Croissance des groupes quantiques discrets

Roland Vergnioux, Rennes, 15 décembre 2008

1 Groupes quantiques discrets

À un groupe discret Γ on associe deux algèbres :

- $\hat{\mathcal{A}} = \mathbb{C}^{(\Gamma)}$ avec la structure d'algèbre « triviale » provenant de celle de $\mathbb{C}$. La structure de groupe induit un coproduit à valeurs dans les multiplicateurs : $\hat{\delta} : \hat{\mathcal{A}} \to \mathcal{M}(\hat{\mathcal{A}} \otimes \hat{\mathcal{A}})$, $\hat{\delta}(f)(r,s) = f(rs)$. L'algèbre $\hat{\mathcal{A}}$ est commutative.
- $\mathcal{A} = \mathbb{C}\Gamma$ avec la structure d'algèbre provenant de la structure de groupe de Γ. On peut munir $\mathcal{A}$ d'un coproduit « trivial » $\delta : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}$, $\delta(r) = r \otimes r$. La cogèbre $\mathcal{A}$ est co-commutative : $\sigma \circ \delta = \delta$, où $\sigma(a \otimes b) = b \otimes a$.

Dans le cas classique, $\hat{\mathcal{A}}$ et $\mathcal{A}$ sont toutes les deux représentées fidèlement sur l'espace $H = \ell^2(\Gamma)$: $\hat{\mathcal{A}}$ agit par multiplication et $\mathcal{A}$ par translation. On note $\hat{A}$ et A les complétions pour la norme d'opérateur : il s'agit respectivement des C^*-algèbres $c_0(\Gamma)$ et $C^*_{\mathrm{red}}(\Gamma)$.

On voudrait axiomatiser la situation en retirant la co-commutativité de $\mathcal{A}$ (resp. la commutativité de $\hat{\mathcal{A}}$), de manière à ce que le cas co-commutatif (resp. commutatif) redonne les groupes discrets. Il faut garder une trace de l'inverse du groupe, ce qui dans le cas non co-commutatif n'est pas aussi simple qu'avec le produit. Exemple d'axiome évident : la co-associativité $(\delta \otimes \mathrm{id}) \circ \delta = (\mathrm{id} \otimes \delta) \circ \delta$, avec déjà une petite subtilité sur les domaines de définition pour $\hat{\delta}$.

La théorie est en fait axiomatisée à trois niveaux équivalents (Woronowicz, Baaj – Skandalis, Van Daele) :
- C^*-algébriquement au niveau de A : « compact quantum groups »,
- hilbertiennement au niveau de H : « compact multiplicative unitaries »,
- algébriquement au niveau de $\hat{\mathcal{A}}$: « multiplier Hopf algebras ».

Présentons la première axiomatisation :

Définition 1.1 *Une C^*-algèbre de Woronowicz est une C^*-algèbre unifère A munie d'un $*$-morphisme $\delta : A \to A \otimes A$ tel que*
- $(\delta \otimes \mathrm{id})\delta = (\mathrm{id} \otimes \delta)\delta$,
- $\delta(A)(1 \otimes A)$ *et* $\delta(A)(A \otimes 1)$ *sont denses dans* $A \otimes A$,

où on note par ex. $\delta(A)(1 \otimes A) = \{\delta(a)(1 \otimes b) \mid a, b \in A\}$.

On parle aussi de C^*-algèbre de Hopf bisimplifiable. Dans le cas co-commutatif on montre qu'on retrouve les C^*-algèbres (réduites, mais aussi pleines, ou entre les deux) des groupes discrets, et donc qu'on peut reconstruire un groupe Γ à partir de (A, δ).

