Présentation

Le point commun aux travaux recueillis ici est l'interaction entre géométrie et probabilités. Cette interaction se décline principalement en deux variantes. Dans l'une, on munit un espace géométrique d'une mesure de probabilité « naturelle » en rapport avec sa géométrie, et on se demande ensuite quelles sont les propriétés géométriques « typiques » dans cet espace, c'est-à-dire celles qui seront réalisées avec une probabilité très proche de 1. Dans l'autre, on utilise les probabilités pour accéder à certains éléments de l'espace, soit « typiques » (par exemple en effectuant une marche aléatoire dans l'espace), soit au contraire répondant à des propriétés très particulières (on montre un théorème d'existence en prouvant qu'une certaine construction aléatoire fournit l'objet voulu avec probabilité strictement positive).

Sharp phase transition theorems for hyperbolicity of random groups, *Growth and cogrowth of generic groups*, *Concentrated spaces seen as product spaces*, *Concentration spectrale dans les graphes* relèvent du premier point de vue ; *Vitesse de convergence des opérateurs de croisement*, *Un algorithme génétique dans l'espace des arbres*, *La démographie du PRA*, du second.

Les résultats principaux de cette thèse sont les trois théorèmes sur les groupes aléatoires présentés dans *Sharp phase transition theorems for hyperbolicity of random groups*. Nous donnons ci-dessous une introduction, destinée aux non-spécialistes, à la théorie des groupes aléatoires.

Growth and cogrowth of generic groups résout une question qui se posait naturellement au vu des théorèmes du texte précédent. Elle concerne la croissance et la cocroissance des groupes aléatoires et étend un théorème de Champetier [Ch], et peut simplifier certains aspects de la démonstration du texte [Gro4] de Gromov. Certaines parties de ce texte ne sont encore qu'ébauchées.

On a small cancellation theorem of Gromov, le seul texte entièrement déterministe de ce recueil, donne une démonstration élémentaire d'un théorème annoncé par Gromov dans [Gro4], qui étend la théorie ordinaire de la petite simplification et est à la base de la construction par Gromov de groupes dont le graphe de Cayley contient une famille d'expanseurs. Ce texte ne fait donc que donner une démonstration combinatoire d'un résultat de [Gro4].

Le court *Concentrated spaces seen as product spaces* est une étude en cours sur le lien entre espaces concentrés et espaces produits (voir plus bas une introduction à cette problématique). Il est bien connu que les espaces produits sont

concentrés. Nous obtenons un début de réciproque : sur un espace concentré, on peut trouver une ébauche de structure produit. Ce résultat n'est que le commencement d'une recherche et peut très probablement être amélioré.

Concentration spectrale dans les graphes est un texte plus ancien. Il applique des méthodes connues en concentration de la mesure à un cas apparemment non traité dans la littérature mais ne présentant pas de difficulté particulière.

Les textes de la section « Autour des algorithmes génétiques » sont nettement plus anciens. *Vitesse de convergence des opérateurs de croisement* se rapproche de la biologie des populations en étudiant la vitesse du brassage des gènes introduit par la reproduction sexuée, et résout une question posée dans [RRS]. *Un algorithme génétique dans l'espace des arbres* décrit une tentative pour résoudre le problème de la reconstitution phylogénétique à l'aide d'un algorithme génétique explorant l'espace des arbres sur un ensemble de feuilles fixé, faisant intervenir un croisement d'arbres. Enfin, *La démographie du PRA* contient quelques résultats simples sur un procédé utilisé en théorie algorithmique des groupes, le « PRA », résultats inspirés par la ressemblance entre ce procédé et un algorithme génétique.

* * *

1 Groupes hyperboliques et groupes aléatoires

1.1 L'intérêt des groupes aléatoires

La théorie (si l'on peut déjà lui accorder ce nom) des groupes aléatoires s'intéresse aux propriétés d'un groupe « typique ». Il faut bien sûr commencer par donner un sens précis à cette expression.

Notons qu'outre son intérêt propre consistant à décrire les propriétés les plus fréquentes des groupes, cette théorie a déjà servi à construire un groupe aux propriétés inhabituelles répondant à une question ouverte (cf. [Gro4]). Pour un exposé général, on pourra consulter le texte du récent séminaire Bourbaki consacré à ces questions, par Étienne Ghys, [Gh].

Nous nous intéresserons ici aux groupes discrets engendrés par un nombre fini m de générateurs (et leurs inverses), disons $a_1^{\pm 1}, \ldots, a_m^{\pm 1}$. Tout tel groupe peut être vu comme un quotient du groupe libre F_m à m générateurs par un ensemble de relations R. Se donner un groupe au hasard, c'est simplement se donner l'ensemble R définissant le groupe au hasard.

On est donc ramené à se donner au hasard des mots en les $a_1^{\pm 1}, \ldots, a_m^{\pm 1}$. Une longueur de mots ℓ étant choisie, le plus simple consiste ensuite à choisir les mots uniformément parmi tous les mots de longueur ℓ en les générateurs. En fait, on peut toujours supposer que les relations apparaissant dans R sont des mots *réduits* (c'est-à-dire ne contenant pas de séquence $a_i a_i^{-1}$ ou $a_i^{-1} a_i$), et il est donc plus naturel de choisir nos mots aléatoires uniformément parmi l'ensemble des $(2m)(2m-1)^{\ell-1}$ mots réduits de longueur ℓ.

Ces choix étant faits, le modèle de groupe aléatoire ne dépend plus que du nombre de mots que l'on prend : plus l'ensemble de relateurs est grand, plus le groupe sera petit. Le modèle dit *à densité*, introduit par M. Gromov (cf. [Gro2]), s'est révélé extrêmement fécond et semble être la bonne manière d'évaluer la « taille » de l'ensemble R.

MODÈLE À DENSITÉ – *Choisir un nombre d entre 0 et 1. Se donner une longueur de mots ℓ très grande. Poser $N = (2m-1)^{d\ell}$. Pour l'ensemble de relations R, tirer N fois de suite (indépendamment) un mot réduit au hasard uniformément parmi les $(2m)(2m-1)^{\ell-1}$ mots réduits possibles.*

Si l'on veut pouvoir appliquer des théorèmes de probabilités, comme des lois des grands nombres, il est nécessaire d'avoir un paramètre tendant vers l'infini. C'est la raison pour laquelle on prend ℓ grand.

