazhdan par un morphisme (continu) est de Kazhdan.*

Mais aussi :

Contre-exemples – *Un groupe moyennable n'est de Kazhdan que s'il est compact. En particulier, $\mathbb{Z}$ n'est pas de Kazhdan.*

Démonstration (ébauche) – L'idée est de considérer l'action à gauche du groupe G sur son graphe de Cayley Γ, qui définit une représentation de G sur $L^2(\Gamma)$ par translation (*représentation régulière gauche*). Si G est moyennable, en prenant un ensemble A grand et de petit bord, une fonction constante sur A est presque invariante, car si on la translate par des éléments de G, la différence est concentrée vers le bord de A. Si le groupe était de Kazhdan, il existerait donc une fonction invariante ; comme l'action de G sur son graphe de Cayley est transitive, cette fonction serait constante. Or dès que G est infini, il n'y a évidemment pas de fonction constante non nulle L^2-intégrable sur Γ. □

En particulier, ces propriétés mises bout à bout montrent qu'un groupe de Kazhdan est très non commutatif, au sens ou son abélianisé est compact (en effet, il est de Kazhdan comme image d'un groupe de Kazhdan, et il est abélien donc moyennable, donc compact). Ceci permet de dire, par exemple, qu'un groupe libre n'est pas de Kazhdan.

Il existe d'autres définitions de la propriété de Kazhdan. L'une d'elles demande que toute action *affine* isométrique du groupe sur un Hilbert ait un point fixe. Une autre est en rapport avec la cohomologie du groupe...

Jusqu'ici, nous n'avons guère vu d'exemples intéressants. On va s'intéresser à $SL_k(\mathbb{Z})$ qui nous resservira par la suite. On sait que ce groupe est de Kazhdan, et on a même une évaluation de la constante de Kazhdan par rapport aux matrices élémentaires. Une *matrice élémentaire* dans $SL_k(\mathbb{Z})$ est une matrice qui ne contient que des 1 sur la diagonale, qui contient un unique ± 1 quelque part en-dehors de la diagonale, et des 0 ailleurs. Ces matrices engendrent $SL_k(\mathbb{Z})$. Un raisonnement élaboré montre alors, avec des outils relativement élémentaires, que (cf [Sh]) :

Théorème 1 (D. Kazhdan ; Y. Shalom) – *$SL_k(\mathbb{Z})$ est de Kazhdan pour $k \geqslant 3$, et il existe une constante C telle que C/k^2 est une constante de Kazhdan pour le système générateur constitué des matrices élémentaires.*

Nous utiliserons ce théorème plus loin, dans notre étude de la convergence des marches aléatoires dans les groupes.

Mentionnons enfin le

Problème ouvert – *La propriété de Kazhdan est-elle invariante par quasi-isométrie ?*

1.3 Groupes aléatoires et généricité des groupes hyperboliques et de Kazhdan

Prouver qu'un groupe est hyperbolique ou de Kazhdan est souvent difficile. Cependant, on peut montrer qu'en un certain sens, presque tous les

groupes sont hyperboliques, et, qu'au-dessus d'une certaine densité de relations, presque tous les groupes sont de Kazhdan. Ce sont les très élégants théorèmes que nous énonçons ici.

L'idée est de partir du groupe libre engendré par $a_1, \ldots, a_k$, et de construire des groupes en quotientant par des relations (une relation est simplement un mot en les a_i et a_i^{-1}). Tout groupe à k générateurs peut être obtenu de la sorte. Si on met beaucoup de relations, on a des chances que le quotient soit simplement le groupe trivial. On va choisir la quantité de relations que l'on met à partir d'une densité, que nous définissons maintenant.

On fixe le nombre k de générateurs. On considère les groupes présentés par ces k générateurs, et des relations de longueur ℓ entre ces générateurs. Si l'on simplifie les relations contenant les sous-mots triviaux aa^{-1}, le nombre de mots de longueur ℓ sur k générateurs est $2k(2k-1)^{\ell-1}$. Soit un groupe G présenté par r relations de longueur ℓ. On dit que cette présentation est de densité d si $(2k-1)^{d.\ell}/C \leqslant r \leqslant C(2k-1)^{d.\ell}$ pour une certaine constante $C \geqslant 1$.

On définit un groupe aléatoire $G_{k,d,\ell}$ à k générateurs, avec densité d et relations de longueur ℓ, comme le groupe obtenu en prenant une présentation uniformément au hasard parmi toutes les présentations sur k générateurs, de densité d et de relations de longueur ℓ.

