Sous-groupes aléatoires d'un groupe libre.

Cyril Nicaud

Laboratoire d'Informatique Gaspard-Monge, Université Paris-Est, CNRS
Avec Frédérique Bassino, Dominique Gouyou-Beauchamps, Armando Martino, Enric Ventura et Pascal Weil

ALEA – mars 2010

60 ans de Dominique Gouyou-Beauchamps à Orsay le 7 mai.
http ://www.lri.fr/~orteel/

Frédérique Bassino

Dominique Gouyou-Beauchamps

Armando Martino

Enric Ventura

Pascal Weil

I. Groupe Libre

Groupe

- Un *groupe* est un ensemble muni d'une loi de composition interne associative, avec un élément neutre 1, et telle que tout élément x possède un inverse x^{-1}.
- Soit H un sous-groupe de G, pour tout $g \in G$, la classe à gauche de g est
$$gH = \{gh \mid h \in H\}$$
- L'*indice* d'un sous-groupe est le nombre de classes à gauche.
- Si $gH = Hg$, pour tout $g \in G$, on dit que que le sous-groupe est *normal* (ou encore *distingué*).
- Si H est normal, alors l'ensemble des classes à gauche a naturellement une structure de groupe, on le note G/H, c'est le *groupe quotient* de G par H.

Groupe libre

- On se donne le *rang* $r \geq 2$ et un alphabet A de cardinal r comme base.
- Pour construire le groupe libre $F = F(A)$, on ajoute les inverses formels des lettres de A, l'alphabet A^{-1}, et on considère des mots *réduits* sur $A \cup A^{-1}$.
- Réduit signifie qu'il n'y a pas une lettre suivie par son inverse dans le mot (ni aa^{-1} ni $a^{-1}a$).
- Exemples :

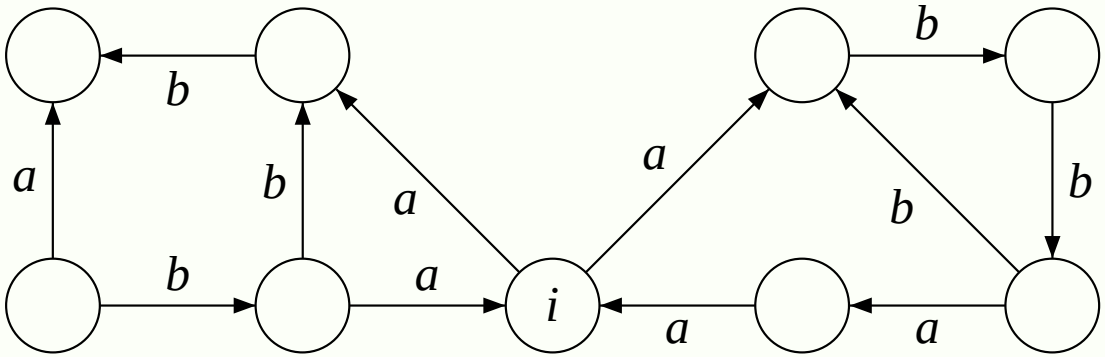
$$aab^{-1}a^{-1}abcca^{-1} \qquad ab^{-1}b^{-1}aaba^{-1}$$

- On a une structure de groupe pour la concaténation/réduction.

Sous-groupes

- Les sous-groupes d'un groupe libre sont libres (Théorème de Nielsen-Schreier).
- On s'intéresse aux sous-groupes finiment engendrés : on prend k générateurs $U = \{u_1, \cdots, u_k\}$ et on considère tous les mots (réduits) obtenus en multipliant des éléments de U ou des inverses d'éléments de U.
- De tels sous-groupes peuvent être représentés, de façon unique, par un graphe fini (une sorte d'automate fini).
- Cette description est très utilisée, on peut lire un certain nombre de propriétés du sous-groupe directement sur son graphe.

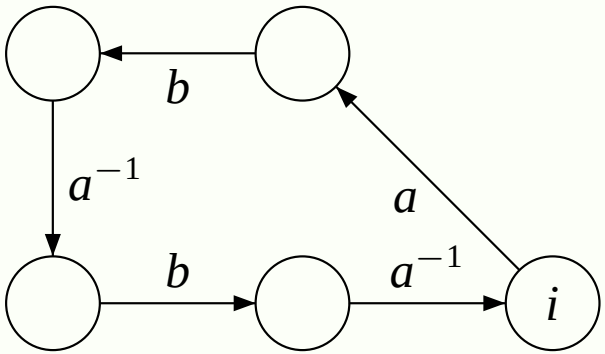
Exemple de tel graphe



$aba^{-1}bba^{-1}$ est dans le sous-groupe mais pas $a^{-1}a^{-1}b$.

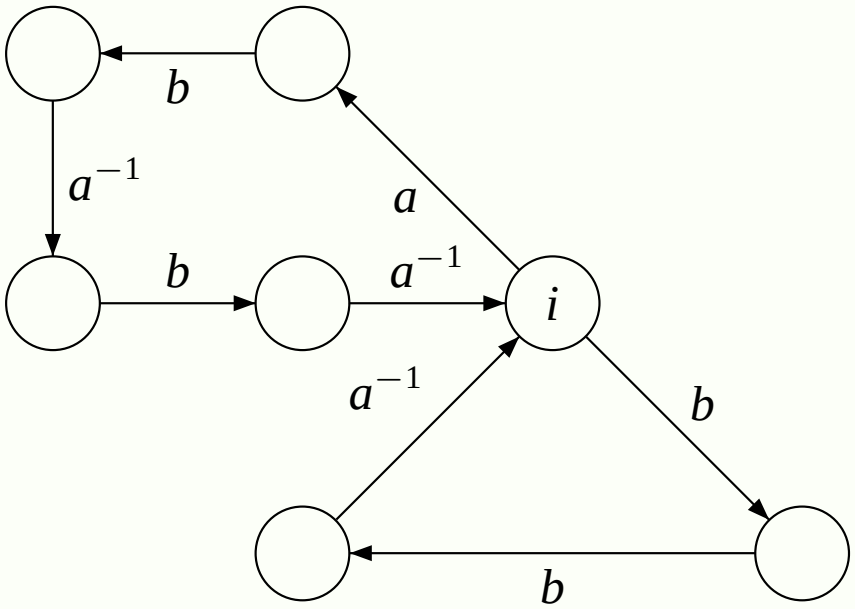
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



