Deux Mariages et aucun Enterrement

Christoph Dürr
rapport de stage de DEA d'informatique à Orsay

16 septembre 1994

Résumé

Dans ce rapport nous décrivons des méthodes d'approximation basées sur la notion de *relation auto-réductible* et utilisant des chaînes de Markov. En particulier nous présentons une telle approximation randomizée du nombre de couplages parfaits, fonction #P-complet. Puis nous tentons d'appliquer ces méthodes à une estimation du nombre de chemins d'un coin à un autre dans une grille.

Mots-clés : approximation, (ϵ, δ)-approximation, génération aléatoire, problème de comptage, #P, couplage parfait, permanent, chaîne de Markov, systèmes monomère-dimère.

Ce rapport est accessible par `ftp://lri.lri.fr/LRI/articles/durr/grille.ps`.

Table des matières

1 Présentation

On associe aux problèmes de décision de la classe NP les problèmes de comptage de la classe #P. Si un problème de décision se formalise par la question "Pour un x donné existe-t-il un y, qui satisfait la relation xRy?", alors le problème de comptage associé est de la forme "Quel est le nombre de y qui satisfont xRy?".

Beaucoup de fonctions intéressantes ont été montrés #P-complètes, donc on ne peut espérer trouver un algorithme polynomial à ces problèmes. C'est la raison pour laquelle il est intéressant d'approcher ces fonctions, pour au moins avoir un résultat suffisamment précis en temps acceptable[1].

De nombreux résultats, ces dernières années, lient l'approximation à la génération uniforme. On considère ici des relations *auto-réductibles*, relations $R(x, y)$ qui s'expriment récursivement en fonction d'entrées plus petites. Pour ces relations, un algorithme randomizé d'approximation peut être construit à partir d'un générateur uniforme. Il a été montré qu'un générateur presque-uniforme randomizé suffit également.

Les chaînes de Markov s'imposent alors pour générer des éléments d'un ensemble $\mathcal{N}$. En principe elles sont réalisées par un processus aléatoire, qui pendant un certain temps effectue des modifications locales à partir d'un élément de départ. A la sortie de ce processus, on espère trouver un élément de $\mathcal{N}$ avec une probabilité presque-uniforme. Les transitions effectuées par le processus définissent un graphe sous-jacent de la chaîne de Markov sur $\mathcal{N}$.

La difficulté consiste alors à prouver le mélange rapide de la chaîne, propriété nécessaire, pour assurer que le processus génère presque-uniformément des éléments d'un ensemble de taille exponentielle en temps polynomial.

Le travail original de Sinclair à été de caractériser le mélange rapide par une propriété structurelle sur le graphe sous-jacent, la *conductance*. Avec Jerrum il a alors donné un algorithme d'approximation du nombre de couplages parfaits, problème #P-complet.

Dans ce rapport nous commençons par rappeler certaines notions de complexité et décrivons ensuite les principaux formalismes utilisés pour l'approximation. Ensuite nous décrivons les résultats qui ont été obtenus pour les relations auto-réductibles. Après une brève introduction aux chaînes de Markov, nous exposons l'approximation du nombre de couplages parfaits, fruit des travaux de Jerrum et Sinclair.

Cette section est suivi par l'apport personnel de ce rapport: une approximation du nombre de chemins simples dans une grille. Cette approximation utilise toutes les méthodes décrites dans les section précédentes.

1. Par temps acceptable on sous-entend temps polynomial en la taille de l'entrée du problème

2 Notions de complexité

2.1 Classes

La théorie de la complexité se propose de classifier des problèmes selon leur degré de difficulté. Parmi les problèmes décidables on peut distinguer trois classes importantes P, NP et #P.

L'instance des problèmes est un mot x d'un alphabet fini d'une longueur qu'on note n. Un problème de décision consiste à décider si x appartient à un langage L ou non. Un problème de calcul est alors de fournir en sortie un mot y tel que x et y sont dans une relation R.

Définition 1 (p-prédicat) *Un prédicat $p(x, y)$ est un p-prédicat si*

1. *$\exists$ un polynôme q tel que $\forall x, y : p(x, y) \Rightarrow |y| = O(q(|x|))$*

2. *p est décidable en temps polynomial.*

Un problème de décision L est dans la classe NP s'il existe un p-prédicat p tel que $x \in L$ si $\exists y : p(x, y)$. L est donc décidable par une machine non-déterministe polynomiale qui devine dans un premier temps y puis qui décide ensuite $p(x, y)$.

Une fonction f est dans #P s'il existe un p-prédicat p tel que $f(x) = |\{y : p(x, y)\}|$. Autrement dit f correspond au nombre de feuilles acceptantes de l'arbre d'exécution de la machine non-déterministe qui devinerait dans un premier temps y puis qui déciderait $p(x, y)$.

2.2 Réductions

Un problème L est réductible en temps polynomial à un autre problème L' s'il existe une fonction $f(x)$ polynomiale en la taille de x qui vérifie que $x \in L$ ssi $f(x) \in L'$.

Une fonction f est many-one-réductible en temps polynomial à une autre fonction g s'il existe une fonction $h(x)$ polynomiale dans la taille de x qui vérifie $f(x) = g(h(x))$.

Un problème L est NP-complet si tout problème L' de NP est réductible en temps polynomial à L.

Une fonction f est #P-complète si toute fonction g de #P est réductible en temps polynomial à f.

2.3 La classe #P

La classe de fonctions #P a été introduite dans les années 70 par Valiant. Cette classe contient de nombreux et intéressants problèmes comme #SAT (compter le nombre de modèles satisfaisant une formule booléenne donnée) ou #EXT (compter le nombre d'extensions linéaires d'un ordre partiel donné).

Tout problème NP est #P-facile, car décider s'il existe une solution, revient à vérifier que le nombre de solutions n'est pas nul. Elle comporte aussi les deux problèmes similaires d'un point de vue logique #DNF et #CNF qui ont une propriété surprenante. #DNF est approximable [KL] tandis que #CNF ne l'est pas si NP≠RP. Pour l'instant il n'existe pas de caractérisation des problèmes qui sont #P-complets et approximables. Comme DNF est dans P alors que CNF est NP-complet on pourrait penser qu'il y un lien entre la classe du problème de décision et le fait que sa version de comptage est approximable ou non. Cependant le problème n'est pas aussi facile car il y a des problèmes polynomialement décidable comme l'existence d'un couplage parfait, alors que le problème de compter le nombre de couplages parfaits semble être difficilement approximable. C'est cette dernière observation qui a motivé l'étude de #P.

En s'appuyant sur la caractérisation de NP par Fagin, une telle caractérisation a été faite pour #P [SST, p. 170]. Un problème Q de #P peut toujours se décrire par une fonction f_Q et utilisant une formule du premier ordre $\phi(z,T)$ défini par

$$f_Q(A) = |\{\langle z,T\rangle : A \models \phi(z,T)\}|$$

où A est une structure finie, muni d'un ordre, représentant l'entrée du problème, z et T sont respectivement des séquences de variables du premier et du second ordre.

3 Approximation

3.1 Pourquoi approcher

Au désespoir des utilisateurs de l'informatique certains problèmes courants ont été montrés NP-complets ou même #P-complets. Référez vous à l'annexe pour des exemples de tels problèmes. Beaucoup de problèmes intéressants ne sont calculables que dans un temps exponentiel en fonction de la taille de l'entrée. Si par contre on se contente d'une solution non-optimale on a une chance de trouver un algorithme faisable (en temps polynomial).

3.2 Différentes formes d'approximation

Soit $f(x)$ une fonction réelle positive, sur Σ^*.

Définition 2 (Approximation multiplicative) *Si $g(x)$ est une fonction réelle positive, ont dit que $g(x)$ approche $f(x)$ dans un rapport r pour un réel $r \geq 1$ si pour toute entrée x, on a :*

$$f(x)/r \leq g(x) \leq f(x)r.$$

Définition 3 ((ϵ,δ)-approximation) *Une fonction $g(x,\epsilon)$ est un schéma d'approximation entièrement polynomial, randomizé ((ϵ,δ)-approximation) pour $f(x)$ dans un rapport $(1+\epsilon) \geq 1$ si g se calcule en temps polynomial par rapport à $|x|$ et $1/\epsilon$ et que g satisfait pour toute entrée x*

$$\Pr[g(x,\epsilon) \text{ approche } f(x) \text{ dans un rapport } (1+\epsilon)] \geq 3/4.$$

Par des appels successifs de g, on peut augmenter cette probabilité à $(1-\delta)$, pour un certain $0 < \delta < \frac{1}{2}$. La preuve de cette augmentation à δ est dans [JVV, p. 182] et utilise la borne de Chernoff. C'est la raison pour laquelle on peut trouver la définition équivalente :

Définition 4 ((ϵ, δ)-approximation) *Un (ϵ, δ)-schéma d'approximation randomizé entièrement polynomial pour la fonction $f(x)$ est une fonction $g(x)$ polynomiale en $|x|$, $1/\epsilon$ et $\log(1/\delta)$ et qui satisfait pour toute entrée x*

$$\Pr[f(x)/(1+\epsilon) \leq g(x) \leq (1+\epsilon)f(x)] \geq (1-\delta).$$

Si on regarde de près cette forme d'approximation se défend, car la défaillance du matériel et du système d'exploitation introduit déjà un petit risque d'erreur. Il suffit alors de choisir une valeur négligeable pour δ. Un praticien se contentera d'un tel programme.

Définition 5 (Approximation déterministe) *Une $(\epsilon, 0)$-approximation est une approximation déterministe.*

On définit les générateurs approximant de manière équivalente.

Définition 6 (Générateur presque-uniforme) *Un algorithme randomizé G sur l'entrée (x, ϵ) est un générateur presque-uniforme d'éléments de l'ensemble $R(x)$ s'il existe une fonction $\Phi : \Sigma^* \times \mathbf{R} \rightarrow]0, 1]$ telle que pour tout y*

$$y \notin R(x) \Rightarrow \Pr[G(x,\epsilon) \textit{ génère } y] = 0$$

et

$$y \in R(x) \Rightarrow \frac{\Phi(x,\epsilon)}{1+\epsilon} \leq \Pr[G(x,\epsilon) \textit{ génère } y] \leq (1+\epsilon)\Phi(x,\epsilon).$$

Si de plus le temps de calcul de G est borné en $|x|$ et $\lg \frac{1}{\epsilon}$, alors G est un générateur presque-uniforme entièrement polynomial.

Notez que contrairement aux schémas d'approximation l'erreur tolérée est ici exponentiellement petite, on peut s'imaginer que la valeur de $\frac{1}{\epsilon}$ est écrite en notation unaire sur le ruban d'entrée.

3.3 Échantillonner

Supposons qu'on ait un ensemble fini U d'éléments et un sous-ensemble $G \subseteq U$ de bons éléments. Supposons encore qu'on dispose d'une fonction caractéristique $f : U \rightarrow \{0, 1\}$ calculable efficacement, telle que $G = \{x : f(x) = 1\}$. Notre but est maintenant d'estimer le cardinal de G, connaissant exactement celui de U et disposant d'un générateur uniforme d'éléments de U.

Pour réaliser cette estimation, nous allons générer uniformément aléatoirement une nombre N d'éléments de U. Soit $u \in U$ le i-ème élément généré et $Y_i = f(u)$. Notons $Y = \sum_{i=1}^{N} Y_i$ le nombre de bons éléments générés. Le résultat de l'estimation est $\frac{Y}{N}$.

Théorème 1 (Théorème d'échantillonnage) *Soit μ le rapport de bons éléments, à savoir $\mu = \frac{|G|}{|U|}$. Si $N \geq \frac{1}{\mu} \cdot \frac{2}{\epsilon^2} \cdot \ln(\frac{2}{\delta})$, alors l'algorithme décrit ci-haut est une (ϵ, δ)-approximation.*

Preuve : Les variables aléatoires Y_i pour $i \in \{1, \ldots, N\}$ satisfont

$$Y_i = \begin{cases} 1 & \text{avec probabilité } \mu, \\ 0 & \text{avec probabilité } 1-\mu. \end{cases}$$

Donc la variable aléatoire Y suit une distribution binomiale (N, μ), ce qui nous permet d'utiliser les inégalités de Chernoff

$$\begin{aligned} \Pr[Y \leq (1-\epsilon)N\mu] &\leq e^{-\epsilon^2 \frac{N\mu}{2}} \text{ et} \\ \Pr[Y \geq (1-\epsilon)N\mu] &\leq e^{-\epsilon^2 \frac{N\mu}{2}}. \end{aligned}$$

Pour que l'algorithme décrit précédemment soit une (ϵ, δ)-approximation, il faut que la condition suivante soit satisfaite :

$$2e^{-\epsilon^2 \frac{N\mu}{2}} \leq \delta,$$

ou

$$N \geq \frac{1}{\mu} \cdot \frac{2}{\epsilon^2} \cdot \ln(\frac{2}{\delta}).$$

□

Remarque : Le schéma d'approximation randomizé précédent est une (ϵ, δ)-approximation, si le rapport de bons éléments μ est $O(1/q(|U|))$ pour un polynôme q donné.

3.4 Une (ϵ, δ)-approximation pour #DNF

Soit f une formule en forme normale disjonctive sur n variables données et V l'ensemble des 2^n assignations des variables. On note $f(v)$, pour un $v \in V$, l'évaluation de f pour l'assignation v. Notre but est de calculer le nombre d'assignations qui satisfont f.

A ce propos allons essayer d'utiliser le théorème d'échantillonnage. Comme nous avons remarqué précédemment, le problème est que le nombre d'assignations qui valident f ne doit pas être trop petit. En particulier si ce nombre est exponentiellement petit le nombre N d'échantillons à faire doit être exponentiellement grand.

Nous allons présenter une méthode qui résout ce problème [KLM]. Notons $f = C_1 \vee \ldots \vee C_m$, où les C_i sont des conjonctions de littéraux. Soit D_i l'ensemble des assignations satisfaisant C_i et $D = \bigcup_{i=1}^m D_i$. Si C_i contient l variables alors $|D_i| = 2^{n-l}$.

Notre but se résume alors à estimer le cardinal de D, car une assignation v satisfait C_i pour un certain i si et seulement si v satisfait f.

Soit U l'ensemble des paires (v, i), tel que v satisfait C_i. On a $|U| = \sum_{i=1}^m |D_i|$. Définissons maintenant une fonction $g : U \to \{0, 1\}$ comme suit.

$$g(v,i) = \begin{cases} 1 & \text{Si } i \text{ est le plus petit indice des } C_i \text{ satisfait par } v. \\ 0 & \text{Sinon.} \end{cases}$$

On a

$$\sum_{(v,i) \in V} g(v,i) = |D|.$$

Maintenant nous voulons compter les éléments de U qui satisfont f, qu'on décrit par l'ensemble

$$G = \{(v,i) : g(v,i) = 1\}.$$

Puisque qu'une assignation v satisfaisant f, valide au plus m conjonctions C_i, on a un rapport de $\mu = \frac{|G|}{|U|} geq \frac{1}{m}$.

Il est donc assuré, par le théorème d'échantillonnage, qu'un nombre polynomial d'échantillons suffit. Il ne nous reste plus qu'à montrer qu'on peut générer uniformément aléatoirement des éléments de U, et que $g(u,i)$ peut être évalué efficacement.