Alors, si on a beaucoup de relations, on obtient presque sûrement le groupe trivial ; si on a peu de relations, on obtient presque sûrement un groupe hyperbolique.

Théorème 2 (M. Gromov) – *Si $d > 1/2$, quand $\ell \to \infty$, la probabilité que $G_{k,d,\ell}$ soit le groupe trivial $\{e\}$ tend vers 1.*

Si $d < 1/2$, quand $\ell \to \infty$, la probabilité que $G_{k,d,\ell}$ soit infini et hyperbolique tend vers 1.

Ce qui se produit à la densité critique $d = 1/2$ reste un mystère.

Par ailleurs :

Théorème 3 (A. Żuk) – *Si $d > 1/3$, quand $\ell \to \infty$, la probabilité que $G_{k,d,\ell}$ soit de Kazhdan tend vers 1.*

En particulier, entre $1/3$ et $1/2$, on a des groupes non triviaux hyperboliques de Kazhdan.

2 Marches aléatoires dans les graphes

2.1 Marches aléatoires et laplacien dans les graphes

On donne ici quelques rappels sur les marches aléatoires dans les graphes, et, en particulier, dans des graphes de Cayley. Tous les graphes que nous considérerons seront orientés, avec éventuellement des boucles et des arêtes multiples. On supposera aussi que de chaque point il part au moins une arête.

Définition 9 (Marche aléatoire) – *Soit Γ un graphe. On appelle* marche aléatoire sur Γ *le processus markovien qui, partant d'un point quelconque, se déplace vers un point voisin en choisissant une arête au hasard uniformément parmi toutes les arêtes partant de ce point.*

À chaque étape, on note π_t la mesure sur Γ qui est la loi du point atteint au temps t par la marche aléatoire.

La marche aléatoire peut être vue comme un opérateur h sur les mesures sur Γ ou, plus généralement, sur les fonctions sur Γ dans $\mathbb{R}$ ou $\mathbb{C}$, défini par :

$$(h.f)(x) = \sum_{y \sim x} \frac{1}{\deg y} f(y)$$

où $\deg y$ est le nombre d'arêtes partant de y et où $y \sim x$ signifie qu'il y a une arête allant de y à x. On a alors $\pi_{t+1} = h.\pi_t$.

L'opérateur $\Delta = \mathrm{Id} - h$ est appelé *laplacien* sur le graphe.

Définition 10 (Graphes réguliers, symétriques) – *Un graphe est dit* régulier de degré d *si de tout sommet, il part exactement d arêtes. Un graphe est dit* symétrique *si $x \sim y \Rightarrow y \sim x$.*

Désormais, on ne considérera plus que des graphes réguliers symétriques. C'est en particulier le cas du graphe de Cayley d'un groupe.

Proposition 3 – *Sur un graphe fini régulier, une fonction est invariante par h si et seulement si elle est constante sur chaque composante connexe.*

Démonstration – Tous les points ayant même degré, la valeur de $h.f$ en un point est la moyenne de la valeur de f sur ses voisins. Regarder un point où f est de module maximal (il en existe car le graphe est fini), en déduire que f a la même valeur sur tous les voisins et utiliser la connexité (connexité au sens des graphes orientés). □

Si Γ est le graphe de Cayley d'un groupe G pour un système de générateurs S, alors h est l'opérateur de convolution (à gauche) avec la fonction qui vaut $1/|S|$ en chaque générateur de S, et 0 ailleurs.

Notons que si le graphe est régulier de degré d et symétrique, alors l'opérateur h sur $L^2(\Gamma)$ est autoadjoint. En effet :

$$\langle h.f, g \rangle = \sum (h.f)(x)\, g(x) = \sum_x \frac{1}{d} \sum_{y \sim x} f(y)\, g(x)$$

cette dernière expression étant symétrique en f et g.