Comme $(2m)(2m-1)^{\ell-1}$ est presque égal à $(2m-1)^{\ell}$, on voit que ce modèle consiste à prendre un nombre N de mots égal au nombre total de mots, à la puissance d. L'exposant $d\ell$ est à interpréter comme une dimension, à savoir la dimension de l'ensemble R qu'on va tirer. En effet, la dimension d'un ensemble peut être vue comme le nombre d'équations qu'on peut s'imposer, de manière à ce que, génériquement, il existe un élément de cet ensemble vérifiant ces équations. C'est précisément ce qui se passe ici, pour la bonne notion d'« équation ». Pour des mots en certaines lettres, une équation sera de la forme « imposer la k-ième lettre du mot ». Si on se donne L équations imposant les L premières lettres d'un mot réduit, la probabilité qu'un mot réduit choisi au hasard les satisfasse est $1/(2m)(2m-1)^{L-1}$ soit environ $1/(2m-1)^{L}$. Pour un ensemble de N mots choisis au hasard, la probabilité qu'un mot au moins satisfasse les équations imposées sera donc non négligeable si N est de l'ordre de $(2m-1)^{L}$. On voit donc que pour $N = (2m-1)^{d\ell}$, on peut imposer $d\ell$ « équations » à un mot de l'ensemble.

L'intérêt du modèle à densité est justifié par le théorème suivant, dû à M. Gromov (cf. [Gro2]) :

THÉORÈME 1 : TRANSITION DE PHASE POUR LES GROUPES ALÉATOIRES – *Soit R un ensemble de relations aléatoires tirées selon le modèle à densité, et soit $G = F_m/\langle R\rangle$ le groupe aléatoire ainsi défini.*

Si $d < 1/2$, la probabilité que G soit infini et hyperbolique tend vers 1 lorsque $\ell \to \infty$.

Si $d > 1/2$, le groupe G est soit $\{e\}$ soit $\mathbb{Z}/2\mathbb{Z}$, avec probabilité tendant vers 1 quand $\ell \to \infty$.

Selon la densité de l'ensemble de relations, on a donc une transition de phase extrêmement précise entre des groupes infinis (dont on connaît aussi d'autres caractéristiques) et des groupes triviaux. Ce qui se passe à la densité critique $1/2$ est pour le moment totalement inconnu.

L'occurrence possible de $\mathbb{Z}/2\mathbb{Z}$ ne doit pas surprendre : si ℓ est pair, on ne met que des relations de longueur paire et donc le quotient est au moins $\mathbb{Z}/2\mathbb{Z}$.

Avant de rappeler ce qu'est un groupe hyperbolique, donnons une esquisse de preuve de la partie triviale du théorème.

Prendre $d > 1/2$ revient à prendre pour R un nombre de mots supérieur à la racine carrée du nombre total de mots possibles. Il est élémentaire et bien connu (lemme des anniversaires ou principe des tiroirs probabiliste) que si l'on tire N objets parmi moins de N^2 objets (pour N grand), avec grande probabilité on tire deux fois le même objet. Ceci signifie que dans R on rencontre deux fois le même relateur. Cela peut aussi s'interpréter en termes de dimension comme ci-dessus : la dimension de R est $d\ell$, la dimension des couples d'éléments de R est $2d\ell$, et imposer l'égalité de deux mots de longueur ℓ revient à poser ℓ équations ; « donc », si $2d\ell > \ell$, on a une chance que ces équations soient satisfaites par un couple.

Par un raisonnement analogue en n'imposant que $\ell - 1$ équations, on obtient aussi que, dans R, se rencontrent probablement deux mots $r_1 = xa_i$ et $r_2 = xa_j$ où x est un mot de longueur $\ell - 1$ et où a_i et a_j sont deux générateurs. Dans le groupe quotient $G = F_m/\langle R \rangle$, cela signifie que $xa_i = e$ et $xa_j = e$. Ceci implique $a_i = a_j$: les deux générateurs sont devenus égaux. Comme $d > 1/2$ cette situation se produit même une infinité de fois (pour ℓ grand), avec i et j tirés au hasard ; et donc, dans le groupe G, tous les couples de générateurs ainsi que leurs inverses sont égaux... il est alors facile de voir que G est soit $\{e\}$ soit $\mathbb{Z}/2\mathbb{Z}$.

1.2 Groupes hyperboliques

Il peut être utile de rappeler ce qu'est un groupe hyperbolique.

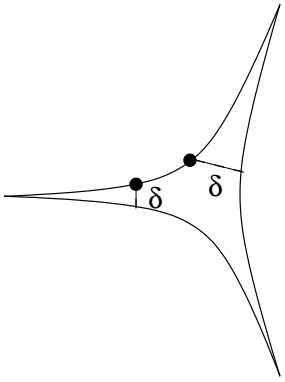
Soit G un groupe engendré par les éléments $a_1, \ldots, a_m$. Le *graphe de Cayley* de G (pour ce système générateur) est le graphe dont les sommets sont tous les éléments de G, et dont les arêtes correspondent à la multiplication à droite par l'un des générateurs $a_1, \ldots, a_m$. Par exemple, le graphe de Cayley de $\mathbb{Z}/n\mathbb{Z}$ est un cycle à n arêtes. Puisque les générateurs engendrent le groupe, ce graphe est connexe.

Le graphe de Cayley est naturellement un espace métrique : il suffit de décréter que chaque arête est de longueur 1.

Une *géodésique* entre deux points dans le graphe de Cayley est un chemin de longueur minimale (un tel chemin n'est pas nécessairement unique). Un *triangle* est la donnée de trois points du graphe de Cayley, ainsi que de trois géodésiques reliant ces points deux à deux qu'on appellera *côtés* du triangle.

DÉFINITION : TRIANGLES δ-FINS – *Soit δ un nombre positif. On dit qu'un triangle est* δ-fin *si, pour tout point sur un côté du triangle, ce point est à distance au plus δ de l'un des deux autres côtés.*

Intuitivement, cela signifie que le triangle est très aplati, et que l'espace laissé au milieu est de largeur environ δ.



DÉFINITION : GROUPES HYPERBOLIQUES – *Un groupe est dit* hyperbolique *s'il existe un nombre $\delta \geqslant 0$ tel que tous les triangles du graphe de Cayley sont δ-fins.*

C'est un théorème non trivial que l'hyperbolicité d'un groupe ne dépend pas du système générateur choisi (dont dépend le graphe de Cayley).

Cette définition n'est pas spécifique aux groupes : elle a un sens dans tout espace métrique où des géodésiques existent. La terminologie est justifiée par les deux faits suivants : le plan hyperbolique standard est hyperbolique (!!) ; et le groupe fondamental d'une variété hyperbolique compacte est hyperbolique.

Par exemple, dans un arbre tous les triangles sont 0-fins ; donc, les groupes libres, dont le graphe de Cayley (pour le système de générateurs standard) est un arbre, sont des groupes hyperboliques. Les groupes hyperboliques sont les groupes dont le graphe de Cayley, « vu de loin », ressemble à un arbre (en un sens très précis) ; ce sont donc des groupes qui, « vus de loin », ressemblent à des groupes libres.

Les groupes hyperboliques ont été introduits par M. Gromov dans [Gro1] et leur intérêt ne s'est pas démenti depuis. Pour plus de renseignements on pourra consulter l'excellent [GH].