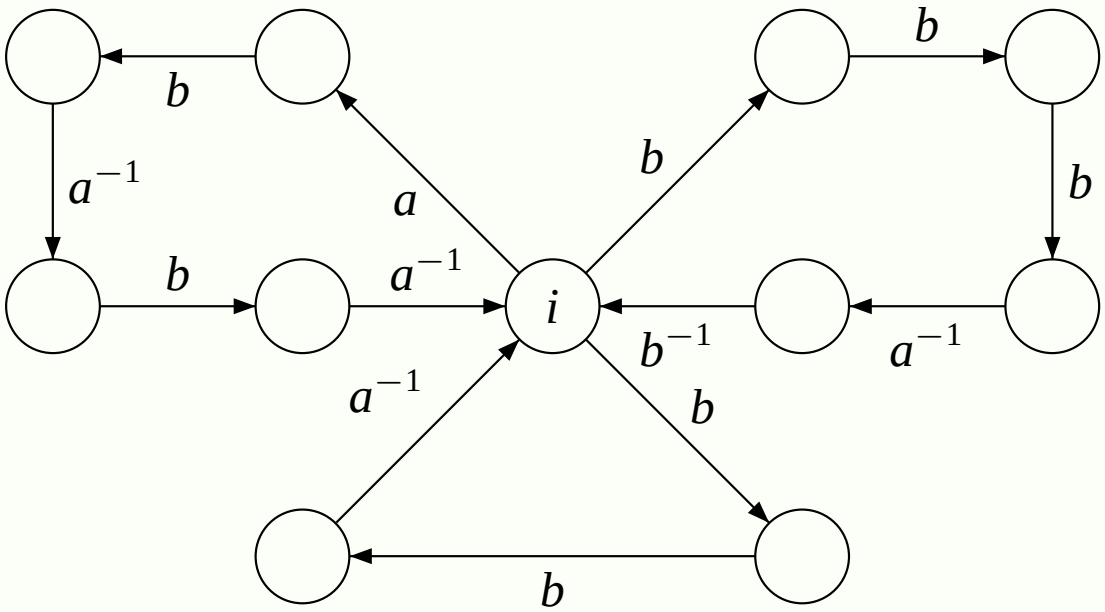
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



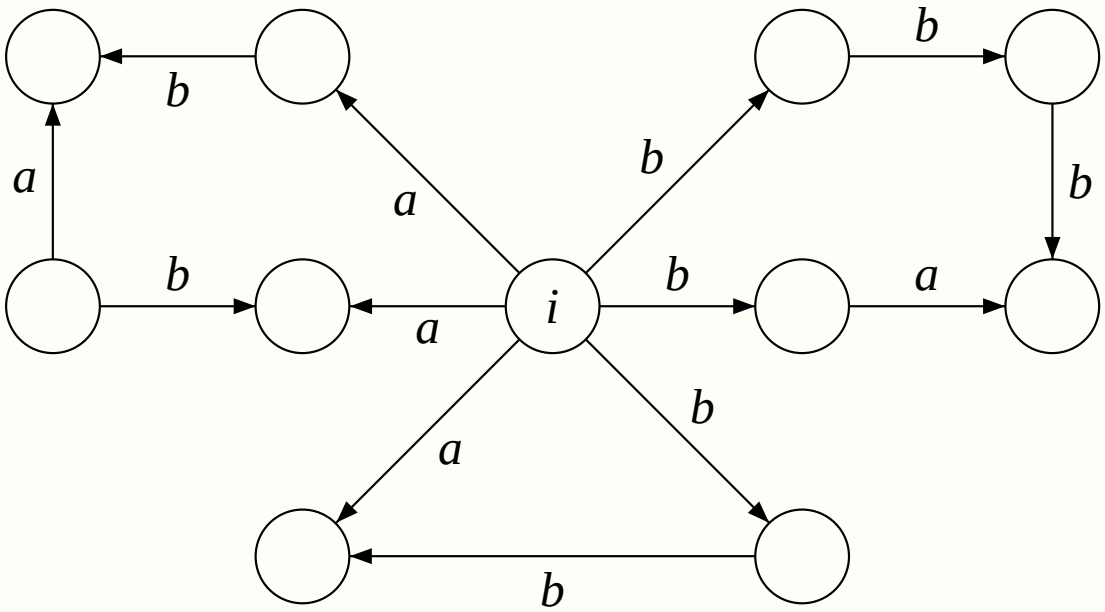
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



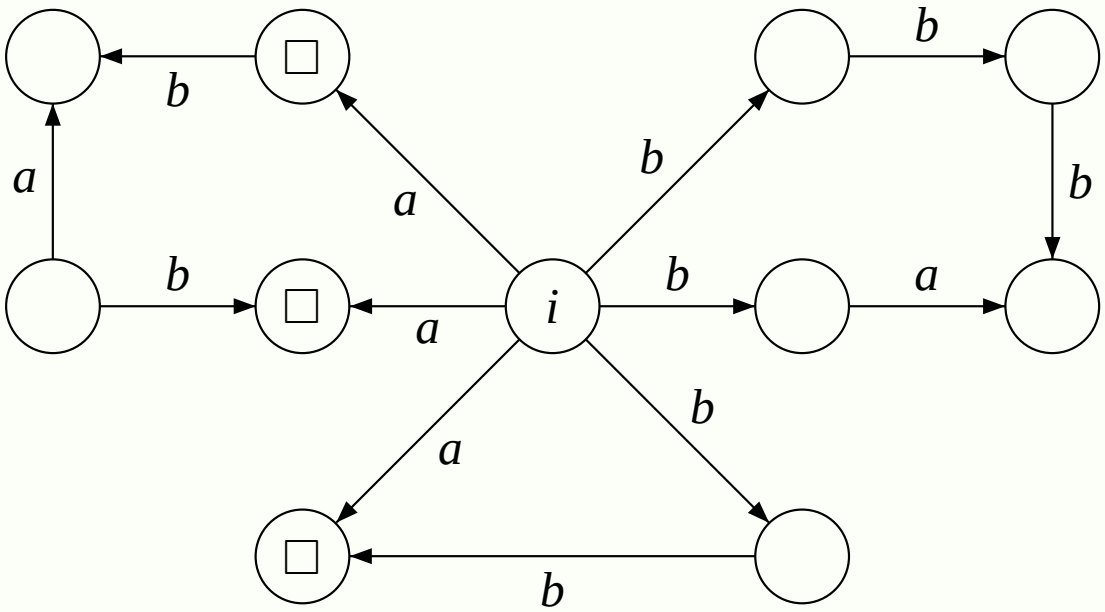
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



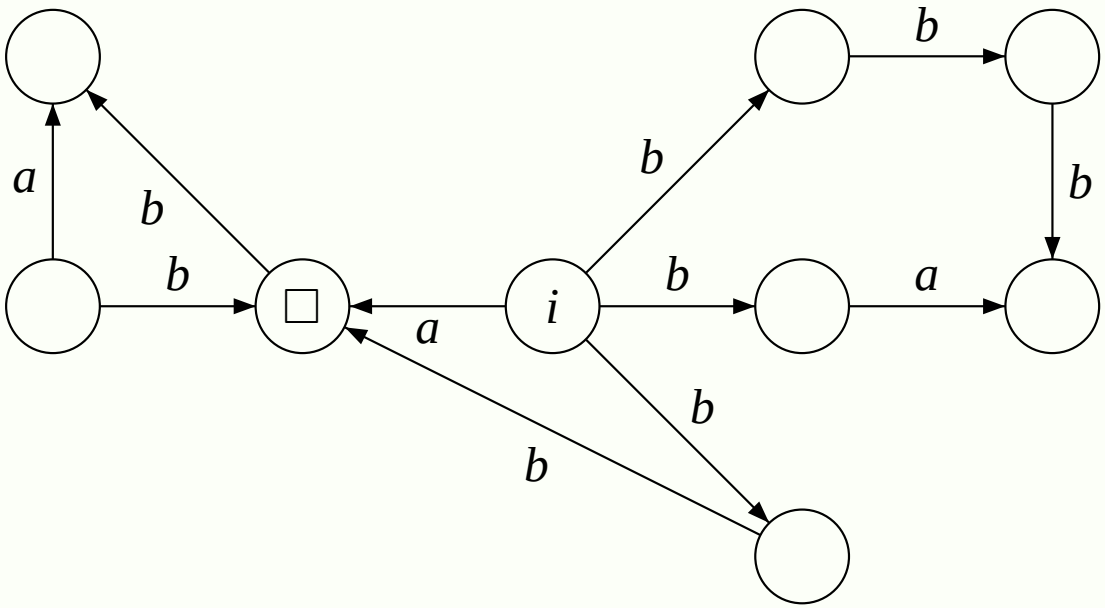
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