Sur un graphe fini, la théorie classique des chaînes de Markov (ou le théorème de Perron-Frobenius) affirme que les valeurs propres de l'opérateur h sont comprises entre -1 et 1. Pour éviter les problèmes de périodicité et d'oscillations causés par les valeurs propres négatives, on considère une variante :

Définition 11 (Marche aléatoire paresseuse) – *On appelle* marche aléatoire paresseuse *sur un graphe le processus markovien qui, à chaque étape, avec probabilité* $1/2$*, soit reste sur place, soit fait un pas de marche aléatoire.*

L'opérateur associé sur les fonctions sur le graphe est donc $(\mathrm{Id} + h)/2$. Abusons des notations et notons encore h cet opérateur, associé à la marche aléatoire paresseuse (comme si à chaque sommet du graphe, on ajoutait $d/2$ arêtes en boucle). Ses valeurs propres sont comprises entre 0 et 1, le sous-espace propre associé à 1 étant constitué des fonctions constantes sur chaque composante.

Pour deux mesures de probabilité μ, ν sur h, on note

$$|\mu - \nu| = \frac{1}{2} \sum |\mu(x) - \nu(x)| = \sup_{A \subset \Gamma} |\mu(A) - \nu(A)| \leqslant 1$$

En écrivant h (autoadjoint) dans une base diagonalisante, et en utilisant l'inégalité de Cauchy-Schwarz $\|\mu - \nu\|_1 \leqslant \sqrt{|\Gamma|}\, \|\mu - \nu\|_2$, on obtient :

Proposition 4 – *Sur un graphe fini régulier symétrique, la loi* π_t *au temps* t *de la marche aléatoire paresseuse partant d'un point quelconque converge vers la mesure uniforme* U *sur la composante connexe du point de départ. De plus, si* λ *est la plus grande valeur propre de* h *inférieure à* 1*, on a*

$$|\pi_t - U| \leqslant \frac{\sqrt{|\Gamma|}}{2} \lambda^t$$

et le temps de relaxation vérifie donc

$$\tau \leqslant \frac{\frac{1}{2} \log |\Gamma| + 1}{-\log \lambda} \leqslant \frac{\frac{1}{2} \log |\Gamma| + 1}{1 - \lambda}$$

Le temps de relaxation est, conventionnellement, le plus petit temps tel que $|\pi_t - U| \leqslant 1/e$.

La quantité $1 - \lambda$, première valeur propre non nulle du laplacien, est appelée *trou spectral* du graphe ; plus il est grand, plus les marches aléatoires convergent rapidement. L'évaluation du trou spectral pour certains graphes définis par des actions de groupes de Kazhdan fait l'objet de la section suivante.

2.2 Propriété de Kazhdan et spectre du laplacien

La connaissance de constantes de Kazhdan pour des systèmes générateurs d'un groupe permet de déduire des propriétés spectrales pour certains opérateurs agissant dans une représentation du groupe. Nous allons utiliser ce lien

pour évaluer le trou spectral du laplacien d'un groupe de Kazhdan agissant sur certains graphes (cf. [HRV]).

Soient G un groupe, S un système générateur fini symétrique, et π une représentation unitaire de G sur un Hilbert $\mathcal{H}$. Soit

$$\kappa(\pi, S) = \inf_{\xi \in \mathcal{H}, \|\xi\|=1} \max_{s \in S} \|\pi(s)\xi - \xi\|$$

la constante de Kazhdan associée à S et π (qui ne peut évidemment être non nulle que si π ne contient pas la représentation identité).

On définit de plus

$$h = \frac{1}{|S|} \sum_{s \in S} \pi(s) \ \in L(\mathcal{H})$$

Par exemple, si π est la représentation régulière gauche de G, alors h est simplement l'opérateur « moyenne sur les voisins » dans le graphe de Cayley de G pour le système générateur S ($h = 1 - \Delta$).

On obtient dans ce cadre une évaluation du trou spectral du laplacien :

Proposition 5 – *Soit $z \in \operatorname{Sp} h$. Alors*

$$|z - 1| \geqslant \frac{\kappa(\pi, S)^2}{2\,|S|}$$

En particulier, si G est un groupe de Kazhdan et κ une constante de Kazhdan par rapport à S, alors pour toute représentation unitaire de G, le trou spectral de h est supérieur à $\kappa^2/2\,|S|$. C'est cette propriété qui nous servira par la suite.

Démonstration – Nous utiliserons le

Lemme 1 – *Soient $\mathcal{H}$ un espace de Hilbert, $\xi \in \mathcal{H}$ un vecteur normé. Soient $y_1, \dots y_n \in L(\mathcal{H})$ tous de norme inférieure ou égale à 1. On pose $h = \dfrac{1}{n} \sum y_i \ \in L(\mathcal{H})$.*

Si $\|y_j\xi - \xi\| \geqslant \varepsilon$ pour un certain j, alors $\|h\xi - \xi\| \geqslant \dfrac{\varepsilon^2}{2n}$.