Donnons une caractérisation très utile des groupes hyperboliques. Lorsqu'un groupe G engendré par $a_1^{\pm 1}, \ldots, a_m^{\pm 1}$ est défini par un ensemble de relateurs R, tout mot w en les générateurs représentant l'élément neutre de $G = F_m/\langle R\rangle$ est un élément de $\langle R\rangle$, c'est-à-dire qu'il s'écrit comme un produit de conjugués d'éléments de R ou de leurs inverses :

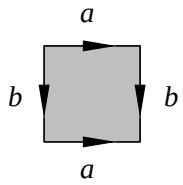
$$w = e \text{ dans } G \Leftrightarrow w = \prod u_i r_i^{\pm 1} u_i^{-1},\ r_i \in R$$

l'égalité ayant lieu dans le groupe libre (c'est-à-dire modulo les simplifications $a_i a_i^{-1}$).

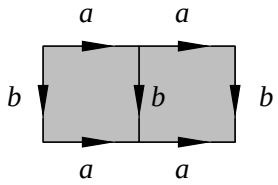
Une question naturelle qui se pose alors est : en présence d'un mot dont on sait qu'il représente l'élément neutre, combien de relateurs r_i comporte, au minimum, une telle décomposition ? Un des premiers faits de la théorie des groupes hyperboliques est le suivant.

PROPOSITION – *Un groupe $G = \langle a_1, \ldots, a_m \mid R \rangle$ est hyperbolique si et seulement s'il existe une constante C telle que pour tout mot w de longueur L représentant l'élément neutre de G, w peut s'écrire comme un produit d'au plus $C.L$ conjugués de relateurs.*

Il existe une interprétation géométrique de ces produits de conjugués de relateurs. Étant donné une présentation de groupe $G = \langle a_1, \ldots, a_m \mid R \rangle$, pour chaque relateur $r \in R$ (supposé réduit), de longueur L_r, on définit un *relateur géométrique* comme un disque bordé par L_r arêtes, chaque arête portant un générateur a_i comme suit : la k-ième arête porte le générateur correspondant à la k-ième lettre de r (on met une orientation inverse sur l'arête si la k-ième lettre de r est a_i^{-1}). Voici par exemple le relateur géométrique associé au relateur $aba^{-1}b^{-1}$.



On peut former des puzzles avec ces relateurs géométriques, où l'on s'autorise à recoller deux relateurs géométriques le long d'arêtes identiques (on peut aussi utiliser les relateurs inverses). Cela définit un *diagramme de van Kampen*. Van Kampen a prouvé qu'un mot (réduit) représente l'élément neutre dans G si et seulement si ce mot peut être lu sur le bord d'un diagramme de van Kampen. Voici par exemple une preuve que si a et b commutent, alors a^2 et b commutent.



Les diagrammes de van Kampen sont liés aux produits de conjugués de relateurs de la manière suivante : choisir un point-base dans le diagramme, suivre un chemin jusqu'à un premier relateur, faire le tour du relateur, revenir au point-base, suivre un chemin jusqu'à un deuxième relateur, en faire le tour, revenir au point-base, etc. On décrit alors un mot de la forme $\prod u_i r_i^{\pm 1} u_i^{-1}$, les u_i correspondant aux trajets entre le point-base et les relateurs.

Cet outil est à la base des théorèmes d'hyperbolicité des groupes aléatoires. Nous sommes désormais en mesure de donner l'idée de la démonstration de la partie non triviale du Théorème 1.

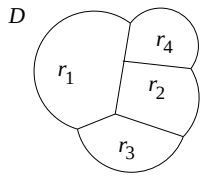
L'hyperbolicité d'un groupe dit que tout mot w représentant l'élément neutre peut être écrit comme un produit d'au plus $C.L$ relateurs où L est la longueur de w. Cela signifie qu'il existe un diagramme de van Kampen D le long du bord

duquel on lit w, et vérifiant l'inégalité isopérimétrique suivante entre son bord et son nombre de faces :

$$|\partial D| \geqslant |D| / C$$

Pour prouver l'hyperbolicité d'un groupe, il suffit donc de prouver que ses diagrammes de van Kampen satisfont une telle inégalité isopérimétrique linéaire (comparer avec l'inégalité isopérimétrique bien connue dans le plan qui lie le *carré* de la longueur du bord d'une figure à sa surface).

Revenant aux groupes aléatoires, considérons donc une présentation $G = \langle a_1, \ldots, a_m \mid R \rangle$ où R est un ensemble aléatoire de relations obtenu selon le modèle à densité. Soit D un diagramme de van Kampen pour cette présentation.



Considérons deux relateurs r_i, r_j de ce diagramme recollés sur une longueur L_{ij}. Comme ces relateurs sont choisis au hasard, la probabilité qu'un tel recollement puisse avoir lieu est $1/(2m-1)^{L_{ij}}$. Si tous les relateurs présents dans le diagramme sont distincts, donc choisis indépendamment, la probabilité d'un tel diagramme est donc $1/(2m-1)^L$ où L est la longueur interne totale du diagramme. (Traiter les relateurs apparaissant plusieurs fois est plus délicat car cela fait perdre de l'indépendance.)

Maintenant, le nombre de choix pour les $|D|$ relateurs du diagramme parmi les $|R|$ relateurs de la présentation est $|R|^{|D|} = (2m-1)^{d\ell|D|}$ par définition du modèle à densité. La probabilité d'existence d'un tel diagramme de van Kampen est donc inférieure à $(2m-1)^{d\ell|D|-L}$ où L est la longueur interne totale.

Mais la longueur du bord du diagramme est $|\partial D| = \ell\,|D| - 2L$ (sommer les longueurs des faces et enlever deux fois les longueurs des recollements). Maintenant, pour que la probabilité d'existence du diagramme ne soit pas petite (plus précisément, pas exponentiellement décroissante en ℓ), on doit avoir $L \leqslant d\ell\,|D|\,(1+\varepsilon)$ d'après notre majoration de cette probabilité. Mais alors :

$$|\partial D| = \ell\,|D| - 2L \geqslant \ell\,|D|\,(1 - 2d - 2\varepsilon)$$

ce qui donne l'inégalité isopérimétrique souhaitée si $d < 1/2$ (en prenant par exemple $\varepsilon = (1-2d)/4$). Autrement dit : soit un diagramme de van Kampen vérifie l'inégalité isopérimétrique, soit la probabilité que des relateurs aléatoires le forment décroît comme $(2m-1)^{-\varepsilon\ell}$.

Ceci ne concerne qu'un seul diagramme possible, alors qu'il y en a une infinité. Mais un théorème profond de géométrie hyperbolique (théorème de Cartan-Hadamard-Gromov), qui affirme que l'hyperbolicité est un phénomène « semi-local », permet de ne tester l'inégalité isopérimétrique que sur un nombre fini de diagrammes. Le Théorème 1 est donc démontré.