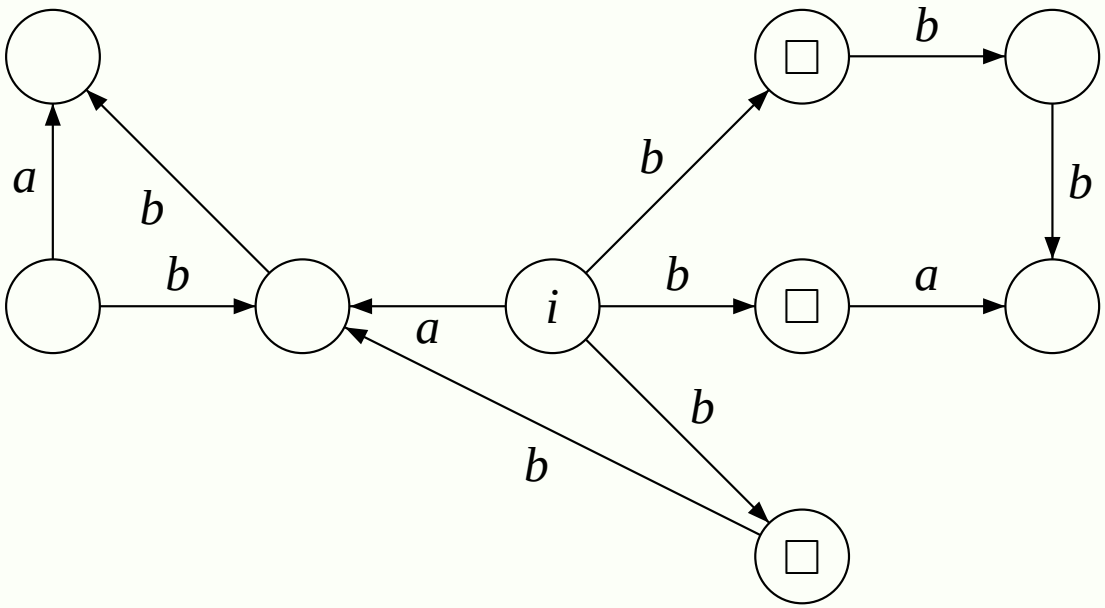
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



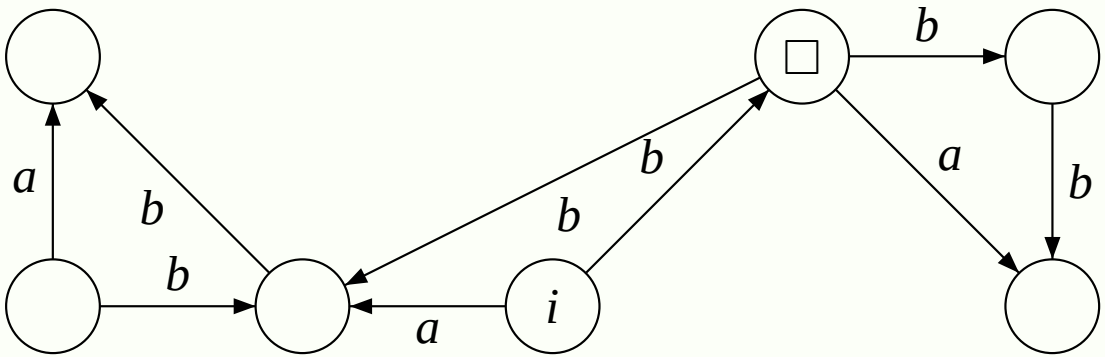
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



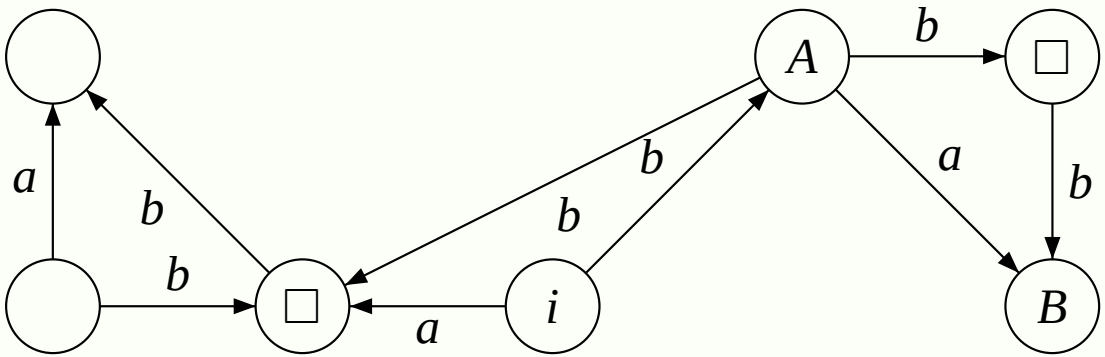
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



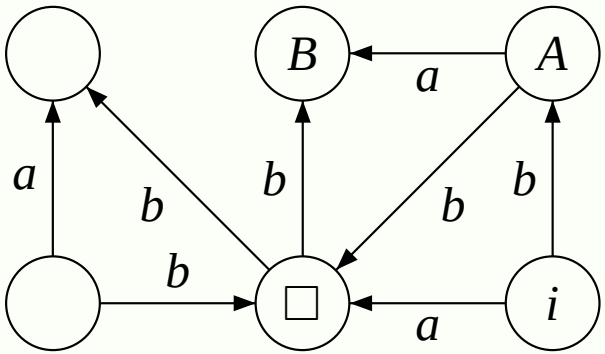
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



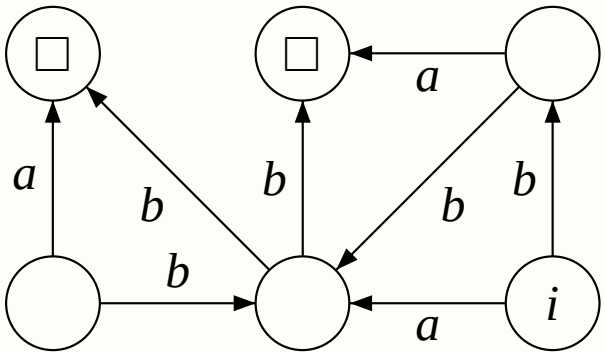
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



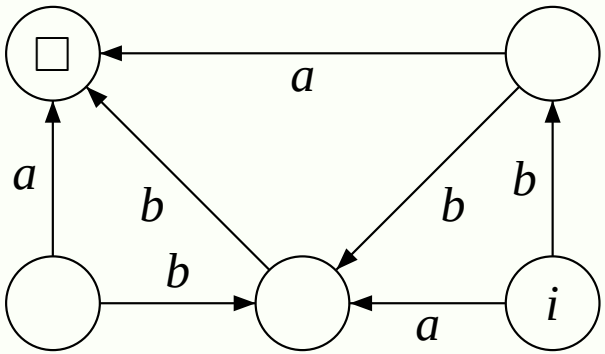
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