Démonstration du lemme – Utilisant que $\|y_j\xi - \xi\|^2 = \|y_j\xi\|^2 + \|\xi\|^2 - 2\Re\langle y_j\xi, \xi\rangle$, on obtient que $\Re\langle y_j\xi, \xi\rangle \leqslant 1 - \varepsilon^2/2$.

Par ailleurs, comme les y_i sont de norme inférieure à 1, on a $\Re\langle y_i\xi, \xi\rangle \leqslant 1$. Par conséquent, $\Re\langle h\xi, \xi\rangle = \dfrac{1}{n} \sum \Re\langle y_i\xi, \xi\rangle \leqslant 1 - \varepsilon^2/2n$.

Pour tous $\eta, \eta' \in \mathcal{H}$, on a $\Re\langle \eta, \eta'\rangle \geqslant \|\eta\|\,(\|\eta\| - \|\eta' - \eta\|)$ (évident sur un dessin). Ceci donne $1 - \varepsilon^2/2n \geqslant 1 - \|h\xi - \xi\|$, d'où le lemme. □

Revenons à la proposition. h est un opérateur hermitien sur $\mathcal{H}$ (car S est symétrique et π unitaire). On veut montrer que pour tout $w \in \mathbb{C}$ tel que $|w - 1| < \dfrac{\kappa(\pi, S)^2}{2\,|S|}$, $h - w\,\mathrm{Id}$ est inversible.

Soit $\xi \in \mathcal{H}$ unitaire. Par définition de $\kappa(\pi, S)$, il existe un $s \in S$ tel que $\|\pi(s)\xi - \xi\| \geqslant \kappa(\pi, S)$. Le lemme implique alos que $\|h\xi - \xi\| \geqslant \kappa(\pi, S)^2/2\,|S|$. Par conséquent, $\|h\xi - w\xi\| \geqslant \kappa(\pi, S)^2/2\,|S| - |w-1|$, ce qui suffit à montrer que l'opérateur hermitien $h - w\,\mathrm{Id}$ est inversible. □

3 Le PRA

3.1 Présentation du PRA

Un problème fréquemment rencontré en théorie algorithmique des groupes consiste à engendrer un élément aléatoire d'un groupe fini, selon la loi uniforme. Le but est de déterminer, par ordinateur, des propriétés d'un groupe donné comme une boîte noire : sont donnés un ensemble de générateurs du groupe et une fonction qui multiplie deux éléments. En outre, on sait dire si un élément est l'élément neutre. Disposer, dans un tel cadre, d'éléments aléatoires uniformément répartis dans le groupe permet de tester différentes propriétés (ordre...), et de répondre à des questions sur la nature du groupe donné, éventuellement avec une certaine probabilité d'erreur.

Le PRA (pour *partial replacement algorithm*) est un algorithme heuristique destiné à produire de tels éléments aléatoires dans un groupe fini G. L'idée est de partir d'un k-uplet générateur $(g_1, \ldots, g_k)$ et de le transformer en un autre, en multipliant entre eux des éléments du k-uplet. En répétant cette transformation un nombre de fois assez grand, on espère aboutir à un k-uplet aléatoire d'éléments du groupe.

Définition 12 (PRA) – *On part d'un k-uplet générateur $(g_1, \ldots, g_k)$ d'un groupe fini G. On lui applique itérativement la transformation suivante. À chaque étape, on choisit deux indices distincts $1 \leqslant i, j \leqslant k$, et on multiplie, au choix, g_i à droite ou à gauche par g_j ou par g_j^{-1}, avec égale probabilité, en laissant les autres générateurs invariants.*

On a donc $4k(k-1)$ opérations de base :

$$\begin{aligned} R_{ij}^{\pm} &: (g_1, \ldots, g_i, \ldots, g_k) \mapsto (g_1, \ldots, g_i g_j^{\pm 1}, \ldots, g_k) \\ L_{ij}^{\pm} &: (g_1, \ldots, g_i, \ldots, g_k) \mapsto (g_1, \ldots, g_j^{\pm 1} g_i, \ldots, g_k) \end{aligned}$$

qu'on choisit, à chaque étape, avec probabilité égale.

Notons que si l'on part d'un k-uplet générateur, on obtient encore un k-uplet générateur.