1.3 Transitions de phase pour les quotients aléatoires

On va désormais s'intéresser à des généralisations du Théorème 1. Ce dernier affirme qu'un groupe aléatoire, autrement dit un quotient aléatoire d'un groupe libre, est hyperbolique. On peut se demander si un quotient aléatoire d'un groupe hyperbolique reste hyperbolique. Ceci est d'autant plus vraisemblable que, au sens ci-dessus, un groupe hyperbolique ressemble à un groupe libre.

Ce résultat constitue le théorème principal de *Sharp phase transition theorems for hyperbolicity of random groups*. On rappelle qu'un groupe est *sans torsion* s'il n'existe pas d'élément x (à part e) tel qu'il existe un entier $n > 1$ avec $x^n = e$. Un groupe hyperbolique est dit *élémentaire* s'il est fini ou s'il contient un sous-groupe d'indice fini isomorphe à $\mathbb{Z}$ (l'analyse des quotients aléatoires de tels groupes élémentaires est facile).

THÉORÈME 2 : TRANSITION DE PHASE POUR LES QUOTIENTS ALÉATOIRES – *Soit G_0 un groupe hyperbolique sans torsion et non élémentaire, engendré par les éléments $a_1, \dots, a_m$. Soit $0 \leqslant d \leqslant 1$ une densité et soit R un ensemble de relations aléatoires tirées selon le modèle à densité. Soit $G = G_0/\langle R \rangle$ le quotient aléatoire. Il existe une densité critique d_0 (dépendant de G_0) ayant la propriété suivante.*

Si $d < d_0$, alors le quotient aléatoire G est infini et hyperbolique avec probabilité tendant vers 1 quand $\ell \to \infty$.

Si $d > d_0$, alors le quotient aléatoire G est $\{e\}$ ou $\mathbb{Z}/2\mathbb{Z}$ avec probabilité tendant vers 1 quand $\ell \to \infty$.

Sur l'hypothèse « sans torsion » : on connaît une hypothèse moins restrictive, légèrement plus compliquée, et qui est nécessaire et suffisante pour que le théorème soit vrai. On a aussi une idée relativement claire de ce qui se passe lorsque cette hypothèse n'est pas vérifiée.

De plus, on sait caractériser explicitement la densité critique d_0 en fonction de G_0 : on a $d_0 = 1 - \eta$ où η est la *cocroissance* du groupe G_0, notion introduite par R. Grigorchuk dans [Gri]. La cocroissance d'un groupe est l'exposant de croissance du nombre de mots réduits représentant l'élément neutre du groupe.

Plus précisément, soit L une longueur paire et soit W_L l'ensemble des mots réduits en les générateurs $a_1^{\pm 1}, \dots, a_m^{\pm 1}$ qui sont égaux à e dans le groupe G_0. La cocroissance de G_0 par rapport à ce système de générateurs est

$$\eta = \lim_{\substack{L \to \infty \\ L \text{ pair}}} \frac{1}{L} \log_{2m-1} \#W_L$$

On peut montrer que la limite existe. Cette définition n'a pas de sens pour un groupe libre (W_L est vide), mais une formule liant en général la cocroissance et le rayon spectral du laplacien sur le graphe de Cayley du groupe permet de conclure que $\eta(F_m) = 1/2$, ce qui est en accord avec le fait que le Théorème 2 généralise le Théorème 1.

Dans un groupe libre, la notion de mot réduit coïncide avec celle de *mot géodésique* (de longueur minimale parmi les mots représentant le même élément). Ce n'est pas le cas dans un groupe hyperbolique quelconque. Il est donc naturel de se demander comment se comportent des quotients aléatoires par des mots géodésiques plutôt que réduits. Il se trouve que dans ce cas, la densité critique est $1/2$ pour tout groupe, mais le théorème est légèrement plus compliqué à énoncer.

Il existe aussi une troisième variante de ce théorème dans laquelle on prend des mots quelconques plutôt que réduits ou géodésiques. Ces trois variantes sont trois cas particuliers d'un théorème plus général qui contrôle les quotients aléatoires par des éléments tirés selon une mesure sur le groupe vérifiant une liste de quatre axiomes naturels mais difficiles à exprimer simplement.

1.4 Autres résultats sur les groupes aléatoires, questions en suspens

Bien d'autres propriétés des groupes aléatoires sont connues. Par exemple, au vu du théorème ci-dessus, on peut naturellement se demander quel sort subit la cocroissance lors d'un quotient aléatoire. La réponse, fournie dans *Growth and cogrowth of generic groups*, est que la cocroissance d'un quotient aléatoire est arbitrairement proche (pour ℓ assez grand) de celle du groupe de départ. Appliqué en particulier aux quotients aléatoires d'un groupe libre, ceci donne que, génériquement, la cocroissance d'un groupe aléatoire est très proche de $1/2$. Outre son intérêt propre, ce résultat simplifie le problème des quotients aléatoires successifs utilisés dans [Gro4], où le contrôle de la cocroissance des quotients successifs est obtenu par la voie détournée de la propriété T.

Mentionnons quelques thèmes étudiés en rapport avec les groupes aléatoires. La petite simplification, les éléments de torsion, la topologie du bord, la propriété T, les sous-groupes libres, la planarité du graphe de Cayley... ont été étudiés. Donnons quelques noms, outre bien sûr Gromov : Arzhantseva, Champetier, Cherix, I. Kapovich, Ol'shanskiĭ, Schupp, Schpilrain, Żuk...

Ces travaux concernent l'étude des propriétés génériques des groupes pour elles-mêmes, mais elles ont aussi des applications non probabilistes. Ainsi du dénombrement *à isomorphisme près* des groupes à un relateur, obtenu par I. Kapovich, Schupp et Schpilrain à l'aide de considérations de généricité. Ou encore, de la construction par Gromov d'un groupe dont le graphe de Cayley contient une famille d'expanseurs, ce qui a des applications en théorie des opérateurs (conjecture de Baum-Connes). Les implications de la construction ne sont pas encore bien comprises.

Dans tous ces travaux, l'hyperbolicité est omniprésente.

Une autre approche sur les groupes génériques, topologique plutôt que probabiliste, a été développée par Champetier. Là encore l'hyperbolicité est fondamentale. Cette approche a des liens importants avec la théorie du premier ordre des groupes développée entre autres par Sela. On pourra consulter le récent

séminaire Bourbaki par Frédéric Paulin sur ces sujets ([Pau]).

Donnons enfin quelques pistes de recherche suggérées par l'étude des groupes aléatoires. Commençons par deux thèmes ne relevant pas de la philosophie des propriétés génériques, mais qui sont apparus dans ce cadre.

On rencontre fréquemment, dans cette théorie, des groupes ayant une propriété un peu plus forte que l'hyperbolicité. Un groupe hyperbolique est un groupe dans lequel, étant donné un mot représentant l'élément neutre, *il existe* un diagramme de van Kampen bordé par ce mot, et vérifiant une inégalité isopérimétrique linéaire. Or, dans les groupes hyperboliques rencontrés le plus souvent dans l'étude des groupes aléatoires, *tous* les diagrammes de van Kampen (réduits) satisfont une telle inégalité. Cette propriété est bien connue pour les groupes à petite simplification, mais les groupes aléatoires dans le modèle à densité ne sont pas, en général, à petite simplification (du moins pas dans le système générateur naturel).