L'algorithme de génération de U fonctionne comme suit:

1. Choisir i aléatoirement avec une probabilité de tirage

$$\Pr[i \text{ est choisit}] = \frac{|D_i|}{|U|}.$$

2. Choisir uniformément $v \in D_i$.

La génération de (v,i) est bien uniforme car

$$\Pr[(u,i) \text{ est choisit}] = \frac{|D_i|}{|U|} \cdot \frac{1}{|D_i|} = \frac{1}{|U|}.$$

Pour évaluer $g(u,i)$, il faut évaluer les C_k, pour $k \leq i$ ce qui se fait en temps polynomial en $m \cdot n$.

Pour estimer le nombre d'assignations de f, il suffit alors d'estimer le rapport $\frac{|G|}{|U|}$ puis de multiplier le résultat avec $|U|$. Le calcul de $|U|$ et des $|D_i|$ est réalisé également en temps polynomial. Il existe donc une (ϵ, δ)-approximation pour #DNF.

4 Chaînes de Markov

Dans la section suivante nous présentons le rapport entre génération et comptage d'éléments d'un ensemble. Les chaînes de Markov peuvent dans certains cas servir à générer de tels éléments.

La chaîne de Markov est aussi un modèle probabiliste très utilisé en physique pour la simulation. Je veux ici introduire les notions nécessaires pour la suite du rapport. Une bonne introduction peut être trouvée en [F].

4.1 Définitions

Une chaîne de Markov consiste en un ensemble d'états $\mathcal{N}$ de cardinal N et une matrice stochastique $|\mathcal{N}| \times |\mathcal{N}|$ de transitions P. On note $H(\mathcal{N}, P)$ le graphe probabiliste sous-jacent. On peut s'imaginer les éléments de $\mathcal{N}$ comme des états d'un système physique où $P(i,j)$ est la probabilité que le système transite de l'état i à l'état j.

Le comportement d'une chaîne de Markov à travers le temps est décrit par une suite de variables aléatoires $(X_t)_{t=0}^{\infty}$ sur $\mathcal{N}$ qu'on appelle *marche aléatoire*. On a alors les probabilités $p_{ij} = \Pr[X_{t+1} = j | X_t = i]$ et $p_{ij}^{(s)} = \Pr[X_{t+s} = j | X_t = i]$ définie par $P^s = (p_{ij}^{(s)})$. La distribution sur X_t est le vecteur $\pi^{(t)} = (\pi_i^{(t)})_{i=0}^{N-1}$ avec $\pi_i^{(t)} = \Pr[X_t = i]$ et $\pi^{(t+1)} = \pi^{(t)} \cdot P$.

En général nous utiliserons une chaîne de Markov pour générer des éléments d'un ensemble, qui constitueront les sommets du graphe sous-jacent. L'idée est de partir de n'importe quel élément, de faire une marche aléatoire, avec les probabilités décrits par P, pendant un certain temps, jusqu'à ce que la distribution soit proche de la distribution stationnaire. On veut que ceci soit rapidement le cas, propriété qu'on appelle *mélange rapide*.

Dans la suite on notera P la matrice stochastique de la chaîne de Markov, H le graphe sous-jacent, $\mathcal{N}$ son ensemble de sommets qui est de taille N. $\pi^{(k)}$ sera la distribution sur $\mathcal{N}$ à l'instant k, $\pi^{(0)}$ la distribution initiale et π' la distribution stationnaire si elle existe. En général, nous utiliserons une distribution initiale simple telle que $\pi^{(0)}$ est 1 pour un certain $i \in \mathcal{N}$ et 0 ailleurs.

Définition 7 (ergodique) *On dit que la chaîne est* ergodique *si elle tend vers une probabilité stationnaire ce qui se caractérise par*

$$\exists \pi \textit{ tel que } \forall i, j : \lim_{s \to \infty} P^s(i, j) = \pi(j)$$

Dans ce cas la la limite de la distribution est indépendante de la distribution initiale. La distribution stationnaire est l'unique vecteur π qui satisfait $\pi P = \pi$ et est donc l'unique vecteur propre normalisé de P avec la valeur propre 1 associée.

La distribution stationnaire est uniforme ssi pour $\pi = (N^{-1}, \ldots, N^{-1})$ P satisfait $\pi P = \pi$. Ceci est le cas ssi pour toute colonne j, la somme des $P(i, j)$ est 1. Ceci implique que la distribution stationnaire est uniforme si P est symétrique.

Les figures 1 et 2 illustrent des chaînes ergodiques respectivement non-ergodiques.

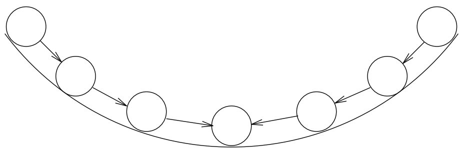


FIG. 1 - *Le comportement d'un ballon dans une vallée est ergodique. Peu importe la position initiale, le ballon va se trouver au centre au bout d'un moment.*

Définition 8 (irréductible) *Une chaîne est irréductible si*

$$\forall i, j \in \mathcal{N}\, \exists s \in \mathbf{N} : p_{ij}^{(s)} > 0$$

autrement dit si tout point est accessible de tout point en un nombre fini d'étapes.

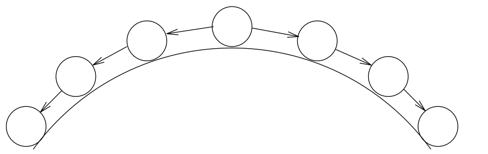


FIG. 2 - *Le comportement d'un ballon sur une colline n'est pas ergodique. La distribution stationnaire est différente suivant que l'états de départ est un ballon sur le coté gauche ou droite.*

Ceci exprime que le graphe sous-jacent est fortement connexe. La chaîne de la figure 2 n'est pas irréductible car il n'y a pas de chemin de l'état “posé sur la pente de droite” à l'état “posé sur celle de gauche”.

Définition 9 (apériodique) *Une chaîne est apériodique si pour tout* $i, j \in [N]$

$$\text{pgcd}\{s : P^s(i,j) > 0\} = 1$$

Une chaîne est apériodique si elle n'oscille pas. Par exemple si le pgcd était $k > 1$ pour un couple i, j, alors on pourrait atteindre j de i en $k, 2k, \dots$ étapes mais pas en $k+1, 2k+1, \dots$ étapes.

En ajoutant des boucles à chaque état de probabilité $\frac{1}{2}$ par l'opération $P' = \frac{1}{2}(P + I_{N\times N})$ on peut cependant rendre toute chaîne apériodique.

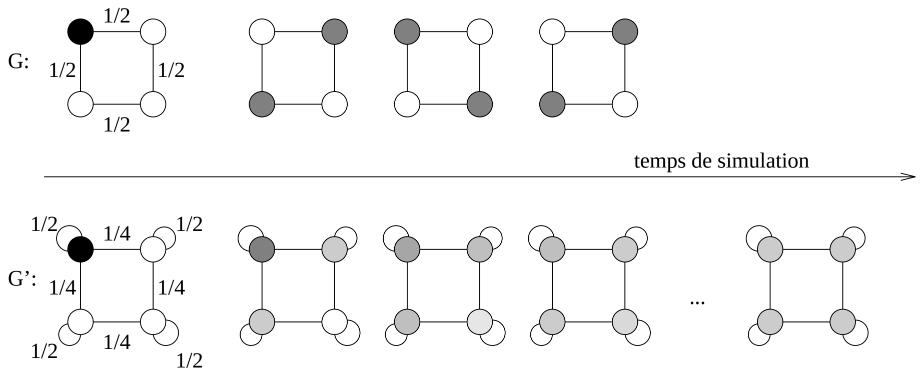


FIG. 3 - *Deux chaînes de Markov: G périodique et G' apériodique. Les arrêtes sont étiquetées par leur probabilité de transition respective. La distribution est représenté par la coloration des sommets, où noir est 1 et blanc 0. Le lecteur observera que G' tend vers une distribution stationnaire uniforme alors que G oscille.*

Théorème 2 *Deux conditions nécessaires et suffisantes pour l'ergodicité d'une chaîne sont*

1. *qu'elle est irréductible et*
2. *qu'elle est apériodique.*

Définition 10 (réversible) *Une chaîne est réversible si la condition de balance suivante est satisfaite.*

$$\forall i, j\; p_{ij}\pi_i = p_{ji}\pi_j$$

On note alors $Q_{ij} = p_{ij}\pi_i$ *le poids de l'arête* (i, j) *de* G.

4.2 Caractérisation du temps de mélange

On veut se servir d'une chaîne de Markov pour générer des éléments d'un ensemble dont les éléments sont des structures combinatoires. Nous nous intéressons alors au temps de mélange de cette chaîne, c'est-à-dire le temps pendant lequel il faut faire une marche aléatoire dans la chaîne pour générer presque uniformément des éléments. Typiquement le cardinal d'un tel ensemble va être exponentiel en n, la taille de l'entrée du problème, et le temps de mélange devrait être polynomial en n.

Pour cela considérons la chaîne suivante. Soit X l'ensemble des états avec $N = |X|$. Soit P la matrice de transition sur les états. Supposons que P soit ergodique et π l'unique distribution stationnaire. Supposons encore que P soit réversible en temps, on définit alors pour tout $x, y \in X$ $Q(x, y) = \pi(x)P(x, y) = \pi(y)P(y, x)$, la *capacité* associée aux arrêtes du graphe sous-jacent.

L'algorithme de génération va être le suivant. On part d'un état arbitraire $x \in X$, puis pendant un temps t on effectue une marche aléatoire dans la chaîne et le sommet courant y de l'instant t est la résultat de la génération. La distribution de la sortie de l'algorithme est donc $P^t(x, \cdot)$. Pour quantifier la différence de cette distribution par rapport à la distribution stationnaire nous allons introduire la notion suivante.

Définition 11 (distance variationnelle) *La distance variationnelle entre la distribution stationnaire et la distribution* $P^t(x, \cdot)$ *est la quantité*

$$\Delta_x(t) = \max_{S \subseteq X} |P^t(x, S) - \pi(S)| \quad (1)$$

$$= \frac{1}{2} \sum_{y \in X} |P^t(x, y) - \pi(y)| \quad (2)$$

La figure 4 illustre la différence des distributions π et $P^t(x, \cdot)$, qui tend a diminuer quand le temps t augmente : Pour un t proche de 0, uniquement les sommets à distance d'au plus t du sommet initial $x \in X$ ont une probabilité non-nulle d'être atteint. Normalement l'espace des états est discret, mais pour faciliter l'illustration nous avons représenté X par un scalaire. La surface grise illustre la différence entre les deux distributions.

Cette quantité nous permet alors de définir le temps de mélange.

Définition 12 (temps de mélange) *Le temps d'exécution de l'algorithme de génération décrit ci-dessus pour être à* ϵ *près de la distribution stationnaire est*

$$\tau_x(\epsilon) = \min\{t : \forall t' \geq t\; \Delta_x(t') \leq \epsilon\}$$

avec $\tau(\epsilon) = \max_x \tau_x(\epsilon)$.

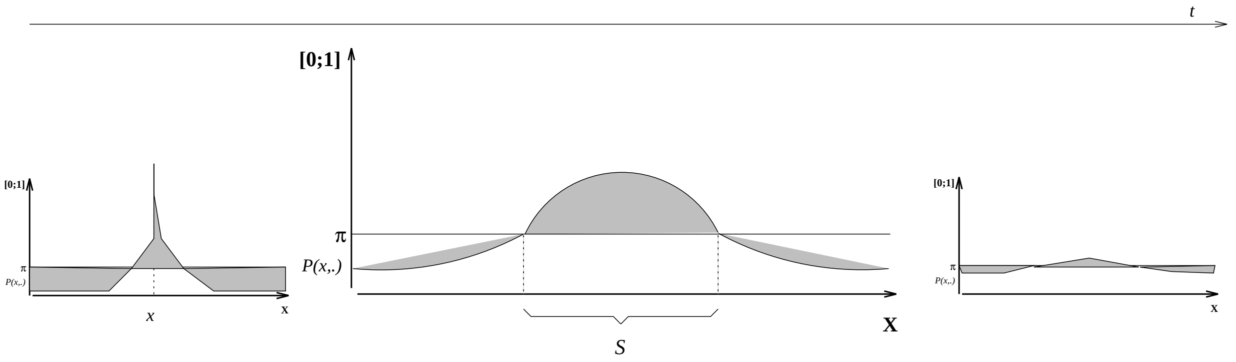


FIG. 4 - *Evolution de la distribution $P^t(x, \cdot)$ par rapport à π.*

En tant que matrice stochastique P a N valeurs propres réels qu'on peut ordonner comme suit. $1 = \lambda_0 > \lambda_1 \geq \dots \lambda_{N-1} \geq -1$. (Notez: On sait que P est ergodique ssi $\lambda_0 = 1$). Le temps de mélange dépend de $\lambda_{\max} = \max\{\lambda_1, |\lambda_{N-1}|\}$, or en pratique on va ajouter une probabilité $\frac{1}{2}$ de rester sur place, c'est-à-dire remplacer P par $(I+P)/2$, ce qui a pour effet de rendre toutes les valeurs propres positives. Dans la suite nous allons alors seulement parler de λ_1. L'écart spectral $\lambda_0 - \lambda_1 = 1 - \lambda_1$ caractérise le temps de mélange comme suit :

$$\forall x \in X : \tau_x(\epsilon) \leq \frac{1}{1-\lambda_1}(\ln \frac{1}{pi_x} + \ln \frac{1}{\epsilon}, \tag{3}$$

$$max_{x \in X} \tau_x(\epsilon) \geq \frac{\lambda_1}{2(1-\lambda_1)} \ln \frac{1}{2\epsilon}. \tag{4}$$

On peut dire plusieurs choses sur cette caractérisation :

- Pour être avoir une distribution plus proche de la distribution stationnaire, (on diminue ϵ), la chaîne doit être simulée plus longuement, ce qui est assez intuitif.

- En pratique il faut choisir une état initial x qui a une probabilité stationnaire π_x maximale, pour minimiser le temps de simulation.

- Pour avoir un temps de mélange polynomial en n, la taille de la description de X, il faut que l'écart spectral soit l'inverse d'un polynôme en n.

Conductance

Une première approche consiste à caractériser $1 - \lambda_1$ par une mesure faite sur le graphe sous-jacent, la *conductance*. L'idée de cette mesure est que si la chaîne ne mélange pas rapidement, c'est que le graphe contient un goulot d'étranglement, il existe alors une partie du graphe qu'une marche aléatoire ne quitte qu'avec une très faible probabilité. On appelle *flot ergodique* d'une partie du graphe $S \subseteq X$, la probabilité $Q(S, \bar{S}) = \sum_{x \in S, y \in \bar{S}} Q(x, y)$ de sortir de S et *capacité* la probabilité $\pi_S = \sum_{x\in S} \pi_x$ de s'y trouver. La conductance Φ est alors le rapport entre ces deux mesures minimisé sur S :

$$\Phi = \min_{\substack{S\subseteq X\\ 0<\pi_S\leq\frac{1}{2}}} \frac{Q(S,\bar{S})}{\pi_S}$$

La conductance caractérise l'écart spectral seulement au carré près.

$$\frac{\Phi^2}{2} \leq 1-\lambda_1 \leq 2\Phi$$

Ceci est suffisant pour montrer que le temps de mélange est polynomial dans la taille de l'entrée, mais en pratique, nous nécessitons une mesure plus précise.

