# Journées mathématiques X-UPS

## Année 2025

## Combinatoire et géométries exotiques

Arnaud DE MESMAY

**Algorithmique des matroïdes et polynômes log-concaves**

*Journées mathématiques X-UPS* (2025), p. 105-149.
https://doi.org/10.5802/xups.2025-03



Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

*Publication membre du*
*Centre Mersenne pour l'édition scientifique ouverte*
www.centre-mersenne.org

Journées mathématiques X-UPS
2025, p. 105–149 doi: 10.5802/xups.2025-03

# ALGORITHMIQUE DES MATROÏDES ET POLYNÔMES LOG-CONCAVES

*par*

Arnaud de Mesmay

***Résumé.*** L'objectif de ce texte est de faire découvrir un pendant algorithmique des résultats présentés dans les textes d'Omid Amini [3] et de Mathieu Piquerez [42] en théorie des matroïdes, en nous concentrant sur des algorithmes récents d'Anari, Liu, Oveis Gharan et Vinzant permettant de compter et d'échantillonner de façon très efficace des bases de matroïdes. Nous commençons par un survol des enjeux de la théorie des matroïdes en informatique théorique, qui permettent de généraliser à des contextes plus larges le cadre, désormais très bien compris, des graphes. Nous introduisons ensuite les polynômes log-concaves (également connus sous le nom de polynômes lorentziens dans les travaux de Brändén et Huh), dont les définitions d'apparence simple cachent des propriétés très riches qui sont intimement liées aux sujets traités dans les deux autres textes. Ces propriétés en font un outil très efficace pour résoudre de multiples problèmes combinatoires et algorithmiques, et nous esquissons comment elles sont exploitées dans les algorithmes suscités pour résoudre des problèmes d'informatique théorique ouverts depuis une trentaine d'années.

## Table des matières



***Publication originelle dans*** Journées X-UPS 2025. Combinatoire et géométries exotiques. Éditions de l'École polytechnique, 2026.

L'objectif de ces notes est de proposer un survol de quelques versants algorithmiques des combinatoires et géométries exotiques présentées dans les autres textes. Le point focal est une série de papiers assez récents d'Anari, Liu, Oveis Gharan et Vinzant [6, 5, 4, 8], en particulier le deuxième et le troisième, où les auteurs ont montré de façon remarquable comment résoudre des vieux problèmes d'informatique théorique avec des outils modernes d'origine géométrique, regroupés sous le thème des *polynômes log-concaves*. Le résultat principal auquel nous aspirerons est le suivant.

***Théorème 1*** **([5, Cor. 1.4]).** *Il existe un algorithme randomisé qui, pour tout matroïde à $n$ éléments de rang $r$ fourni par un oracle d'indépendance et pour tous $\varepsilon \in ]0,1[$ et $\delta \in ]0,1[$, compte le nombre de bases de $M$ à facteur multiplicatif de $1 \pm \varepsilon$ près, avec probabilité $1-\delta$ et en temps polynomial en $n, r, 1/\varepsilon$ et $\log(1/\delta)$.*

En parallèle, Brändén et Huh [10] ont développé une théorie des *polynômes lorentziens*, qui sont très proches des polynômes log-concaves, et ont obtenu des résultats similaires. Nous adopterons plutôt dans ces notes le point de vue plus informatique du premier groupe d'auteurs. Cela a l'avantage, ou le défaut, selon le point de vue, de cacher la théorie de Hodge derrière des atours étonnamment élémentaires. En particulier, nous proposerons une preuve presque complète du théorème 1 dans ce texte, ainsi que de plusieurs autres résultats qui découlent de la théorie. Quelques remarques feront le lien entre notre point de vue très combinatoire et les aspects géométriques mis en avant dans les autres textes.

Mais tout cela est probablement assez abscons pour l'instant, donc commençons par présenter le contexte, en débutant par l'usage des matroïdes en informatique.

## 1. Des matroïdes en informatique

Un matroïde est un objet combinatoire introduit par Whitney [49] généralisant en même temps la notion d'indépendance en algèbre linéaire et la notion d'acyclicité en théorie des graphes. Il y a de nombreuses définitions équivalentes et nous nous concentrons sur l'une d'elles pour fixer les notations. Un *matroïde* fini $M = (E, \mathcal{I})$ est constitué d'un ensemble fini $E$ et d'une famille $\mathcal{I}$ de sous-ensembles de $E$, appelés *ensembles indépendants* tels que :

(1) L'ensemble vide est indépendant.
(2) Pour tous $A \subseteq B \subseteq E$, si $B \in \mathcal{I}$ alors $A \in \mathcal{I}$.
(3) Si $A$ et $B$ sont dans $\mathcal{I}$ et que $A$ a strictement plus d'éléments que $B$, alors il existe un $x$ dans $A \setminus B$ tel que $B \cup \{x\}$ est indépendant.

L'intuition à avoir est celle de l'algèbre linéaire. Il est immédiat de vérifier que les familles de vecteurs indépendantes satisfont les axiomes ci-dessus. De nombreux autres concepts des matroïdes sont directement inspirés de ce cadre. Ainsi les *bases* sont des ensembles indépendants de taille maximale, et on peut facilement prouver qu'elles ont toutes la même cardinalité, appelé le *rang* du matroïde. De manière similaire, pour tout sous-ensemble $A$ de $E$, son rang $r(A)$ sera la cardinalité maximale d'un sous-ensemble indépendant de $A$.

Il est important de noter cependant que c'est une généralisation stricte : certains matroïdes ne sont pas obtenus de cette façon. On dit qu'un matroïde obtenu comme l'ensemble des vecteurs indépendants d'un espace vectoriel sur un corps $\mathbb{F}$ est *représentable* sur $\mathbb{F}$.

De façon moins évidente, un matroïde est aussi une généralisation d'un graphe. Dans toutes ce texte, un graphe $G = (V, E)$ est juste un ensemble fini de sommets $V$ et un ensemble fini d'arêtes $E \subseteq V^2$ qui sont des paires de sommets. En particulier nous autorisons les boucles mais pas les arêtes multiples. Un tel graphe définit un matroïde en considérant pour $E$ l'ensemble des arêtes $E$ (les notations sont bien choisies), et pour les ensembles indépendants $\mathcal{I}$ les

ensembles d'arêtes ne contenant aucun cycle. On peut facilement vérifier que cela satisfait bien aux axiomes des matroïdes. Une autre façon de s'en convaincre est de considérer la *matrice d'incidence* d'un graphe, définie comme la matrice $I$ telle que $I_{v,e} = 1$ si et seulement si le sommet $v$ est incident à une arête $e$ qui n'est pas une boucle, et d'observer que ses vecteurs colonnes engendrent un sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^{|E|}$, où une famille de vecteurs est indépendante si et seulement si les arêtes correspondantes ne contiennent pas de cycle. Ainsi, les *matroïdes graphiques* que nous venons de définir sont représentables sur $\mathbb{Z}/2\mathbb{Z}$, et en fait sur n'importe quel corps. De tels matroïdes, représentables sur n'importe quel corps, sont dits *réguliers*.

Pour un élément $x$ de $E$, on définit un matroïde où $x$ a été *supprimé* $M \setminus x := (E \setminus x, \{I \cap (E \setminus x) \mid I \in \mathcal{I}\})$, et un matroïde où $x$ a été *contracté* $M/x = (E \setminus x, \{I \cap (E \setminus x) \mid I \cup \{x\} \in \mathcal{I}\}$. L'intuition pour ces deux notions vient de la théorie des graphes, où on peut obtenir de manière similaire deux graphes différents en supprimant ou en contractant une arête.

