Algorithmes qui détectent les facteurs libres et applications

Rosique Lambert
Master 2 Mathématiques Fondamentales, 2011-2012

12 juin 2012

Sous la direction d'Arnaud HILION

Table des matières

Introduction

Soit F_k le groupe libre à k générateurs, de base fixée $X = \{x_1, ..., x_k\}$ et $H \leq J \leq F_k$ deux sous-groupes de type fini.

Dans un premier temps on va étudier les "core graphs" (ou graphes de Stallings) de H et de J, en particulier le moyen de passer de l'un à l'autre grâce aux quotients immédiats et les propriétés de ces derniers par rapport aux groupes libres.

Ensuite, on s'intéressera à l'algorithme de Puder qui permet de déterminer si un groupe est facteur libre d'un autre groupe, ou si un mot est primitif (c'est-à-dire s'il appartient à une base du groupe considéré). Cela nous permettra d'identifier les éléments d'une base quelconque.

Enfin, on fera le lien entre primitivité et préservation de la mesure, à l'aide d'un théorème non encore démontré complètement.

Chapitre 1

Préliminaires

1.1 Définitions et notations

Définition 1. *Un groupe J est dit **libre** s'il existe un sous-ensemble S de J tel que tout élément de J s'écrive de manière unique (réduite) comme produit fini d'éléments de S (ou de leurs inverses).*

*Les éléments de J sont des **mots**. Dans la suite, on ne parlera essentiellement que de mots réduits c'est-à-dire tels qu'il n'y a jamais consécutivement une lettre et son inverse dans le mot.*

*De plus, un mot sera dit **primitif** s'il appartient à une certaine base de J. Cela revient à avoir l'existence d'un automorphisme de J qui envoit le mot sur un élément de la base*

Définition 2. *Soit H un sous-groupe du groupe libre J (noté $H \leq J$). H est **facteur libre** de J, noté $H \preccurlyeq J$ s'il existe $H' \leq J$ tel que $H * H' = J$.*

De manière équivalente, si toute base de H peut s'étendre en une base de J, ou encore s'il existe une base de H qui peut s'étendre en une base de J.

Définition 3. *$H \leq F_k$ est dit de **type fini**, noté $H \trianglelefteq F_k$ s'il existe un ensemble de générateurs de H fini.*

Définition 4. *La **caractéristique d'Euler**, notée $\chi()$ est le nombre de sommets moins le nombre d'arêtes d'un graphe.*

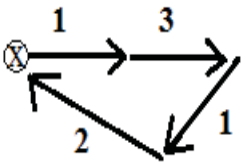
Elle servira à calculer le rang des sous-groupes de type fini J, de core graph $\Gamma_X(J)$, par la formule $rk(J) = 1 - \chi(\Gamma_X(J))$

1.2 Quotient de core graphs

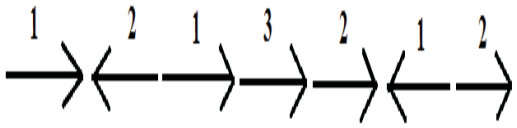
1.2.1 Core graphs

Définition 5. *A chaque sous-groupe $H \leq F_k$ on associe un graphe orienté, étiqueté, "pointed" noté $\Gamma_X(H)$. Les étiquettes sur les arêtes correspondent aux indices de la base $X = \{x_1, x_2, ..., x_k\}$. On l'appelle le core graph associé à H (sous-réserve de l'avoir réduit par un processus explicité plus loin).*

Par exemple,



représente le core graph $H =< x_1x_3x_1x_2 >$, et



représente le mot $w = x_1 x_2^{-1} x_1 x_3 x_2 x_1^{-1} x_2$.

$\otimes$ correspond au mot trivial 1 de H.

Remarque 1. *Les core graphs ont été introduits par Stallings en 1983, mais pour des raisons pratiques, on va légèrement en modifier la définition pour permettre les cas où le degré de $\otimes$ vaut 1 (le degré étant le nombre d'arêtes ayant ce sommet à une extrémité).*

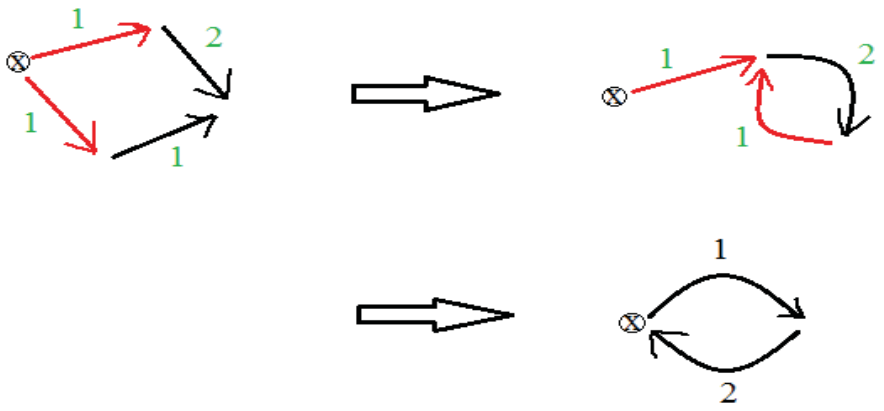
D'autre part, on demandera à n'avoir que des graphes orientés et étiquetés.