Chemins canoniques

Soit $\Gamma = \{\gamma_{xy}\}$ une collection de chemins simples[2] dans la chaîne tel que pour tout couple (x, y) de sommets de X, Γ contient un seul chemin γ_{xy}, qu'on appelle alors chemin canonique. L'idée de l'analyse qui va suivre est que si le graphe sous-jacent de la chaîne de Markov contient un goulot d'étranglement, alors quel que soit la manière de choisir Γ, les arrêtes de ce goulot seront surchargées de chemins, c'est-à-dire seront contenu dans (feront partie de) trop de chemins canoniques. C'est cette surcharge d'arrêtes qu'on essaye de quantifier avec les mesures suivantes qui sont tous décrit dans [S2].

Dans une première approche nous allons associer la charge $\pi_x\pi_y$ aux chemins γ_{xy}. Le chargement maximal d'une arrête pondérée par sa capacité est alors

$$\rho(\Gamma) = \max_e \frac{1}{Q(e)} \sum_{\gamma_{xy}\ni e} \pi_x\pi_y$$

(En posant $\rho = \min_\Gamma \rho(\Gamma)$ on ne s'intéressera dans une analyse qu'aux *bonnes* collections de chemins, sans toutefois être obligé de trouver le minimum.) Cette mesure est lié comme suit a la conductance

$$\Phi \geq \frac{1}{2\rho}$$

et caractérise donc l'écart spectral également uniquement dans un ordre carré, en appliquant la borne donnée par la conductance, par

$$1-\lambda_1 \geq \frac{1}{2\rho^2}.$$

Un meilleur résultat peut être obtenu en faisant intervenir la longueur d'un chemin dans sa charge. Soit maintenant $\pi_x\pi_y|\gamma_{xy}|$ la charge des chemins γ_{xy}. La nouvelle mesure devient alors

$$\bar{\rho}(\Gamma) = \max_e \frac{1}{Q(e)} \sum_{\gamma_{xy}\ni e} \pi_x\pi_y|\gamma_{xy}|.$$

2. Un chemin simple est un chemin sans boucle.

La caractérisation de cette mesure est directement

$$1 - \lambda_1 \geq \frac{1}{\bar{\rho}}.$$

La preuve de cette minoration utilise la caractérisation variationnelle de la première valeur propre du Laplacien $L = I - P$. Elle est d'ailleurs pratiquement la même pour la mesure similaire de Diaconis et Strook [DS] qui remplace dans la définition de $\bar{\rho}$ $|\gamma_{xy}|$ par la quantité

$$|\gamma_{xy}|_{Q,e} = \sum_{e' \in \gamma_{xy}} \frac{Q(e)}{Q(e')},$$

donnant lieu à la mesure $\bar{\rho}_{DS}$. Notez ici que ces deux mesure sont équivalentes si Q est uniforme pour tout les e, bien qu'il existe des chaînes de Markov où la mesure de Sinclair et d'autres qui favorisent celle de Diaconis et Strook.

Nous pouvons déduire immédiatement une simplification de cette mesure. En posant $l(\Gamma) = \max_{p \in \Gamma} |p|$ on obtient la minoration

$$1 - \lambda_1 \geq \frac{1}{\rho l},$$

qui en pratique peut être plus facilement applicable que $\bar{\rho}$ et aussi plus précis que ρ si l est d'un plus petit ordre que ρ.

Flot multi-charges

Plutôt de ne s'intéresser qu'au chemins canoniques on peut essayer de généraliser les mesures décrites ci-dessus au flots multi-charges. On considère alors $\mathcal{P}_{x,y}$ l'ensemble de tous les chemins simples de x à y et on pose $\mathcal{P} = \bigcup_{x \neq y} \mathcal{P}_{xy}$. Un flot est alors une fonction $f : \mathcal{P} \to \mathbf{R}^+$ satisfaisant pour tout $x, y \in X$, avec $x \neq y$,

$$\sum_{p \in \mathcal{P}_{xy}} = \pi_x \pi_y.$$

On peut voir f comme une fonction qui repartie la charge $\pi_x \pi_y$ sur les chemins simples entre x et y. Notons ici que les chemins canoniques ne sont qu'un flot particulier, où la charge est porte par un seul chemin. Nous allons maintenant étendre f sur les arrêtes en posant

$$f(e) = \sum_{p \ni e} f(p),$$

qui est la charge supportée par l'arrête e, et

$$\bar{f}(e) = \sum_{p \ni e} f(p)|p|.$$

Comme dans la partie précédente nous posons $\rho(f) = \max_e f(e)/Q(e)$, $\bar{\rho}(f) = \max_e \bar{f}(e)/Q(e)$ ainsi que $l(f) = \max_{f(p) \neq 0} |p|$. Soit encore ce que Sinclair appelle la résistance $\rho = \inf_f \rho(f)$. Nous obtenons les mêmes minorations comme ci-dessus avec ces mesures plus générales.

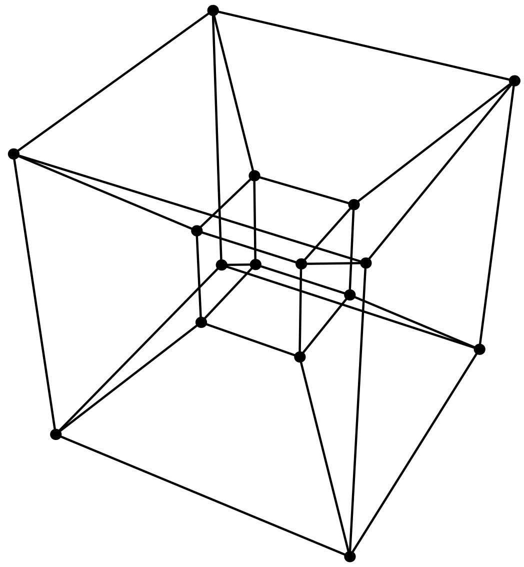


FIG. 5 - *Un hypercube de dimension $n = 4$.*

Exemple: Hypercube

Pour faciliter la compréhension de ces mesures, nous allons les appliquer sur un exemple de marche dans un hypercube. Soit n la dimension de l'hypercube. L'ensembles de ses points est $X = \{0,1\}^n$ avec $N = |X| = 2^n$. Notons par $\Delta(x,y)$ la distance de Hamming entre x et y, c'est-à-dire, le nombre de bits différents entre x et y. On définit alors la matrice de transition par

$$P_{xy} = \begin{cases} \frac{1}{2} & x = y \\ \frac{1}{2n} & \Delta(x,y) = 1 \\ 0 & \text{sinon} \end{cases} .$$

Cette chaîne de Markov est apériodique, grâce aux boucles sur les sommets, elle est irréductible, car l'hypercube est un graphe connexe. Elle est donc ergodique et l'unique distribution est uniforme, c'est-à-dire $\pi = (1/N)$. P est symétrique, donc la chaîne est aussi réversible en temps d'où $Q(x,y) = \pi(x)P(x,y) = \pi(y)P(y,x) = 1/(2nN)$ pour les arrêtes (x,y) du cube, avec $x \neq y$. Nous allons maintenant analyser le temps de mélange de cette chaîne.

Dans un premier temps ne considérons seulement des chemins canoniques. Etant donnés deux point $x, y \in X$, leur distance $\Delta(x,y)$ indique le nombre de bits différents, et est donc aussi la longueur du plus court chemin entre x et y. Donnons un ordre quelconque sur ces bits, et changeons les un après l'autre, nous avons ainsi un chemin canonique entre x et y. Quel est la charge supporte par une arrête par ces chemins? Soit $e = (a,b)$ une arrête du cube, avec $a = (u0v)$, $b = (u1v)$ et $u \in \{0,1\}^{k-1}$, $v \in \{0,1\}^{n-k}$. e relie deux hyperplans, celui des $x \in X$ qui ont un 0 à la k-ème position et celui des x qui y ont un 1. Chaqu'un des plans contient $N/2$ points. De plus entre ces deux plan il y a $N/2$ arrêtes comme e

(pour chaque u et v). Par symétrie des arrêtes le nombre de chemins passant par e est $(N/2)^2/(N/2) = N/2$. On obtient alors

$$\begin{aligned}\rho(\Gamma) &= \min_e \frac{1}{Q(e)} \sum_{\gamma_{xy} \ni e} \pi_x \pi_y \\ &= 2nN \frac{N}{2} \frac{1}{N^2} \\ &= n,\end{aligned}$$

qui nous donne la minoration $1 - \lambda_1 \geq \frac{1}{8n^2}$ de l'écart spectral.

Tentons maintenant de faire cette analyse pour des flots. Entre x et y il y a $\Delta(x, y)!$ plus courts chemins, correspondant aux différentes manières de choisir l'ordre des bits à changer. On pose alors

$$f(p) = \begin{cases} \frac{1}{\Delta(x,y)!N^2} & \text{pour } p \text{ plus court chemin de } x \text{ à } y \\ 0 & \text{sinon} \end{cases}.$$

On majore pour un tel p très grossièrement par $f(p) \leq 1/(\Delta(x, y)N^2)$ et on en déduit que $\bar{f}(p) \leq 1/N^2$. L'extension de $\bar{f}$ aux arrêtes donne alors

$$\bar{f}(e) = \sum_{p \ni e} \bar{f}(p) \leq \frac{N}{2} \frac{1}{N^2} \leq \frac{1}{2N}.$$

Ceci nous mène à la résistance suivante,

$$\begin{aligned}\bar{\rho}(f) &= \max_e \frac{\bar{f}(e)}{Q(e)} \\ &\leq \frac{\frac{1}{2N}}{\frac{1}{2nN}} \\ &= n.\end{aligned}$$

La caractérisation est alors nettement meilleure par cette dernière mesure, qui donne $1 - \lambda_1 \geq \frac{1}{n}$, sachant que la valeur exacte est $1 - \lambda_1 \geq \frac{c}{n}$, pour une constante c [S1].

4.3 Génération presque uniforme

Ici on va se servir des chaînes pour générer presque uniformément des éléments d'un ensemble exponentiellement grand. Notre générateur effectue alors une marche aléatoire jusqu'à ce que la distribution point à point soit inférieure à un ϵ donné. La sortie du programme est l'état final. Si la chaîne se mélange rapidement, le générateur sera polynomial même pour un ensemble de taille exponentielle. Un exemple de preuve de mélange rapide sera donné au chapitre suivant dans le cadre d'une approximation randomizée du permanent d'une matrice 0-1.

5 Générer est aussi difficile que compter

La plupart des problèmes peuvent être représentés par une relation binaire $R'(x,y)$ où x est l'instance du problème et y une solution associée. On peut supposer que x et y sont des mots d'un alphabet fini Σ. On note $R(x) = \{y : R'(x,y)\}$ l'ensemble des solutions de x. Par exemple, x peut être un entier et y une partition de x, ou encore x est un graphe et y un couplage de celui-ci. Pour une telle relation et un x donné différentes questions peuvent être posées. La liste suivante les présente dans leur ordre de difficulté.

Existence Existe-t-il un mot $y \in \Sigma^*$ tel que $R'(x,y)$?

Construction Exhiber un mot $y \in \Sigma^*$ qui satisfait $R'(x,y)$ s'il en existe.

Génération (uniforme) Générer uniformément (avec une probabilité $1/|R(x)|$) aléatoirement un mot $y \in \Sigma^*$ satisfaisant $R'(x,y)$.

Comptage Combien de de mots $y \in \Sigma^*$ satisfont $R'(x,y)$?

Le problème de l'existence est réductible à la construction, car cette dernière en fournit un témoin. De même la construction est réductible à la génération uniforme. Par contre les liens entre génération et comptage sont un peu plus cachés.

5.1 Génération versus Comptage

Pour certaines relations R il est possible de construire un générateur uniforme utilisant un oracle de comptage. Il faut pour cela que la relation donnée soit *auto-réductible*. L'idée est de construire une solution en étapes récursives en partant d'instances de plus en plus courtes.

Définition 13 *Une relation R est auto-réductible [SJ, p. 99] si*

1. *Il existe une fonction calculable en temps polynomial $g : \Sigma^* \to \mathbf{N}$ telle que $\forall y \in R(x) : |y| = g(x)$.*

2. *Pour tout x tel que $g(x) = 0$ on peut décider en temps polynomial si $R(x) = \emptyset$ ou $R(x) = \{\Lambda\}$, où Λ représente le mot vide. On nomme un tel x un atome.*

3. *Il existe des fonctions calculables en temps polynomial $\phi : \Sigma^* \times \Sigma^* \to \Sigma^*$ et $\sigma : \Sigma^* \to \mathbf{N}$ satisfaisant pour tout $x, w \in \Sigma^*$*

$$\sigma(x) = O(\log |x|)$$

$$g(x) > 0 \Rightarrow \sigma(x) > 0$$

$$|\phi(x,w)| \leq |x|$$

et pour tout $x \in \Sigma^*, y = y_1 \ldots y_n \in \Sigma^*$

$$\langle x, y_1 \ldots y_n \rangle \in R \Leftrightarrow \langle \phi(x, y_1 \ldots y_{\sigma(x)}), y_{\sigma(x)+1} \ldots y_n \rangle \in R$$

Notez que dans cette définition toutes les solutions y d'une instance x ont la même longueur $g(x)$, quitte à ajouter des espaces supplémentaires aux y plus petits.

Autrement dit on peut reformuler R comme suit

$$R(x) = \bigcup_{w \in \Sigma^{\sigma(x)}} \{wy : y \in R(\phi(x, w))\}.$$

5.1.1 Exemple sur les couplages

Proposition 1 (Couplages) *La relation $M(G)$ qui à un graphe donné associe ses couplages est auto-réductible.*

Preuve : Cette notion appliquée à l'exemple des couplages parfaits nous donne la définition auto-réductible suivante:

$$M(G) = \{e\} \times M(G^-) \cup M(G^+)$$

où $M(G)$ est l'ensemble des couplages parfaits de G, $e = (u, v)$ une arête de $G(V, E)$, G^- le sous-graphe de G sans les sommets u et v et G^+ le sous-graphe de G sans l'arête e.