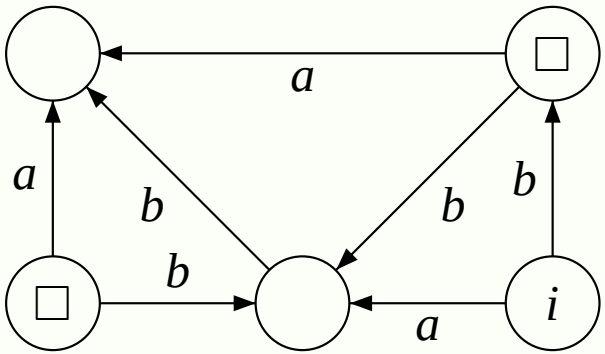
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



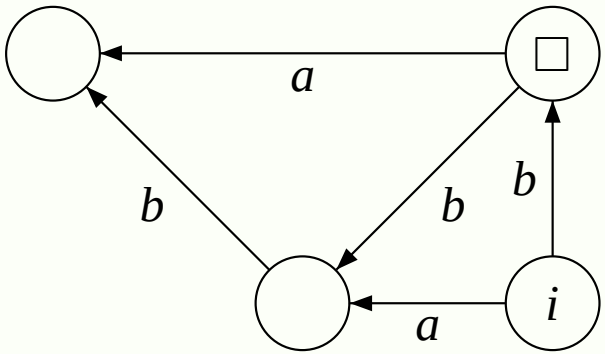
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



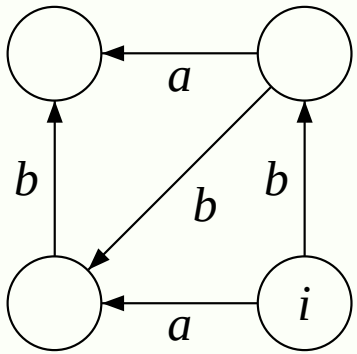
Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



Repliage de Stallings (Stallings foldings)

On part de $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$.



Repliage de Stallings (Stallings foldings)

On applique autant de fois que possible les simplifications sur les configurations :

On obtient le même résultat si on change l’ordre des simplifications.

Automate inversible (inverse automaton)

- L'automate obtenu est un automate inversible, il est déterministe et co-déterministe : l'action de chaque lettre est une injection partielle de l'ensemble des états dans lui-même.
- Réciproquement, si on se donne un automate inversible tel que
  - un état est le seul état initial et le seul état final
  - tous les états sont accessibles (au sens non-orienté)
  - à part l'état initial, tous les états sont adjacents à au moins deux transitions.

  Alors il représente, de façon unique, un sous-groupe finiment engendré du groupe libre. Un tel automate inversible est dit *réduit*.

Automate inversible (inverse automaton)

- L’automate obtenu est un automate inversible, il est déterministe et co-déterministe : l’action de chaque lettre est une injection partielle de l’ensemble des états dans lui-même.
- Réciproquement, si on se donne un automate inversible tel que
  - un état est le seul état initial et le seul état final
  - tous les états sont accessibles (au sens non-orienté)
  - à part l’état initial, tous les états sont adjacents à au moins deux transitions.

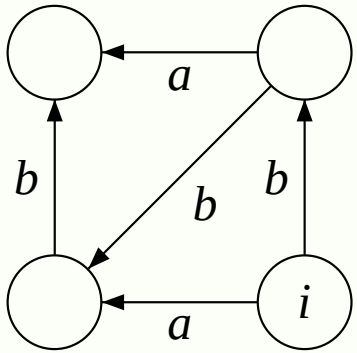
  Alors il représente, de façon unique, un sous-groupe finiment engendré du groupe libre. Un tel automate inversible est dit *réduit*.

Automate réduit – exemples d’utilisation

- On peut tester facilement si un mot réduit est dans le sous-groupe.
- On peut calculer une base et le rang du sous-groupe.
- On peut calculer le produit de deux sous-groupes.
- On peut tester si le sous-groupe est d’indice fini.

Exemple de rang

Pour $Y = \{aba^{-1}ba^{-1}, b^2a^{-1}, b^3a^{-1}b^{-1}\}$, on a trouvé



On peut en déduire que $\{b^2a^{-1}, aba^{-1}b^{-1}\}$ est une base.

Considérations algorithmiques

- Le repliement se calcule en $O(n \log^* n)$ en utilisant du “Union and Find”. (Touikan)
- Pour trouver une base, on replie puis on fait un arbre couvrant. Chaque arête qui n’est pas dans la base permet de former un générateur de la base.
- Pour calculer le rang : nombre d’arcs - nombre de sommets + 1
- L’intersection de deux sous-groupes en temps et espace $O(n_1 n_2)$.

Hanna Neumann conjecture 1957

- Howson : l'intersection de deux sous-groupes finiment engendrés est finiment engendrée.
- Conjecture d'Hanna Neumann :

$$rang(H \cap K) - 1 \leq (rang(H) - 1)(rang(K) - 1)$$

- Elle a prouvé

$$rang(H \cap K) - 1 \leq 2(rang(H) - 1)(rang(K) - 1)$$

Hanna Neumann conjecture 1957

- Howson : l'intersection de deux sous-groupes finiment engendrés est finiment engendrée.
- Conjecture d'Hanna Neumann :

$$rang(H \cap K) - 1 \leq (rang(H) - 1)(rang(K) - 1)$$

- Elle a prouvé

$$rang(H \cap K) - 1 \leq 2(rang(H) - 1)(rang(K) - 1)$$

II. Deux distributions

Distribution sur les générateurs (Jitsukawa)

- On fixe k, le nombre de générateurs et n la taille maximale de chaque générateur.
- On considère donc la distribution uniforme sur les k-uplets de mots réduits de longueur au plus n.
- Soit R_n le nombre de mots réduits de longueur n, on a

$$R_n = 2r(2r-1)^{n-1}$$

- Mots sans deux fois la même lettre de suite : les mots de Smirnov.
- La longueur d'un mot d'un k-uplet aléatoire est proche de n.

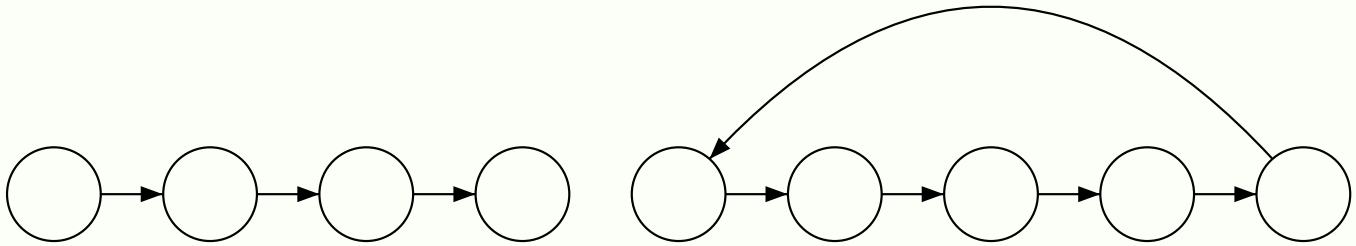
Distribution sur les générateurs (Jitsukawa)

- On fixe k, le nombre de générateurs et n la taille maximale de chaque générateur.
- On considère donc la distribution uniforme sur les k-uplets de mots réduits de longueur au plus n.
- Soit R_n le nombre de mots réduits de longueur n, on a

$$R_n = 2r(2r-1)^{n-1}$$

- Mots sans deux fois la même lettre de suite : les mots de Smirnov.
- La longueur d'un mot d'un k-uplet aléatoire est proche de n.