Ces opérations définissent un graphe $\Gamma_k(G)$ dont les sommets sont tous les k-uplets générateurs de G, et dont les arêtes correspondent aux mouvements de base. Le PRA est alors simplement la marche aléatoire sur ce graphe.

On appellera *PRA paresseux* l'algorithme consistant à suivre une marche aléatoire paresseuse dans ce graphe (ne rien faire la moitié du temps).

Maintenant, l'algorithme consiste à itérer un grand nombre de fois ces transformations, et à renvoyer un élément au hasard (mettons le premier) parmi le k-uplet obtenu.

Le premier problème qui se pose est celui de l'évaluation de la convergence. D'après la proposition 4, on sait que la loi du k-uplet obtenu au temps t converge exponentiellement vers la loi uniforme sur les k-uplets générateurs situés dans la composante connexe du k-uplet de départ. Il s'agit donc, d'une part, d'évaluer le trou spectral du graphe $\Gamma_k(G)$, pour connaître la vitesse de convergence. Ce sera l'objet du théorème final, pour G abélien. L'évaluation fera intervenir de manière cruciale la propriété de Kazhdan de $SL_k(\mathbb{Z})$. D'autre part, reste un problème de connexité. Une construction assez explicite (cf.[B]) montre que si $k \geqslant 2\log_2|G|$, le graphe du PRA est connexe : on peut passer d'un k-uplet générateur à n'importe quel autre.

Le second problème est le suivant : on obtient, en sortie de l'algorithme, un k-uplet générateur uniformément choisi parmi tous les k-uplets générateurs de G. Il n'est pas sûr qu'en prenant un élément dans ce k-uplet, on obtienne un élément uniformément réparti dans G : la répartition des éléments composant un k-uplet générateur est biaisée. Par exemple, l'élément neutre apparaît moins souvent qu'un autre dans un k-uplet générateur pris au hasard.

Quantifions. Soit $X \subset G^k$ l'ensemble des k-uplets générateurs de G. Soient U_k la mesure de probabilité uniforme sur G^k, et U_X la mesure de probabilité uniforme sur X. Soit p la première projection de G^k sur G, et soit $U = p.U_k$ la mesure uniforme sur G. Si l'on attend assez longtemps, l'algorithme rend un k-uplet générateur de loi π que l'on espère proche de U_X. En prenant au final le premier élément de ce k-uplet, on obtient un élément distribué selon $p.\pi$. Alors :

$$\begin{aligned}
|p.\pi - U| &\leqslant |\pi - U_k| \\
&\leqslant |\pi - U_X| + |U_X - U_k| \\
&= |\pi - U_X| + \frac{1}{2}\left(\sum_{x\in X}\left|\frac{1}{|X|} - \frac{1}{|G|^k}\right| + \sum_{x\in G^k\setminus X}\frac{1}{|G|^k}\right) \\
&= |\pi - U_X| + \left(1 - \frac{|X|}{|G|^k}\right)
\end{aligned}$$

Le problème est donc d'évaluer la proportion de k-uplets qui sont générateurs. Donnons une évaluation très simple, qui peut être raffinée :

Proposition 6 – *Si $k \geqslant 2N(1+\log_2|G|)$, alors un k-uplet d'éléments de G choisi au hasard est générateur avec probabilité supérieure à $1 - 1/2^N$ (N est un entier).*

Démonstration – L'idée de base est la suivante : un sous-groupe strict est d'indice au moins deux. Si $g_1, \ldots, g_i$ sont des éléments de G qui engendrent un sous-groupe H_i non égal à G, un élément pris au hasard dans G appartient donc à H_i avec probabilité inférieure à $1/2$. En ajoutant un élément au hasard à un tel système, on passe donc à un sur-groupe $H_{i+1} \supsetneq H_i$ avec probabilité supérieure à $1/2$. Le cardinal de H_{i+1} est, pour la même raison, au moins le double de celui de H_i.

Par conséquent, en prenant des éléments au hasard, avec probabilité supérieure à $1/2$ à chaque étape on double au moins la taille du sous-groupe engendré, tant qu'on n'a pas atteint tout G. Si on tire k éléments, il suffit donc de faire $1 + \log_2 |G|$ bons tirages parmi ces k. Si $k = 2(1 + \log_2 |G|)$, la probabilité d'avoir fait $1 + \log_2 |G|$ bons tirages est supérieure à $1/2$. En faisant $2N(1 + \log_2 |G|)$ tirages, la probabilité de ne pas avoir fait assez de bons tirages est inférieure à $1/2^N$, d'où le résultat. □

La même veine de raisonnement montre aussi qu'un système générateur minimal de G ne peut pas avoir plus de $1 + \log_2 |G|$ éléments.