EXEMPLES 1.2

- $A = C^*_{\mathrm{red}}(\Gamma)$, mais aussi $A = C^*(\Gamma)$, avec Γ groupe discret. C'est le cas co-commutatif.
- $A = C(G)$ avec G groupe compact et le coproduit $\delta(f)(r,s) = f(rs)$. C'est le cas commutatif : le premier axiome donne les monoïdes compacts, et le deuxième axiome correspond à leur bi-simplifiabilité, qui dans le cas compact implique l'existence d'une unité et d'un inverse continu.
- $A = C_q(G)$ avec G groupe de Lie réel compact connexe simplement connexe et $q \in]0,1]$ — c'est-à-dire que les groupes quantiques à la Jimbo-Drinfeld, ou « q-déformations », sont inclus dans la théorie de Woronowicz.
- $A = A_u(I_n)$, $A_o(I_n)$ définis par générateurs et relations et qui admettent eux-mêmes des q-déformations :
$$A_u(Q) = \big\langle u_{ij}, 1 \le i,j \le n \;\big|\; (u_{ij})_{ij} \text{ et } Q(u^*_{ij})_{ij}Q^{-1} \text{ unitaires}\big\rangle,$$
$$A_o(Q) = \big\langle u_{ij}, 1 \le i,j \le n \;\big|\; (u_{ij})_{ij} = Q(u^*_{ij})_{ij}Q^{-1} \text{ et unitaire}\big\rangle,$$
avec $Q \in GL(n,\mathbb{C})$. Ce sont les groupes quantiques compacts universels (unitaires et orthogonaux) introduits par Wang. Le coproduit est donné par $\delta(u_{ij}) = \sum u_{ik} \otimes u_{kl}$. Pour l'étude du cas orthogonal on fait l'hypothèse que $Q\bar{Q}$ est scalaire.
- Autres familles d'exemples « universels » : groupes symétriques libres $A_s(n)$, groupes de symétries complexes libres $A_h^s(n)$, groupe orthogonal semi-libéré, ... □

La structure de (A,δ) peut être comprise à l'aide de ses coreprésentations. Une coreprésentation α de (A,δ) sur un espace de Hilbert de dimension finie H_α est un unitaire $\alpha \in L(H_\alpha) \otimes A$ tel que $(\mathrm{id}\otimes\delta)(\alpha) = \alpha_{12}\alpha_{13}$. On a des notions naturelles de morphismes $\mathrm{Mor}(\alpha,\beta) \subset L(H_\alpha, H_\beta)$, de somme directe, produit tensoriel, conjuguée avec $H_{\alpha\oplus\beta} = H_\alpha \oplus H_\beta$, $H_{\alpha\otimes\beta} = H_\alpha \otimes H_\beta$, $H_{\bar\alpha} = \bar H_\alpha$. Si ω est une forme linéaire sur $L(H_\alpha)$ on dit que $(\omega\otimes\mathrm{id})(\alpha)$ est un coefficient de α, les coefficients des coreprésentations engendrent une sous-algèbre $\mathcal{A} \subset A$.

Théorème 1.3 *Soit (A,δ) une C^*-algèbre de Woronowicz.*

- *Il existe un unique état $h \in A'$ bi-invariant :* $(\mathrm{id}\otimes h)\delta = (h\otimes\mathrm{id})\delta = 1h$.
- *Les coreprésentations de (A,δ) sont sommes directes d'irréductibles.*
- *$\mathcal{A}$ est dense et munie d'une structure d'algèbre de Hopf (δ,ϵ,S).*

Le bon cas particulier pour se faire une idée du comportement de la catégorie des coreprésentations est celui des groupes compacts : en effet quand $A = C(G)$ on a $L(H_\alpha)\otimes A \simeq C(G, L(H_\alpha))$ et les co-représentations de (A,δ)

correspondent exactement aux représentations unitaires de G. Dans ce cas la forme linéaire $h : C(G) \to \mathbb{C}$ est simplement l'intégration contre la mesure de Haar.