Définition 6. *Un* ***morphisme de graphes*** $\phi : \Gamma = (V_1, E_1) \longrightarrow \Delta = (V_2, E_2)$ *où pour $i \in 1, 2$, V_i est un ensemble de sommets et E_i d'arêtes, est une fonction qui préserve la structure de graphe. C'est-à-dire l'orientation des arêtes, l'étiquetage, qui envois des sommets sur des sommets et des arêtes sur des arêtes.*

Définition 7. *Pour obtenir le core graph de n'importe quel graphe, il suffit de "coller" les arêtes qui ont la même étiquette et un sommet en commun.*

*Cette opération est dite "**Stalling's folding**".*

Voici un exemple pratique :



La première étape consiste à coller les deux arêtes rouges étiquetées par 1, puis on refait pareil à l'étape 2.

Remarque 2. *- L'ordre des collages n'a pas d'importance et ne modifie pas le résultat.*

- On obtient bien un core graph (le processus se termine lorsque le groupe associé au graphe est de rang fini)

Proposition 1. *Soit $H \leq F_k$ de core graph Γ.*

1) $rk(H) < \infty \iff \Gamma$ est fini

2) $rk(H) = 1 - \chi(\Gamma)$

3) Soit Λ graphe fini, "pointed" (cela signifie que l'on désigne un sommet comme étant la racine de l'arbre), orienté avec les arêtes étiquetée par $x_1, ..., x_k$. Alors Λ est un core graph si et seulement si :

- Λ est connecté ;

- Chaque sommet est de degré au moins 2 (à l'exception éventuellement de $\otimes$) ;

- Pour tout $1 \leq j \leq k$, deux j-arêtes (i.e. deux arêtes étiquetées par j) ne partagent jamais la même origine ou la même arrivée.

4) On a une bijection entre les sous-groupes de F_k et les core graphs

5) On a une bijection entre les sous-groupes de rang fini de F_k et les core graphs finis

6) Si $rk(H) < \infty$ alors Γ peut être construit via un procédé de "collages" appliqué à n'importe quelle base donnée de H.

La première propriété est facile à voir : comme H est de rang fini, on peut trouver un ensemble fini de générateurs dont on construit le core graph (en appliquant le protocole décrit précédemment) qui est fini. Inversement, le core graph donne un ensemble de générateurs pour H.

La seconde, qui nous intéresse beaucoup, découle de la formule généralisée de la Caractéristique d'Euler pour les CW-Complexes (finis) : c'est la somme alternée des $(k_n)_{n\geq 0}$ (= le nombre de cellules de dimension n).

Pour le reste, on peut trouver les démonstrations dans les ouvrages cités à la fin de ce mémoire.

Proposition 2. *Soient $H_1, H_2 \leq F_k$ et Γ_1, Γ_2 leurs core graphs. Alors :*

1) Il existe un morphisme $\eta : \Gamma_1 \longrightarrow \Gamma_2$ si et seulement si $H_1 \leq H_2$. Si tel est le cas, alors $\eta* : \pi_1(\Gamma_1) \longrightarrow \pi_1(\Gamma_2)$ est injective.

2) Si le morphisme existe alors il est unique.

3) Chaque morphisme est une immersion (i.e. localement injectif sur les sommets).

Une fois encore, les démonstrations ressemblent à celles de la proposition précédente donc il faut se rapporter aux ouvrages si on souhaite les lire.

1.2.2 Quotient

Définition 8. *Soient Γ_1, Γ_2 des core graphs correspondant aux sous-groupes de F_k : H_1 et H_2. On dira que Γ_2 est un **quotient** de Γ_1 s'il existe un morphisme surjectif $\eta : \Gamma_1 \longrightarrow \Gamma_2$, écrit aussi $\eta : \Gamma_1 \twoheadrightarrow \Gamma_2$.*

On utilisera aussi éventuellement l'appellation "Γ_1 couvre Γ_2" ou encore "H_1 couvre H_2" (bien que le morphisme ne soit pas nécessairement localement bijectif).

Remarque 3. *- Surjectif désigne ici "surjectif à la fois sur les sommets et les arêtes". Cette notion dépend évidemment de notre choix de base X, mais dans la suite on ne prendra pas la peine de le repréciser.*

- Par rapport à la proposition précédente, on sait que $H_1 \longrightarrow H_2$ surjectif $\Longrightarrow$ $H_1 \leq H_2$. La réciproque est fausse.