Le codage d'un graphe à n sommets pourrait être une matrice d'adjacence, donc dans ce cas $|G| = n^2$. On pourrait par exemple coder un couplage comme une liste de couples arête-booléen. Le booléen indiquera si l'arête fait partie du couplage ou pas. Si on code maintenant une arête par un couple d'entiers représentant deux sommets, alors la taille maximale d'un couplage est $g(G(V, E)) = |V| \log |V| = n \log n$. Pour un graphe sans arête $g(G) = 0$ et $M(G) = \{\emptyset\}$. A chaque étape de la réduction on décide si on ajoute une arête au couplage. Donc on peut définir $\sigma(G) = 1 + 2 \log n$ pour G à l'exception des graphes sans arêtes $\sigma(G) = 0$ sinon. Il ne nous reste maintenant plus qu'à définir la fonction ϕ

$$\phi(G, \langle b, e \rangle) = \begin{cases} G^- & \text{si } b = 0 \\ G^+ & \text{si } b = 1 \end{cases}$$

Ces fonctions satisfont les conditions pour que M soit une relation auto-réductible. $\square$

5.1.2 Générer des éléments de $R(x)$

Pour un x donné et une relation auto-réductible R avec $R(x) \neq \emptyset$ construisons un arbre $T_R(x)$ [SJ, p. 100] où chaque nœud est étiqueté par une *instance* x' de R et par w un *préfixe* d'une solution de x :

1. La racine est étiquetée par l'instance x et le préfixe Λ.
2. Pour tout nœud v dans $T_R(x)$, si $z = \text{instance}(v)$ est un atome, alors v est une feuille. Sinon nous définissons les fils de v avec

   $$W(v) = \{w \in \Sigma^{\sigma(x)} : R(\phi(z, w)) \neq \emptyset\}.$$

   A chaque $w \in W(v)$ on associe un nœud à l'instance $\phi(z, w)$ et au préfixe qui est le préfixe de v concatené avec w.

La profondeur et le degré de cet arbre sont d'ordre polynomial, car $|\Sigma^{\sigma(x)}|$ et $g(x)$ le sont.

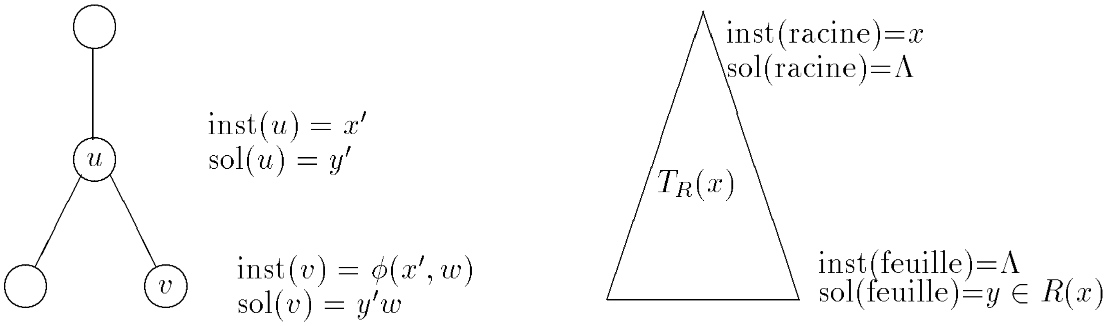


FIG. 6 - *L'arbre* $T_R(x)$

Proposition 2 *Si le problème de l'existence est dans P alors la construction l'est aussi.*

Preuve : Il suffit de parcourir l'arbre $T_R(x)$ de la racine à une feuille sur un chemin arbitraire et de sortir la solution attachée à la feuille. □

Proposition 3 *Etant donné un compteur exact pour la relation auto-réductible* $R(x)$ *on peut construire un générateur uniforme.*

Preuve : Il suffit de faire un parcours du sommet aux feuilles dans l'arbre $T_R(x)$ et de sortir la solution attachée à la feuille. A chaque nœud v on choisit un des fils v_w avec une probabilité $|R(inst(v_w))|/|R(inst(v))|$, donc les feuilles sont équiprobables. L'arbre étant de profondeur polynomiale ceci nous donne le générateur uniforme polynomial suivant, où le premier appel sera $Génère(x,\Lambda)$.

fonction *Génère*(inst,sol)
début
  si $l_R(\mathrm{inst}) = 0$ **alors** retourner sol
  sinon
    choisit $w \in \Sigma^{\sigma(inst)}$ **avec une probabilité de**

$$\frac{Compte(\phi(\mathrm{inst}, w))}{\sum_{w'} Compte(\phi(\mathrm{inst}, w'))}$$

    $Génère(\phi(\mathrm{inst}, w), \mathrm{sol} \cdot w)$
  fin
fin

□

Proposition 4 ([JVV]) *Soit R une relation auto-réductible et k_R une constante telles que pour tout $(x,y) \in R$ on a $|y| = O(|x|^{k_R})$. Etant donné un compteur approximatif dans un rapport de $1 + O(n^{-k_R})$ pour la relation auto-réductible $R(x)$, on peut construire un générateur presque uniforme complètement polynomial avec rejet. De plus si le compteur est déterministe il existe un générateur uniforme avec rejet.*

Une preuve simple peut-être trouvé dans [S1, p. 28–31]. L'idée est d'ajouter une correction dans l'algorithme pour les compteurs exacts, qui consiste à ne retourner l'élément généré qu'avec une probabilité inversement proportionnelle à l'erreur cumulée.

On voit qu'une petite erreur du compteur, peut être corrigé par un correction en fin de parcours de l'arbre $T_R(x)$, donnant lieu à un générateur uniforme avec rejet. Plus précisément l'erreur tolérée est de $1 + O(n^{k_R})$, où k_R est une constante dépendant de R. Cette technique ne peut pas être utilisée avec des compteur à plus faible précision, car l'erreur accumulée lors du parcours est alors trop grande pour être corrigée. L'idée de Mark Jerrum était de construire une chaîne de Markov en permettant des retours lors du parcours de l'arbre. Cette nouvelle technique ne requiert plus qu'un compteur approximatif dans un rapport de $1 + n^{\beta}$ pour une constante β arbitraire.

Soit C un tel compteur approximatif déterministe dans un rapport de $p(|x|) = 1 + n^{\beta}$.

Sans perte de généralité on peut suppose C croissant, et exact si l'entrée est un atome. Notons $m = g(x)$ et $r = p(|x|)$. Pour toute arête (u,v) de E on définit son poids

$$f(u,v) = \begin{cases} C(\mathrm{inst}(u)) & \text{si } v \text{ est le père de } u, \\ C(\mathrm{inst}(v)) & \text{sinon.} \end{cases}$$

Maintenant définissons pour tout sommet v un *degré*, où $\Gamma(v)$ est l'ensemble des sommets adjacents à v,

$$d(v) = \sum_{u \in \Gamma(v)} f(u,v).$$

Remarquez que $d(v) \geq 1$ pour tout sommet v et $d(v) = 1$ si v est une feuille, car C est exact pour les atomes. Définissons maintenant la probabilité de transition de la chaîne de Markov entre deux sommets u et v par

$$p_{uv} = \begin{cases} \frac{f(u,v)}{2d(v)} & \text{si } (u,v) \in E, \\ \frac{1}{2} & \text{si } u = v, \\ 0 & \text{sinon.} \end{cases}$$

Du aux boucles sur les sommets, la chaîne est apériodique. Elle est aussi irréductible, grâce à la structure d'arbre, et donc ergodique. Les probabilités de transitions ont été choisit de sorte que la chaîne vérifie la condition de balance, et elle est alors réversible avec la distribution stationnaire $\pi' = (\pi_v)$ pour

$$\pi_v = \frac{d(v)}{D}$$

avec $D = \sum_v d(v)$. Comme $d(v)$ est 1 pour les feuilles, la distribution est uniforme pour eux.

Lemme 1 *La probabilité d'être dans une feuille pendant la distribution stationnaire est au moins* $\frac{1}{rm}$.

Preuve : La somme D des degrés sur les sommets de l'arbre $T_R(x)$ peut se récrire par

$$D = \sum_v d(v) = \sum_{e \in E} f(e).$$

Considérons les arêtes d'un niveau dans l'arbre. Leur poids approche dans un rapport r le nombre de feuilles du sous-arbre attaché au sommet bas de l'arête. La somme des poids de ces arêtes est au plus $r\#R(x)$, ce qui nous mène, en sommant sur tous les niveaux, à la borne

$$D = \sum_{e \in E} f(e) \leq \frac{1}{rm}.$$

La probabilité stationnaire d'être dans une feuille est donc

$$\sum_{\text{feuilles } v} \pi_v = \frac{\#R(x)}{D} \geq \frac{1}{rm}.$$

$\square$

Lemme 2 *Soit G la graphe sous-jacent de la chaîne de Markov décrite précédemment. La conductance a comme borne inférieure*

$$\Phi(G) \geq \frac{1}{4r^2 m}.$$

5.2 Compter les éléments de $R(x)$

Pour compter le nombre d'éléments de $R(x)$ nous allons parcourir l'arbre $T_R(x)$ de la racine à une feuille, en estimant à chaque nœud interne, le rapport des nombre de feuilles de chaque sous-arbre. Cette estimation est réalisée par un échantillonnage suffisamment grand, pour être assez précis. On choisit à chaque niveau, le fils avec le plus grand sous-arbre. Ceci permet de minimiser l'erreur faite lors de l'estimation.

6 Approximation du nombre de couplages parfaits

Définition 14 (k-Couplage) *Un k-couplage d'un graphe $G(V, E)$ est un ensemble de cardinal k d'arêtes disjoints de G.*

Définition 15 (Permanent) *Le permanent d'une matrice $n \times n$ $A = (a_{ij})$ est*

$$perm(A) = \sum_\sigma \prod_{i=1}^n a_{i\sigma_i}$$

où la somme est sur tous les permutations σ de $\{1, \ldots, n\}$.

Soit A la matrice d'adjacence aux entrées 0 et 1 d'un graphe biparti $G(U, V, E)$. Le nombre de couplages de G est égal au permanent de A car une permutation correspond à une bijection $U \to V$.

Le permanent ressemble syntaxiquement au déterminant, mais les signes des permutations sont tous positifs. Cependant le permanent est #P-complet [V], alors que le déterminant est dans NC^2. Même pour les graphes bipartites denses[3] ce problème reste #P-complet [B].

Le meilleur algorithme déterministe requiert $2^{n+O(\log n)}$ étapes [Ry]. Il existe un algorithme d'approximation randomizé pour tout graphe qui fonctionne en $\exp(O(\sqrt{n}\log^2 n))$ étapes [JV]. Une (ϵ, δ)-approximation, qui cependant ne s'applique qu'aux graphes denses, est décrit dans cette section.

Si NP$\neq$RP alors le permanent n'est pas approximable [S1, p. 37]. Ceci est vrai, car s'il existait une approximation déterministe g de la fonction $\#R$, pour un problème NP-complet R donné, alors d'après la définition d'une telle approximation, g devrait retourner 0 pour une entrée $x \notin R$ et retourner une valeur supérieure à 0 pour un $x \in R$.

Le permanent est compris entre 0 et $n!$. Pour la probabilité d'arête p l'espérance est $p^n n!$, mais la variance est trop grande pour que cette valeur puisse servir d'approximation.

Zuckerman [Z] a montré que le permanent d'une matrice $\{-1, 0, 1\}$ est difficile à approcher, c'est-à-dire est non-approximable sous des hypothèses raisonnables. Par contre pour des matrices 0-1 Broder [B] a proposé un schéma d'approximation, réfuté plus tard par Mihail [M]. Jerrum et Sinclair donnent une correction et décrivent une autre approche markovienne pour ce problème que nous présentons ici.

6.1 Approximation de Jerrum et Sinclair

Soit $G = (U, V, E)$ un graphe biparti tel que $|U| = |V| = n$. Soit $M_k(G)$ l'ensemble des k-couplages de G. Notons $m_k = |M_k(G)|$ pour un G fixé et $M_*(G) = \bigcup_k M_k(G)$. L'idée est de calculer approximativement m_n en approximant les rapports m_k/m_{k-1}, car

$$m_n = \frac{m_1}{m_0}\frac{m_2}{m_1}\cdots\frac{m_n}{m_{n-1}}$$

et on connaît $m_0 = 1$ et $m_1 = |E|$.

Broder avait proposé de construire une chaîne de Markov sur les couplages parfaits et presque parfaits, puis de générer presque uniformément un état de cette chaîne pour ainsi approcher le rapport m_n/m_{n-1}. Pour approcher m_k/m_{k-1} il allait approcher m_n/m_{n-1} sur une transformation du graphe. Par contre, Jerrum et Sinclair proposent d'estimer directement m_k/m_{k-1} par le biais des systèmes monomère-dimère.

3. $G(U, V, E)$ avec $n = |V| = |U|$ est dense si le degré minimal est $\frac{n}{2}$

6.1.1 Systèmes monomère-dimère

Un système monomère-dimère est un modèle physique comme suit : Considérons un ensemble d'atomes susceptibles de former deux à deux des molécules, qu'on appelle dimère. Entre certains atomes proches existe un poids p, qui est la probabilité relative[4] de former une telle liaison, que, pour simplifier, nous allons supposer uniforme. Ce système est modélisé par un graphe probabiliste sur les atomes, qui est en général une grille. Deux atomes liés forment un dimère, un atome non-lié un monomère. Une configuration de monomère-dimère correspond à un couplage dans le graphe.

Pour un graphe $G(V, E)$ on peut associer le poids d'une configuration M donnée comme suit

$$W(G, M) = \prod_{e \in M} p = p^{|M|}$$

et la fonction de partition

$$Z(G) = \sum_{M \in M_*(G)} W(G, M).$$

De $Z(G)$ on peut déduire beaucoup de propriétés thermodynamiques. Le calcule exact de cette fonction est #P-difficile, car le nombre de couplages parfaits y est réductible. Jerrum et Sinclair proposent aussi une (ϵ, δ)-approximation pour Z que nous n'allons cependant pas exposer dans ce cadre.

On veut alors un générateur de couplages pour le graphe $G(V, E)$, qui donne approximativement à M la probabilité $W(G, M)/Z(G)$. Pour cela nous allons construire une chaîne de Markov $\mathcal{MC}_{md}(G)$ sur $\mathcal{N} = M_*(G)$.

Soit $M \in \mathcal{N}$ et $e = (u, v) \in E$ une arête choisie uniformément au hasard. Plusieurs transitions sont alors possibles à partir de M.

1. Si $e \in M$, faire une transition de *suppression* vers $M' = M \backslash e$ avec la probabilité $1/(1 + p)$.

2. Si $e \notin M$ et si ni u ni v ne sont couplés dans M, faire une transition d'*ajout* vers $M' = M \cup \{e\}$ avec la probabilité $p/(1 + p)$.

3. Si $e \notin M$ et u n'est pas couplé dans M mais v l'est avec w, faire une transition de *remplacement* vers $M' = (M \cup \{e\}) \backslash (v, w)$ avec la probabilité $1/2$.

4. Dans les autres cas, rester sur place.

De ces probabilités de transition on peut s'apercevoir que si $p < 1$ alors la chaîne va être aspirée vers des couplages de faible taille. A l'opposé si $p > 1$ elle va tendre vers des couplages de grande taille.

Pour assurer l'apériodicité de la chaîne on a ajouté une auto-boucle de $1/2$. Elle est irréductible, car, par une suite de transitions du premier puis du deuxième type, on peut

4. La probabilité de liaison croit avec p

atteindre tout couplage à partir de tout couplage. De ces deux propriétés, on déduit que la chaîne est ergodique.