Dans le cas co-commutatif $A = C^*_{\text{red}}(\Gamma)$ qui nous intéresse plus, il est très facile de donner des exemples de coreprésentations : $\text{id}\otimes r \in L(\mathbb{C})\otimes A$ est une coreprésentation irréductible pour tout $r \in \Gamma$, et on vérifie que cela induit une identification entre le groupe Γ et l'ensemble des classes de coreprésentations irréductibles muni du produit tensoriel. Plus généralement, tout coreprésentation est isomorphe à une matrice $\text{diag}(r_1, \dots, r_n) \in M_n(A) \simeq L(\mathbb{C}^n)\otimes A$ avec $r_1, \dots, r_n \in \Gamma$. Par ailleurs dans ce cas h est la trace canonique sur $C^*_{\text{red}}(\Gamma)$ donnée par $h(r) = \delta_{e,r}$.

2 Croissance et marches aléatoires

Considérons à nouveau un groupe discret Γ et supposons qu'il est engendré par un sous-ensemble fini $S \subset \Gamma$. On peut supposer que $S = S^{-1}$ et $e \notin S$, on note n le cardinal de S. À S on associe la coreprésentation « fondamentale » $u = \text{diag}(s_1, \dots, s_n) \in L(\mathbb{C}^n)\otimes\mathbb{C}\Gamma$. La puissance tensorielle k^{e} de u est une coreprésentation sur $\mathbb{C}^{kn}$ qui est diagonale dans la base canonique et dont les éléments diagonaux sont les mots de longueur k sur S.

On obtient ainsi une description en termes de coreprésentations pour la longueur des mots sur Γ (relativement à S) et pour la probabilité de retour à l'origine en $2k$ pas (dans la marche aléatoire sur Γ engendrée par S) :

$$l(r) = \min\{k \mid r \subset u^{\otimes k}\},$$
$$p_k = n^{-2k} \dim \text{Mor}(1, u^{\otimes 2k}) = n^{-2k} h(\chi_u^{2k}),$$

si on note $\chi_u = (\text{Tr}\otimes\text{id})(u) = \sum u_{ii}$ le caractère de la coreprésentation u. Notons que, comme dans le cas des groupes compacts, on a $h(\chi_\alpha) = 0$ pour toute coreprésentation irréductible $\alpha \neq 1$, et $h(\chi_1) = 1$.

On peut donc poser les définitions suivantes dans le cas général. Remarquons que la marche aléatoire évoquée peut être définie de manière indépendante dans le cadre des processus aléatoires quantiques à la Biane.

Définition 2.1 *On dit qu'une C^*-algèbre de Woronowicz (A, δ) est de type fini si elle est engendrée par les coefficients d'une coreprésentation u de dimension finie n — on peut alors supposer $\bar{u} = u$ et $1 \not\subset u$. La longueur d'une coreprésentation irréductible α relativement à u est*

$$l(\alpha) = \min\{k \mid \alpha \subset u^{\otimes k}\}.$$

La probabilité de retour à l'origine en $2k$ pas dans la marche aléatoire engendrée par u est

$$p_k = n^{-2k} \dim \text{Mor}(1, u^{\otimes 2k}) = n^{-2k} h(\chi_u^{2k}).$$

En ce qui concerne la croissance, une première idée peut être de compter les coreprésentations irréductibles de longueur k et donc de considérer la suite $s_k = \#\{\alpha \mid l(\alpha) = k\}$. On s'aperçoit cependant que cette idée est trop naïve et le bon analogue du « volume des sphères » est en fait

$$S_k = \sum_{l(\alpha)=k} (\dim \alpha)^2.$$

On peut également considérer le « volume des boules » $B_k = \sum_{l=0}^{k} S_l$. On dit que (A, δ) est à croissance polynômiale (resp. exponentielle) si c'est le cas de la suite (S_n). Ce sont des notions qui ne dépendent pas de u, ainsi que l'exposant de croissance dans le cas polynômial.