*Algorithmes gloutons.* Une des premières raisons de s'intéresser aux matroïdes en informatique est qu'ils donnent la structure combinatoire sous-jacente à tout problème pour lequel un *algorithme glouton* est optimal. Un algorithme glouton apparaît naturellement dès que l'on considère un problème où l'on a un nombre fini objets $E$ (là encore, la notation n'est pas choisie au hasard), chacun ayant un certain coût ou une certaine valeur $w(e)$, et on cherche à choisir un sous-ensemble de $E$ de coût minimal ou de valeur maximale mais soumis à certaines conditions. Par exemple, il peut s'agir d'acheter des produits avec la condition qu'on ne veut jamais deux exemplaires du même produit et on veut minimiser le coût. L'algorithme glouton consiste alors à choisir un premier élément de coût minimal, puis un second parmi les éléments restants compatibles de coût minimal, et ainsi de suite. Lorsque les ensembles admissibles sont stables par inclusion, la question de savoir si la solution trouvée est globalement optimale revient exactement à se demander s'ils forment les ensembles indépendants d'un matroïde : la propriété d'ajout (3) montre qu'à n'importe quel moment de l'algorithme glouton, après avoir pris

un élément de coût minimal on peut compléter avec des éléments de la solution optimale, ce qui permet de conclure puisque celle-ci est globalement minimale. La direction opposée de l'équivalence n'est pas beaucoup plus dure à établir en jouant sur les coûts.

Ce point de vue permet d'éclairer et de généraliser des algorithmes classiques de théorie des graphes. Par exemple, un problème fondamental d'algorithmique des graphes est de trouver un *arbre couvrant minimal*, c'est-à-dire un sous-ensemble d'arêtes de poids total minimal ne formant pas de cycles dans un graphe. Comme on l'a vu, les ensembles d'arêtes ne contenant pas de cycles définissent un matroïde, et donc l'idée naturelle est d'appliquer un algorithme glouton : c'est ce que fait le célèbre algorithme de Kruskal [35].

Pour voir où cette idée mène à des problèmes de recherche contemporains, continuons sur notre exemple d'achat de produits, mais dans un cadre où l'on généralise notre fonction de coûts à une fonction *sous-modulaire*, c'est-à-dire une fonction définie non plus sur les objets mais sur les ensembles, et satisfaisant à une propriété de rendements décroissants : pour tous $A \subseteq B \subseteq E$ et $x \notin B$,

$$f(A \cup x) - f(A) \geqslant f(B \cup x) - f(B).$$

C'est un modèle classique en économie et en théorie algorithmique des jeux : par exemple la valeur perçue d'un manteau est moins grande si l'on est déjà habillé des pieds à la tête que si l'on est en tenue d'Ève ou d'Adam. Notez par ailleurs que la fonction de rang d'un matroïde satisfait à une telle propriété de sous-modularité. Si l'on souhaite maximiser la valeur de notre panier sans énumérer tous les achats possibles (ce qui serait algorithmiquement prohibitif puisqu'il y aurait un nombre exponentiel de choix), il est naturel de se tourner encore vers un algorithme glouton et de se demander s'il trouve une solution optimale. Ce ne sera pas le cas en général, même si les paniers admissibles forment un matroïde, mais pour certains matroïdes, la qualité de la solution gloutonne sera sensiblement meilleure que pour d'autres et de nombreux travaux ont été consacrés à de tels problèmes d'*optimisation sous-modulaire*, voir par exemple l'article de survol [34].

*Matroïdes et intersections de matroïdes.* Les matroïdes forment donc un cadre généralisant à la fois les sous-ensembles acycliques d'un graphe et les familles de vecteurs indépendants dans un espace vectoriel. D'autres matroïdes apparaissent également en informatique théorique. Voici une liste non exhaustive de leurs incarnations.

(1) *Matroïde dual et co-graphique.* Bien qu'il n'y ait pas de notion naturelle de dualité pour un graphe (du moins s'il n'est pas plongé), il y en a une pour les matroïdes. Le *matroïde dual* $M^*$ d'un matroïde $M$ a le même ensemble d'éléments $E$ et ses ensembles indépendants $\mathcal{I}^*$ sont les ensembles $U \subseteq E$ tels qu'il existe une base $B$ de $M$ telle que $U$ et $B$ sont disjoints. Il est facile de voir que lorsque le matroïde $M$ est graphique pour un graphe $G$, son dual $M^*$ a pour ensembles indépendants les ensembles d'arêtes dont la suppression laisse $G$ connexe. Tutte a montré qu'un graphe $G$ est planaire si et seulement si son matroïde dual est également graphique, auquel cas c'est le matroïde du graphe dual $G^*$ de $G$, dont les sommets sont les faces de $G$ (composantes connexes de $\mathbb{R}^2 \setminus G$) et les arêtes sont les adjacences entre ces faces.

(2) *Matroïde de rigidité.* Des matroïdes différents apparaissent dans l'étude des phénomènes de rigidité. Il s'agit de l'étude des *cadres*, c'est-à-dire des graphes $G = (V, E)$ munis d'une application $f : V \to \mathbb{R}^d$ indiquant la position des sommets, les arêtes étant réalisées par des segments de longueur fixée. Un tel cadre est dit *rigide* s'il n'existe pas de modification locale de l'application $f$ préservant la longueur des arêtes, modulo les symétries de $\mathbb{R}^d$ qui sont bien sûr toujours présentes. La motivation vient de l'ingénierie : une structure se doit d'être rigide pour ne pas s'effondrer au moindre coup de vent. De manière similaire, quiconque a monté des étagères en kit sait qu'un empilement de rectangles n'est pas rigide, mais peut le devenir lorsqu'on ajoute un X derrière, comme illustré en figure 1. Il se trouve que la rigidité d'un cadre ne dépend pas de la longueur des segments[(1)], et qu'elle est encodée dans un matroïde :

[(1)]Du moins *génériquement*, c'est-à-dire que la rigidité sera toujours la même sauf pour un ensemble de longueur de segments de mesure nulle. Le choix de l'étagère de la figure 1 n'est d'ailleurs pas tout-à-fait générique, et comme il m'a

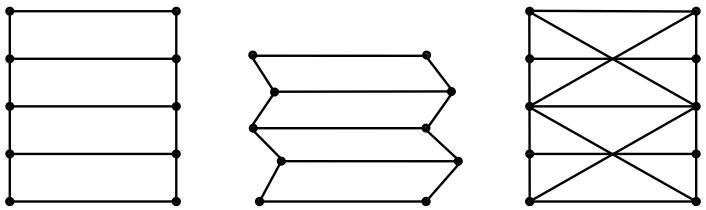

FIGURE 1. À gauche, un graphe non rigide, que l'on peut déformer comme au milieu. À droite, le graphe est rigidifié par l'ajout de deux X. L'exemple de droite est minimalement rigide : le graphe tout entier est une base du matroïde de rigidité, et rajouter des arêtes serait superflu du point de vue de la rigidité, ce qui s'exprimerait comme des dépendances.

le *matroïde de rigidité* d'un graphe a pour éléments les arêtes du graphe, et pour bases les ensembles d'arêtes induisant un sous-graphe rigide minimal. En dimension 2, la structure des matroïdes de rigidité est entièrement décrite grâce à un théorème célèbre de Laman [36] mais, en dimension 3 et plus, ils sont beaucoup moins bien compris.

(3) *Couplages et graphes bipartis.* Les matroïdes apparaissent également dans d'autres problèmes classiques de théorie des graphes. Par exemple, considérons un graphe biparti $G = (U, V, E)$, c'est-à-dire que l'ensemble des sommets est partitionné en $U$ et $V$ et il n'y a pas d'arête entre sommets de $U$ ou entre sommets de $V$. Il est très fréquent de vouloir calculer un *couplage*, c'est-à-dire un ensemble d'arêtes sans sommets en commun, avec certaines propriétés, dans un graphe biparti (pensez à Parcoursup).

- On peut voir cela sous l'angle des matroïdes en considérant un premier *matroïde de partition* $M_U$ dont les éléments sont les arêtes $E$ et les ensembles indépendants sont les familles d'arêtes n'ayant pas d'extrémités en commun dans $U$. De manière similaire, on définit l'autre matroïde de partition $M_V$. Un couplage

été signalé pendant le cours, elle peut être rigidifiée en rajoutant un seul X au lieu de deux. Mais la théorie de la rigidité montre que cela est impossible dès que les longueurs sont un peu perturbées : c'est par exemple le cas si les suites d'arêtes de chaque côté de l'étagère ne sont pas tout-à-fait verticales.

est alors un ensemble indépendant commun aux deux matroïdes. Calculer un couplage de taille maximale revient donc à calculer un ensemble indépendant commun à deux matroïdes de taille maximale, et un théorème classique d'Edmonds [14] permet de résoudre ces deux problèmes en temps polynomial.