Proposition 5 *La chaîne $\mathcal{MC}_{md}(G)$ est réversible.*

Preuve : Pour montrer que la chaîne est aussi réversible il nous suffit de montrer que pour tous les couplages M, M' on a la condition de balance $p_{M'M}\pi_{M'} = p_{MM'}\pi_M$. Ceci est vrai pour $\pi_M = W(G, M)$ comme le montrent les équations suivantes:

1. Soit $M'(V', E') = M \backslash e$ et $k = |E'|$.

$$\begin{aligned} p_{MM'}\pi_M &= 1/(1+p)p^{k+1} \\ &= p/(1+p)p^k \\ &= p_{M'M}\pi_{M'} \end{aligned}$$

2. Soit $M' = (M \cup \{e\}) \backslash (v, w)$ et k comme précédemment. $p_{MM'}\pi_M = 1/2p^k = p_{M'M}\pi_{M'}$.

$\square$

Maintenant il nous suffit d'exhiber une borne sur la conductance pour prouver le mélange rapide de la chaîne. Pour cela nous allons procéder en plusieurs étapes :

- Dans un premier temps nous décrivons un ensemble de chemins canoniques dans le graphe sous-jacent définissant un unique chemin entre deux sommets donnés.
- Puis nous allons majorer la somme des poids de tels chemins qui contiennent une arête t fixée, en décrivant une injection des chemins qui passent par t dans les sommets de H.
- Ensuite nous montrons que cette borne minore la conductance du graphe.

Définition 16 (Chemins canoniques) *Soit H le graphe sous-jacent de $\mathcal{MC}_{md}(G)$. Un ensemble de chemins canoniques dans H, est tel que pour tout couple de couplages $\langle I, F\rangle \in \mathcal{N}^2$ il existe exactement un chemin canonique de I à F.*

Nous décrivons l'ensemble des chemins par l'algorithme suivant qui pour un couple $\langle I, F\rangle$ donné, effectue les transitions nécessaire pour changer I et F. La suite de ces transitions décrit un chemin dans le graphe H.

Notons $P(t)$ l'ensemble des chemins passant par la transition t. Dans la suite nous allons confondre le chemin canonique de I à F par le couple de ses extrémités $\langle I, F\rangle$.

Pour tout $I, F \in \mathcal{N}$ on peut noter la différence symétrique $I \oplus F$ comme une séquence $Q_1, \ldots, Q_r$ de chemins disjoints. Ces chemins correspondent aux arêtes qu'il faut changer dans I pour arriver à F et correspondent à des suites alternées d'arêtes de I et de F.

Un chemin de I à F consiste en une suite de transitions dans la chaîne H transformant pas à pas I en F. Nous allons pour cette transformation traiter dans l'ordre les Q_i de la

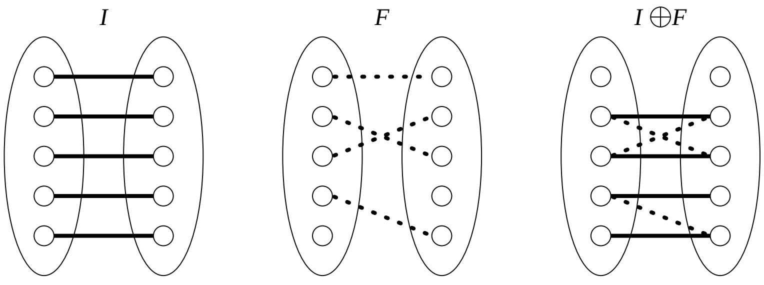


FIG. 7 - *La différence symétrique de deux couplages*

différence symétrique. Comme pour toute structure codée sur le ruban d'une machine de Turing, il existe un ordre sur les chemins, ainsi que sur leurs sommets. Ceci nous permet de considérer dans tout chemin un sommet de départ, qui serait la plus petite des extrémités d'un chemin et le plus petit sommet dans le cas d'une boucle. Décrivons maintenant les transitions à faire pour chaque chemin Q_i.

1. Q_i n'est pas un cycle. Dans ce cas, soit Q_i la suite $(v_0, v_1, \ldots, v_l)$ de sommets avec v_0 le sommet de départ. Si $(v_0, v_1) \in F$ on fait une suite de transitions de remplacement de (v_{2j+1}, v_{2j+2}) par (v_{2j}, v_{2j+1}) pour $j = 0, 1, \ldots$, et on finit avec une transition d'ajout de (v_{j-1}, v_j) si j est impair. Par contre si $(v_0, v_1) \in I$ on débute avec une transition de suppression de (v_0, v_1), puis on continue comme précédemment sur la suite $(v_1, \ldots, v_l)$.

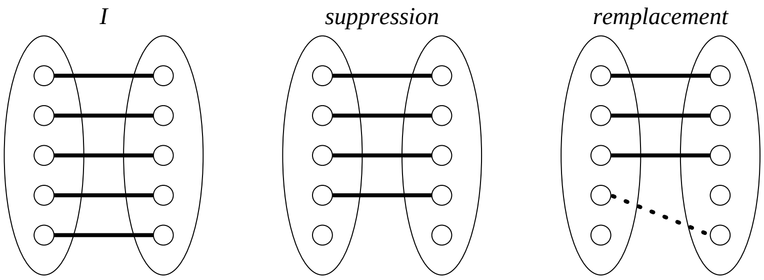


FIG. 8 - *Déroulement d'un chemin simple*

2. Q_i est un cycle. Soit Q_i une suite $(v_0, v_1, \ldots, v_{2l+1})$ de sommets où toutes les arêtes (v_j, v_{j+1}) pour j pair sont dans I et les autres dans F. Le déroulement de Q_i débute par une transition de suppression de (v_0, v_1), qui donne un chemin simple O. Ce chemin a un sommet de départ qui est soit v_0 soit v_1. Supposons que le sommet de départ ne soit *pas* v_k pour $k = 0$ ou 1. On va alors dérouler O comme un chemin simple, mais en prenant v_k comme sommet de départ. Ceci nous permet par la suite de distinguer le déroulement d'un cycle du déroulement d'un chemin.

□

Maintenant que nous avons défini les chemins canoniques il nous faut sommer le poids des chemins qui passent par une transition donnée. Soit t une transition de M à M'. Nous allons définir une injection $\sigma_t : P(t) \rightarrow \mathcal{N}$ telle qu'à partir des connaissances de t et de $\sigma_t(I, F)$ on peut reconstituer I et F. (Ceci est la condition que σ_t soit une injection).

Lemme 3 (Injection) *Il existe une injection des chemins canoniques passant par une même arête t dans les couplages.*

Preuve : On définit

$$\sigma_t(I, F) = \begin{cases} I \oplus F \oplus (M \cup M') \backslash \{e_{I,t}\} & \text{si } t \text{ est une transition de remplacement} \\ & \text{et le chemin courant est un cycle,} \\ I \oplus F \oplus (M \cup M') & \text{sinon.} \end{cases}$$

Ici $e_{I,t}$ est l'arête de I adjacente aux sommet de départ du chemin courant. Il est alors possible de reconstituer I et F de $\sigma_t(I, F)$ et de la connaissance de t. Pour cela il suffit de calculer dans un premier temps

$$I \oplus F = \begin{cases} \sigma_t(I, F) \oplus (M \cup M') \cup \{e_{I,t}\} & \text{si } t \text{ est une transition de remplacement} \\ & \text{et le chemin courant est un cycle,} \\ \sigma_t(I, F) \oplus (M \cup M') & \text{sinon} \end{cases}$$

qui consiste en une séquence de chemins $Q_1, \ldots, Q_r$ dont un chemin particulier Q_i est en train d'être déroulé. Ce chemin est déterminé par t. De plus il nous est possible de déterminer si Q_i est le déroulement d'un cycle ou d'un chemin, car le sens de déroulement est alors différents. Ces informations nous permettent de déterminer les arêtes de $I \backslash F$ et de $F \backslash I$. Avec la connaissance de $I \cap F = M \backslash I \oplus F$ on peut reconstituer I et F, ce qui prouve que σ_t est bien une injection. $\square$

Lemme 4 *Pour tout $\langle I, F \rangle \in P(t)$ nous avons*

$$\pi_I \pi_F \leq 4|E| p_{\max}^2 w_t \pi_{\sigma_t(I,F)}$$

avec $p_{\max} = \max\{1, p\}$.

Idée de la preuve : Une étude cas par cas des différentes types de transitions t prouve ce résultat. $\square$

Lemme 5 *La somme des poids des chemins passant par une même arête t satisfait*

$$\sum_{\langle I,F \rangle \in P(t)} \pi_I \pi_F \leq 4|E| p_{\max}^2 w_t$$

Preuve : Du résultat précédent on peut déduire

$$\begin{aligned}\sum_{\langle I,F\rangle\in P(t)} \pi_I\pi_F &\leq \sum_{\langle I,F\rangle\in P(t)} 4|E|p_{\max}^2 w_t \pi_{\sigma_t(I,F)} \\ &\leq 4|E|p_{\max}^2 w_t \sum_{\langle I,F\rangle\in P(t)} \pi_{\sigma_t(I,F)} \\ &\leq 4|E|p_{\max}^2 w_t\end{aligned}$$

□

Théorème 3 ([JS, p. 1164]) *Pour un graphe $G(V, E)$ donné avec un poids d'arêtes p, la conductance du graphe sous-jacent de la chaîne de Markov $\mathcal{MC}_{md}(G)$ est borné inférieurement par $1/(8|E|p_{\max}^2)$ où $p_{\max} = \max\{1, p\}$.*

Lemme 6 *Soit $t = (M, M')$ une arête de H de poids $w_t = p_{MM'}\pi_M$ associé. S'il existe un b tel que le nombre $|P(t)|$ de chemins passant par t est*

$$\sum_{\langle I,F\rangle\in P(t)} \pi_I\pi_F \leq bw_t \tag{5}$$

alors la conductance satisfait

$$\phi(H) \geq \frac{1}{2b}$$

Preuve : Supposons qu'entre toute paire $\langle I, F\rangle$ il existe un chemin canonique dans H de poids $\pi_I\pi_F$. Pour tout sous-ensemble S de sommets de H, le nombre de chemins allant de S à son complément $\bar{S}$ est

$$\sum_{I\in S, F\in\bar{S}} \pi_I\pi_F = C_S C_{\bar{S}} \geq \frac{C_S}{2}.$$

Supposons encore qu'on sait que les chemins passant par un sommet t fixé satisfont (5), cela nous permet d'écrire l'inéquation suivante où $\text{coupe}(S) = E \cap (S \times \bar{S})$ est l'ensemble des arêtes entre S et $\bar{S}$.

$$\begin{aligned}F_S = \sum_{t\in\text{coupe}(S)} W_t &\geq \frac{1}{b} \sum_{t\in\text{coupe}(S)} \sum_{\langle I,F\rangle\in P(t)} \pi_I\pi_F \\ &\geq \frac{1}{b} \sum_{I\in S,\, F\in\bar{S}} \pi_I\pi_F \\ &\geq \frac{C_S}{2b}.\end{aligned}$$

Par la définition de la conductance on obtient le résultat à montrer

$$\phi(H) \geq \frac{1}{2b}$$

□

On a donc montré que la conductance satisfait $\phi(H) \geq (8|E|p_{\max}^2)^{-1}$ et alors la chaîne mélange rapidement si p est l'inverse d'un polynôme en n. Justement, comme nous décrivons plus tard, p va être avoir une valeur qui satisfait cette condition.

6.2 Le schéma d'approximation

Pour estimer les rapports m_k/m_{k+1} Jerrum et Sinclair utilisent la chaîne de Markov précédente. Il est alors important que ce rapport reste polynomial, pour que l'erreur de l'estimateur ne soit pas trop grande.

Proposition 6 *Le rapport m_{n-1}/m_n entre le nombre de couplages presque parfaits et le nombre de couplages parfaits est polynomial si le graphe est dense.*

Preuve : Pour montrer cela il suffit de montrer qu'à un couplage presque parfait on peut associer l'unique plus proche couplage parfait et qu'inversement pour un couplage parfait il y a au plus n^2 plus proches couplages presque parfaits. Soit $M \in M_{n-1}(G)$ un couplage presque parfait. Il existe alors exactement deux sommets $u \in U$ et $v \in V$ qui ne sont pas adjacents à une arête en M. Si l'arête (u,v) existe en G, on associe à M le plus proche couplage parfait $M \cup \{(u,v)\}$. Sinon par la propriété de densité il existe une arête (u',v') dans M tel que (u,v') et (u',v) sont dans G. Le couplage parfait associé est alors $(M \cup \{(u,v'),(u',v)\})/(u',v')$ pour la plus petite arête (u',v') selon un ordre sur les couples de sommets. Inversement à un couplage parfait M on associe au plus $n + n(n-1) = n^2$ couplages presque parfaits obtenu par suppression d'une arête, éventuellement suivi d'un transition de remplacement. □

Proposition 7 ([JS, p. 1166]) *La suite des rapports m_k/m_{k+1} pour tout k est croissante, c'est-à-dire*

$$\frac{m_{k-1}}{m_k} \leq \frac{m_k}{m_{k+1}}$$

ce qui est équivalent à

$$m_{k-1}m_{k+1} \leq m_k^2$$

Idée de la preuve : Pour prouver cette propriété Jerrum et Sinclair partent de deux ensembles arbitraires $A \in M_{k+1} \times M_{k-1}$ et $B \in M_k \times M_k$. L'approche est alors de prouver que $|A| \leq |B|$. Pour cela ils partitionnent ces ensembles comme suit

$$\begin{aligned} A_r &= \{\langle M, M' \rangle \in A : M \oplus M' \text{ contient } r+1 \ M\text{-chemins et } r-1 \ M'\text{-chemins}\} \\ B_r &= \{\langle M, M' \rangle \in B : M \oplus M' \text{ contient } r \ M\text{-chemins et } r \ M\text{-chemins}\} \end{aligned}$$

Un chemin appartenant à $M \oplus M'$ est un M-chemin s'il contient plus d'arêtes de M que de M'. Le problème est alors réduit à montrer

$$\frac{|B_r|}{|A_r|} > 1.$$

Ceci est prouvé en montrant que le nombre d'éléments de B_r accessibles par la méthode de déroulement de chemin à partir d'un élément de A_r est exactement le nombre de M-chemins de $M \oplus M'$, à savoir $r+1$. Inversement le nombre de d'éléments de A_r à partir d'un élément de B_r est r. □

Il est alors important de choisir le bon poids d'arête p afin que le probabilité de générer un couplage de taille k ou $k+1$ soit au moins l'inverse d'un polynôme en n. Pour cela, nous allons choisir p tel que les k-couplages soient les plus probables. La condition que le rapport m_{k+1}/m_k soit aussi polynomial assure que la probabilité de générer un $k+1$-couplage ne soit pas trop petite. Ceci est le cas pour $p = m_{k-1}/m_k$. En voici la preuve.

Soit p_i la probabilité de générer un couplage de taille i. Pour $i \geq k$ nous obtenons l'inéquation suivante :

$$\begin{aligned}
\frac{p_k}{p_i} &= \frac{m_k p^k}{m_i p^i} \\
&= p^{k-i} \prod_{j=k}^{i-1} \frac{m_j}{m_{j+1}} \\
&\geq \left(\frac{m_{k-1}}{m_k}\right)^{k-i} \left(\frac{m_{k-1}}{m_k}\right)^{i-k} \\
&= 1
\end{aligned}$$

Pour $i \leq k$ on a de manière équivalente la même inéquivalence.