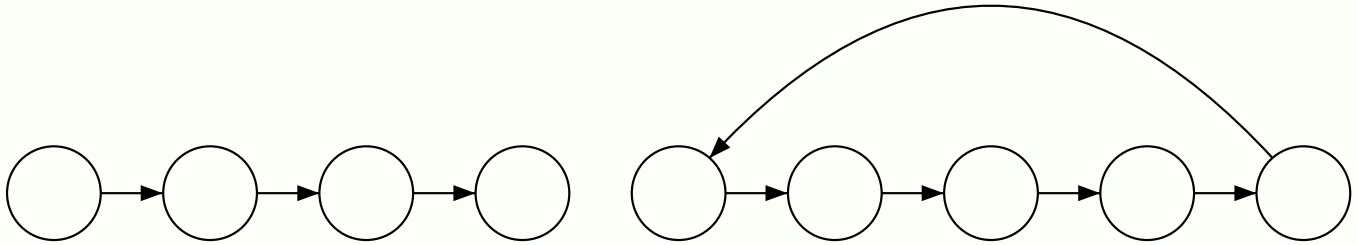
Injections partielles



- On a soit des séquences soit des cycles.
- Ensemble(Cycle ou Sequence non vide)
- Par la méthode symbolique :

$$I(z) = \exp\left(\log\frac{1}{1-z} + \frac{z}{1-z}\right) = \frac{1}{1-z}e^{z/(1-z)}$$

Injections partielles



- On a soit des séquences soit des cycles.
- Ensemble(Cycle ou Sequence non vide)
- Par la méthode symbolique :

$$I(z) = \exp\left(\log\frac{1}{1-z} + \frac{z}{1-z}\right) = \frac{1}{1-z}e^{z/(1-z)}$$

Asymptotique

Cas d'école pour la méthode du col :

$$I(z) = \frac{1}{1-z} \exp\left(\frac{z}{1-z}\right)$$

$$\frac{1}{n!}[z^n]I(z) \sim \frac{e^{-\frac{1}{2}}}{2\sqrt{\pi}} e^{2\sqrt{n}} n^{-\frac{1}{4}}$$

Asymptotique

Cas d'école pour la méthode du col :

$$I_p(z) = \frac{1}{(1-z)^p} \exp\left(\frac{z}{1-z}\right)$$

$$\frac{1}{n!}[z^n]I(z) \sim \frac{e^{-\frac{1}{2}}}{2\sqrt{\pi}} e^{2\sqrt{n}} n^{-\frac{1}{4}} n^{\frac{p-1}{2}}$$

Résultat probabiliste

Théorème

La probabilité qu'un automate inversible de taille n soit réduit tend vers 1 quand n tend vers l'infini.

On peut donc voir un automate réduit comme un r-uplet d'injections partielles.

- un état est le seul état initial et le seul état final
- tous les états sont accessibles (au sens non-orienté)
- à part l'état initial, tous les états sont adjacents à au moins deux transitions.

Résultat probabiliste

Théorème

La probabilité qu'un automate inversible de taille n soit réduit tend vers 1 quand n tend vers l'infini.

On peut donc voir un automate réduit comme un r-uplet d'injections partielles.

- un état est le seul état initial et le seul état final
- tous les états sont accessibles (au sens non-orienté)
- à part l'état initial, tous les états sont adjacents à au moins deux transitions.

Résultat probabiliste

Théorème

La probabilité qu'un automate inversible de taille n soit réduit tend vers 1 quand n tend vers l'infini.

On peut donc voir un automate réduit comme un r-uplet d'injections partielles.

- un état est le seul état initial et le seul état final
- tous les états sont accessibles (au sens non-orienté)
- à part l'état initial, tous les états sont adjacents à au moins deux transitions.

Connexité

Théorème

La probabilité que r injections partielles de taille n forment un graphe (faiblement) connexe est

$$p_n = 1 - \frac{2^r}{n^{r-1}} + o\left(\frac{1}{n^{r-1}}\right)$$

Preuve

Bender : $1 + J(z) = \exp(C(z))$ d'où $C(z) = \log(1 + J(z))$. Il faut vérifier que $j_n = o(j_{n-1})$ et que

$$\sum_{k=s}^{n-s} |j_k j_{n-k}| = O(j_{n-s})$$

Connexité

Théorème

La probabilité que r injections partielles de taille n forment un graphe (faiblement) connexe est

$$p_n = 1 - \frac{2^r}{n^{r-1}} + o\left(\frac{1}{n^{r-1}}\right)$$

Preuve

Bender : $1 + J(z) = \exp(C(z))$ d'où $C(z) = \log(1 + J(z))$. Il faut vérifier que $j_n = o(j_{n-1})$ et que

$$\sum_{k=s}^{n-s} |j_k j_{n-k}| = O(j_{n-s})$$

Nombre moyen de séquences

- Soit $I(z,u) = \sum I_{n,k} z^n u^k / n!$ la série génératrice où $I_{n,k}$ est le nombre d'injections partielles de taille n contenant k séquences, on obtient :

$$I(z,u) = \exp\left(\frac{zu}{1-z} + \log\left(\frac{1}{1-z}\right)\right) = \frac{1}{1-z}\exp\left(\frac{zu}{1-z}\right)$$

- On trouve, par la méthode du col qu'en moyenne il y a $\sim \sqrt{n}$ séquences, et que la probabilité d'avoir plus de $2\sqrt{n}$ séquences tend vers 0.

Nombre moyen de séquences

- Soit $I(z,u) = \sum I_{n,k} z^n u^k / n!$ la série génératrice où $I_{n,k}$ est le nombre d'injections partielles de taille n contenant k séquences, on obtient :

$$I(z,u) = \exp\left(\frac{zu}{1-z} + \log\left(\frac{1}{1-z}\right)\right) = \frac{1}{1-z}\exp\left(\frac{zu}{1-z}\right)$$

- On trouve, par la méthode du col qu'en moyenne il y a $\sim \sqrt{n}$ séquences, et que la probabilité d'avoir plus de $2\sqrt{n}$ séquences tend vers 0.

Preuve avec les mains

- La probabilité qu'un indice soit une extrémité (soit un début ou une fin de séquence) est en $O(1/\sqrt{n})$.
- La probabilité qu'un indice soit isolé est $O(1/n)$.

La probabilité qu'il y ait un indice qui soit une extrémité pour une lettre et isolé pour une autre tend vers 0.

Preuve avec les mains

- La probabilité qu'un indice soit une extrémité (soit un début ou une fin de séquence) est en $O(1/\sqrt{n})$.
- La probabilité qu'un indice soit isolé est $O(1/n)$.

La probabilité qu'il y ait un indice qui soit une extrémité pour une lettre et isolé pour une autre tend vers 0.

III. Génération aléatoire

On utilise des rejets

Automate réduit aléatoire

```
1 repeat
2     for a ∈ A do
3         action de a = injection aléatoire
4 until Automate n'est pas réduit
```

Le nombre moyen d'itérations est $1 + o(1)$.