- Un autre matroïde $M_T(U)$, appelé *matroïde transversal*, apparaît lorsqu'on fixe un côté de la bipartition comme ensemble d'éléments, par exemple $U$, et que l'on choisit comme ensembles indépendants les sous-ensembles $U'$ de $U$ qui peuvent être couplés parfaitement dans le graphe $G$, c'est-à-dire tels qu'il existe un ensemble d'arêtes disjointes dans $G$ reliant chaque sommet de $U'$ à un sommet de $V$. Si $|U| \geqslant |V|$, l'existence d'un couplage parfait (où tous les sommets sont appareillés) pour $G$ se ramène donc à l'existence d'un ensemble indépendant de taille $|U|$ dans $M_T(U)$.

*Problèmes de fiabilité.* Il est maintenant possible de motiver un peu notre théorème 1. Pour toutes les structures décrites par ces matroïdes, un problème fondamental est celui de calculer leur *fiabilité*. Regardons d'abord au cas par cas de quoi il s'agit.

(1) Étant donné un graphe, s'il modélise un réseau de distribution d'électricité, une propriété primordiale à conserver est sa connexité. Si certaines arêtes viennent à dysfonctionner, indépendamment avec une certaine probabilité, quelle est la probabilité que le graphe reste connexe ?

(2) Étant donné un cadre, s'il modélise un bâtiment ou un meuble, on voudra conserver sa rigidité lorsque certaines arêtes viennent à faillir, indépendamment avec une certaine probabilité. Quelle est la probabilité que le cadre perde sa rigidité ?

(3) Étant donné un graphe biparti, s'il modélise un système d'affectation d'étudiants, on veut que chaque étudiant ait une formation. Si l'on ajoute un certain nombre d'étudiants aléatoirement, quelle est la probabilité que ce soit le cas ?

(4) Un *code correcteur binaire linéaire* est un sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^n$ tel que tout vecteur est assez éloigné de chaque autre

vecteur. Cette propriété de *distance* permet de reconstruire un message (pensé comme une suite de bits 0 ou 1, donc comme un élément de $(\mathbb{Z}/2\mathbb{Z})^n$) s'il venait à être corrompu lors d'un transfert d'informations. Si le canal de transfert venait à être corrompu au point que l'on perde complètement l'information contenu dans le $k$-ième bit, pour des valeurs de $k$ choisies indépendamment avec une certaine probabilité, quelle est la probabilité pour que le code correcteur fonctionne encore ?

Lorsque l'on demande la probabilité dans tous ces problèmes, c'est un problème de nature *algorithmique* : on cherche à trouver un bon algorithme qui, prenant comme entrée un graphe, un cadre, etc., va déterminer la probabilité de fiabilité de cet objet. Via les différentes incarnations des matroïdes que nous avons vues, ces problèmes peuvent être pensés comme des cas particuliers du problème de fiabilité de matroïde : Étant donné un matroïde $M = (E, \mathcal{I})$ et un entier $k$, comment calculer la probabilité que si l'on choisit $k$ éléments distincts aléatoirement et uniformément, ceux-ci soient indépendants ? Ce problème est $\#P$-complet [47] : cela signifie que modulo les conjectures classiques de théorie de la complexité, il n'existe pas d'algorithme capable de le résoudre exactement en temps polynomial.

On va donc chercher à l'approximer. Calculer la probabilité de fiabilité revient à calculer le quotient $|\mathcal{I}_k|/\binom{|E|}{k}$, où on a noté $\mathcal{I}_k$ les ensembles indépendants de taille $k$, et donc à compter efficacement le nombre d'ensembles indépendants d'une taille fixée dans un matroïde. Notez que tout matroïde peut être *tronqué* à une certaine taille $k$, c'est-à-dire qu'on peut retirer des ensembles indépendants tous les ensembles de taille strictement plus grande que $k$, et obtenir un matroïde de rang $k$. Les ensembles indépendants de taille $k$ deviennent alors des bases. Nous avons donc enfin tous les ingrédients pour apprécier une des forces du théorème 1 : celui-ci permet, en temps polynomial, de résoudre de façon approximée (avec une approximation aussi bonne qu'on le souhaite), tous les problèmes de fiabilité que nous avons mentionnés.

***Remarque 1.*** Il faut faire attention au modèle de calcul lorsque l'on traite d'algorithmique des matroïdes. Lorsqu'on prend un matroïde

en entrée d'un algorithme, si cette entrée contient tous les ensembles indépendants du matroïde, elle est de taille considérable. Notamment, pour les matroïdes graphiques, elle peut facilement être exponentiellement plus grande que le graphe correspondant. Il y a alors beaucoup moins d'intérêt à développer des algorithmes polynomiaux lorsque l'entrée est énorme. C'est pourquoi il est plus standard de considérer, comme dans le théorème 1, un modèle avec *oracle* : plutôt que de fournir tous les ensembles indépendants en entrée de l'algorithme, on considère que celui-ci a accès à un oracle, c'est-à-dire qu'il peut demander à tout instant, pour un coût 1, si un ensemble donné est indépendant. Demander tous les ensembles indépendants nécessiterait possiblement alors un temps exponentiel, ce qui rend encore plus remarquable la dépendance polynomiale annoncée dans le théorème 1.

Nous concluons cette introduction au domaine par quelques notes historiques. Le problème de fiabilité dans les graphes est un problème classique, datant au moins des années 80, qu'on ne peut résoudre en temps polynomial si l'on admet les hypothèses standard en théorie de la complexité [47, 43]. Karger a montré en 95 [32] comment approximer efficacement la probabilité qu'un graphe devienne déconnecté, et il a fallu attendre Guo et Jerrum en 2017 [19] pour avoir un algorithme correspondant pour estimer la probabilité que le graphe reste connecté[(2)]. Ainsi, le théorème 1 généralise grandement ces résultats en englobant des objets combinatoire bien plus variés que les graphes.

---

[(2)]De façon un peu contre-intuitive, lorsque l'on traite d'algorithmes d'$(1+\varepsilon)$-approximation avec une garantie multiplicative, ce qui est le cas ici, deux problèmes complémentaires ne sont pas équivalents. Dans le premier cas, pour une probabilité $p$ que le graphe soit déconnecté, l'algorithme fournit une valeur $p'$ telle que

$$p(1-\varepsilon) < p' < p(1+\varepsilon),$$

alors que dans le second cas on a

$$(1-p)(1-\varepsilon) < (1-p') < (1-p)(1+\varepsilon),$$

et donc

$$p(1-\varepsilon)+\varepsilon > p' > p(1+\varepsilon)-\varepsilon,$$

ce qui est très sensiblement différent par exemple lorsque $p \ll \varepsilon$.

## 2. Algorithmes de comptage, échantillonnage et marches aléatoires

### 2.1. Comptage et échantillonnage

L'algorithme derrière le théorème 1 est très simple, et c'est son analyse qui s'avère délicate. Un algorithme randomisé naturel pour compter les bases d'un matroïde est de calculer d'abord son rang $r$, puis de générer aléatoirement un ensemble de $r$ éléments et de tester, via l'oracle, s'il est indépendant. En répétant ce test un nombre suffisant de fois, on obtient une estimation de la probabilité qu'un ensemble de $r$ éléments soit indépendant, et donc une estimation du nombre de bases. Cela peut être formalisé avec des inégalités de type Markov, comme par exemple les bornes de Chernoff [41, Chap. 4]. Le problème de cette approche est que si le nombre de bases est très petit par rapport à $\binom{|E|}{r}$, l'oracle répondra négativement la plupart du temps, et il faudra un temps très long, peut-être exponentiel, pour obtenir une estimation correcte, comme celle promise par le théorème 1.