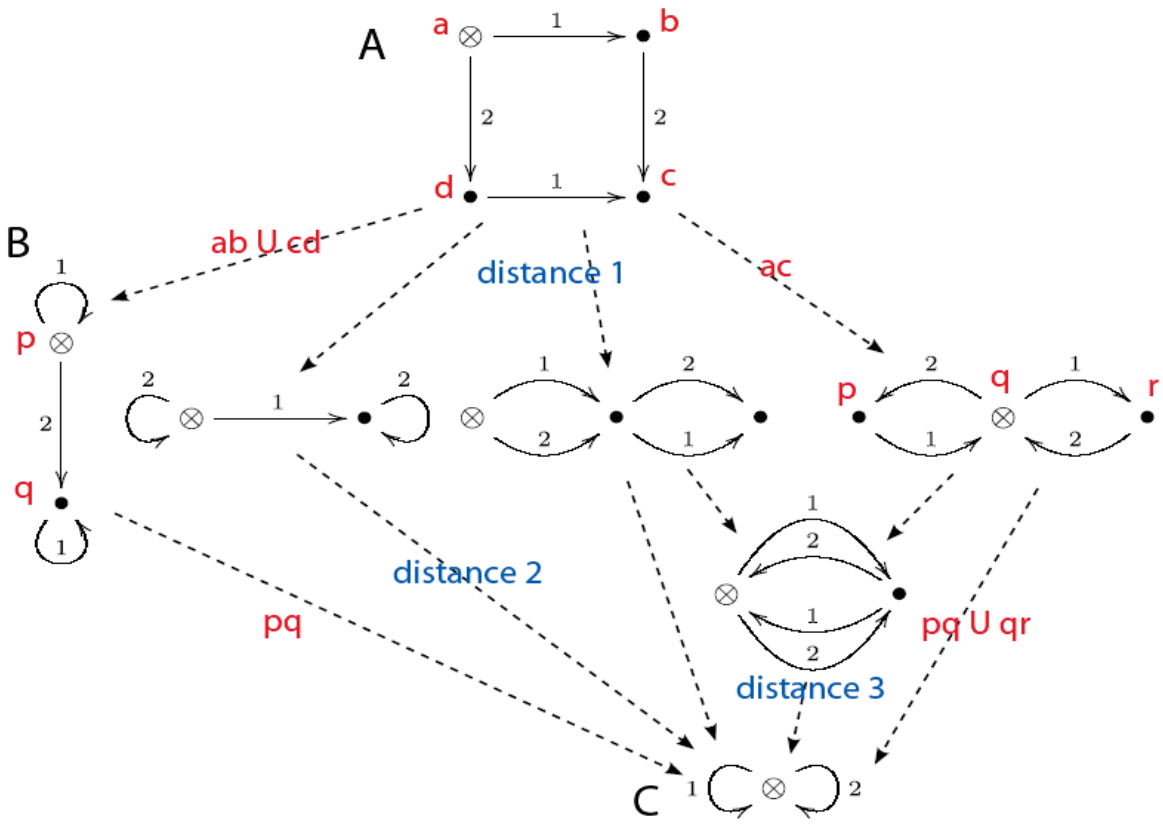
- La relation quotient donne un ordre partiel sur l'ensemble des core graphs, donc on va s'interesser aux quotients les plus "proches" des groupes quotientés : les quotients immédiats.

Définition 9. *Considérons à présent une partition P de $V(\Gamma)$ où Γ est un core graph. Soit Δ le quotient de core graph obtenu à partir de P et de Γ (c'est-à-dire qu'on colle les sommets qui sont dans les "mêmes ensembles" de P). On dit alors que Δ est généré de Γ à partir de P.*

Définition 10. *Soit P une partition de $V(\Gamma)$ telle que chaque ensemble de P contient exactement 1 sommet, à l'exception d'un seul qui en contient deux. Alors, Δ est dit être un **quotient immédiat** de Γ.*

On peut voir assez facilement qu'en termes de groupes libres associés, celà signifie que, si p_u, p_v sont des mots partant de $\otimes$ et d'extrémités respectivement u et v, alors coller u et v revient à rajouter le mot $w = p_u p_v^{-1}$ à H. Autrement dit, à travailler avec $J =< H, w >$.

On peut construire le sous graphe D_k de tous les quotients d'un graphe (ses sommets sont donc des graphes), tel que chaque arête soit orientée et relie un graphe à ses quotients immédiats.



Par exemple, pour passer du graphe A au graphe B il suffit de coller les sommets a et b (ou c et d) puis d'appliquer le protocole pour obtenir un core graph. Le résultat est bien un quotient immédiat (à distance 1 puisqu'on a collé que 2 sommets).
On remarque aussi que le graphe C est à distance "2 ou 3" suivant par quelle chaine de quotients immédiats on passe donc c'est pour ca qu'on définit ϱ comme un minimum, et c'est aussi la raison pour laquelle l'algorithme de Puder demande à construire D_k (car trouver un chemin ne suffit pas).

Définition 11. *On définit $\varrho_X(H_1, H_2)$ ou $\varrho(\Gamma_1, \Gamma_2)$ comme étant la plus courte distance dans D_k, en terme de chaine de quotients immédiats, pour aller de Γ_1 à Γ_2 (la longueur d'une arête est fixée à 1).*

Avec notre remarque précédente, on voit que c'est aussi le nombre minimum de paires de sommets à identifier pour obtenir Γ_2 à partir de Γ_1 (en fait, on colle et on utilise le "folding" si on peut pour garder un core graph). Par conséquent, le rang

du sous-groupe associé à un quotient immédiat a augmenté d'au plus 1 (par rapport au sous-groupe non encore quotienté).
Autrement dit,
$$H \twoheadrightarrow J \Longrightarrow rk(J) - rk(H) \leq \varrho_X(H, J)$$

Théorème 1. *Si $H, J \trianglelefteq F_k$ avec $H \twoheadrightarrow J$ alors*
$rk(J) - rk(H) \leq \varrho(H, J) \leq rk(J)$.