Reste donc le problème de la convergence vers l'équilibre du PRA, qui est traité ensuite dans le cas des groupes abéliens.

3.2 Propriété de Kazhdan et PRA

On va exploiter la propriété de Kazhdan d'un certain groupe agissant sur le graphe du PRA pour en déduire une minoration du trou spectral de ce graphe.

La remarque fondamentale est qu'un mouvement de base du PRA correspond à un automorphisme du groupe libre à k éléments. Ainsi, on peut faire agir un sous-groupe A de $\mathrm{Aut}(F_k)$ sur le graphe $\Gamma_k(G)$ des k-uplets générateurs du groupe G considéré. Si le sous-groupe A est de Kazhdan, alors d'après les raisonnements ci-dessus, on pourra contrôler la vitesse de convergence de la marche aléatoire sur $\Gamma_k(G)$.

Malheureusement, on ne sait pas si $\mathrm{Aut}(F_k)$ est de Kazhdan. Cependant, si le groupe G est commutatif, l'action se factorise en une action de $SL_k(\mathbb{Z})$, qui, lui, est de Kazhdan pour $k \geqslant 3$. C'est le résultat que nous énoncerons.

Explicitons. Considérons par exemple le mouvement R_{ij}^+ du PRA qui passe de $(g_1, \ldots, g_i, \ldots, g_k)$ à $(g_1, \ldots g_i g_j, \ldots, g_k)$. On lui associe un morphisme a_{Rij+} de F_k dans lui-même de la manière suivante : si F_k est engendré par $a_1, \ldots, a_k$, le morphisme est celui qui associe $a_i a_j^{-1}$ à a_i et laisse invariants les autres générateurs (on met un inverse pour obtenir une action à gauche plus tard). Comme le k-uplet obtenu est à nouveau générateur, ce morphisme est bijectif.

Maintenant, soit $A^+ \subset \mathrm{Aut}(F_k)$ le sous-groupe engendré par ces automorphismes. On considère un groupe fini G, ainsi que le graphe $\Gamma_k(G)$ associé.

Chaque arête de ce graphe correspond à un mouvement du PRA, définissant lui-même un élément $a \in A^+$. Ceci définit une action des générateurs de A^+ sur le graphe $\Gamma_k(G)$, consistant, pour un générateur, à suivre les arêtes correspondantes.

Vérifions que suivre deux arêtes de suite revient bien à composer les automorphismes de F_k associés à ces arêtes. En termes plus algébriques, un k-uplet générateur de G est un morphisme surjectif de F_k sur G, $(g_1, \dots, g_k)$ s'identifiant à $(a_1, \dots, a_k) \mapsto (g_1, \dots g_k)$. $\Gamma_k(G)$ s'identifie donc à $\mathrm{Epi}(F_k, G)$. De plus $\mathrm{Aut}(F_k)$ agit sur $\mathrm{Epi}(F_k, G)$ par $\alpha.\varphi = \varphi \circ \alpha^{-1}$, pour $\alpha \in \mathrm{Aut}(F_k), \varphi \in \mathrm{Epi}(F_k, G)$: c'est bien une action à gauche, respectant la composition. Les mouvements du PRA correspondent, pour cette action, à des éléments $s_i, i = 1 \dots 4k(k-1)$ de $\mathrm{Aut}(F_k)$, explicités ci-dessus, qui engendrent un sous-groupe A^+.

Cette action de A^+ sur le graphe $\Gamma_k(G)$ se transpose directement en une représentation de A^+ dans $L^2(\Gamma_k(G))$ par $s_i.f(x) \mapsto f(s_i^{-1}.x)$. Chaque mouvement du PRA étant inversible, l'action est bijective sur les points du graphe, et donc cette représentation est isométrique.

Par définition, l'action A^+ est transitive sur chacune des composantes connexes de $\Gamma_k(G)$. Une fonction de $L^2(\Gamma_k(G))$ ne peut donc être invariante que si elle est constante sur chaque composante connexe.

On se restreint désormais à une composante connexe C de $\Gamma_k(G)$. De plus, on s'intéresse à $L^2(C) \ominus \mathbb{C}$, i.e. on enlève les fonctions constantes (ou encore, on se restreint aux fonctions de moyenne nulle). Ceci nous laisse une représentation de A^+ sans vecteurs invariants.