Cet algorithme, bien que trop lent, illustre une propriété fondamentale commune à de nombreux problèmes de comptage : il y a un lien fort entre le problème d'*échantillonner* correctement (c'est-à-dire de générer aléatoirement uniformément un élément) un ensemble et de compter sa taille. Ici, l'obstacle est le même dans les deux cas : l'ensemble des bases d'un matroïde peut être tellement petit qu'un échantillonnage naïf amènera à de trop nombreux rejets. Un théorème fondateur, dû à Jerrum, Valiant et Vazirani [31] montre que cette connexion est valide dans les deux sens pour une très large classe de problèmes, appelés problèmes auto-réductibles (*self-reducible*), dont le problème de compter les bases de matroïde fait partie. Par souci de simplicité, nous ne l'énonçons que pour ce cas particulier. On dit qu'un problème spécifié par un entier $n$ et un ensemble cible $M_n$ admet un *algorithme polynomial d'échantillonnage approximé randomisé uniforme*, si, pour tout $\varepsilon \in ]0,1[$, il existe un algorithme polynomial en $\log(1/\varepsilon)$ et $n$ qui échantillonne un élément $u$ de l'ensemble $M_n$ selon une probabilité $\pi$ telle que $\|\pi - \mu\|_1 \leqslant \varepsilon$, où $\mu$ est la distribution uniforme sur $M_n$. Le nom étant assez lourd, on utilisera

l'abréviation consacrée, qui est FPAUS pour *Fully Polynomial Approximate Uniform Sampler*. La distance $\ell_1$ dans ce contexte est appelée *distance de variation totale*[3] : pour deux distributions de probabilités $\pi$ et $\mu$ dont la distance de variation totale est faible, chaque événement arrive avec presque la même probabilité pour $\pi$ et pour $\mu$.

***Théorème 2.*** *Il existe un algorithme polynomial de* comptage *randomisé approximé*[4] *des bases de matroïde (au sens du théorème* 1*) si et seulement il existe un algorithme polynomial d'*échantillonnage *approximé randomisé uniforme des bases de matroïde.*

*Ébauche de preuve.* Nous présentons les idées principales de la preuve sans fournir l'analyse probabiliste dans le détail et nous renvoyons à l'article [31] ou au livre [29, Prop. 3.4] pour celle-ci. Fixons un matroïde $M = (E, \mathcal{I})$ et notons $\mathcal{B}(M)$ l'ensemble de ses bases.

• Imaginons d'abord que l'on sache compter efficacement les bases d'un matroïde. On peut alors échantillonner efficacement de la façon suivante : on fixe un élément $x$ de $E$ et on utilise notre algorithme pour compter les bases qui contiennent cet élément. De manière similaire, on compte les bases qui ne le contiennent pas. Cela nous permet d'estimer la probabilité $p(x)$ qu'une base aléatoire tirée uniformément contienne $x$. On peut alors tirer au sort, selon la probabilité $p(x)$, si $x$ est dans notre base, et appliquer le même algorithme récursivement dans le matroïde $M/x$ si $x$ y est ou dans le matroïde $M \setminus x$ sinon.

• Dans l'autre sens, imaginons que l'on sache échantillonner efficacement les bases d'un matroïde. On fixe encore un élément $x$ de $E$, et on échantillonne un nombre de fois suffisant pour obtenir une bonne estimation de la probabilité $p(x)$ qu'il soit dans une base, ou bien de la probabilité $1 - p(x)$ qu'il ne soit pas dans une base. De manière cruciale, au moins l'une de ces deux probabilités n'est pas trop petite, et il n'est pas difficile de montrer que, dans ce contexte, le nombre

[3] Les experts objecteront ici que ces deux distances diffèrent d'un facteur 2, que nous négligerons.

[4] L'abréviation consacrée est FPRAS pour *Fully Polynomial Randomized Approximation Scheme*.

suffisant est de taille polynomiale (c'est la différence avec notre algorithme naïf : pour l'un des deux choix, on peut contrôler le nombre de rejets). La probabilité $p(x)$ vaut $|\mathcal{B}(M/x)|/|\mathcal{B}(M)|$ et la probabilité $1-p(x)$ vaut $|\mathcal{B}(M \smallsetminus x)|/|\mathcal{B}(M)|$. On peut alors appliquer récursivement le même algorithme dans $M/x$ ou $M \smallsetminus x$ jusqu'à arriver au matroïde vide, qui a une unique base de taille 1. La quantité $1/\mathcal{B}(M)$ s'obtient en prenant le produit télescopique de toutes les probabilités estimées. □

Ce résultat fondamental montre que le cœur du problème est donc d'échantillonner efficacement des bases de matroïde. Pour ce faire, l'algorithme utilisé consiste en une marche aléatoire très facile à décrire, appelée *marche d'échange de bases*. Il s'agit simplement de partir d'une base quelconque $B$, et de la modifier en une base $B'$ en

(1) retirant un élément $x$ de $B$ au hasard uniformément,

(2) et en rajoutant un élément $y$ à $B \smallsetminus x$, choisi aléatoirement uniformément parmi ceux tels que $(B \smallsetminus x) \cup y$ est une base.

Une conjecture célèbre de 1989 de Mihail et Vazirani stipulait que cette marche aléatoire permet d'échantillonner une base efficacement. Le moteur derrière le théorème 1 est une preuve de cette conjecture.

***Proposition 3*** **([5, Cor. 1.3]).** *Pour un matroïde de rang $r$ avec $n$ éléments, appliquer la marche d'échange de bases pendant un temps $O(r^2 \log(n/\varepsilon))$ donne un FPAUS.*

Précédemment, il y avait une longue ligne de travaux autour des algorithmes d'approximation pour les problèmes de matroïdes. Pour une classe particulière de matroïdes appelés matroïdes *équilibrés*, Feder et Mihail [17] ont obtenu dès les années 90 des résultats d'échantillonnage de bases, mais très peu de choses étaient connus dans le cas général avant les travaux d'Anari, Liu, Oveis Gharan et Vinzant [5].

**2.2. Mélange de marches aléatoires.** Avant de prouver la proposition 3, prenons un peu de recul. Notre objectif est d'analyser combien de temps une marche aléatoire met pour se propager uniformément dans un espace fixé. Cela se rattache à la théorie des *chaînes*

*de Markov*, et plus précisément au *temps de mélange* qu'elles mettent pour converger (presque) à leur *distribution stationnaire*. Si vous n'êtes pas familiers avec ces concepts, voici quelques notions qui permettent d'appréhender de quoi il retourne. Nous renvoyons à l'article de survol de Hoory, Linial et Wigderson pour une introduction au sujet [25, § 3] et au livre classique de Levin, Peres et Wilmer [38] pour une référence plus poussée.

On modélise une marche aléatoire avec un graphe dirigé $G$ : ses sommets sont les différentes étapes de la marche, et on met une arête dirigée $uv$ lorsque la marche a une probabilité non nulle de passer de $u$ à $v$, et une autre arête dirigée $vu$ lorsque la marche a une probabilité non nulle de passer de $v$ à $u$. Nous nous restreignons dans cette discussion au cas où $G$ est fini, qui suffira pour notre application. En général, une marche aléatoire est spécifiée par une *matrice de transition* $M$, qui spécifie pour chaque arête la probabilité que la marche emprunte cette arête, de telle sorte que ces probabilités somment à 1 autour de chaque sommet. Pour la marche d'échange des bases, la marche est symétrique (c'est-à-dire qu'il y a une arête $uv$ si et seulement s'il y a une arête $vu$ et elles ont les mêmes probabilités) et le graphe est connexe. Dans ce contexte, il est facile de voir qu'il existe une unique *distribution stationnaire* pour la marche aléatoire, c'est-à-dire une distribution de probabilités $\mu$ sur les sommets du graphe telle que si l'on choisit un sommet selon $\mu$ et que l'on réalise une étape de la marche, la probabilité de se retrouver quelque part est également gouvernée par $\mu$. De façon équivalente, en voyant $\mu$ comme un vecteur de $\mathbb{R}^V$, il existe une unique solution à $M\mu = \mu$, ce qui découle du théorème de Perron-Frobenius. Dans notre cas simplifié où $M$ est symétrique, on a même $\mu = (1, \dots, 1)$ puisque $\mu^T M = \mu^t$ (les probabilités sortant d'un sommet somment à 1) et $M$ est symétrique, et donc la distribution stationnaire est la distribution uniforme. Notre problème se ramène ainsi à étudier un opérateur $M$ qui a un unique point fixe, pour voir s'il converge vers ce point fixe et, si oui, à quelle vitesse.