Ceci prouve que pour $p = m_{k-1}/m_k$ la probabilité p_k est au moins $\frac{1}{n+1}$.

6.3 Analyse par des graphes aléatoires

On a vu que l'approximation randomizée précédente ne fonctionnait que pour les graphes denses. Cependant Jerrum et Sinclair [JS, p. 1172] montrent que l'approximation fonctionne pour presque tout graphe. Cette analyse à été faite dans le modèle des graphes aléatoires $G_{n,p}$ dont l'ensemble des sommets est $U \cup V$ avec $U = V = [n]$ et où p dénote la probabilité d'arête.

Leur observation est que si le degré maximal n'est plus que $n/(2+\delta)$ pour un $\delta > 0$ alors on peut construire un graphe pour lequel le rapport entre le nombre de couplages parfaits et presque-parfaits est d'ordre exponentiel. Cependant presque tout graphe aléatoire est q-amenable, c'est-à-dire est tel qu'il n'a pas de couplages parfaits, ou que le rapport est polynomial.

6.4 Approximation de Rasmussen

Début 1994 Lars Eilstrup Rasmussen [Ra] propose une approche plus simple d'approcher le permanent, qui toutefois est exponentielle en $n$dans le pire des cas,où n est la dimension de la matrice fournie en entrée, bien qu'en moyenne elle soit polynomiale. L'auteur utilise la définition alternative de Laplace du permanent:

$$\text{perm}(A) = \sum_{j=1}^{n} A(1,j)\text{perm}(A_{1j}),$$

où A_{1j} est obtenue en enlevant à la matrice A le première ligne et la j-ème colonne, avec perm() = 1, pour la matrice vide. Il propose alors la fonction suivante pour approcher le permanent:

Estimateur(A de dimension n)
Si $n = 0$ alors
    retourner 1
Sinon $W = \{j : A(1, j) = 1\}$
    Si $W = \emptyset$ alors
        retourner 0
    Sinon
Choisir uniform ement au hasard j de W
        retourner $|W|$Estimateur(A_{1j})

Rasmussen montre que l'espérance de cette fonction est perm(A). Pour plus de détails référez-vous à [Ra].

7 Approximation du nombre de chemins dans une grille

L'entrée du problème est une grille $(n+1) \times (n+1)$ et deux points s et t qui sont des coins opposés de cette grille. Notons les sommets de la grille par les coordonnées $(x, y) \in \{0, \ldots, n\}^2$. Fixons les points $s = (0, 0)$ et $t = (n, n)$. On cherche à calculer le nombre de chemins simples menant de s à t. Notons $p(n)$ ce nombre.

Définition 17 (Bons Chemins) *Un bon chemin dans une grille carrée G est un chemin sans boucle qui mène de s à t.*

Dans cette section nous allons dans un premier temps exposer les résultats d'une analyse énumérative. Puis nous allons situer ce problème dans l'hierarchie de la complexité, en considérant d'une part une généralisation du problème de comptage de chemins qui n'est pas approximable (sous de hypothèses structurelles raisonables) et d'autre par un cas particulier de grilles où ce problème est calculable en temps polynomial. Ce dernier résultat nous permet de donner une borne supérieure à $p(n)$. Finalement nous présentons notre approche pour approximer $p(n)$.

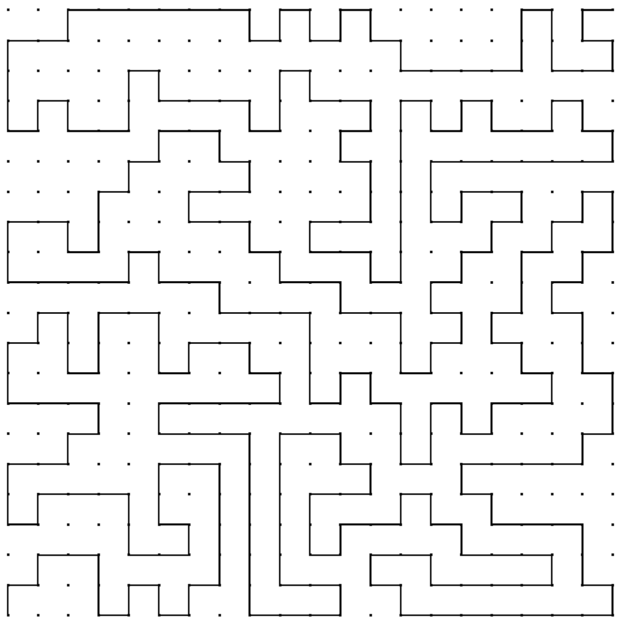


FIG. 9 - *Exemple d'un chemin typique dans une grille pour* $n = 20$

Le tableau suivant montre le nombre de chemins dans une grille $(n+1) \times (n+1)$ pour les premières valeurs de n. On s'aperçoit que ce nombre croit rapidement avec n.

n	$p(n)$
1	2
2	12
3	184
4	8 512
5	1 262 816
6	575 780 564

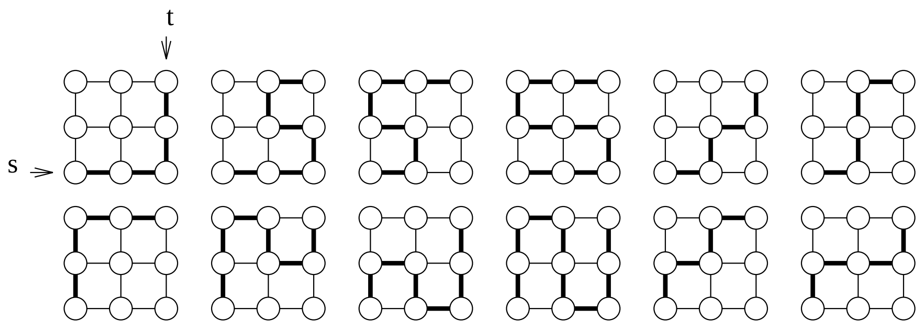
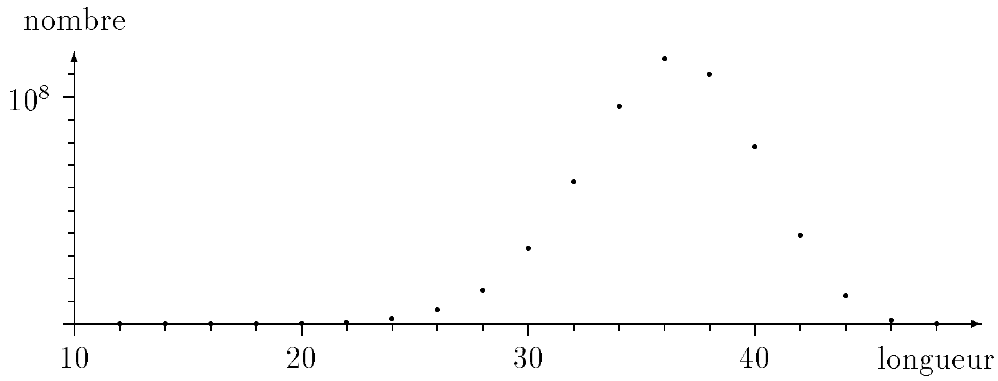


FIG. 10 - *Tous les douze bons chemins dans une grille pour* $n = 2$.

Une analyse énumérative nous a donné les résultats suivants pour le nombre des chemins d'une certaine longueur. Pour une grille 6×6 nous avons obtenu cette distribution de

Poisson:



Le résultat d'une autre analyse du nombre de chemins passant par un sommet donné est montré en figure 11. On peut observer que les deux extrémités s et t sont des maxima, car tous les chemins passent par eux. Ensuite le nombre de chemins passant par un sommet semble être proportionnel à son degré.

7.1 Borne supérieure

Le nombre d'arêtes dans une grille de taille $(n+1) \times (n+1)$ est $n(n+1) + (n+1)n = 2n(n+1)$. Un chemin dans une grille est un sous-ensemble des arrêtes ce qui donne une première majoration grossière de $2^{2n(n+1)}$ pour $p(n)$. Cependant cette borne peut être légèrement améliorée:

Proposition 8 *Le nombre de chemins d'un coin s au coin opposé t d'une grille carrée de taille $(n+1) \times (n+1)$ est majoré par 2^{n^2}.*

Preuve : Un carré dans une grille est délimité par quatre arêtes. Dans une grille G $(n+1) \times (n+1)$ il y a n^2 carrés. Une coloration noir et blanc d'une grille est une coloration de ses carrés. Il y a donc 2^{n^2} colorations de G.

Un chemin dans une grille partitionne l'ensemble des cases en deux parties, celles qui sont à gauche d'un chemin (colorées en noir) et celles qui sont à droite d'un chemin (colorées en blanc). La notion gauche et droite d'un chemin est définit en fonction d'un parcours de s à t.

Pour montrer que ceci est bien une injection nous allons expliquer comment à partir d'une coloration on peut reconstituer l'unique chemin s'il y en a un.

On ajoute des cases autour de la grille. Celles adjacentes au bord haut et gauche seront noir, les autres blanches. Si la coloration correspond à un bon chemin il est alors possible de le reconstituer arête par arête par un un parcours dans la grille comme suit: Nous partons

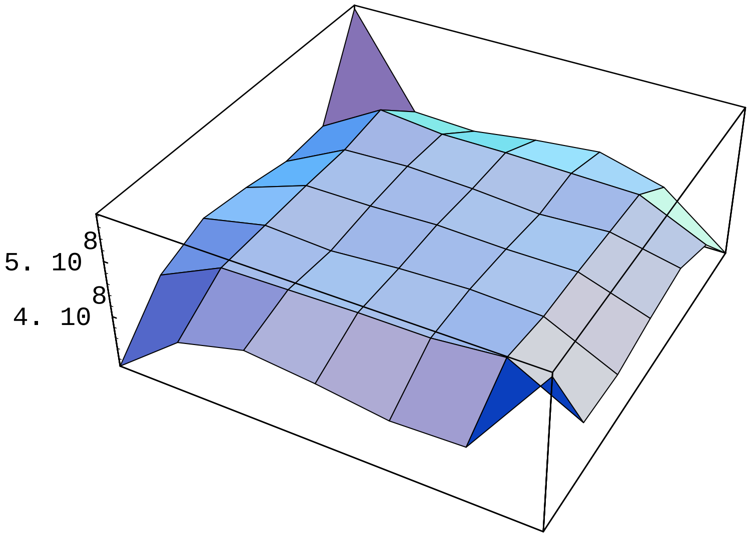


FIG. 11 - *Le nombre de chemins (en hauteur) passant par les sommet d'une grille pour* $n = 6$.

du sommet s. On empreinte une arête qui ait une case blanche à sa droite et une case noire à sa gauche. Si une telle arête n'existe pas ou n'est pas unique, le coloriage est rejeté, car alors il ne correspond pas à un chemin. Si à la fin on arrive en t et qu'on soit passé par toutes les arêtes entre une case blanche et une case noire, alors on a reconstitué le chemin qui menait à cette coloration. Sinon la coloration ne correspondait pas à un chemin. □

Nous avons montré qu'un coloriage ne correspond à un bon chemin si et seulement si l'ensemble des cases noires et connexe et l'ensemble des cases blanches aussi. Pour la connexion nous considérons un graphe sur les cases de la grille et les cases ajoutées au bord, où deux cases sont reliées par une arête si elle sont adjacentes. Dans la suite nous allons désigner un tel coloriage un *bon coloriage*.

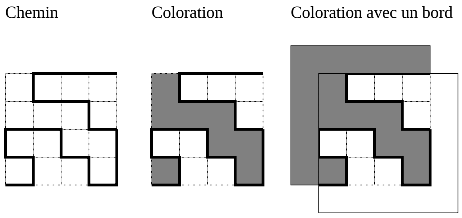


FIG. 12 - *La bicoloration des cases d'une grille en fonction d'un chemin.*

Remarque : Ce dernier résultat nous permettrait d'utiliser le théorème d'échantillonnage pour estimer le nombre de chemins en générant uniformément des coloriages. Pour cela il faut que le rapport entre le nombre de coloriages et le nombre de chemins soit polynomial en n. Il est alors nécessaire de trouver une minoration du nombre de chemins qui soit dans un rapport polynomial en n avec cette majoration.

7.2 Grille de hauteur constante

Théorème 4 *Le nombre de chemins simple dans une grille $n \times c$ pour une constante c d'un coin au coin opposé est calculable en temps linéaire en n.*

Preuve : Soit G une grille $(c+1) \times (n+1)$. G contient cn cases identifiées par leur coordonnées $(x, y) \in \{1..c\} \times \{1..n\}$. Nous avons vu dans la section précédente que compter les bons chemins revient à compter les bonnes colorations.

Une coloration d'une grille est une suite de n colorations de colonnes. Une bonne coloration satisfait les propriétés de connexion suivantes :

1. Une case blanche est soit adjacente au bord blanc, soit adjacente à une autre case blanche qui elle est connecté au bord blanc.
2. Idem pour les cases noires et le bord noir.

Nous allons définir une bijection entre une suite de colorations de colonnes et une suite de configuration des colonnes. Une configuration est une coloration muni d'information supplémentaire que nous allons définir tout de suite. Au lieu de compter les bonnes colorations (suites de colorations de colonnes) il est possible de compter les suites de configurations, qui vérifient que deux configurations adjacentes soient *compatibles*, notion que nous introduisons dans la suite.

Définition 18 (Configuration) *Une configuration d'une colonne de hauteur c est un triplet (w, v, P) des mots $w \in \{\circ, \bullet\}^c$, $v \in \{\perp, \cdot\}^c$ et d'une partition P de $\{1, \dots, c\}$ qui satisfait les propriétés suivantes :*

1. *Les cases qui sont adjacentes au bord portant leur couleur sont connectées au bord :*
$$\begin{aligned} w_1 = \bullet \quad &\Rightarrow \quad v_1 = \perp \\ w_c = \circ \quad &\Rightarrow \quad v_c = \perp. \end{aligned}$$
2. *Une case adjacente (dans la même colonne) à une case de même couleur connectée au bord l'est aussi :*
$$\forall 1 \leq i < c : w_i = w_{i+1} \Rightarrow v_i = v_{i+1}.$$
3. *Les ensembles de la partition P contiennent des cases de même couleur et qui sont toutes soit connectées au bord soit :*
$$\forall I \in P\, \forall i, j \in I : w_i = w_j \wedge v_i = v_j.$$

4. *Deux cases adjacentes de même couleur sont dans un même ensemble de P :*

$$\forall 1 \leq i < c : w_i = w_{i+1} \Rightarrow \exists I \in P : \{i, i+1\} \subseteq P.$$

5. *S'il existe un ensemble de P contenant des cases connectées au bord d'une couleur donnée, alors il est unique :*

$$\forall i \forall j\, 1 \leq i < j \leq c \Rightarrow (w_i = w_j \wedge v_i = v_j = \perp \Rightarrow \exists ! I \in P : \{i, j\} \subseteq I).$$

L'interprétation informelle d'une configuration (w, v, P) d'une colonne donnée est la suivante. Le mot w indique la coloration des cases et v indique quelles sont les cases qui sont connectées au bord de leur couleur, tel qu'un chemin reliant la case et le bord ne dépasse pas vers la droite la colonne. La partition P indique quelles sont les cases qui sont connectées entre eux toujours dans le sens où un chemin reliant reliant deux cases ne passe uniquement par des cases de la colonne ou celles à gauche d'elle.