Soit π cette représentation. Soit $h = \dfrac{1}{4k(k-1)} \sum \pi(s_i)$ défini comme à la section 2.2. Soit κ la constante de Kazhdan de A^+. Si A^+ est de Kazhdan, on a $\kappa > 0$.

La proposition de la section 2.2 donne alors que les valeurs propres de h sont éloignées de 1 d'au moins $\kappa^2/8k(k-1)$. Or, comme les arêtes du graphe correspondent exactement aux générateurs s_i de A^+, l'opérateur h n'est autre que l'opérateur de la marche aléatoire sur le graphe. En passant à la marche aléatoire paresseuse pour éviter les problèmes d'oscillation, et en reprenant les notations ci-dessus pour le PRA, on a donc démontré que :

$$|\pi_t - U| \leqslant |G|^{k/2} \left(1 - \frac{\kappa^2}{16k(k-1)}\right)^t$$

Fort malheureusement, on ne sait pas si le groupe $A^+ \subset \mathrm{Aut}(F_k)$ ainsi défini est de Kazhdan.

Par contre, ce raisonnement se transpose dans le cas où le groupe G est abélien, en remplaçant le groupe libre F_k par son analogue abélien $\mathbb{Z}^k$. Dans ce cas, on a $\mathrm{Aut}(\mathbb{Z}^k) = GL_k(\mathbb{Z})$.

Alors le groupe A^+ est remplacé par $SL_k(\mathbb{Z})$. En effet, sur $\mathbb{Z}^k$, un mouvement du PRA revient à ajouter (ou soustraire) le j-ième générateur au i-ième ; la matrice d'une telle transformation linéaire de $\mathbb{Z}^k$ est la diagonale plus un 1 en position (i, j). Ces telles matrices engendrent $SL_k(\mathbb{Z})$.

Or ce groupe est de Kazhdan pour $k \geqslant 3$. Mieux, on connaît (théorème 1) une estimation de la constante de Kazhdan κ pour ce système de générateurs : il existe une constante C telle que $\kappa \geqslant C/k^2$ pour $k \geqslant 3$.

On a ainsi démontré :

Théorème 4 (A. Lubotzky, I. Pak) – *Soient G un groupe commutatif fini engendré par $(g_1, \ldots, g_k)$, $k \geqslant 3$, et soit π_t la loi du k-uplet générateur obtenu par application de t étapes du PRA paresseux. Soit U la mesure uniforme sur la composante connexe de $(g_1, \ldots, g_k)$ dans le graphe du PRA. Il existe une constante C indépendante de G et k telle que*

$$|\pi_t - U| \leqslant |G|^{k/2} \left(1 - \frac{C}{k^6}\right)^t$$

En particulier, le temps de relaxation est de l'ordre de $k^7 \log |G|$.

Le principal point à noter est la dépendance logarithmique en $|G|$ du temps de relaxation. L'exposant de k n'est pas optimal. L'évaluation croît avec k, ce qui est normal puisqu'on demande la convergence dans un graphe plus grand.

Enfin, la restriction à une composante connexe peut être contournée quand on sait (cf. [B]) que pour $k \geqslant 2 \log_2 |G|$, le graphe du PRA est connexe.

Références

[B] L. Babai, *Randomization in group algorithms : conceptual questions*, in *Groups and computation II*, édité par L. Finkelstein et W. M. Kantor, DIMACS series **28**, AMS, Providence, 1997.

[GH] *Sur les Groupes hyperboliques d'après Mikhael Gromov*, édité par É. Ghys et P. de la Harpe, Progress in Math. **83**, Birkhäuser, Boston (1990).

[Gr] M. Gromov, *Hyperbolic groups*, in *Essays in group theory*, édité par S. M. Gersten, M.S.R.I. Publ. **8**, Springer (1987), p. 75–263.

[HV] P. de la Harpe, A. Valette, *La propriété (T) de Kazhdan pour les groupes localement compacts*, Astérisque **175**, SMF (1989).

[HRV] P. de la Harpe, A. G. Robertson, A.Valette, *On the spectrum of the sum of generators for a finitely generated group*, Israel J. Math. **81** (1993), p. 65–96.

[Sh] Y. Shalom, *Bounded generation and Kazhdan's property (T)*, Publ. Math. IHÉS **90** (1999), p. 145–168.