Dans le cas où le graphe est $d$-régulier (c'est-à-dire que les degrés de tous les sommets ont la même valeur $d$) et que les probabilités

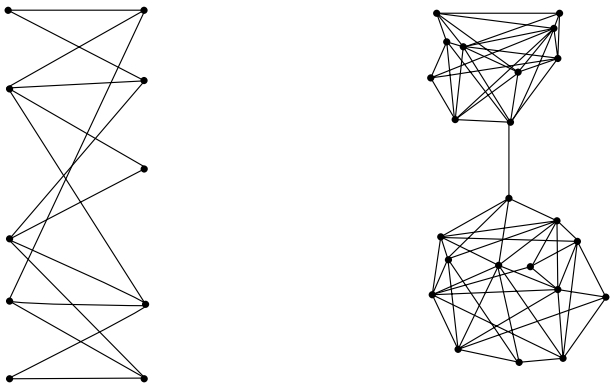

FIGURE 2. À gauche, un graphe biparti dans lequel une marche aléatoire n'a aucune chance de converger. À droite, un goulot d'étranglement qui limitera fortement la vitesse de convergence d'une marche aléatoire.

sont uniformes (égales à $1/\deg^+(v)$ pour chaque arête autour d'un sommet $v$, où $\deg^+$ est le degré sortant du sommet), le comportement de la marche est complètement gouverné par la géométrie du graphe $G$, qui a donc un impact direct sur le temps que la marche aléatoire mettra à converger. Cet impact se caractérise de deux façons très différentes :

(1) Il peut y avoir un problème de *période*. Si le graphe $G$ est biparti, les temps pairs de la marche aléatoire seront toujours d'un côté de la bipartition, alors que les temps impairs seront toujours de l'autre. Dans ces conditions, il est impossible que la marche aléatoire converge vers une distribution fixe.

(2) Il peut y avoir un problème d'*expansion*. Par exemple, si le graphe $G$ est déconnecté, la marche ne pourra jamais passer d'une composante connexe à l'autre. De façon plus subtile, s'il est *mal connecté*, comme illustré dans la figure 2, quand bien même la marche finira par converger, le goulot d'étranglement aura un fort impact sur le temps de convergence.

Le premier problème est généralement résolu en rendant la marche aléatoire *paresseuse* : on va modifier celle-ci pour qu'à chaque itération, avec probabilité $1/2$, on reste paresseusement au même sommet, et avec probabilité $1/2$ on se déplace comme indiqué par la matrice $M$. Cela résout tous les problèmes de période, comme vous pouvez le vérifier sur notre exemple d'un graphe biparti. En terme de graphe, cela revient à rajouter des boucles sur chaque sommet de $G$.

Le deuxième problème est sensiblement plus épineux et constitue tout le nœud du sujet. On peut quantifier la connectivité d'un graphe $d$-régulier via la *constante de Cheeger* qui est définie comme

$$h(G) = \min\Big\{ \frac{|\partial A|}{d|A|} \;\Big|\; A \subseteq V,\ 0 < |A| \leqslant \frac{1}{2}|V(G)| \Big\},$$

où $\partial A$ désigne l'ensemble d'arêtes ayant exactement une extrémité dans $A$. Cette constante mesure dans quelle proportion des goulots d'étranglement séparent des gros morceaux du graphe. Dans l'exemple de la figure 2, où il y a un goulot d'étranglement constitué par une arête coupant le graphe en deux, la constante de Cheeger $h(G)$ vaut donc environ $1/d|V|/2$. Plus cette constante est petite, moins le graphe est bien connecté.

La matrice $M$ étant stochastique, par le théorème de Perron-Frobenius, sa plus grande valeur propre est 1 et correspond à l'unique vecteur propre $\mathbf{1} := (1, \dots, 1)$. Il se trouve que la constante de Cheeger $h(G)$ est intimement reliée à la valeur de la *deuxième* valeur propre $\lambda_2$, lorsqu'on les ordonne $\lambda_1 \geqslant \lambda_2 \cdots \geqslant \lambda_n$. Cela est généralement exprimé via le *trou spectral* $\gamma := \lambda_1 - \lambda_2 = 1 - \lambda_2$ :

***Lemme 4* (inégalité de Cheeger).** *Pour tout graphe $G$ où tous les sommets sont de degré $d$, si on dénote par $\gamma$ le trou spectral de la matrice d'adjacence normalisée*[(5)] *$M := A(G)/d$, on a :*

$$h(G)^2/2 \leqslant \gamma \leqslant 2h(G).$$

[(5)]La littérature en théorie spectrale des graphes utilise parfois la matrice d'adjacence, parfois la matrice laplacienne. Parfois elle les normalise et parfois non. Nous fixons ici le choix de matrices d'adjacence normalisées, qui est le choix naturel pour l'étude des marches aléatoires mais tous les résultats se transcrivent facilement d'un cadre à l'autre.

*Démonstration.* Nous prouvons juste la borne supérieure dans ces notes puisque c'est celle qui nous intéresse, et renvoyons à [38, Th. 13.3] pour la preuve complète. Notons par $n$ le nombre de sommets de $G$, il y a donc $dn/2$ arêtes.

La clé est d'exploiter les interprétations variationnelles (formules de Courant-Fischer) des valeurs propres. En effet, comme $\mathbf{1}$ est vecteur propre associé à $\lambda = 1$, on a

$$\lambda_1(G) = \max_{x\neq 0} \frac{x^T M x}{x^T x} \qquad \text{et} \qquad \lambda_2(G) = \max_{\substack{x\neq 0\\ x\perp \mathbf{1}}} \frac{x^T M x}{x^T x},$$

et donc

$$1-\lambda_2(G) = \min_{\substack{x\neq 0\\ x\perp \mathbf{1}}} \frac{\sum_{u,v\in V} M_{u,v}(x_u - x_v)^2}{2x^T x} = \min_{\substack{x\neq 0\\ x\perp \mathbf{1}}} \frac{\sum_{u,v\in E}(x_u - x_v)^2}{2dx^T x}.$$

D'un autre côté,

$$\begin{aligned}
h(G) &= \min\Big\{ \frac{|\partial A|}{d|A|} \mid A\subseteq V,\ 0<|A|\leqslant \frac{1}{2}|V(G)| \Big\} \\
&= \min_{\substack{x\neq \mathbf{0}\\ x\in\{0,1\}^n\\ \sum_u x_u \leqslant n/2}} \frac{\sum_{u,v\in E}|x_u - x_v|}{d\sum_{u\in V} x_u} \\
&\geqslant \min_{\substack{x\neq \mathbf{0}, x\neq \mathbf{1}\\ x\in\{0,1\}^n}} \frac{\sum_{u,v\in E}|x_u - x_v|}{2d(\sum_{u\in V} x_u)(n-\sum_{u\in V} x_u)/n} \\
&= \min_{\substack{x\neq \mathbf{0}, x\neq \mathbf{1}\\ x\in\{0,1\}^n}} \frac{\sum_{u,v\in E}(x_u - x_v)^2}{2d(\sum_{u\in V} x_u)(n-\sum_{u\in V} x_u)/n} \\
&= \min_{\substack{x\neq \mathbf{0}, x\neq \mathbf{1}\\ x\in\{0,1\}^n}} \frac{\sum_{u,v\in E}(x_u - x_v)^2}{2d\sum_{u,v\in V}(x_u - x_v)^2/n} \\
&\geqslant \min_{\substack{x\neq \mathbf{0}, x\neq \mathbf{1}\\ x\in\mathbb{R}^n}} \frac{\sum_{u,v\in E}(x_u - x_v)^2}{2d\sum_{u,v\in V}(x_u - x_v)^2/n} \\
&= \min_{\substack{x\neq \mathbf{0}, x\neq \mathbf{1}\\ x\in\mathbb{R}^n, x\perp \mathbf{1}}} \frac{\sum_{u,v\in E}(x_u - x_v)^2}{2d\sum_{u,v\in V}(x_u - x_v)^2/n} \\
&= \min_{\substack{x\neq \mathbf{0}, x\neq \mathbf{1}\\ x\in\mathbb{R}^n, x\perp \mathbf{1}}} \frac{\sum_{u,v\in E}(x_u - x_v)^2}{4dx^T x} = \frac{1-\lambda_2(G)}{2}.
\end{aligned}$$

□

Pour obtenir une borne inférieure sur la constante de Cheeger, il suffit donc d'obtenir une borne inférieure sur le trou spectral de la matrice de transition.