Cette hyperbolicité forte semble liée à des propriétés topologiques, comme le fait d'avoir une dimension du bord à l'infini égale à 1. Les liens entre cette propriété, la petite simplification, la dimension du bord et la dimension du groupe lui-même ne sont pas clairs et méritent d'être étudiés. Ce problème, bien que suggéré par les groupes aléatoires, n'a rien de probabiliste.

Un autre type de groupe surgit naturellement de ces constructions aléatoires : les limites d'une infinité de quotients aléatoires successifs. Ces groupes ne sont pas hyperboliques (car ils sont de présentation infinie). Néanmoins, ils conservent une forme d'inégalité isopérimétrique. Si D est un diagramme de van Kampen (réduit), et si on note $|\partial f|$ la longueur d'une face $f \in D$, alors ces diagrammes vérifient l'inégalité isopérimétrique linéaire

$$|\partial D| \geqslant \alpha \sum_{f \in D} |\partial f|$$

pour une certaine constante $\alpha > 0$. Ceci donne un aspect « fractal » à ces groupes. Malheureusement, le comportement de cette propriété par changement de système générateur n'est pas clair. Cette hyperbolicité faible mériterait elle aussi d'être étudiée.

Par ailleurs, un argument heuristique semble indiquer que les groupes aléatoires peuvent difficilement avoir des quotients finis (non triviaux). Préciser cet argument permettrait de résoudre la question classique de savoir s'il existe des groupes hyperboliques sans quotients finis.

Mentionnons maintenant des problèmes appartenant en propre à la problématique des groupes aléatoires.

Le modèle à densité conserve une partie de son mystère dans la mesure où on ne sait pas prouver que les groupes obtenus à différentes densités sont essentiellement différents. Cela fournirait un grand nombre de groupes non isomorphes. On aimerait trouver des invariants du groupe obtenu, dépendant de la densité. Voici deux invariants candidats : le nombre minimal de générateurs

(il est facile de montrer qu'au voisinage de la densité critique il tombe à 2) ; la cohomologie L^p pour diverses valeurs de p, qui mesure en quelque sorte le taux de branchement d'un espace, qui devrait être lié à la densité.

Les propriétés cohomologiques des groupes aléatoires sont mal connues : on sait qu'ils sont de dimension cohomologique 2, et que par ailleurs, en densité supérieure à $1/3$ ils ont la propriété T (avec évaluation des constantes de Kazhdan). Mais on ne sait pas si, en densité inférieure à $1/3$, la propriété T apparaît ou non.

Enfin, il existe des modèles généralisant le modèle à densité. Ce dernier présente l'inconvénient que toutes les relations ajoutées doivent avoir la même longueur. Cet obstacle est partiellement levé dans *Sharp phase transition theorems for hyperbolicity of random groups*, où demeure tout de même la contrainte que les longueurs des relateurs doivent rester dans un rapport borné. Un modèle plus général très naturel mais encore très mal compris est le modèle dit *à température* (que nous n'expliciterons pas), qui fournit des groupes de présentation infinie, donc non hyperboliques, avec des relateurs de toutes les longueurs. Ce modèle a la propriété intéressante de donner des groupes sans quotient fini (à part $\{e\}$), à comparer avec le même problème évoqué plus haut concernant les groupes hyperboliques.

Comme on le voit, les problèmes ouverts en théorie des groupes aléatoires, et les retombées potentielles sur les groupes non aléatoires, ne manquent pas.

2 La concentration de la mesure

La concentration de la mesure est un phénomène mêlant géométrie et probabilités, qui apporte une explication conceptuelle et des généralisations puissantes à certains des théorèmes de probabilités les plus banals, comme la loi des grands nombres ou le théorème central limite. On peut consulter l'introduction donnée par Talagrand dans [Tal]. Le point de vue géométrique est fortement développé par Gromov dans [Gro3].

Historiquement, la première observation de la concentration de la mesure est la suivante : dans la sphère S^n de grande dimension, munie de la mesure riemannienne normalisée à 1, une petite bande de largeur environ $1/\sqrt{n}$ autour d'un équateur contient presque toute la mesure, comme un calcul direct le montre aisément. Autrement dit, un petit voisinage d'une demi-sphère contient déjà presque toute la mesure.

Cette observation permet de démontrer un résultat d'apparence étrange : une fonction lipschitzienne sur la sphère S^n de grande dimension est presque constante (à $1/\sqrt{n}$ près) !

En effet, soit f une fonction 1-lipschitzienne (pour la normalisation) de S^n vers $\mathbb{R}$. Soit m la médiane de f et soient S_+ et S_- les parties de la sphère où f est respectivement supérieure et inférieure à sa médiane. Par définition de la médiane, ces deux ensembles sont de mesure supérieure à $1/2$ (strictement si f

vaut m sur une partie de mesure non nulle, auquel cas on peut tronquer un peu S_+ et S_- pour obtenir des parties de mesure $1/2$).

Dans le plan, il est bien connu que la figure minimisant la longueur de son bord, à surface donnée, est le cercle. On peut remplacer « longueur du bord » par « aire d'un petit voisinage ». On démontre de même que dans la sphère, la mesure d'un ε-voisinage d'une partie A est toujours supérieure à la mesure du ε-voisinage d'une calotte de même mesure que A. Revenant en particulier à S_+ qui est de mesure $1/2$, on voit que la mesure d'un ε-voisinage de S_+ est supérieure à la mesure d'un ε-voisinage d'une demi-sphère. Or, comme on l'a dit plus haut, pour ε de l'ordre de $1/\sqrt{n}$ cette mesure est presque 1. Autrement dit, une majorité de points sont à distance au plus $1/\sqrt{n}$ de S_+. Par définition de S_+, et comme f est 1-lipschitzienne, si un point x est à distance r de S_+, alors $f(x) \geqslant m - r$. Donc, pour une majorité (en mesure) de points x, on a $f(x) \geqslant m - 1/\sqrt{n}$. En raisonnant symétriquement avec S_-, on obtient que pour une majorité de points, f est comprise entre $m - 1/\sqrt{n}$ et $m + 1/\sqrt{n}$. (On a omis une constante devant $1/\sqrt{n}$ pour simplifier.)

En résumé, on a démontré le théorème suivant, que l'on peut faire remonter à Paul Lévy dans les années 1920 :

THÉORÈME 3 : CONCENTRATION DE LA MESURE SUR LA SPHÈRE – *Une fonction 1-lipschitzienne sur la sphère S^n, pour n grand, est presque constante à $1/\sqrt{n}$ près.*

Donnons un autre exemple plus proche des probabilités classiques et (en apparence) plus éloigné de la géométrie. Il est bien connu que, si l'on fait une série de n tirages à pile ou face avec n grand et que l'on compte la proportion de « pile » qui sont apparus, les résultats sont proches d'une gaussienne centrée en $1/2$ et d'écart-type $1/2\sqrt{n}$.