(La démonstration de ce théorème est donnée par D. Puder dans son article)

Chapitre 2

Caractérisation des groupes libres

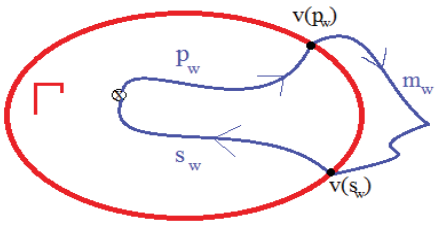
2.1 Théorème

Théorème 2. *Soit $H \trianglelefteq J \trianglelefteq F_k$ tel que $H \twoheadrightarrow J$. On a alors*
$\varrho(H, J) = rk(J) - rk(K) \iff H \lessdot J$

Démonstration. Remarquons que coller deux sommets de $\Gamma_X(H)$ revient à ajouter un générateur à H. Donc si $\varrho(H, J) = rk(J) - rk(H)$ alors J s'obtient de H en ajoutant $rk(J) - rk(H)$ générateurs à H, ie $H \lessdot J$.
Réciproquement, si $H \lessdot J$, on pose $t = rk(J) - rk(H)$, $\Gamma = \Gamma_X(H)$, $\Delta = \Gamma_X(J)$.
Intéressons-nous au cas où $t > 0$ (car $t < 0$ est impossible, et si $t = 0$ alors $H = J$) :

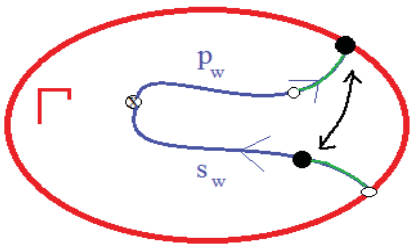
- Si $t = 1$

Soit $w \in F_k$ tel que $J =< H, w >$;
p_w : le plus long préfixe de w dans Γ
s_w : le plus long suffixe de w dans Γ
Si $|p_w| + |s_w| < |w|$ alors il existe un certain $m_w \in F_k$ réduit, différent de 1, tel que $w = p_w m_w s_w$. Notons $v(p_w)$ la dernière lettre du mot p_w et $v(s_w)$ la première de s_w.
On a ainsi le schéma suivant



On peut rajouter une "hanse" allant de $v(p_w)$ à $v(s_w)$ dans Γ, tel que le core graph obtenu soit équivalent à celui de J, ie c'est Δ.
D'où Γ est un sous-graphe propre de Δ (c'est-à-dire qu'il est strictement contenu dedans), ce qui est contradictoire avec le fait que Δ est un quotient de Γ (on a supposé $H \twoheadrightarrow J$ ce qui en revient au même).

Par conséquent, $|p_w| + |s_w| \geq |w|$. Ainsi, p_w et s_w ont une partie commune et il existe une paire de sommets dans Γ qui, en les collant, ajoute w à H comme générateur complémentaire pour J.



On obtient que $\varrho(H, J) = 1$.

- Si $t \geq 2$
On raisonne par récurrence, avec les notations suivantes :
Soit $(w_i)_{i \leq t}$ une base complémentaire de H pour J, ordonnée, telle que pour tout i on ait $J_i =< H, w_1, ..., w_i >$ avec $H = J_0 \lessdot J_1 \lessdot ... \lessdot J_t = J$ et Γ_i core graph de J_i.
p_i, s_i les plus longs préfixes / suffixes de w_i dans Γ_{i-1},

$$h(\Gamma_{i-1}, w_i) := \begin{cases} |w_i| - |p_i| - |s_i| \text{ si c'est positif} \\ 0 \qquad\qquad\qquad\qquad \text{sinon} \end{cases}$$

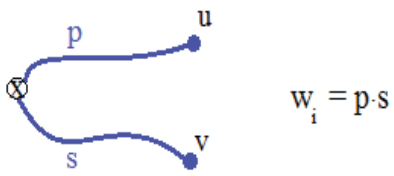
D'après ce qui précède, on a Γ_i quotient immédiat de Γ_{i-1} ssi $h(\Gamma_{i-1}, w_i) = 0$.

Pour chaque base ordonnée $(w_1, ..., w_t)$ on considère $(h(\Gamma_{i-1}, w_i))_{i\leq t}$: on fixe les w_i de sorte à avoir la deuxième suite minimale lexicographiquement.
On veut montrer que c'est une suite de zéros.

a) Si tous les $h(\Gamma_{i-1}, w_i)$ sont strictement positifs alors Γ_{i-1} est un sous-graphe propre de Γ_i, pour tout $i \Longrightarrow \Gamma$ sous-graphe propre de Δ, ce qui est contradictoire avec le fait que $H \twoheadrightarrow J$.

b) Si $h(\Gamma_0, w_1) = 0$, alors $\varrho(H, J_1) = 1$. On a :
$H \twoheadrightarrow J_1 \twoheadrightarrow J$ (car sinon le morphisme de Γ dans Δ passant par Γ_1 ne pourrait pas être surjectif).
Or, $J_1 \lessdot J$ et $rk(J) - rk(J_1) = t - 1$ d'après l'hypothèse de récurrence, donc $\varrho(J_1, J) = t - 1$ ce qui implique que $\varrho(H, J) = t$.

c) Supposons dorénavant que $h(\Gamma_{i-2}, w_{i-1}) > 0$ et $h(\Gamma_{i-1}, w_i) = 0$ pour tout i.
Autrement dit, Γ_{i-1} s'obtient de Γ_{i-2} en ajoutant une hanse représentant m_{i-1}.



Soit $w_i = ps$ (Γ_i s'obtient de Γ_{i-1} en identifiant u et v). On peut supposer que p ne traverse pas m_{i-1} "plus que nécessaire" (en multipliant par le bon élément de J_{i-1} sinon). En effet, si $u \notin m_{i-1}$ alors p évite m_{i-1} et si $u \in m_{i-1}$ alors seule la fin de p est dans m_{i-1} (jusqu'à u). Idem pour s et v.
On distingue trois cas :

α. Si $u, v \in V(\Gamma_{i-2})$ alors $h(\Gamma_{i-2}, w_i) = 0$ (car w_i est dans Γ_{i-2}) donc on peut échanger w_i et w_{i-1} pour réduire lexicographiquement la suite, ce qui est contradictoire.