On a aussi une formule plus conceptuelle — en termes d'intégrale des fonctions caractéristiques des sphères de rayon k — pour S_k. Notons que dans le cas classique les irréductibles sont de dimension 1 donc $s_k = S_k$. Le choix de S_k est également justifié par le résultat suivant :

Proposition 2.2 *(A, δ) est à croissance polynômiale si et seulement si le groupe quantique discret associé à (A, δ) est moyennable et a la propriété de décroissance rapide (RD).*

Quelques exemples :
- Si G est un groupe de Lie réel compact, $C(G)$ est à croissance polynômiale — cf plus loin. En revanche les q-déformations sont à croissance exponentielle : en fait un groupe quantique discret à croissance polynômiale est forcément unimodulaire.
- Dans le cas de $A = A_o(I_n)$ avec $n \geq 2$, les coreprésentations irréductibles sont naturellement indexées par $\mathbb{N}$, avec $\alpha_0 = 1$, $\alpha_1 = u$ (matrice des générateurs), et les règles de fusion suivantes :

  $$\alpha_k \otimes \alpha_l = \alpha_{|k-l|} \oplus \alpha_{|k-l|+2} \oplus \cdots \oplus \alpha_{k+l}.$$

  On a en particulier la relation de récurrence $n \dim \alpha_k = \dim \alpha_{k+1} + \dim \alpha_{k-1}$. Ainsi $s_k = 1$ est à croissance polynômiale tandis que $S_k = \dim \alpha_k$ est à croissance exponentielle dès que $n \geq 3$. Or le groupe quantique discret associé à $A_o(I_n)$ n'est pas moyennable (en revanche il a la propriété RD).
- Dans le cas de $A = A_u(I_n)$ avec $n \geq 2$, les coreprésentations irréductibles sont naturellement indexées par les mots en deux lettres u, $\bar{u}$ de manière à ce que la longueur $l(\alpha)$ coïncide avec la longueur du mot α. Ainsi (s_k) et (S_k) sont toutes deux à croissance exponentielle.

Discutons maintenant plus en détail le cas d'un groupe de Lie réel G compact, connexe et simplement connexe. La théorie des coreprésentations de $C(G)$ correpond à celle des représentations de G, qui est connue, et on doit donc pouvoir calculer tous les invariants introduits précédemment.

Soit $X = \hat{T}$ le dual d'un tore maximal de G, R_+ un choix de racines positives dans X et $X_{++} \subset X$ le cône des poids dominants associés. Les représentations irréductibles de G sont indexées par leurs plus hauts poids qui parcourent X_{++}. Soit ϖ_i, $1 \leq i \leq r$, les poids fondamentaux, qui forment une base de X_{++}. La norme ℓ^1 associée à cette base coïncide avec la longueur des représentations associée au choix de $u = \bigoplus \varpi_i$ comme représentation fondamentale. En particulier s_k est contrôlé par k^{r-1}.

En ce qui concerne les dimensions, on a la formule des dimensions de H. Weyl :

$$\dim \alpha = \prod_{\lambda \in R_+} \Big(1 + \frac{(\alpha|\lambda)}{(\rho|\lambda)}\Big), \quad \text{où} \quad 2\rho = \sum \varpi_i.$$

Chaque terme du produit croît linéairement avec la norme de α. On obtient ainsi facilement l'estimée $S_k \leq Ck^{d-1}$, où $d = r + 2\#R_+$. En faisant attention, on obtient également l'inégalité dans l'autre sens (avec une autre constante).

Pour un tel groupe compact G, on obtient donc une estimée de croissance très simple : $B_k \approx k^d$, et d s'interprète comme la dimension réelle de G. Je ne sais pas s'il y a une preuve directe de ce résultat.