Définition 19 *Deux configurations $d = (w, v, P)$ et $d' = (w', v', P')$ de colonnes adjacentes dans l'ordre (d, d') sont compatibles si :*

1. *Un ensemble de P contenant des cases non-connectées au bord, doit contenir une case adjacente à une case de d' de même couleur :*

$$\forall I \in P : (\forall i \in I : v_i \neq \perp) \Rightarrow (\exists i \in I : w_i = w'_i).$$

2. *L'ensemble de P' contenant des cases marquées comme connectées au bord, doit soit contenir une case adjacente au bord de même couleur, soit être adjacent à une case de d, qui elle est connectée au bord :*

$$\forall I' \in P' \, (\forall i \in I' : v'_i \neq \perp) \quad \Rightarrow \quad (1 \in I' \;\wedge\; w'_1 = \bullet \;\vee\; c \in I' \;\wedge\; w'_c = \circ) \vee$$
$$(\exists i \in I' : w_i = w'_i \;\wedge\; v_i = \perp).$$

3. *Toutes les cases d'un ensemble de P' donné doivent être connectées entre eux en considérant les deux colonnes :*

$$\forall I' \in P' \, \forall i, j \in I' : i < j \quad \Rightarrow \quad (\exists k \in I' : i < k < j) \vee$$
$$(\exists I \in P : i \in I \wedge j \in I).$$

Dans la suite nous désignerons par une *bonne suite de configuration* une suite dont chaque configuration est compatible avec la configuration suivante.

Maintenant nous décrivons la bijection entre les bonnes coloration et les suites de configurations compatibles.

configurations vers coloration Soient les deux configurations du bord gauche et droite $d_0 = (\bullet^c, \perp^c, \{\{1, \ldots, c\}\})$ et $d_{n+1} = (\circ^c, \perp^c, \{\{1, \ldots, c\}\})$. Fixons nous une une suite de configurations $d_1 = (w_1, v_1, P_1), \ldots, d_n = (w_n, v_n, P_n)$, qui pour tout $0 \leq i \leq n$ vérifie que d_i soit compatible avec d_{i+1}. Alors la suite $w_1, \ldots, w_n$ est une bonne coloration.

coloration vers configuration Fixons nous une une bonne suite de colorations $w_1, \ldots, w_n$. Nous allons alors la compléter avec de l'information supplémentaire. d_0 étant fixé supposons qu'une bonne suite de configurations $d_1, \ldots, d_i$ à déjà été construite. Il existe une unique manière de choisir v_{i+1} et P_{i+1}, tel que d_i soit compatible avec $d_{i+1} = (w_{i+1}, v_{i+1}, P_{i+1})$.

Pour calculer le nombre de bonnes suites de configurations introduisons le nombre $f(d, i, d')$ qui dénote le nombre de bonnes suites de configurations de la forme $d = d_1, \ldots, d_i = d'$. $f(d, 1, d')$ à donc la valeur 1 si d et d' sont compatible et 0 sinon. f satisfait alors

$$f(d, i+j, d') = \sum_{d''} f(d, i, d'') f(d'', j, d')$$

et en particulier

$$f(d, i+1, d') = \sum_{d'' \text{ compatible avec } d'} f(d, i, d'').$$

Soit $D(c)$ l'ensemble de configurations d'une colonne de hauteur c. L'algorithme qui calculera itérativement f sera de complexité $O(|D(c)|^2 n)$. Une version plus astucieuse calculera les valeurs de f pour les puissances de 2 jusqu'à atteindre n et sera de complexité $O(|D(c)|^3 \log n)$. En fonction de la valeur de $|D(c)|$ on choisira alors une des deux stratégies pour résoudre le problème. $\square$

7.3 Grille carrée

Théorème 5 *Soit G une grille $(n+1) \times (n+1)$ et s, t deux coins opposés de G. Il existe un schéma d'approximation randomizé pour le nombre de chemins simples de s à t dans G.*

L'idée est que ce problème est auto-réductible, ce qui ramène le problème à une génération presque uniforme de chemins dans un certain sous-graphe de la grille. Cette génération sera faite par une marche aléatoire dans une chaîne de Markov $\mathcal{MC}_{st}(n)$ construite sur les bons chemins.

7.4 Motivation

Il a été montré que si NP$\neq$RP alors on ne peut approcher le nombre de chemins simple entre deux sommets donnés dans un graphe arbitraire. Il est donc intéressant de trouver des approximations pour des graphes particuliers comme par exemple les grilles.

C'est pour pouvoir comparer nos algorithmes d'approximation avec les algorithmes sur les graphes quelconques, que la complexité est exprimé en n. Or ceci n'est pas correct car la complexité d'un algorithme s'exprime par rapport à la taille de l'entrée. Or dans notre cas, l'entrée étant le chiffre n, la taille de l'entrée est $O(\log n)$. Par contre notre approche se défend si on essaye ensuite de généraliser le problème aux sous-graphes des grilles, qui eux se codent en $O(n^2)$ bits sur le ruban d'entrée.

La connaissance du nombre $p(n)$ de chemins simples dans une grille $(n+1)\times(n+1)$ entre deux coins opposés s et t permet de calculer le taux de succès d'une stratégie particulière σ de commande de robot dans un milieu incertain. Une stratégie dirige un robot dans une des quatre directions (ou décide de rester sur place) en fonction de l'historique des positions du robot. Dans ce milieu, où les incertitudes sont sur tous les sommets de la grille, les déplacements du robots se déroulent comme suit :

1. Si la stratégie décide de rester sur place, le robot reste sur place.

2. Si la stratégie décide d'avancer dans une direction d, le robot se déplace avec une probabilité $1/4$ dans une des quatre directions. Les sommets du bords font toutefois exception où le robot, se déplace avec une probabilité $1/4$ dans une des directions possibles, et reste sur place sinon.

Trivialement dans un milieu incertain une stratégie n'a que le choix de se déplacer ou de rester sur place. La stratégie σ est alors la suivante

– Si la position du robot est t, rester sur place.

– Si la position du robot a déjà atteinte durant le trajet, rester sur place.

– Dans les autres cas, envoyer la commande de déplacement.

Le taux de succès du robot pour un temps de marche de $(n+1)^2$ se formalise par le rapport

$$\Pr[s \xrightarrow{\sigma} t] = \frac{|P(n)|}{f(n)}.$$

Ici $f(n)$ est le nombre de chemins (avec ou sans boucle) de longueur $(n+1)^2$ qui vont de s à n'importe quel sommet. Cette fonction se calcule en temps polynomial de n par la fonction récurrente suivante :

$$\begin{aligned}
f(n) &= g(0,0,n,n^2)\\
g(x,y,n,l) &= \begin{cases}
1 & \text{si } l=0\\
0 & \text{si } (x,y)\notin\{0,\dots,n\}\times\{0,\dots,n\}\\
(g(x-1,y,n,l-1)+ & \\
+g(x+1,y,n,l-1)+ & \\
+g(x,y-1,n,l-1)+ & \\
+g(x,y+1,n,l-1)) & \text{dans les autres cas.}
\end{cases}
\end{aligned}$$

Ici $g(x,y,n,l)$ calcule le nombre de chemins de longueur l dans une grille $(n+1)\times(n+1)$ entre les points (x,y) et $t=(n,n)$.

Soit n fixé. Pour calculer g on calcule itérativement pour un l de 0 à $(n+1)^2$, les $(n+1)^2$ valeurs de g. Chaqu'une des valeurs se résout en un nombre constant d'étapes en fonction des résultats de g pour $l-1$. La fonction $f(n)$ est donc réalisé en $O(n^4)$.

7.5 Formalisation

La longueur des bons chemins est comprise entre $2n$ et $(n+1)^2-1$ (respectivement $(n+1)^2-2$ pour n pair). Par la symétrie de la grille, le nombre de chemins sera toujours pair. De manière plus générale un chemin bon sera de longueur $2n+2i$. On peut décrire un chemin comme un mot sur l'alphabet $\Sigma = \{\uparrow, \downarrow, \leftarrow, \rightarrow\}$. On définit deux fonctions sur les mots w de Σ^*:

$$\begin{array}{rcl} \Delta_h(w) & = & |w|_{\rightarrow} - |w|_{\leftarrow} \\ \Delta_v(w) & = & |w|_{\uparrow} - |w|_{\downarrow} \end{array}$$

décrivant la différence des coordonnées horizontales (respectivement verticales) du début et de la fin du chemin. Un mot w de Σ^* correspond seulement a un bon chemin s'il satisfait [5]

$$\forall u \leq_L w : \forall v <_L u : \quad \begin{array}{l} \Delta_h(u) \neq \Delta_h(v) \quad \text{et} \\ \Delta_v(u) \neq \Delta_v(v) \end{array}$$

ce qui indique que le chemin est sans boucle et

$$\forall u \leq_L w : \quad \begin{array}{l} \Delta_h(u) \in [0,n] \quad \text{et} \\ \Delta_v(u) \in [0,n] \end{array}$$

ce qui indique que le chemin ne sort pas de grille et

$$\begin{array}{l} \Delta_h(w) = n \quad \text{et} \\ \Delta_v(w) = n \end{array}$$

qui précise que la destination est bien t.

7.6 Approcher

Il existe deux approches pour approcher $p(n)$.

- La première consiste à approcher m_k/m_{k-2}, le rapport entre le nombre de chemins de longueur k et de longueur $k+2$. Comme on connaît la valeur de m_{2n}, qui est $\binom{2n}{n}$, nous pourrons ainsi estimer le nombre de chemins de toute longueur.
- Dans une deuxième approche on va estimer le rapport de chemins dans une sous-grille qui partent dans une certaine direction. Ces notions seront introduites dans la suite.

La chaîne de Markov $\mathcal{MC}_{st}(n)$ est construite sur les bons chemins. Une transition entre w et w' existe si les chemins sont proches. Deux chemins w et w' sont proches si il suffit d'une petite modification locale, pour passer du premier chemin au deuxième. Voici les modifications que nous permettons.

1. Soit $w = udv\bar{d}x$ où $u, v, w \in \Sigma^*$, $d \in \Sigma$ est une direction et $\bar{d}$ son opposé. Si $w' = uvx$ est un bon chemin une transition dite de suppression w et w' est autorisée.

5. On note par $v \leq_L w$ (respectivement $v <_L w$) que v est préfixe (resp. strict) de w

2. De façon symétrique soit $w = uvx$ et si $w' = udv\bar{d}x$ est un bon chemin une transition dite d'ajout est autorisée.

3. Soit $x = udbv$ où $u, v, w \in \Sigma^*$, $d, b \in \Sigma$. Si $w' = ubdv$ est un bon chemin une transition dite d'échange est autorisée.

4. De plus une transition de w à lui-même est autorisée.

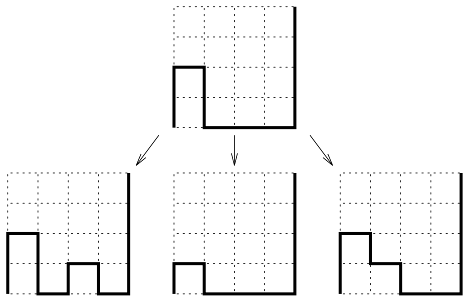


FIG . 13 - *Exemple d'une transition d'*ajout*, de* suppression *et d'*échange

De la définition des transitions on peut s'apercevoir que les transitions sont réversibles, et donc tout chemin dans la chaîne de Markov est réversible.

La procédure de transition est alors la suivante. Pour simplifier les notations nous déclarons que d, b et e sont des directions, u, v, w' et x des mots sur les directions.

fonction *Transition*(w)
Soit $l = |w|$.
Traiter avec une probabilité $\frac{1}{3}$ un des trois cas.
1er cas
Choisir uniformément au hasard $a \in [0, l-1]$
Décomposer w en $ud^{m+1}v$ tel que $|u| = a$ et v ne commence pas par d.
Choisir avec une probabilité $\frac{1}{2}$ une direction b orthogonale à d.
Choisir uniformément au hasard $j \in [0, m]$.
Si $w' = ubd^{j+1}\bar{b}d^{m-j}v$ est un bon chemin
retourner w'
sinon retourner w.
2nd cas
Choisir uniformément au hasard $a \in [0, l-3]$
Décomposer w en $ubd^{1+i}ed^{j}v$ tel que $|u| = a$, $e \neq d$ et v de commence par pas d.
Si $e = \bar{b}$ et $w' = ud^{1+i+j}v$ est un bon chemin
Avec une probabilité $\frac{1}{2(1+i+j)}$ **retourner** w'
sinon retourner w.
3ème cas
Choisir uniformément au hasard $a \in [0, l-2]$

Soit $w = udbv$ tel que $|u| = a$.
Si $w' = ubdv$ est un bon chemin
retourner w'
sinon retourner w.
fin

Proposition 9 *Les probabilités de la chaîne $\mathcal{MC}_{st}(n)$ sont symétriques.*

Preuve : Soient les chemins $w = ud^{1+m}x$ et $w' = ubd^{1+j}\bar{b}d^{m-j}x$. La probabilité d'effectuer une transition à partir de w vers w‘ est

$$\frac{1}{3} \cdot \frac{1}{|w|} \cdot \frac{1}{2} \cdot \frac{1}{m+1}.$$

De même la probabilité d'effectuer une transition à partir de w' vers w est

$$\frac{1}{3} \cdot \frac{1}{|w'| - 2} \cdot \frac{1}{2(m+1).}$$

Or $|w'| = |w| + 2$, ce qui prouve que les probabilités sont identiques. Cette propriété est aussi vérifiée pour la transition d'échange de $udbv$ à $udbv$ et la transition symétrique. $\square$

Proposition 10 *$\mathcal{MC}_{st}(n)$ est irréductible.*

Preuve : Notons L le chemin $\rightarrow^n\uparrow^n$. Il nous suffit de montrer que de tout chemin on peut atteindre L. Comme les transitions sont réversibles on pourrait aller de w à w' en passant par L.

L'idée est qu'on procédera par une suite de transitions de suppression destinées à *aplatir* w. Ceci va nous donner un chemin de longueur $2n$ qu'on va transformer en L par une suite de transitions d'échange.

Définition 20 *Un chemin w est aplati si $\Delta_v(w) + \Delta_h(w) = |w|$, autrement dit si on ne peut plus appliquer une suppression.*

Supposons que w soit de longueur $2n + 2i$ pour un $i \geq 1$ et qu'aucune transition de suppression n'est possible. Soit $w = udv\bar{d}x$. Sans perte de généralité on peut supposer que v ne contient ni d ni $\bar{d}$ et ne contient donc qu'une seule direction. Ceci implique que v est aplati. Si la suppression de d et $\bar{d}$ n'est pas possible ce ne peut être que pour deux cas:

1. Le chemin uvx ainsi obtenu a une boucle. Dans ce cas v se superpose avec une autre partie y de w. Du fait que w est sans boucle, y est plus court que v et est entouré de la forme $dy\bar{d}$. Par hypothèse de récurrence sur la longueur de y ce cas n'est pas possible.