β. Si $v \in V(\Gamma_{i-2})$ mais $u \in V(\Gamma_{i-1})$, $u \notin V(\Gamma_{i-2})$ (c'est-à-dire u est sur m_{i-1} alors l'hanse nécessaire pour ajouter w_i à Γ_{i-2} est plus petite que $h(\Gamma_{i-2}, w_{i-1})$, donc on peut échanger w_i et w_{i-1} pour réduire la suite.

γ. Si u, v sont dans $V(\Gamma_{i-1})$ mais pas dans $V(\Gamma_{i-2})$ alors on peut multiplier w_i par des éléments de J_{i-1} pour que le chemin p (resp. s) ne passse pas par v (resp.

u).
Alors $h(\Gamma_{i-2}, w_i) < h(\Gamma_{i-2}, w_{i-1})$ donc on peut échanger w_i et w_{i-1}, ce qui achève la démonstration.

□

2.2 Algorithme de Puder

Dans cette section, nous allons présenter l'algorithme mis en place par Doron Puder pour détecter les facteurs libres (ou les mots primitifs), puis nous verrons quelques applications simples.
Données : Soient $H, J \trianglelefteq F_k$ avec les ensembles qui les génèrent.

Proposition 3. *Soient $H, J, K \leq F_k$:*
- La relation de "facteur libre" est transitive i.e. $H \lessdot J \lessdot K \Longrightarrow H \lessdot K$.
- S'il existe un plongement $\eta : \Gamma_X(H) \longrightarrow \Gamma_X(J)$ alors $H \lessdot J$.
- Si $H \lessdot J$ alors H est facteur libre de tout sous-groupe M tel que $H \leq M \leq J$.

Démonstration. Les deux premières propriétés sont immédiates.
Pour la troisième, supposons que $H \lessdot J$ et soit Y une base de J telle que $J =< H, Y >$. En particulier, $\Gamma_Y(H)$ et $\Gamma_Y(J)$ sont des bouquets (i.e. un unique sommet avec $rk(H)$ resp. $rk(J)$ boucles).
Pour tout sous-groupe M entre H et J considérons le morphisme $\eta : \Gamma_Y(H) \longrightarrow \Gamma_Y(M)$. Or, un morphisme de core-graph sur un bouquet est nécessairement un plongement donc nécessairement $H \lessdot M$.

□

Algorithme

$1^{ère}$ étape : Construire les core graphs associés et le morphisme.
Il faut construire $\Gamma = \Gamma_X(H)$ et $\Delta = \Gamma_X(J)$ à partir des générateurs de H et de J comme vu précédemment. Ensuite, il faut trouver un certain morphisme $\eta : \Gamma \to \Delta$, car s'il n'en existe pas, H ne peut pas être un sous-groupe de J.
Pour construire cet η, on suit le protocole suivant :
Le point base de Γ est envoyée sur celui de Δ ;

Tant que η n'est pas complètement déterminé, il existe une certaine j-arête $e = (u, v)$ dont l'image n'est pas encore donnée mais telle que l'image d'un de ses sommets u ou v est connue (mettons qu'il s'agisse de u). De fait, $\eta(e)$ ne peut prendre au plus qu'une seule valeur, car du sommet $\eta(u)$ part au plus une j-arête. Remarquons que $\eta(v)$ doit être le sommet terminal de l'arête $\eta(e)$ car sinon on aurait une contradiction (deux valeurs pour un même sommet).
Si le processus de construction n'échoue pas, c'est que H est bien un sous-groupe de J et on a notre morphisme. Sinon, le théorème n'a pas lieu de s'appliquer.

$2^{ème}$ étape : Réduire les groupes grâce au morphisme.
On considère le graphe $\Delta' = \eta(\Delta)$. C'est un core graph par construction ; notons J' le sous-groupe lui correspondant.
Comme Δ' est le graphe obtenu de Δ en ayant enlevé toutes les arêtes et sommets non-présents dans l'image de η, on voit qu'il s'agit d'un quotient de Γ, et donc on a une surjection entre H et J'.
D'après les résultats qui précèdent,

$$H \lessdot J \iff H \lessdot J'$$

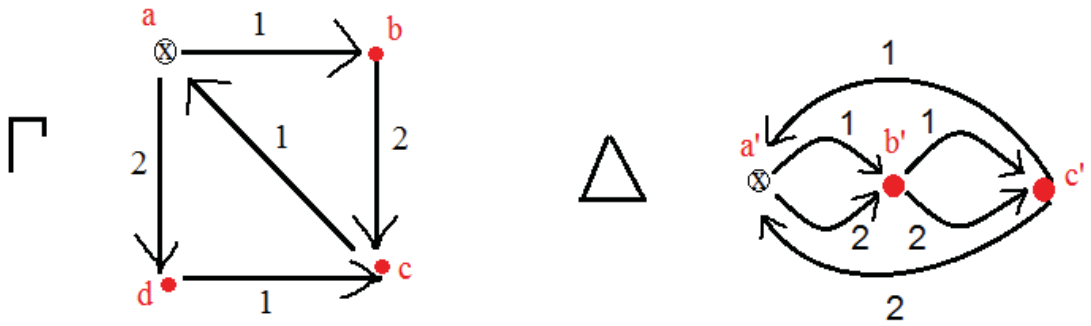
Du coup il nous suffira de travailler avec H et J' (on pourra y appliquer le théorème) :

$3^{ème}$ étape : Calculer la distance de H à J'.
En effet, $\varrho_X(H, J') = rk(J') - rk(H)$ si et seulement si $H \lessdot J'$. Le rang se calcule, rappelons-le, à l'aide le χ.