Une autre façon d'analyser la convergence de la marche aléatoire, qui ne requiert pas d'hypothèse de régularité et qui prend en compte simultanément le problème de période et celui d'expansion, est de penser à $t$ étapes de la marche aléatoire comme une application de $M^t$. En diagonalisant $M$, on voit que $M^t$ est semblable à la matrice $\mathrm{diag}(\lambda_1^t = 1, \lambda_2^t, \dots, \lambda_n^t)$, et donc les contributions qui ne sont pas celles de la distribution stationnaire $\mathbf{1}$, associée à la valeur propre 1, disparaissent d'autant plus vite que $\lambda_* = \max(|\lambda_2|, |\lambda_n|)$ est faible, et donc que le *trou spectral absolu* $1-\lambda_*$ est grand. On arrive ainsi à la proposition suivante, où le *$\varepsilon$-temps de mélange* $t_\varepsilon$ d'une marche aléatoire est le temps au bout duquel, pour n'importe quelle distribution de départ, la distribution $\mu$ obtenue après $t_\varepsilon$ application de la marche aléatoire satisfait à $\|\mu - \mathbf{1}/n\|_1 \leqslant \varepsilon$ (comparer avec la définition d'un FPAUS).

***Proposition 5.*** *Pour un graphe $G$ connexe et une marche aléatoire symétrique sur $n$ sommets, le temps de mélange de la marche aléatoire satisfait à*

$$t_\varepsilon = O\Big(\frac{\log n/\varepsilon}{1-\lambda_*}\Big).$$

*Démonstration.* Soit $v_1, \dots, v_n$ une base orthonormale de $M$. Pour toute distribution de départ $\pi$, on écrit $\pi = \sum_i \pi_i$ où chaque $\pi_i$ est un multiple de $v_i$. On a $\pi_1 = \mathbf{1}/n$ puisque $\pi$ est une distribution de probabilité. Donc

$$\begin{aligned}
\|M\pi - \mathbf{1}/n\|^2 &= \|M\pi_1 + M\pi_2 + \cdots + M\pi_n - \mathbf{1}/n\|^2 \\
&= \|M\pi_2 + \cdots + M\pi_n\|^2 \\
&\leqslant \lambda_*^2(\|\pi_2^2 + \cdots + \pi_n^2\|) \\
&= \lambda_*^2\|\pi - \mathbf{1}/n\|^2.
\end{aligned}$$

Et donc

$$\|M^\ell\pi - \mathbf{1}/n\| \leqslant \lambda_*^\ell\|\pi - \mathbf{1}/n\| \leqslant \lambda_*^\ell\|\pi\| \leqslant \lambda_*^\ell\|\pi\|_1 \leqslant \lambda_*^\ell.$$

On conclut avec une application de Cauchy-Schwarz :

$$\|M^\ell \pi - \mathbf{1}/n\|_1 \leqslant \|M^\ell \pi - \mathbf{1}/n\| \sqrt{n},$$

qui est donc au plus $\varepsilon$ pour

$$\ell = O(\log(\varepsilon/n)/\log \lambda_*) = O(\log(n/\varepsilon)/(1-\lambda_*)). \qquad \square$$

Notons que la plus petite valeur propre $\lambda_n$ satisfait toujours à $|\lambda_n \leqslant 1|$ pour une matrice stochastique, et que lorsqu'on rend une marche paresseuse, on ajoute $\mathrm{Id}/2$ à $M$. Cela a donc pour effet de pousser $\lambda_n$ loin de $-1$, et donc de réconcilier le trou spectral qui intervient dans l'expansion avec le trou spectral absolu qui intervient dans la borne de la proposition 5.

Pour analyser le trou spectral de notre marche d'échange de bases, on se lance maintenant dans une longue digression.

## 3. Polynômes log-concaves

L'outil principal derrière la preuve du théorème 1 et de la proposition 3 est l'étude d'une certaine classe de polynômes qui a l'air, de prime abord, complètement déconnectée de nos considérations de fiabilité et de comptage.

**3.1. Définitions et mises en bouches.** On considère des polynômes homogènes multivariés d'inconnues $z_1, \ldots, z_n$ et à coefficients réels positifs. On dit qu'un tel polynôme $p$ est *log-concave* sur $\mathbb{R}^n_{\geqslant 0}$ si $\log p$ est concave dans l'*orthant positif*

$$\mathbb{R}^n_{\geqslant 0} := \{z_1, \ldots, z_n \in \mathbb{R}^n \mid \forall i,\, z_i \geqslant 0\}.$$

Pour que le logarithme soit défini, il faut déjà que $p$ soit positif sur cet orthant positif, ce qui est garanti par la positivité des coefficients. De façon équivalente, la log-concavité s'exprime comme la propriété que pour tous $u, v \in \mathbb{R}^n_{\geqslant 0}$ et $\lambda \in [0,1]$, on a

$$p(\lambda u + (1-\lambda)v) \geqslant p(u)^\lambda \cdot p(v)^{1-\lambda}.$$

Pour un vecteur $v \in \mathbb{R}^n$, on désigne par $D_v$ la dérivée directionnelle par rapport à $v$, c'est-à-dire

$$D_v = \sum_{i=1}^{n} v_i \partial_i,$$

où $\partial_i$ est la dérivée partielle $\partial/\partial z_i$. Un polynôme est dit *complètement log-concave* si pour toute famille de vecteurs $v_1, \dots, v_k \in \mathbb{R}^n_{\geqslant 0}$, le polynôme $D_{v_1} \dots D_{v_k} p$ est positif et log-concave sur $\mathbb{R}^n_{\geqslant 0}$.

***Remarque 2.*** Dans cette définition de polynôme complètement log-concave, il est important de considérer les dérivées directionnelles et pas seulement les dérivées partielles. Par exemple, le polynôme $p(z_1, z_2) = z_1^3 + z_2^3$ a pour dérivées partielles $\partial_1 p = 3z_1^2$ et $\partial_2 p = 3z_2^3$ qui sont tous deux log-concaves, mais la dérivée directionnelle $(\partial_1 + \partial_2)p = 3z_1^2 + 3z_2^2$ n'est pas log-concave. On verra plus loin (théorème 13) qu'avec des hypothèses en plus, les dérivées partielles suffiront.

Une propriété immédiate est la suivante :

***Lemme 6.*** *Si $p(z_1, \dots, z_n)$ est complètement log-concave, pour toute transformation affine $T : \mathbb{R}^m \to \mathbb{R}^n$ telle que $T(\mathbb{R}^m_{\geqslant 0}) \subseteq T(\mathbb{R}^n_{\geqslant 0})$, le polynôme $p \circ T$ est complètement log-concave.*

*Démonstration.* Pour tout $u, v \in \mathbb{R}^m_{\geqslant 0}$ et pour tout $\lambda \in [0, 1]$,

$$p(T(\lambda u + (1-\lambda)v)) = p(\lambda T(u) + (1-\lambda)T(v)) \geqslant p(T(u))^{\lambda} p(T(v))^{1-\lambda},$$

puisque $T(u)$ et $T(v)$ sont dans $\mathbb{R}^n_{\geqslant 0}$ par hypothèse. Cela montre que la log-concavité est préservée sous l'action de $T$.