Calculer le nombre d'injections partielles

$$I(z) = \frac{1}{1-z} \exp\left(\frac{1}{1-z}\right)$$

$$I'(z) = \frac{2-z}{(1-z)^3} \exp\left(\frac{1}{1-z}\right) = \frac{2-z}{(1-z)^2} I(z)$$

$$I_n = 2nI_{n-1} - (n-1)^2 I_{n-2}$$

Calculer le nombre d'injections partielles

$$I(z) = \frac{1}{1-z} \exp\left(\frac{1}{1-z}\right)$$

$$I'(z) = \frac{2-z}{(1-z)^3} \exp\left(\frac{1}{1-z}\right) = \frac{2-z}{(1-z)^2} I(z)$$

$$I_n = 2nI_{n-1} - (n-1)^2 I_{n-2}$$

Calculer le nombre d'injections partielles

$$I(z) = \frac{1}{1-z} \exp\left(\frac{1}{1-z}\right)$$

$$I'(z) = \frac{2-z}{(1-z)^3} \exp\left(\frac{1}{1-z}\right) = \frac{2-z}{(1-z)^2} I(z)$$

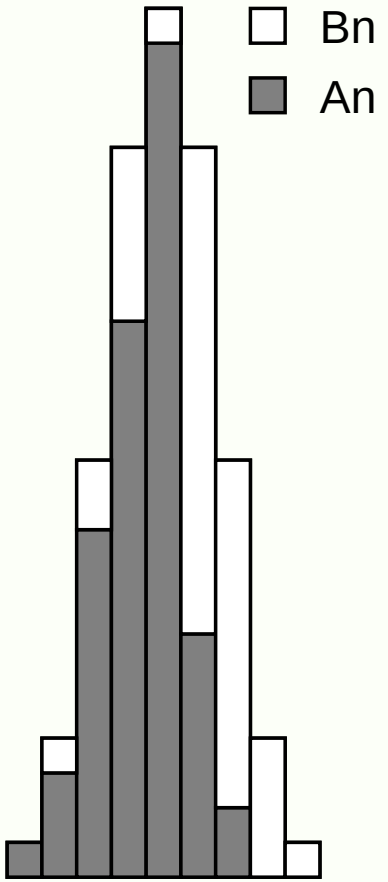
$$I_n = 2nI_{n-1} - (n-1)^2 I_{n-2}$$

Méthode récursive

$$\mathcal{I} = \mathcal{S}et\,(\text{Cycles ou Séquences})$$
$$\Theta\mathcal{I} = \Theta\,(\text{Cycle ou Séquence}) \times \mathcal{S}et\,(\text{Cycles ou Séquences})$$

On extrait une composante de taille k en temps $O(k)$, l'algorithme est linéaire une fois qu'on a précalculé les I_n.

Méthode d'Alonso



- On veut générer des objets de taille n "décomposés" selon un paramètre k. Pour Alonso, c'étaient des arbres unaires-binaires avec k noeuds binaires.
- On tire au sort k avec la bonne probabilité, puis un objet uniformément parmi ceux de paramètre valant k.
- Pour tirer k, on sur-approxime par une binomiale, et on utilise des rejets.

Conditions

- Sur-approximation par une binomiale.
- Faire un rejet avec acceptation en $A_{n,k}/B_{n,k}$ facilement.
- Aires proches pour limiter le nombre de rejets.
- Savoir construire facilement un objet de taille n avec un paramètre valant k.

Soit $I_{n,k}$ le nombre d'injections partielles de $[n]$ avec un domaine de taille k.

$$I_{n,k} = \frac{n!^2}{(n-k)!^2 k!}$$

La séquence est unimodale avec le mode en $\mu_n = n + \frac{3}{2} - \frac{1}{2}\sqrt{4n+5}$

- On choisit k selon une Binomiale$(2\mu_n - 1, \frac{1}{2})$
- On rejette avec une probabilité de la forme :

$$\prod \frac{\alpha_i}{\beta_i}$$

- Le nombre moyen de rejet est en $n^{1/4}$.

La complexité de l'algorithme est $O(n^{5/4})$ en ne manipulant que des entiers de taille au plus $2n$.

Soit $I_{n,k}$ le nombre d'injections partielles de $[n]$ avec un domaine de taille k.

$$I_{n,k} = \frac{n!^2}{(n-k)!^2 k!}$$

La séquence est unimodale avec le mode en $\mu_n = n + \frac{3}{2} - \frac{1}{2}\sqrt{4n+5}$

- On choisit k selon une Binomiale$(2\mu_n - 1, \frac{1}{2})$
- On rejette avec une probabilité de la forme :

$$\prod \frac{\alpha_i}{\beta_i}$$

- Le nombre moyen de rejet est en $n^{1/4}$.

La complexité de l'algorithme est $O(n^{5/4})$ en ne manipulant que des entiers de taille au plus $2n$.

Soit $I_{n,k}$ le nombre d'injections partielles de $[n]$ avec un domaine de taille k.

$$I_{n,k} = \frac{n!^2}{(n-k)!^2 k!}$$

La séquence est unimodale avec le mode en $\mu_n = n + \frac{3}{2} - \frac{1}{2}\sqrt{4n+5}$

- On choisit k selon une Binomiale$(2\mu_n - 1, \frac{1}{2})$
- On rejette avec une probabilité de la forme :

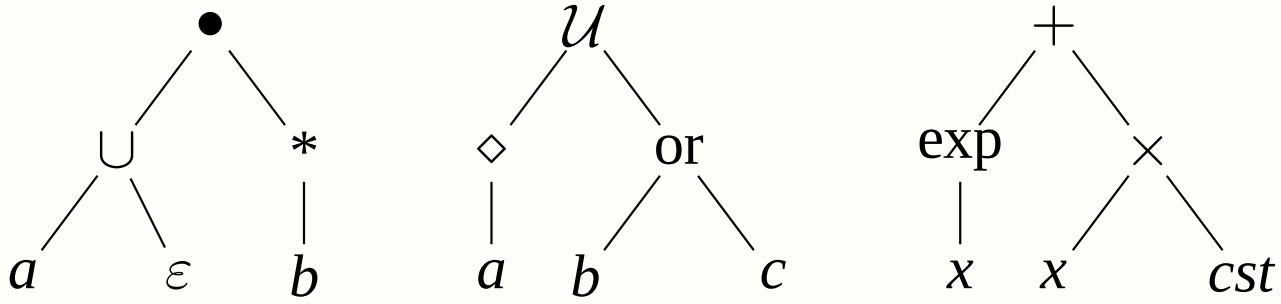
$$\prod \frac{\alpha_i}{\beta_i}$$

- Le nombre moyen de rejet est en $n^{1/4}$.

La complexité de l'algorithme est $O(n^{5/4})$ en ne manipulant que des entiers de taille au plus $2n$.

Au passage ...