Géométrisons ce résultat. On considère le cube discret $\{0,1\}^n$ muni de la mesure de probabilité uniforme qui donne un poids $1/2^n$ à chaque point. Ce cube modélise bien sûr le résultat d'une suite de n tirages à pile ou face, et la proportion de « pile » est une fonction sur ce cube, qui varie de $1/n$ sur chaque arête du cube. Le théorème central limite affirme que cette fonction est presque constante égale à $1/2$, avec des fluctuations gaussiennes de l'ordre de $1/\sqrt{n}$.

Or ce résultat est loin de n'être valable que pour cette fonction particulière. Talagrand a ainsi démontré :

THÉORÈME 4 : CONCENTRATION DE LA MESURE SUR LE CUBE – *Soit le cube discret $\{0,1\}^n$ muni de la mesure uniforme, et de la métrique qui attribue une longueur $1/n$ à chaque arête (de manière à ce que le diamètre du cube soit 1). Soit f une fonction du cube vers $\mathbb{R}$ qui soit 1-lipschitzienne pour cette métrique. Alors f est presque constante à $1/\sqrt{n}$ près, et les fluctuations sont contrôlées par des gaussiennes. Ceci au sens où il existe un nombre m tel que pour tout $t \geqslant 0$:*

$$\Pr(|f - m| \geqslant t) \leqslant 2e^{-nt^2/2}$$

Ainsi, une fonction de n variables indépendantes dans laquelle chaque variable influe d'au plus $1/n$, est constante à $1/\sqrt{n}$ près. Ceci généralise très fortement les théorèmes habituels, où l'on ne considère que des fonctions qui sont la somme de variables indépendantes identiquement distribuées.

La démonstration de ce théorème relativement récent n'est pas très compliquée. Elle utilise le même outil isopérimétrique que nous avons présenté ci-dessus sur la sphère.

Il existe de très nombreux variantes et raffinements de ces théorèmes de concentration. Pour ne citer que le plus simple, une fonction de n variables indépendantes telle que la i-ième variable influe sur la fonction d'au plus c_i, sera constante à $\sqrt{\sum c_i^2}$ près. L'indépendance des variables correspondant au produit des espaces de probabilité sous-jacents, ce théorème signifie qu'un produit d'espaces de probabilité bornés est concentré.

La concentration de la mesure n'est pas toujours gaussienne. En particulier, obtenir une estimation de la première valeur propre non nulle du laplacien (sur une variété, sur un graphe) permet de démontrer des théorèmes de concentration où les variations ne sont plus contrôlées par une gaussienne mais par une simple exponentielle. C'est ce que nous faisons, par exemple, dans *Concentration spectrale dans les graphes* ; ce texte applique des techniques bien connues par ailleurs à un cas particulier.

Cependant, il semble que l'indépendance, c'est-à-dire la structure produit, conduise toujours à de la concentration gaussienne. Ainsi en est-il de la concentration spectrale dans les graphes : si l'on prend un produit de graphes manifestant de la concentration exponentielle, le produit montre de la concentration gaussienne au moins à petite échelle.

Sachant que la concentration gaussienne apparaît systématiquement lorsque l'on utilise des espaces produits, on peut se demander si la réciproque est vraie, à savoir : est-ce qu'un espace présentant de la concentration gaussienne est nécessairement proche d'un espace produit ? On doit cependant prendre en compte la remarque élémentaire suivante : si X, Y sont des espaces métriques mesurés, et si on a une application $f : X \to Y$ 1-lipschitzienne qui envoie la mesure de X sur la mesure de Y, alors toute forme de concentration qui existe sur X sera évidemment vérifiée sur Y.

Une contraction (en ce sens) d'un espace concentré est donc concentrée. On peut alors se demander si tout espace présentant de la concentration gaussienne est proche d'une contraction d'un espace produit.

Nous avons un début de résultat en ce sens : sur un espace présentant de la concentration gaussienne, il est possible de trouver des « coordonnées indépendantes », c'est-à-dire une famille de fonctions (non triviales) $f_1, \dots, f_k$ vérifiant une inégalité du type

$$\Pr(|f_1| \geqslant a_1, \dots, |f_k| \geqslant a_k) \leqslant A e^{-(\sum a_i^2)/C}$$

où la constante C est (à un petit facteur près) la même que celle intervenant dans l'hypothèse de concentration gaussienne sur l'espace. Nous renvoyons à *Concentrated spaces seen as product spaces* pour un énoncé précis. Ce théorème n'est que le reflet des débuts d'une recherche en cours qui, nous l'espérons, donnera bientôt des résultats plus précis.

La concentration de la mesure est un sujet récent dont toutes les implications ne sont pas encore éclaircies. Si les aspects probabiliste, statistique et analytique (liens avec la théorie des espaces de Banach, non évoqués ici) de la chose sont désormais relativement bien connus, l'aspect proprement géométrique a été quelque peu laissé de côté. Il a pourtant connu des succès indéniables, lorsque par exemple Gromov a montré que toute variété à courbure de Ricci positive, ainsi que toute variété algébrique complexe, présentait de la concentration gaussienne. Nous espérons continuer cette étude.

3 Quelques exemples d'algorithmes génétiques

3.1 Dynamique de la reproduction sexuée

La situation étudiée est la suivante. On se donne une population composée d'individus caractérisés par leur génome, un génome étant (représenté par) un élément de $\{0,1\}^n$. On suppose qu'à chaque génération, la population est remplacée par une population-fille de la manière suivante : un individu de la population-fille est obtenu en tirant au hasard deux individus dans la population-mère, et le génome de l'enfant est obtenu par mélange probabiliste de ceux des deux parents. Le mélange consiste, pour chaque position dans le génome, à décider que le codon 0 ou 1 présent à cette position sera, avec probabilité $1/2$, celui de l'un ou l'autre des parents (on étudie aussi des méthodes de croisement plus complexes).

L'objectif est d'étudier l'assertion selon laquelle la reproduction sexuée est efficace pour brasser les gènes. La réponse est positive, et le temps de brassage se comporte comme le logarithme de la taille du génome.

On peut faire fonctionner ce processus soit en population finie, soit dans le cas idéalisé d'une population infinie. Une population infinie est une mesure de probabilité sur $\{0,1\}^n$, la mesure d'un élément $x \in \{0,1\}^n$ représentant la proportion des individus de la population présentant ce génome. Une population finie à k individus est simplement un k-uplet d'éléments de $\{0,1\}^n$.