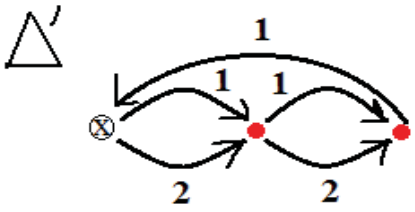
2.2.1 Exemple

1) Facteur libre

Considérons $H =< x_1x_2x_1^{-1}x_2^{-1}, x_2x_1^2 >$ et $J =< x_1^3, x_2^3, x_1x_2^{-1}, x_1x_2x_1 >$ dans F_2.



Construction du morphisme :
$\eta(a) = a'$;
$\eta(1) = 1$;
$\eta(2) = 2$;
$\eta(b) = b'$ (on suit la flêche 1 sur les deux graphes) ;
$\eta(c) = c'$;
$\eta(d) = b'$.
Notre morphisme peut bien être construit, et on voit au passage que l'arête étiquetée par 2 et joignant c' à a' n'a pas d'antécédent par η. Donc on obtient le Δ' suivant :

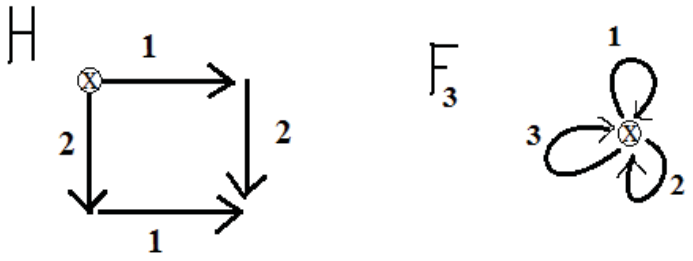


avec $J' =< x_1^3, x_1x_2^{-1}, x_1x_2x_1 >$. On calcule les rangs des groupes :
$rk(H) = 1 - \chi(\Gamma) = 2$
$rk(J') = 1 - \chi(\Delta') = 3$
Donc $rk(J') - rk(H) = 1$
D'autre part, $\varrho(H, J') > 0$ car les deux groupes sont différents. Or, si on colle b et d dans Γ on obtient exactement Δ', d'où Δ' est un quotient immédiat de Γ, ce qui donne
$$\varrho(H, J') = 1 = rk(J') - rk(H) \Longrightarrow H \lessdot J' \Longrightarrow H \lessdot J.$$

2) Mot primitif

Pour étudier si un mot est primitif ou non, il suffit de considérer le groupe engendré par ce mot et d'appliquer l'algorithme en le comparant au groupe libre F_k (le k dépend évidemment de notre mot). Lorsqu'on veut savoir s'il est primitif dans un groupe, il suffit de remplacer F_k par ce groupe.

Concrêtement, considérons le mot $w = x_1 x_2 x_1^{-1} x_2^{-1}$ et regardons s'il est primitif dans F_3. Posons $H =< w >$; voici les core graphs :



- On peut construire le morphisme : on voit que $\eta(H) = F_2$, donc Δ' est le quotient de Γ.

- $\forall k, rk(F_k) = k$

- $rk(H) = 1 - (4 - 4) = 1$

D'où $rk(F_2) - rk(H) = 1$ mais $\varrho(F_2, H) = 2$ donc H n'est pas facteur libre de F_2 (donc de F_3) et w ne peut pas être primitif dans F_3.

Chapitre 3

Lien avec préservation de la mesure

3.1 Théorème

Définition 12. *$w \in F_k$ **préserve la mesure** si pour tout groupe fini G et un homomorphisme pris aléatoirement α_G on a $\alpha_G(w)$ distribué uniformément dans G. Cette notion peut être étendue aux sous-groupes finis de F_k comme suit :*
Si $H \leq F_k$ de type fini alors H préserve la mesure si pour tout groupe fini G et α_G homomorphisme pris aléatoirement on a la restriction de α_G à H qui est uniformément distribuée dans $Hom(H, G)$.

Remarque 4. *On peut voir w dans la base $X = \{x_1, ..., x_k\}$comme l'application $G \times G \times ... \times G \longrightarrow G$ où G un groupe fini arbitraire et on a pris k copies de G. Le $k-uplet$ $(g_1, ..., g_k)$ a pour image le mot obtenu en remplacant les x_i du mot w par les g_i (respectivement) et en évaluant l'expression obtenue comme élément de G.*
Du coup, on dira que w préserve la mesure si, pour une mesure uniforme donnée sur $G \times ... \times G$, w induit une mesure uniforme sur G (pour tout G fini).

Dans la mesure où un homomorphisme dans un groupe libre est entièrement déterminé en choisissant les images des éléments de la base, la probabilité de choisir un homomorphisme en particulier sera toujours de $\frac{1}{|G|^k}$.

- En particulier, si $w \in F_k$ non-trivial préserve la mesure si et seulement si $< w >$ préserve la mesure.
- Les notions de primitivité d'un mot ou de sous-groupe facteur libre amènent directement la propriété de préservation de la mesure par définition. On va donc s'intéresser à une éventuelle réciproque.