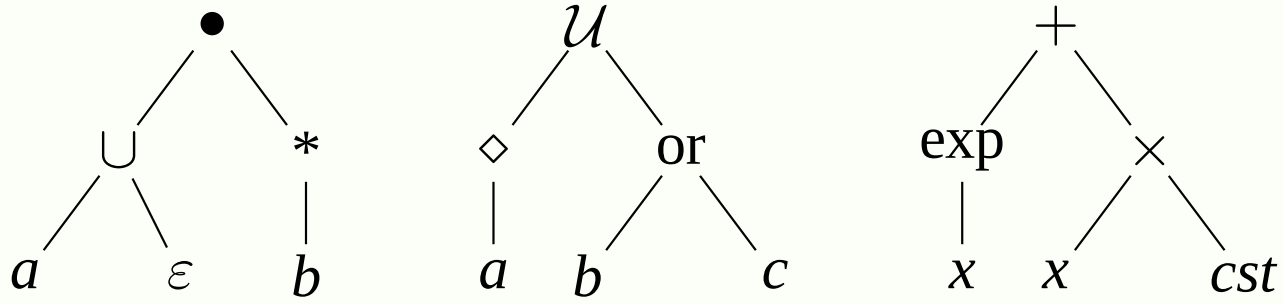
On a appliqué la méthode pour générer aléatoirement des arbres unaires-binaires colorés en temps linéaire.



Egalement : permutations fragmentées, paires d'injections formant un sous-groupe de rang fixé.

Au passage ...

On a appliqué la méthode pour générer aléatoirement des arbres unaires-binaires colorés en temps linéaire.



Egalement : permutations fragmentées, paires d'injections formant un sous-groupe de rang fixé.

IV. Comparer les deux distributions

Méthodologie

- Comment comparer les deux distributions ? il n'y a pas de benchmarks.
- Propriété (fortement) générique : soit (X_n) une famille d'objets et P une propriété. On dit que P est *générique* pour (X_n) quand la probabilité qu'un élément de X_n vérifie P tend vers 1 (exponentiellement vite).
- Propriété (fortement) négligeable : soit (X_n) une famille d'objets et P une propriété. On dit que P est *négligeable* pour (X_n) quand la probabilité qu'un élément de X_n vérifie P tend vers 0 (exponentiellement vite).
- On va examiner des propriétés algébriques et chercher si elles sont génériques ou négligeables pour chaque distribution.

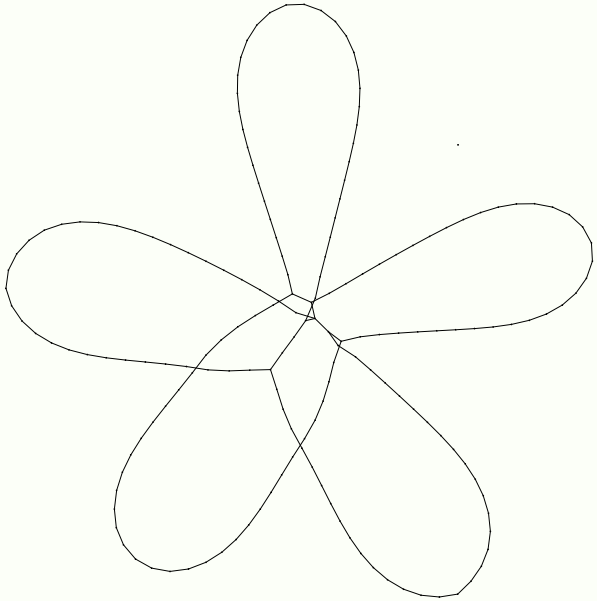
Méthodologie

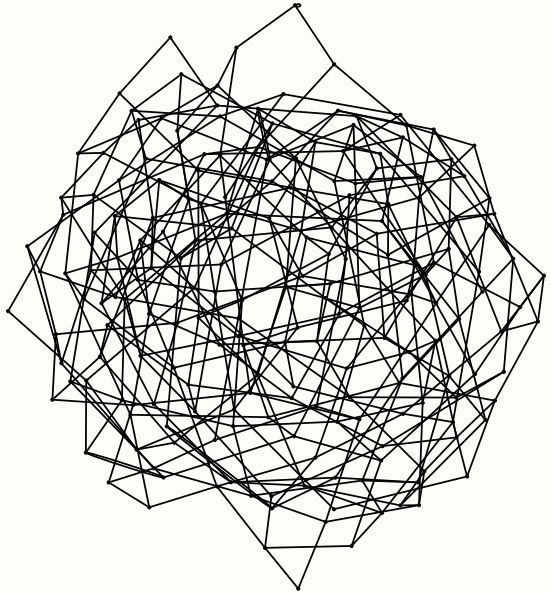
- Comment comparer les deux distributions ? il n'y a pas de benchmarks.
- Propriété (fortement) générique : soit (X_n) une famille d'objets et P une propriété. On dit que P est *générique* pour (X_n) quand la probabilité qu'un élément de X_n vérifie P tend vers 1 (exponentiellement vite).
- Propriété (fortement) négligeable : soit (X_n) une famille d'objets et P une propriété. On dit que P est *négligeable* pour (X_n) quand la probabilité qu'un élément de X_n vérifie P tend vers 0 (exponentiellement vite).
- On va examiner des propriétés algébriques et chercher si elles sont génériques ou négligeables pour chaque distribution.

Méthodologie

- Comment comparer les deux distributions ? il n'y a pas de benchmarks.
- Propriété (fortement) générique : soit (X_n) une famille d'objets et P une propriété. On dit que P est *générique* pour (X_n) quand la probabilité qu'un élément de X_n vérifie P tend vers 1 (exponentiellement vite).
- Propriété (fortement) négligeable : soit (X_n) une famille d'objets et P une propriété. On dit que P est *négligeable* pour (X_n) quand la probabilité qu'un élément de X_n vérifie P tend vers 0 (exponentiellement vite).
- On va examiner des propriétés algébriques et chercher si elles sont génériques ou négligeables pour chaque distribution.

Résultats expérimentaux





Malnormalité

- Rappel : un sous-groupe H de G est normal quand pour tout $g \in G$, $g^{-1}Hg = H$.
- Un sous-groupe est *malnormal* quand pour tout $g \notin H$, $g^{-1}Hg \cap H = 1$.

Théorème

Un sous-groupe du groupe libre n'est pas malnormal ssi il existe deux sommets $x \neq y$ et un mot réduit non vide u, tels qu'il y a un circuit étiqueté par u depuis x et un depuis y.

Malnormalité

- Rappel : un sous-groupe H de G est normal quand pour tout $g \in G$, $g^{-1}Hg = H$.
- Un sous-groupe est *malnormal* quand pour tout $g \notin H$, $g^{-1}Hg \cap H = 1$.

Théorème

Un sous-groupe du groupe libre n'est pas malnormal ssi il existe deux sommets $x \neq y$ et un mot réduit non vide u, tels qu'il y a un circuit étiqueté par u depuis x et un depuis y.

Malnormalité

- Rappel : un sous-groupe H de G est normal quand pour tout $g \in G$, $g^{-1}Hg = H$.
- Un sous-groupe est *malnormal* quand pour tout $g \notin H$, $g^{-1}Hg \cap H = 1$.

Théorème

Un sous-groupe du groupe libre n'est pas malnormal ssi il existe deux sommets $x \neq y$ et un mot réduit non vide u, tels qu'il y a un circuit étiqueté par u depuis x et un depuis y.

Malnormalité

Théorème

Pour la distribution basée sur les générateurs la malnormalité est générique alors qu'elle est négligeable pour la distribution basée sur les graphes.

Démonstration

- La probabilité qu'une injection partielle n'ait pas de cycle est $\sim \frac{1}{\sqrt{n}}$ (permutations fragmentées)
- La probabilité qu'une injection partielle n'ait qu'un seul cycle et qu'il soit de longueur 1 est $\sim \frac{1}{\sqrt{n}}$.