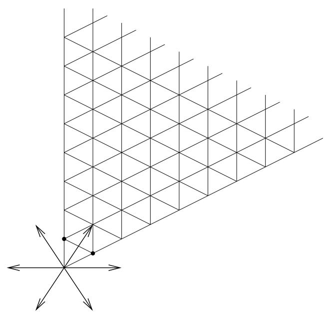

FIG. 1 – $SU(3) : R, X_{++}, (\varpi_1, \varpi_2)$

Considérons maintenant la probabilité de retour à l'origine, toujours pour le même groupe compact G. Dans ce cas, la formule intégrale pour p_k est l'intégrale sur G d'une fonction centrale, et se ramène donc à une intégrale sur le tore maximal choisi par la formule d'intégration de H. Weyl :

$$p_k = n^{-2k} \int_G \chi_u(g)^{2k} \mathrm{d}g = \frac{n^{-2k}}{w(G)} \int_T \chi_u(t)^{2k} \delta_G(t) \mathrm{d}t,$$

où $\delta_G(t) = \prod_{\lambda \in R}(\langle \lambda, t \rangle - 1)$ et $w(g) = \#W$ est le cardinal du groupe de Weyl. Par ailleurs, si $P(u) \subset X$ est la famille des poids de la représentation fondamentale u, on a par définition $\chi_u(t) = \sum_{\lambda \in P(u)} \langle \lambda, t \rangle$. Ici $\langle \cdot\,, \cdot \rangle$ est la dualité entre T et X : dans des identifications $T \simeq \mathbb{T}^r$, $X \simeq \mathbb{Z}^r$ compatibles on a $\langle \lambda, t \rangle = t^\lambda = t_1^{\lambda_1} \cdots t_r^{\lambda_r}$.

On peut exprimer cette intégrale sur T par une somme sur des poids via une transformée de Fourrier :

$$\begin{aligned} p_k &= \frac{n^{-2k}}{w(G)} \int_T \left(\textstyle\sum_{\lambda \in P(u)} \langle \lambda, t \rangle \right)^{2k} \delta_G(t) \mathrm{d}t \\ &= \frac{n^{-2k}}{w(G)} \sum_{(\lambda_i) \in P(u)^{2k}} \int_T \langle \lambda_1 + \cdots + \lambda_{2k}, t \rangle \delta_G(t) \mathrm{d}t \\ &= \frac{n^{-2k}}{w(G)} \sum_{(\lambda_i) \in P(u)^{2k}} \hat{\delta}_G(\lambda_1 + \cdots + \lambda_n). \end{aligned}$$

On se rend compte alors qu'on s'est ramené à une marche aléatoire *classique* dans le réseau des poids, engendrée par les éléments de $P(u)$. À la normalisation près, p_k est l'espérance de $\hat{\delta}_G : X \to \mathbb{R}$ au temps $2k$ de cette marche. Plus généralement, on peut vérifier que l'espérance dans la marche aléatoire quantique d'une fonction $f : \operatorname{Irr}\operatorname{Rep}(G) \to \mathbb{R}$ correspond dans la marche aléatoire classique à l'espérance de la convolée $\tilde{f} * \hat{\delta}_G$, où $\tilde{f} = \sum f(v) \mathbb{1}_{P(v)} : X \to \mathbb{R}$.

Avec un peu d'analyse — connaissant l'expression de $\hat{\delta}_G$ et sachant qu'un marche aléatoire classique converge vers une gaussienne après renormalisation — on obtient une estimée très simple, toujours en fonction de la dimension réelle d de G : $p_k \approx k^{-d/2}$. À nouveau, je ne connais pas de preuve directe de ce résultat.

On remarque immédiatement le parallèle avec le résultat suivant valable dans le cas des groupes discrets :

$$B_k \approx k^d \iff p_k \approx k^{-d/2},$$

qui repose en partie sur l'équivalence entre « croissance polynômiale » et « virtuellement nilpotent », un résultat difficile dû à Gromov. Comme l'équivalence des estimées est valable pour les groupes discrets et les (duaux des) groupes de Lie compacts, on peut se demander si elle est valable pour tout groupe quantique discret. Cela ouvre un champ de recherches très large.