Ensuite, comme $T$ est affine, $T(x) = Ax + b$ pour une matrice $A \in \mathbb{R}^{n \times m}_{\geqslant 0}$ et un vecteur $b \in \mathbb{R}^n_{\geqslant 0}$. Pour un ensemble de vecteurs $v_1, \dots, v_k \in \mathbb{R}^m_{\geqslant 0}$, on a $Av_1, \dots, Av_k \in \mathbb{R}^n_{\geqslant 0}$ et donc $D_{Av_1} \dots D_{Av_k} p$ est log-concave. On conclut en observant que

$$D_{v_1} \dots D_{v_k}(p \circ T) = (D_{Av_1} \dots D_{Av_k} p) \circ T. \qquad \square$$

En particulier, fixer la valeur d'une inconnue d'un polynôme complètement log-concave à une valeur positive, ou bien projeter plusieurs

inconnues sur une seule, sont deux opérations qui préservent la complète log-concavité. Cette observation, d'apparence inoffensive, va se révéler d'une efficacité redoutable dans ce qui suit.

**3.2. Log-concavité et log-concavité.** Un des résultats qui sous-tend le théorème 1 est le théorème suivant :

***Théorème 7*** **([4, Th. 4.1]).** *Pour tout matroïde $M = (E, \mathcal{I})$ où $E$ est constitué de $n$ éléments, le polynôme*

$$g_M(y, z_1, \ldots, z_n) = \sum_{I \in \mathcal{I}} y^{n-|I|} \prod_{i \in I} z_i$$

*est complètement log-concave.*

Le terme *log-concave* fait écho à la log-concavité des *coefficients* de certains polynômes, comme les polynômes de volumes mixtes explorés dans le texte de Mathieu Piquerez [42]. Récemment, Karim Adiprasito, June Huh et Eric Katz [26, 28, 1] ont montré que le *polynôme caractéristique* (Nous renvoyons au texte d'Omid Amini [3] pour la définition) $\chi_M(\lambda) = \sum a_k \lambda^k$ d'un matroïde a des coefficients log-concaves, c'est-à-dire que ceux-ci satisfont à $|a_{k-1}|\,|a_{k+1}| \leqslant |a_k|^2$ pour tout $1 \leqslant k \leqslant r$. Ce résultat majeur, originellement conjecturé par Read [44] et Hoggar [24] pour les graphes, puis par Rota [45], Heron [23] et Welsh [48] pour les matroïdes, a été cité lors de l'obtention de la médaille Fields par June Huh. Les techniques d'Adiprasito, Huh et Katz s'appliquent aussi à la suite $f_k(M)$ qui dénombre le nombre d'ensemble indépendants de taille $k$ d'un matroïde $M$ :

***Théorème 8*** **([1, Conj. 1.2], corollaire de leur théorème 1.4)**
*La suite $f_k(M)$ est log-concave :*

$$f_{k-1}(M) f_{k+1}(M) \leqslant f_k(M)^2 \text{ pour tout } 1 \leqslant k \leqslant r.$$

Ce théorème prouve une conjecture de Mason [40], qui a même conjecturé que les nombres $f_k(M)$ satisfont une propriété plus forte, appelée *ultra log-concavité* :

$$f_k(M)^2 \geqslant \left(1 + \frac{1}{k}\right) \cdot \left(1 + \frac{1}{n-k}\right) \cdot f_{k-1}(M) \cdot f_{k+1}(M),$$

ou de façon équivalente :

$$\left(\frac{f_k(M)}{\binom{n}{k}}\right)^2 \geqslant \frac{f_{k-1}(M)}{\binom{n}{k-1}} \cdot \frac{f_{k+1}(M)}{\binom{n}{k+1}}.$$

Il n'y a, a priori, aucune raison pour que les propriétés de convexité d'un polynôme, vu en tant que fonction, aient un lien avec d'éventuelles propriétés de convexité de ses coefficients. Pourtant, la proposition suivante, d'abord établie par Gurvits [21], montre une telle coïncidence pour les polynômes complètement log-concaves :

***Proposition 9*** **(**[4, Prop. 5.1] **et** [21, Prop. 2.7]**).** *Si*

$$p(y,z) = \sum_{k=1}^{n} c_k y^{n-k} z^k$$

*est complètement log-concave et $n \geqslant 2$, alors la suite $c_0, \dots, c_n$ est ultra log-concave.*

La preuve ferait peut-être un bon exercice difficile de khôlle.

*Démonstration.* Comme $p$ est complètement log-concave, cela implique que pour tout $k$ tel que $1 < k < n$, le polynôme quadratique $q(y,z) = \partial_y^{n-k-1}\partial_z^{k-1}p$ est log-concave sur $\mathbb{R}^2_{\geqslant 0}$. Un calcul immédiat montre que

$$\partial_y^{n-m}\partial_z^m p = (n-m)!m!c_m = n!c_m/\tbinom{n}{m}.$$

Cela nous permet de calculer que la matrice hessienne de $q$ s'écrit

$$Q := \nabla^2 q = \begin{pmatrix} \partial_y^2 q & \partial_y\partial_z q \\ \partial_y\partial_z q & \partial_z^2 q \end{pmatrix} = n! \begin{pmatrix} c_{k-1}/\binom{n}{k-1} & c_k/\binom{n}{k} \\ c_k/\binom{n}{k} & c_{k+1}/\binom{n}{k+1} \end{pmatrix}.$$

D'un autre côté, comme $q$ est log-concave, la hessienne $\nabla^2 \log q$ est définie négative en tout point de $\mathbb{R}^n_{\geqslant 0}$. On calcule

$$\nabla^2 \log(q) = \frac{q \cdot \nabla^2 q - \nabla q \nabla q^T}{q^2}.$$

Le second terme est une matrice de rang 1, et le théorème d'entrelacement de Cauchy montre donc que les valeurs propres de $\nabla^2 \log(q)$ et celles de $Q$ sont entrelacées. En particulier, $Q$ a au plus une valeur propre positive. D'un autre côté, la forme quadratique $Q$ ne peut pas être définie négative, car pour tout $x \in \mathbb{R}^2_{>0}$, $x^T Q x = 2q(x) > 0$

puisque $p$ et donc $q$ ont des coefficients positifs. Le déterminant de $Q$ est donc négatif. Cela implique immédiatement le résultat. □

Cette preuve montre plus généralement que la matrice hessienne de tout polynôme log-concave de degré au moins deux, évaluée en un point de l'orthant positif, a exactement une valeur propre strictement positive. Nous verrons plus tard une réciproque de cette propriété.

Le théorème 7 implique via le lemme 6 que $g_M(y, z, \ldots, z) = \sum_k f_k(M) y^{n-k} z^k$ est complètement log-concave. Avec cette proposition, on obtient donc directement la conjecture la plus forte de Mason. Cela renforce donc un des résultats phares d'Adiprasito, Huh et Katz [1], obtenu initialement avec des techniques inspirées de la théorie de Hodge. Il y a donc quelque chose de très puissant qui se cache derrière ces polynômes (complètement) log-concaves. De façon encore plus remarquable, la preuve du théorème 7 est suffisamment simple pour être entièrement incluse dans ces notes.

**3.3. Inspiration.** Avant de plonger dans la preuve du théorème 7, il est instructif de prendre un peu de recul pour expliquer d'où viennent ces polynômes log-concaves. L'inspiration première est la classe des *polynômes à racines réelles*, polynômes univariés dont le nom contient la définition.