Commencons par énoncer une conjecture dont on s'attachera à un cas particulier :

Conjecture 1. *Soit $w \in F_k$,*
w est primitif $\iff$ w préserve la mesure.
Plus généralement, si $H \trianglelefteq F_k$,
$H \ll F_k \iff H$ préserve la mesure.

Théorème 3. *Soit $H \trianglelefteq F_k$ de rang au moins $k-1$. Alors*
$H \ll F_k \iff H$ préserve la mesure.
En particulier, pour tout $w \in F_2$,
w est primitif $\iff$ w préserve la mesure.

Pour démontrer ce théorème, qui est un cas particulier de la conjecture précédente, nous aurons besoin de plusieurs outils.

3.2 Fonctions

Définition 13. *Le rang primitif d'un mot $w \in F_k$ est*
$\pi(w) = min\{rk(J) | w \in J \leq F_k$ tel que w n'est pas primitif dans $J\}$.
Il s'agit d'un entier compris entre 0 et l'infini (lorsqu'aucun J avec cette propriété n'existe).
Un J pour lequel le minimum est atteint sera dit w-critique.

On étend encore une fois la définition aux sous-groupes $H \trianglelefteq F_k$:
$\pi(H) = min\{rk(J) | H \leq J \leq F_k$ tel que H ne soit pas un facteur libre de $J\}$.

Exemple 1. - *$\pi(w) = 0 \iff w = 1$ car le seul groupe de rang 0 est la racine $\otimes$ (autrement dit, le mot 1), donc tout mot différent de 1 n'est pas dans ce groupe et donc le rang primitif est forcément différent de 0.*

- *$\pi(w) = 1 \iff w = v^d$ pour un certain $v \in F_k$ et $d > 1$. Il suffit de prendre $J =< v >$: $w \in J$ mais w n'y est pas primitif, et d'après ce qui précède $\pi(w) > 0$.*

- *$\pi(H) = \infty \iff H \ll F_k$ (on peut remplacer H par w et le membre de droite par "w est primitif"). En effet, par définition du rang primitif, on a en particulier que H n'est pas un facteur libre de F_k (qui est de rang k) donc $\pi(H) \leq k < \infty$.*

Réciproquement, si $H \lessdot F_k$ alors H est facteur libre de tout sous-groupe le contenant (d'après une proposition précédente). Ainsi, on obtient que $\pi(H) = \infty$.

- Pour tout $H \leq F_k$, $\pi(H) \in \{0, 1, ..., k\} \cup \infty$. De plus, $\pi()$ prend bien toutes les valeurs possibles car, par exemple, pour tout $1 \leq d \leq k, \pi(x_1^2...x_d^2) = d$.

Définition 14. *On définit à présent, pour tout $H \trianglelefteq F_k$, $\alpha_n \in Hom(F_k, S_n)$ homomorphisme pris au hasard uniformément distribué, avec S_n le groupe des permutations,*

$$\Phi_H(n) = Prob[\forall w \in H, \alpha_n(w)(1) = 1] - \tfrac{1}{n^{rk(H)}}.$$

Cette fonction mesure l'écart entre la probabilité que 1 soit un point fixe commun à tous les éléments de H et cette probabilité dans le cas d'un sous-groupe qui préserve la mesure.

Si H préserve la mesure alors évidemment Φ_H s'annule pour tout $n > 0$.

Cette écriture de Φ n'étant pas pratique, D. Puder s'inspire d'un résultat de A. Nica pour l'exprimer comme une série de puissances de $\frac{1}{n}$: Il montre d'abord que (si on note e_Γ (resp. v_Γ) le nombre d'arêtes (resp. de sommets) de Γ,

$$\Phi_H(n) = -\tfrac{1}{n^{rk(H)}} + \textstyle\sum_{\Gamma \in O_X(H)} \frac{1}{n^{e_\Gamma - v_\Gamma + 1}} \times \frac{(1-\frac{1}{n})(1-\frac{2}{n})...(1-\frac{v_\Gamma - 1}{n})}{\prod_{j=1}^{k}(1-\frac{1}{n})...(1-\frac{e_\Gamma^j - 1}{n})}$$

et donc on peut écrire la fonction sous la forme

$$\Phi_H(n) = -\tfrac{1}{n^{rk(H)}} + \textstyle\sum_{i=0}^{\infty} a_i(H)\frac{1}{n^i}$$

où les $a_i(H)$ sont des entiers qui ne dépendent que de H. On pose $\Phi(H)$ le plus petit entier i tel que $a_i(H)$ soit non-nul si la fonction Φ_H n'est pas la fonction nulle, et ∞ sinon.

Par exemple,

$$\begin{aligned}\Phi_{H=<x_1x_2x_1^{-1}x_2^{-1}>}(n) &= -\tfrac{1}{n} + \tfrac{(n-1)(n-2)(n-3)}{n(n-1)n(n-1)} + \tfrac{n-1}{n(n-1)\times n} + \tfrac{n-1}{n\times n(n-1)} + \tfrac{(n-1)(n-2)}{n(n-1)\times n(n-1)} + \\ &\tfrac{(n-1)(n-2)}{n(n-1)\times n(n-1)} + \tfrac{n-1}{n(n-1)\times n(n-1)} + \tfrac{1}{n\times n} \\ &= -\tfrac{1}{n} + \tfrac{1}{n-1} \\ &= \tfrac{1}{n(n-1)} \\ &= \tfrac{1}{n^2} \times \tfrac{1}{1-\frac{1}{n}} \\ &= \textstyle\sum_{i=2}^{\infty} \frac{1}{n^i}.\end{aligned}$$

Ainsi, $a_0(H) = a_1(H) = 0$ et $a_2(H) = 1 \Longrightarrow \Phi(H) = 2$

Evidemment, si H préserve la mesure alors $\Phi(H) = \infty$.