Étant donné une population infinie initiale p_0, le processus à population infinie est déterministe (sur l'espace des mesures de probabilité sur $\{0,1\}^n$). Soit p_t la mesure de probabilité sur $\{0,1\}^n$ obtenue après t générations. On peut montrer (cf. [RRS]) que le processus converge : il existe une mesure de probabilité p_∞ telle que

$$|p_t - p_\infty| \leqslant n^2/2^t$$

où on définit la distance entre deux mesures de probabilité par (distance de variation totale)

$$|p-q| = \frac{1}{2}\sum_{x\in\{0,1\}^n} |p(x)-q(x)| = \sup_{A\subset\{0,1\}^n} |p(A)-q(A)|$$

On voit sur cette expression que le temps de brassage nécessaire pour obtenir une valeur-but de $|p_t - p_\infty|$ est logarithmique en cette valeur-but, logarithmique aussi en la longueur du génome. De plus, cette estimation est essentiellement correcte.

La mesure de probabilité p_∞ peut être caractérisée simplement. Pour $1 \leqslant i \leqslant n$, soit a_i^1 la proportion dans p_0 des individus dont le i-ième bit du génome est un 1, et $a_i^0 = 1 - a_i^1$. Alors, si $x = (x_i) \in \{0,1\}^n$, la mesure p_∞ est définie par

$$p_\infty(x) = \prod_i a_i^{x_i}$$

Autrement dit, les proportions de 0 et de 1 pour chaque bit sont préservées au cours du processus, mais les bits deviennent indépendants les uns des autres. Ainsi si la population initiale est composée pour moitié de l'individu $00\ldots0$ et pour moitié de $11\ldots1$, la population finale sera la mesure uniforme sur tout $\{0,1\}^n$.

En population finie de taille k, la situation est plus complexe et les résultats donnés dans [RRS] étaient insatisfaisants. Cette fois-ci la dynamique est aléatoire sur l'ensemble des k-uplets d'éléments de $\{0,1\}^n$. Soit π_0 le k-uplet initial, supposé donné, et soit π_t le k-uplet aléatoire obtenu après t générations. On s'intéresse à la loi de π_t.

À cause du phénomène bien connu de coalescence, pour t suffisamment grand, avec très grande probabilité le k-uplet π_t sera composé d'une population-clone formée de k individus identiques : en effet, à chaque génération, avec une certaine probabilité une part de l'information génétique est perdue, et (en l'absence de mutations) la diversité génétique ne peut que diminuer. Ceci a au moins le mérite de montrer que le processus converge.

Par contre, cet individu est lui-même une variable aléatoire (connaissant π_0, on ne peut pas prévoir quelle population-clone on va obtenir). Soit q_t la loi du premier élément du k-uplet π_t. C'est sur q_t qu'on va obtenir des estimations.

Le principal résultat est une estimation de la distance entre q_t et une mesure limite p_∞ sur $\{0,1\}^n$. Le k-uplet π_0 formant la population initiale peut naturellement être vu comme une mesure p_0 sur $\{0,1\}^n$ définie par $p_0(x) = \#\{1 \leqslant i \leqslant k, \pi_0(i) = x\}$. Soit p_∞ la mesure obtenue à partir de p_0 par la même définition que ci-dessus en population infinie.

L'estimation que l'on obtient est alors

$$|q_t - p_\infty| \leqslant n^2\left(\frac{1}{k} + \frac{1}{2^t}\right)$$

En particulier, $|q_\infty - p_\infty| \leqslant n^2/k$. Ceci semble être un biais intrinsèque à la population finie. En effet, on peut montrer que pour certaines populations initiales, on a $|q_\infty - p_\infty| \geqslant n/Ck$ pour une certaine constante C.

La vitesse de convergence du processus à population finie est ainsi la même qu'en population infinie ; mais une légère différence, de l'ordre de l'inverse de la taille de la population, apparaît sur le résultat final.

On a ainsi montré que même en population finie, la reproduction sexuée est efficace pour brasser les gènes. Ces résultats s'étendent sans peine à d'autres méthodes de croisement des génomes, qui peut-être modélisent mieux le processus de *crossing-over* biologique.

3.2 L'espace des arbres phylogénétiques

Les algorithmes génétiques sont utiles pour parcourir des espaces qu'on ne connaît pas explicitement ou bien qui sont trop grands pour faire l'objet d'une énumération exhaustive. On a tenté d'exploiter cette propriété pour explorer l'espace des arbres sur un ensemble fixé de feuilles.

Ce problème se pose en particulier pour la reconstruction phylogénétique, c'est-à-dire la recherche de l'arbre évolutif entre les espèces vivantes (il peut aussi se présenter en linguistique). Le problème est le suivant : on étudie un certain nombre d'espèces, qui sont connues à travers certaines caractéristiques comme une partie de leur génome, ou bien un ensemble de traits morphologiques.

Le but est de trouver un arbre ayant ces espèces pour feuilles, et qui minimise un certain critère (comme le nombre total de mutations) censé représenter la plausibilité de l'arbre comme modèle du véritable arbre de l'évolution. Le problème majeur est que le nombre d'arbres possibles sur N feuilles données croît extrêmement vite (au moins comme $N!$ comme le montrent les arbres où chaque espèce se détache l'une après l'autre d'un tronc commun).

On s'est proposé d'écrire un programme de recherche d'arbres phylogénétiques qui fonctionne comme un algorithme génétique : on maintient en permanence une « population » d'arbres candidats, et cette population évolue par sélection, mutation et croisement.

La principale innovation de cette approche par rapport aux programmes existants consiste en l'utilisation d'un croisement entre arbres, analogue du croisement biologique et du croisement des chaînes de $\{0,1\}^n$ étudié ci-dessus. Nous le décrivons ici.

Soit F un ensemble fini (les feuilles de l'arbre, ou les espèces à étudier). Un *nœud* sera une partie non vide de F. Un *arbre* (enraciné) dont l'ensemble des feuilles est F peut être défini par l'ensemble des nœuds qu'il contient. Ainsi l'arbre sur les feuilles $\{a,b,c,d\}$ dans lequel se séparent a et b d'une part, et c et d d'autre part, a comme ensemble de nœuds $\{\{a,b,c,d\},\{a,b\},\{a\},\{b\},\{c,d\},\{c\},\{d\}\}$. Il est facile de voir qu'un ensemble E de nœuds (contenant le nœud complet ainsi que les singletons) définit bien un arbre si et seulement si pour

tous $A, B \in E$, on a soit $A \subset B$, soit $B \subset A$, soit $A \cap B = \varnothing$ (condition de compatibilité, qui exprime que les nœuds peuvent s'emboîter).

L'ensemble des arbres (enracinés, avec un ensemble de feuilles donné) est naturellement muni d'un ordre qui dit qu'un arbre est plus fin qu'un autre si son ensemble de nœuds est plus grand. Étant donné deux arbres, leur inf pour cet ordre est l'arbre dont l'ensemble de nœuds est l'intersection des ensembles de nœuds des deux arbres (consensus strict : un groupement de feuilles appartient à l'inf de deux arbres si et seulement s'il appartient aux deux arbres).