Malnormalité

Théorème

Pour la distribution basée sur les générateurs la malnormalité est générique alors qu'elle est négligeable pour la distribution basée sur les graphes.

Démonstration

- La probabilité qu'une injection partielle n'ait pas de cycle est $\sim \frac{1}{\sqrt{n}}$ (permutations fragmentées)
- La probabilité qu'une injection partielle n'ait qu'un seul cycle et qu'il soit de longueur 1 est $\sim \frac{1}{\sqrt{n}}$.

Groupes finiment présentés

- Tout groupe est le quotient d'un groupe libre.
- L'idée est de quotienter le groupe libre par un sous-groupe finiment engendré aléatoire H.
- Il faut quotienter par la clôture normale de H qui est le plus petit sous-groupe normal contenant H.
- Ca revient à voir chaque mot x de H comme une relation $x = 1$.

Groupes finiment présentés

- Tout groupe est le quotient d'un groupe libre.
- L'idée est de quotienter le groupe libre par un sous-groupe finiment engendré aléatoire H.
- Il faut quotienter par la clôture normale de H qui est le plus petit sous-groupe normal contenant H.
- Ca revient à voir chaque mot x de H comme une relation $x = 1$.

Groupes finiment présentés

- Tout groupe est le quotient d'un groupe libre.
- L'idée est de quotienter le groupe libre par un sous-groupe finiment engendré aléatoire H.
- Il faut quotienter par la clôture normale de H qui est le plus petit sous-groupe normal contenant H.
- Ca revient à voir chaque mot x de H comme une relation $x = 1$.

Exemples

- $H =< aaa >$, soit G le quotient de $F(\{a, b\})$ par la clôture normale de H. On peut voir les éléments de G comme un mot réduit avec en plus la réduction $a^3 = 1$: $abaaa \equiv ab$.
- $H =< aa, aba^{-1}b^{-1} >$, $aababa \equiv baba \equiv bbaa \equiv bb$.

Exemples

- $H =< aaa >$, soit G le quotient de $F(\{a, b\})$ par la clôture normale de H. On peut voir les éléments de G comme un mot réduit avec en plus la réduction $a^3 = 1$: $abaaa \equiv ab$.
- $H =< aa, aba^{-1}b^{-1} >$, $aababa \equiv baba \equiv bbaa \equiv bb$.

Le problème du mot

Problème du mot

Soit G un groupe finiment présenté, le problème du mot est de décider si deux mots réduits sont les mêmes pour G.

La décidabilité ne dépend pas de la présentation. En général, c'est indécidable : la clôture normale est un objet compliqué.
$H =< ba, abaa >$, on a $a \equiv b^{-1}$ et $aa \equiv b^{-1}a^{-1}$ donc

$$aa \equiv b^{-1}a^{-1} \equiv aa^{-1} \equiv 1$$

alors que $aa \notin H$.

Le problème du mot

Problème du mot

Soit G un groupe finiment présenté, le problème du mot est de décider si deux mots réduits sont les mêmes pour G.

La décidabilité ne dépend pas de la présentation. En général, c'est indécidable : la clôture normale est un objet compliqué.
$H =< ba, abaa >$, on a $a \equiv b^{-1}$ et $aa \equiv b^{-1}a^{-1}$ donc

$$aa \equiv b^{-1}a^{-1} \equiv aa^{-1} \equiv 1$$

alors que $aa \notin H$.

Le problème du mot

Problème du mot

Soit G un groupe finiment présenté, le problème du mot est de décider si deux mots réduits sont les mêmes pour G.

La décidabilité ne dépend pas de la présentation. En général, c'est indécidable : la clôture normale est un objet compliqué.

$H =< ba, abaa >$, on a $a \equiv b^{-1}$ et $aa \equiv b^{-1}a^{-1}$ donc

$$aa \equiv b^{-1}a^{-1} \equiv aa^{-1} \equiv 1$$

alors que $aa \notin H$.

Le problème du mot

Problème du mot

Soit G un groupe finiment présenté, le problème du mot est de décider si deux mots réduits sont les mêmes pour G.

La décidabilité ne dépend pas de la présentation. En général, c'est indécidable : la clôture normale est un objet compliqué.
$H =< ba, abaa >$, on a $a \equiv b^{-1}$ et $aa \equiv b^{-1}a^{-1}$ donc

$$aa \equiv b^{-1}a^{-1} \equiv aa^{-1} \equiv 1$$

alors que $aa \notin H$.

Le problème du mot

Problème du mot

Soit G un groupe finiment présenté, le problème du mot est de décider si deux mots réduits sont les mêmes pour G.

La décidabilité ne dépend pas de la présentation. En général, c'est indécidable : la clôture normale est un objet compliqué.
$H =< ba, abaa >$, on a $a \equiv b^{-1}$ et $aa \equiv b^{-1}a^{-1}$ donc

$$aa \equiv b^{-1}a^{-1} \equiv aa^{-1} \equiv 1$$

alors que $aa \notin H$.

Groupes aléatoirement présentés

- Si on prend la distribution sur les générateurs, le groupe quotient est génériquement infini.
- Si on prend la distribution sur les graphes le groupe quotient est génériquement trivial (mauvaise nouvelle)

Si on déplace l'état initial/final, on construit toujours des mots de la clôture normale.
Si on a des boucles de la forme a^m de longueurs premières entre elles, alors $a \equiv 1$.

Groupes aléatoirement présentés

- Si on prend la distribution sur les générateurs, le groupe quotient est génériquement infini.
- Si on prend la distribution sur les graphes le groupe quotient est génériquement trivial (mauvaise nouvelle)

Si on déplace l'état initial/final, on construit toujours des mots de la clôture normale.
Si on a des boucles de la forme a^m de longueurs premières entre elles, alors $a \equiv 1$.

Groupes aléatoirement présentés

- Si on prend la distribution sur les générateurs, le groupe quotient est génériquement infini.
- Si on prend la distribution sur les graphes le groupe quotient est génériquement trivial (mauvaise nouvelle)

Si on déplace l'état initial/final, on construit toujours des mots de la clôture normale.

Si on a des boucles de la forme a^m de longueurs premières entre elles, alors $a \equiv 1$.

Groupes aléatoirement présentés

- Si on prend la distribution sur les générateurs, le groupe quotient est génériquement infini.
- Si on prend la distribution sur les graphes le groupe quotient est génériquement trivial (mauvaise nouvelle)

Si on déplace l'état initial/final, on construit toujours des mots de la clôture normale.
Si on a des boucles de la forme a^m de longueurs premières entre elles, alors $a \equiv 1$.

Trivialité

Théorème

Génériquement, le pgcd des longueurs des cycles dans une **injection partielle** est 1.

Théorème

Génériquement, le pgcd des longueurs des cycles dans une **permutation** est 1.

Trivialité

Théorème

Génériquement, le pgcd des longueurs des cycles dans une **injection partielle** est 1.

Théorème

Génériquement, le pgcd des longueurs des cycles dans une **permutation** est 1.

Trivialité (suite)

Lemme

Soit p un diviseur premier de n, le nombre de permutations dont toutes les longueurs de cycles sont divisibles par p est au plus

$$2n!n^{\frac{1}{p}-1}$$

Lemme

La taille de la “partie permutation” d’une injection partielle aléatoire est en $\sqrt{n}$.

Et après ?

- Paramétriser les distributions.
- Analyse d’algorithmes.
- Cryptographie.