Faisons maintenant le lien entre nos deux fonctions π et Φ :

Proposition 4. *Si $H \trianglelefteq F_k$, $i \leq rk(H)+1$,*
1) $\pi(H) = i \iff \Phi(H) = i$
2) Si $\pi(H) = i$ on a en fait qu'$a_i(H)$ est le nombre de sous-groupes H-critiques de F_k.

Autrement dit, les fonctions coincident sur $0, ..., rk(H)+1$. On peut remarquer que si $\pi(H) = \infty$ alors $H \lessdot F_k$ et donc H préserve la mesure, i.e. $\Phi(H) = \infty$. En effet, la primitivité ou la propriété d'être facteur libre amènent directement la préservation de la mesure car un homomorphisme de $Hom(F_k, G)$ est entièrement déterminé par son image des éléments de la base de F_k, que l'on peut choisir complètement arbitrairement et indépendamment (donc on ne "charge" aucun élément en particulier).

De plus, les deux fonctions sont additives par rapport à la concaténation des mots sur des alphabets distincts :

si $w_1, w_2 \in F_k$ sans lettres en commun alors $\pi(w_1 w_2) = \pi(w_1) + \pi(w_2)$ et idem pour Φ.

On généralise la proposition précédente en une conjecture plus large

Théorème 4. $\forall H \trianglelefteq F_k, \pi(H) = \Phi(H)$
De plus, $a_{\Phi(H)}(H)$ est le nombre de sous-groupes H-critiques de F_k.

Toutefois, on n'a besoin que de la proposition pour démontrer le résultat annoncé dans cette partie :

si $rk(H) \geq k-1$ alors pour tout $i \leq k$, $\pi(H) = i \iff \Phi(H) = i$. Comme de toute facon $\pi(H) \in \{0, 1, 2, ..., k\} \cup \{\infty\}$ on obtient que $\pi(H) = \Phi(H)$, et de fait le résultat puisque, rappelons-le :

- H est facteur libre de $F_k \iff \pi(H) = \infty$;

- H préserve la mesure $\iff \Phi(H) = \infty$.

Pour la preuve, on peut la trouver détailler dans le papier de D. Puder, en voici les idées.

1) On montre que la proposition est vraie pour $i < rk(H)$:
Soit m le plus petit rang d'un groupe $J \leq F_k$ tel que $H \twoheadrightarrow J$. On a $\pi(H) = i \iff m = i$ car H ne peut pas être facteur libre d'un sous-groupe de plus petit rang. Il faut alors prouver que $\Phi(H) = i \iff m = i$ en traitant deux cas, $m < rk(H)$ et $m \geq rk(H)$.

2) Ensuite on s'intéresse à $i = rk(H)$ qui ressemble, à ceci près qu'on a recourt à un lemme disant que $\pi(H) \geq rk(H) \iff \Phi(H) \geq rk(H)$ et qu'on montre que

chaque membre de l'équivalence dans la proposition revient à dire qu'il existe un quotient de rang $rk(H)$ dans $O_X(H)$ autre que $\Gamma_X(H)$.

3) Enfin, le cas $i = rk(H) + 1$ est le plus difficile à mettre en place, puisqu'il faut étudier les contributions à la somme de $\Phi(H)$ des core graphs.

Ceci achève la démonstration du résultat annoncé dans cette partie.

Conclusion

On a longuement présenté le théorème sur les groupes libres et son application principale : l'algorithme de D. Puder, qui permet de déterminer si un mot fait partie d'une base d'un groupe ou non. Toutefois, il est bon de mentionner qu'un autre algorithme, largement plus répandu, existe : celui de Whitehead, dont la complexité est plus élevée que celle qu'on a pu étudier ici. Est-il encore possible d'améliorer l'algorithme, en faisant le lien avec la préservation de la mesure ? En effet, il existe un lien intrinsèque entre les deux notions, même si le théorème les reliant reste à démontrer (i.e. prouver que Φ et π coincident bien). On pourra aussi s'interroger sur le nombre de points fixes d'une permutation aléatoire $\alpha_n(w)$.

Bibliographie

[1] *I. KAPOVICH and A. MYASNIKOV, Stallings foldings and subgroups of free groups 1, Journal of Algebra 248 (2002), no. 2, 608-668.*

[2] *A. MIASNIKOV, E. VENTURA and P. WEIL, Algebraic extensions in free groups, Geometric group theory (G.N. Arzhantseva, L. Bartholdi, J. Burillo and E. Ventura, eds.), Trends Math., Birkhauser, 2007, pp. 225-253.*

[3] *Alexandru NICA, On the number of cycles of given length of a free word in several random permutations, Random Structures and Algorithms 5 (1994), no. 5, 703-730.*

[4] *Doron PUDER, Primitive Words, Free Factors and Measure Preservation, Einstein Institute of Mathematics, Hebrew University of Jerusalem, 12 septembre 2011.*

[5] *John R. STALLINGS, Topology of finite graphs, Inventiones mathematicae 71 (1983), no. 3, 551-565.*