2. Le chemin ainsi obtenu sort de la grille. Comme w ne sort pas de la grille, et que v est au même niveau que le dernier sommet de u dans uvx ce deuxième cas est aussi impossible.

Soit w un chemin aplati. Si $w \neq L$, alors on peut décomposer w en $u \uparrow\rightarrow v$ et effectuer une transition d'échange en $u \rightarrow\uparrow v$. Pour montrer que cette suite de transitions termine en L, nous allons définir une fonction sur les chemins, dont la valeur à chaque transition, jusqu'à atteindre la valeur de L.

Soient les fonctions $g : \Sigma \rightarrow \{0, 1\}$ et $f : \Sigma^{2n} \rightarrow \mathbf{N}$ définit comme suit

$$
\begin{aligned}
g(d) &= \begin{cases} 1 & \text{si } d = \rightarrow \\ 0 & \text{si } d = \uparrow \end{cases} \\
f(w) &= \sum_{i=1}^{2n} i \cdot g(w_i)
\end{aligned}
$$

La valeur minimale de f est alors $f(L) = \frac{n(n+1)}{2}$. La fonction vérifie $f(u \uparrow\rightarrow v) = f(u \rightarrow\uparrow v) - 1$, ce qui prouve la terminaison. De plus la valeur maximale de f est $f(\uparrow^n\rightarrow^n) = n^2 + \frac{n(n+1)}{2}$, ce qui borne le nombre de transitions à effectuer à n^2. □

Remarque : Cette preuve nous montre que le diamètre du graphe sous-jacent de $\mathcal{MC}_st(n)$ est d'ordre n^4. Ceci est un bon signe, car si le degré serait exponentiel en n, la chaîne ne pourrait pas mélanger rapidement.

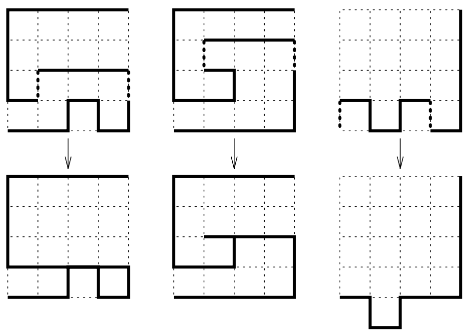


FIG. 14 - *Trois cas où une suppression n'est pas possible*

La chaîne est aussi apériodique grâce aux auto-boucles et donc elle est ergodique. Les probabilités de transition sont symétriques, donc la distribution stationnaire est uniforme. Par conséquence la condition de balance est satisfaite et donc la chaîne est réductible. Ceci nous permet d'utiliser la notion de conductance pour prouver le mélange rapide.

7.7 Réflexion sur une preuve de mélange rapide

Il ne nous reste plus qu'à montrer que la chaîne $\mathcal{MC}_{st}(n)$ mélange rapidement. Malheureusement il n'est pas possible d'appliquer la méthode de Jerrum et Sinclair, utilisant une injection des chemins canoniques dans les états de la chaîne. La raison est qu'on risque alors de créer des boucles.

Par contre il est peut-être possible de construire les chemins canoniques d'une autre manière, sans utiliser la différence symétrique.

7.8 Expériences

Nous avons vérifié expérimentalement que la distribution de la chaîne de Markov est bien stationnaire.

La figure 15 montre deux évolutions de la chaîne de Markov. La première part d'un plus court chemin, la seconde d'un plus long. Le nombre de transitions possible à partir d'un chemin court est $O(n^2)$, alors que pour un plus long chemin il n'est que de $O(n)$. On peut s'apercevoir qu'effectivement dans le deuxième cas la chaîne évolue moins rapidement.

Il ne reste plus qu'à montrer que le problème est posé par une relation auto-réductible, pour prouver l'existence d'Une (ϵ, δ)-approximation à ce problème :

Définition 21 (Chemin en serpentine) *Un chemin S est en serpentine est on plus long chemin qui passe par tous les sommets, sauf* 1 *si n est pair. Supposons n pair. On numérote les sommets de S par un entier $i \in \{0, \ldots, (n+1)^2\}$. Voici la coordonnée (x, y) de chaque sommet numéroté par i :*

$$\begin{array}{rcl} x & = & i \bmod (n+1) \\ y & = & \begin{cases} i \div (n+1) & \textit{si } x \textit{ est pair} \\ (n+1) - (i \div (n+1)) & \textit{si } x \textit{ est impair} \end{cases} \end{array}$$

Définition 22 (Grille partielle) *Soit G une grille $(n+1) \times (n+1)$. On numérote les sommets dans l'ordre induit par le chemin* en serpentine *w passant par tous les sommets (sauf un si n est pair). L'ensemble des sommets est donc $\{1, \ldots, (n+1)^2\}$. Une grille partielle est le sous-graphe de G_i restreint au seuls sommets $\{i, \ldots, (n+1)^2\}$.*

Proposition 11 *La relation $R'(\langle G_i, s, t\rangle, P)$, qui associe à la grille partielle G_i tous les chemins simples P de s à t est auto-réductible.*

Preuve : Au lieu de définir les fonctions nécessaires pour montrer cette propriété, qui sont similaires à la relation $M(G)$ nous donnons seulement cette définition récurrente

$$R(\langle G, s, t\rangle) = \bigcup_{u \in \Gamma(s)} (s, u) \times R(\langle G \backslash \{s\}, u, t\rangle)$$

où (s, u) est une arête arbitraire de G et $\Gamma(s)$ est l'ensemble de tous les voisins de s. Si une telle arête n'existe pas, la relation P donne l'ensemble vide. $\square$

8 Conclusion

Maintenant que nous avons une idée des derniers résultats dans le domaine de l'approximation, différentes voies s'ouvrent pour continuer le travail de Sinclair. Nous avons vu que dans certains cas, le mélange rapide d'une chaîne pouvait aisément être prouvé en donnant une borne supérieure à la résistance du graphe sous-jacent. Il serait intéressant de trouver d'autres méthodes plus générales pour évaluer cette borne, qui seront par exemple facilement appliquable au problème des chemins dans une grille.

En particulier pour le problème des chemins, plusieurs généralisations intéressent les application à la robotique. Considérons par exemple un sous-graphe de la grille, qui résulte de l'interdiction de passage par certains sommets, modélisant des obstacles sur la surface de déplacement.

Voici une question que nous nous posons. Peut-être l'argument d'amplification, utilisé dans la preuve de non-approximabilité du problème appliqué à tous les graphes, s'applique aussi aux graphes planaires. Peut-être aussi tout graphe planaire peut être plongé dans sous-grille. Dans ce cas il faudrait trouver une caractérisation des sous-grilles, distinguant ceux pour lesquelles le nombre de chemins simples est approximable et ceux pour lesquelles ce ne l'est pas.

Nous avons vu que l'approximation du nombre de chemins simples dans une grille permet d'estimer approximativement le taux de succès d'une stratégie de planification de robot dans un milieu où le déplacement est totalement incertain sur tout sommet. Réaliser cette approximation, pour une grille, dont seulement une partie des sommets sont incertains, est une autre généralisation intéressante de ce problème pour la robotique.

D'autre part, maintenant qu'on connaît une (ϵ, δ)-approximation pour #DNF il est naturel de se poser la question de l'existence d'une approximation déterministe à ce problème.

A Liste de problèmes

#DNF

entrée Une formule logique f en forme normale disjonctive.

sortie Le nombre de modèles satisfaisant f.

classe Ce problème #P-complet est facilement approximable.

#CNF

entrée Une formule logique f en forme normale conjonctive.

sortie Le nombre de modèles satisfaisant f.

classe Ce problème #P-complet n'est apparemment pas approximable, bien qu'il soit facile de générer des modèles de f.

#COUPLAGES PARFAITS

entrée Un graphe $G(V, E)$.

sortie Le nombre de sous-graphes M (1-facteurs ou couplages parfaits) de G, tel que tout sommet est de degré 1.

classe Ce problème #P-complet est approximable par une (ϵ, δ)-approximation pour des graphes denses.

EXT

entrée Un ordre partiel.

sortie Le nombre d'extensions total de l'ordre donné.

classe Ce problème #P-complet est approchable.

Bibliographie

[B] Andrei Z. Broder, "How hard is it to marry at random? (On the approximation of the permanent)", *Proc. 18th Annual ACM Symposium on Theory of Computing*, (1986), pp. 50–58,

"Errata to 'How Hard is it to marry at random?' ", *Proc. 20th Annual ACM Symposium on Theory of Computing*, (1988), p. 551

[DS] P. Diaconis & D. Strook, "Geometric bounds for eigenvalues of markov chains", *The Annals of Applied Probability*, **1** (1991), pp. 36–61

[F] W. Feller, "An introduction to probability and its applications" 2 volumes, second edition, *John Wiley and Sons*, (1971)

[JS] M.R. Jerrum et A. Sinclair, "Approximating the permanent", *SIAM Journal of Computation*, (1989), pp. 1149–1178

[JV] M.R. Jerrum et Umesh V. Vazirani, "A midly exponential approximation algorithm for the permanent", *Proc. of the 33rd IEEE Symposium on Foundations of Coumputer Science*, (1992), pp. 320–326

[JVV] M.R. Jerrum, L.G. Valiant et V.V. Vazirani, "Random generation of combinatorial structures from a uniform distribution", *Theoretical Computer Science*, **43** (1986), pp. 196–188

[KL] R.M. Karp et M. Luby, "Monte-Carlo algorithms for enumeration and reliability problems", *Proc. 24th Symp. on Foundations of Computer Sc.*, (1983) pp. 56–64

[KLM] R.M. Karp, M. Luby et N. Madras, "Monte-Carlo approximation algorithms for enumeration problems", *Journal of Algorithms*, **10(3)** (1989), pp. 429–448

[PY] C.H. Papadimitriou et M. Yannakakis, "Optimization, approximation and complexity classes", *Journal of Computer and System Sciences*, **43** (1991), pp. 425–440

[M] M. Mihail, "The approximation of the permanent is still open", *manuscript*, (1987)

[Ry] H.J. Ryser, *Cominatorial Mathematics*, Carus Math. Monograph, **14** (1963)

[Ra] L.E. Rasmussen, "Approximating the permanent: a simple approach", *Random Structures and Algorithms*, Vol. 5, N°. **2** (1994), pp. 349–361

[S1] Alistair Sinclair, "Algorithms of Random Generation & Counting", *Birkhäuser Boston*, (1992)

[S2] Alistair Sinclair, "Improved bounds for mixing rates of markov chains and multicommodity flow", *Combinatorics, Probability & Computing* **1** (1992), pp. 351–370

[SJ] A. Sinclair et M. Jerrum, "Approximate counting, uniform generation and rapidly mixing markov chains", *Information and Computation*, **82** (1989), pp. 93–133

[SST] S. Saluja, K.V. Subrahmanyam et M.N. Thakur, "Descriptive complexity of #P functions", *IEEE* (1992), pp. 169–184

[V] L.G. Valiant, "The complexity of computing the permanent", *Theoretical Computer Science*, **8** (1979), pp. 189–201

[Z] David Zuckerman, "NP-complete problems have a version that's hard to approximate", *Proceedings in Structure in Complexity theory*, (1993), pp. 305–312

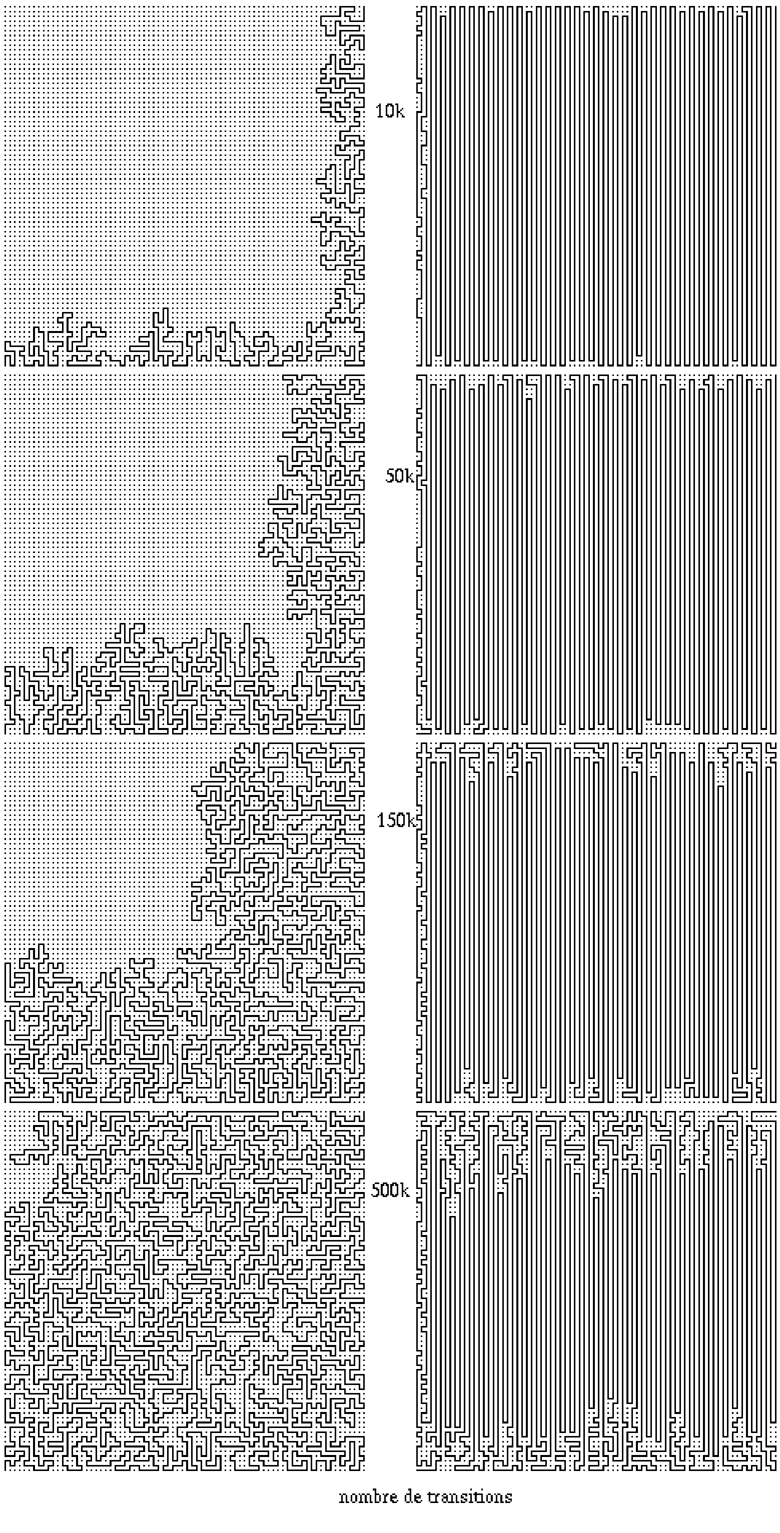


FIG. 15 - *Evolution dans une chaîne de Markov pour une grille avec $n = 75$.*