Cet inf n'est pas un bon candidat pour un croisement d'arbres dans le cadre d'un algorithme génétique. En effet il a tendance à créer des dégénérescences et perd beaucoup d'information : dès que les parents diffèrent, le caractère correspondant de l'enfant n'est pas défini ! Le croisement biologique, et le croisement sur $\{0,1\}^n$ étudié plus haut, choisissent au hasard entre les deux parents en cas de désaccord.

Un bon candidat au croisement d'arbres pourrait être le suivant. Étant donné deux arbres ayant des ensembles de nœuds E et E', considérer la réunion $E'' = E \cup E'$. En général elle ne définit pas un arbre. Ordonner au hasard les éléments de E''. Puis, parcourir la liste de nœuds ainsi obtenue ; dès qu'un nœud ne vérifie pas la condition de compatibilité avec l'un des nœuds qui le précèdent, supprimer ce nœud de la liste. Passer à l'examen du nœud suivant. Par construction, après examen et éventuelle suppression de tous les nœuds, la condition de compatibilité est respectée.

Ce croisement est une opération aléatoire puisqu'il dépend d'un choix aléatoire de l'ordre d'examen des nœuds, dont le résultat dépend en général. De plus, il vérifie la condition naturelle qu'il produit un arbre plus fin que le consensus des deux arbres parents. Enfin, il n'a pas tendance à créer trop de dégénérescences.

On a donc implémenté un algorithme génétique sur l'espace des arbres phylogénétiques utilisant ce croisement, ainsi que des opérateurs de sélection et de mutation standard. On a comparé les résultats à ceux d'un logiciel classique dans le domaine. Le programme a donné des résultats de qualité comparable, mais avec des temps de calcul supérieurs ; en tout état de cause l'intérêt de l'utilisation du croisement n'a pas été clairement démontré. Hors de l'algorithme génétique, qui semble très gourmand en temps de calcul, il pourrait être intéressant de reprendre ce croisement pour l'intégrer à un logiciel classique.

3.3 Le Product Replacement Algorithm

Le Product Replacement Algorithm est une heuristique utilisée en théorie algorithmique des groupes pour produire un élément aléatoire uniformément réparti dans un groupe fini. Le groupe est donné comme une « boîte noire », c'est-à-dire qu'on fournit trois routines effectuant respectivement la multiplication de deux éléments, l'inversion d'un élément, la comparaison d'un élément avec l'élément neutre, ainsi qu'un système générateur. (Ce peut être le cas, typi-

quement, d'un groupe de matrices qu'on ne sait pas décrire explicitement mais dont on connaît un système générateur).

Le but de l'algorithme est de fournir un élément « typique » du groupe, c'est-à-dire un élément aléatoire dont la loi soit (proche de) la loi uniforme sur le groupe. Construire de tels éléments est utile en théorie algorithmique des groupes pour tester (probabilistement) certaines propriétés algébriques.

Le PRA (Product Replacement Algorithm) est un algorithme qui semble fonctionner extrêmement bien en pratique. Ses fondements théoriques sont mal compris (voir [Pak] pour un survol). Son fonctionnement est le suivant.

On se donne un k-uplet générateur $s_1, \ldots, s_k$ du groupe. Ce k-uplet n'est pas forcément minimal et peut par exemple contenir plusieurs fois le même élément. À chaque étape, on modifie ce k-uplet de la manière suivante. On tire au hasard deux indices distincts $1 \leqslant i, j \leqslant k$. Puis on remplace, dans le k-uplet, le générateur s_j par, soit $s_j s_i$, soit $s_j s_i^{-1}$, soit $s_i s_j$, soit $s_i^{-1} s_j$ (en choisissant au hasard entre ces quatre possibilités). On ne touche pas à s_i. Il est immédiat de voir que si le premier k-uplet engendrait le groupe, le nouveau l'engendre encore.

L'idée est que les éléments d'un tel k-uplet vont s'éloigner très vite du k-uplet initial. Si l'on raisonne en termes de longueur, si au temps t les éléments du k-uplet sont à distance en moyenne r de l'origine, au temps $t+1$ la distance moyenne à l'origine sera $r(1+1/k)$ parce qu'on a multiplié un des éléments par un autre. D'où une croissance supposée exponentielle de la distance à l'origine. Ceci s'oppose fortement à l'algorithme le plus simple, la marche aléatoire sur le groupe, où à chaque étape la distance à l'origine augmente au plus de 1.

L'analogie avec un algorithme génétique est claire : on maintient une population d'éléments et on les croise. Ceci a permis d'obtenir un résultat de convergence du PRA lorsque la taille de la population est très grande. Cependant, cette évaluation n'a pas d'intérêt pratique car la méthode utilise qu'en très grande population, une partie du PRA « simule » une marche aléatoire. On ne prouvera donc pas par cette méthode (du moins sans modification importante) que le PRA fait mieux que la marche aléatoire.

On a aussi exhibé un invariant curieux (mais sans application connue) du PRA sur les groupes cycliques, ainsi qu'une sorte de borne inférieure à la qualité de l'algorithme.

* * *

Après avoir donné un aperçu des sujets abordés ici avec plus ou moins de bonheur dans la recherche, nous laissons désormais au lecteur le labeur de parcourir les textes qui suivent.

Références

[Ch] C. Champetier, *Cocroissance des groupes à petite simplification*, Bull. London Math. Soc. **25** (1993), No. 5, 438–444.

[Gh] É. Ghys, *Groupes aléatoires*, séminaire Bourbaki **916** (2003).

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

[Gri] R.I. Grigorchuk, *Symmetrical Random Walks on Discrete Groups*, in *Multicomponent Random Systems*, ed. R.L. Dobrushin, Ya.G. Sinai, Adv. Prob. Related Topics **6**, Dekker (1980), 285–325.

[Gro1] M. Gromov, *Hyperbolic Groups*, in *Essays in group theory*, ed. S.M. Gersten, Springer (1987), 75–265.

[Gro2] M. Gromov, *Asymptotic Invariants of Infinite Groups*, in *Geometric group theory*, ed. G. Niblo, M. Roller, Cambridge University Press, Cambridge (1993).

[Gro3] M. Gromov, *Metric Structures for Riemannian and Non-Riemannian Spaces*, Progress in Math. **152**, Birkhäuser (1999).

[Gro4] M. Gromov, *Random Walk in Random Groups*, Geom. Funct. Anal. **13** (2003), No. 1, 73–146.

[Pak] I. Pak, *What do we know about the product replacement algorithm?*, in *Groups and Computation III*, eds. W. Kantor, A. Seress, de Gruyter, Berlin (2001), 301–347.

[Pau] F. Paulin, *Sur la théorie élémentaire des groupes libres*, Séminaire Bourbaki **922** (2003).

[RRS] Y. Rabani, Y. Rabinovich, A. Sinclair, *A computational view of population genetics*, Random Structures and Algorithms **12** (1998), No. 4, 313–334.

[Tal] M. Talagrand, *A new look at independence*, Ann. Prob. **24** (1996), No. 1, 1–34.

Table des matières