***Lemme 10.*** *Soit $f$ un polynôme à racines réelles et à coefficients positifs. Alors $f$ est une fonction log-concave de $\mathbb{R}_{\geqslant 0}$.*

*Démonstration.* On néglige le coefficient du monôme de plus haut degré qui n'importe pas. En nommant $\alpha_i$ les racines de $f$, on a alors

$$\log f = \log \prod_{i=1}^{n} (x - \alpha_i) = \sum_{i=1}^{n} \log(x - \alpha_i).$$

Comme les coefficients sont positifs, les racines sont négatives, et donc $\log f$ est une somme de fonctions concaves sur $\mathbb{R}_{\geqslant 0}$ et est ainsi elle-même concave. □

Notez que si un polynôme a des racines réelles, tous ses polynômes dérivés également. Cela découle par exemple du théorème de

Gauss-Lucas, qui place en général les racines complexes d'un polynôme dérivé $p'$ dans l'enveloppe convexe de celles de $p$. On obtient donc également la log-concavité complète. L'articulation entre la log-concavité d'un polynôme et celle de ses coefficients est alors une généralisation très puissante de l'équivalence entre « $ax^2+bx+c$ a une racine réelle » et « $b^2-4ac \geqslant 0$ » (pour $a \neq 0$), où le coefficient 4 est celui qui sort de la propriété d'ultra log-concavité.

Dans le cas général de polynômes à racines réelles, le résultat d'ultra-log-concavité des coefficients, qui découle donc de notre proposition 9 et du lemme 10, constitue les *inégalités de Newton*, qui sont plus généralement exprimées via l'expression des coefficients d'un polynôme comme polynôme élémentaire symétrique de ses racines.

Une première tentative de généraliser les polynômes à racines réelles au cas multivarié est la classe des *polynômes réels stables* (souvent juste appelés *polynômes stables*), qui sont les polynômes réels $p$ tels que pour tout $a \in \mathbb{R}^n_{>0}$ et $b \in \mathbb{R}^n$, le polynôme univarié $p(at+b)$ n'est pas nul et a des racines réelles. Une des motivations de cette généralisation est qu'une méthode très puissante pour montrer qu'un polynôme univarié a des racines réelles est d'en définir une version multivariée et de montrer que celle-ci est réelle stable.

Dans le cas multi-affine, c'est-à-dire lorsqu'une variable n'apparaît jamais avec un degré plus grand que 1 dans un monôme, il y a une connexion frappante entre les polynômes réels stables et la théorie des matroïdes. Le *support* d'un polynôme est l'ensemble des collections d'indices de ses monômes non nuls.

***Théorème 11*** **(Choe, Oxley, Sokal, Wagner** [12, Th. 7.1]**)**
*Le support de tout polynôme réel stable homogène multi-affine est l'ensemble des bases d'un matroïde.*

Cependant, la réciproque n'est pas vraie, par exemple Brändén [9] a montré qu'un certain matroïde appelé matroïde de Fano n'est le support d'aucun polynôme réel stable homogène. Cela a motivé l'introduction des polynômes complètement log-concaves, qui sont une classe strictement plus large, et dont les coefficients satisfont aux mêmes propriétés d'ultra-log-concavité que les polynômes à racines

réelles et les polynômes réels stables, et pour lesquels la réciproque voulue au théorème 11 est vraie : elle est donnée par le théorème 7.

**3.4. Réduction au cas quadratique.** La preuve du théorème 7 repose sur une astucieuse réduction au cas quadratique. On dit qu'un polynôme $p$ est *indécomposable* si on ne peut pas l'écrire comme une somme $p = p_1 + p_2$ où $p_1$ et $p_2$ sont des polynômes non nuls ayant des ensembles de variables disjoints.

***Lemme 12.*** *Un polynôme log-concave de degré au moins* 2 *est indécomposable.*

*Démonstration.* Supposons par l'absurde que $p$ log-concave s'écrit $p = p_1 + p_2$ avec $p_1$ et $p_2$ non nuls et ayant des variables disjointes. La matrice hessienne de $p$ s'écrit

$$\nabla^2 p = \begin{pmatrix} \nabla^2 p_1 & 0 \\ 0 & \nabla^2 p_2 \end{pmatrix}.$$

Puisque $p_1$ et $p_2$ peuvent être obtenus de $p$ en mettant certaines variables à zéro, ils sont tous les deux log-concaves par le lemme 6, et donc leurs hessiennes ont chacune une valeur propre strictement positive. Donc la hessienne de $p$ en a au moins deux, ce qui contredit la log-concavité (cf. la preuve de la proposition 9). □

Réciproquement, le résultat de réduction quadratique suivant montre que l'indécomposabilité permet de réduire la log-concavité complète au cas quadratique. Pour un vecteur $\alpha \in \{1, \ldots, n\}^k$, on écrit $\partial^\alpha$ pour $\partial_{\alpha_1} \circ \cdots \circ \partial_{\alpha_k}$.

***Théorème 13.*** *Soit $p$ un polynôme homogène à coefficients positifs de degré $d \geqslant 2$. Le polynôme $p$ est complètement log-concave si et seulement si les deux conditions suivantes sont satisfaites :*

(1) *Pour tout $\alpha \in \mathbb{Z}^n_{\geqslant 0}$, avec $|\alpha| \leqslant d-2$, le polynôme $\partial^\alpha p$ est indécomposable.*

(2) *Pour tout $\alpha \in \mathbb{Z}^n_{\geqslant 0}$, avec $|\alpha| = d-2$, le polynôme quadratique $\partial^\alpha p$ est log-concave.*

On commence par établir quelques lemmes. Le premier est la réciproque d'une observation précédente qui montre que la propriété

d'avoir une matrice hessienne ayant exactement une valeur propre positive caractérise les polynômes log-concaves.

***Lemme 14.*** *Si $p$ est un polynôme homogène à coefficients positifs à $n$ variables et de degré $d \geqslant 2$, et $a \in \mathbb{R}^n_{\geqslant 0}$, alors si $\nabla^2 p_{|z=a}$ a exactement une valeur propre strictement positive, $p$ est log-concave en $a$.*

*Démonstration.* Comme précédemment, on calcule

$$\nabla^2 \log(p) = \frac{p \cdot \nabla^2 p - \nabla p \nabla p^T}{p^2}.$$

L'une des nombreuses identités d'Euler est que pour un polynôme homogène de degré $d$, on a $dp(z_1, \dots, z_n) = \sum_i z_i \partial_i p(z_1, \dots, z_n)$. On a donc, en notant $P := \nabla^2 p_{|z=a}$, que $Pa = (d-1)\nabla p(a)$ et $a^T Pa = d(d-1) \cdot p(a)$. Ainsi,

$$\nabla^2 \log(p) = d(d-1) \frac{a^T Pa \cdot P - \frac{d}{d-1}(Pa)(Pa)^T}{(a^T Pa)^2}.$$

Il s'agit donc d'étudier les valeurs propres de $a^T Pa \cdot P - \frac{d}{d-1}(Pa)(Pa)^T$. On commence par étudier celles de $a^T Pa \cdot P - (Pa)(Pa)^T$. Pour ce faire, prenons $x$ dans $\mathbb{R}^n$. Par hypothèse, $P$ est une forme quadratique qui est négative sur un espace vectoriel de dimension $n-1$ qu'on appelle $L$.

- Si $x$ est colinéaire à $a$,

$$x^T(a^T Pa \cdot P - (Pa)(Pa)^T)x = a^T Pa x^T Px - x^T Paa^T Px = 0.$$

- Sinon, une combinaison linéaire $y$ de $x$ et de $a$ intersecte $L$. On considère la forme quadratique induite par $P$ dans le sous-espace engendré par $x$ et $a$ : elle n'est pas négative parce que $a^T Pa > 0$, mais elle n'est pas positive non plus puisque $y^T Py \leqslant 0$. Donc son déterminant est négatif, et par suite

$$x^T(a^T Pa \cdot P - (Pa)(Pa)^T)x = a^T Pa x^T Px - x^T Paa^T Px \leqslant 0.$$

Ainsi, la forme quadratique associée à $a^T Pa \cdot P - (Pa)(Pa)^T$ est négative. C'est encore le cas lorsqu'on soustrait $\frac{1}{d-1}(Pa)(Pa)^T$, ce qui conclut la preuve. □

***Remarque 3.*** Cette propriété justifie l'appellation de *polynôme lorentzien* utilisée par Brändén et Huh [10], qui est équivalente à notre notion de polynôme complètement log-concave. En effet, la signature de la hessienne d'un polynôme log-concave à coefficients positifs est $(+,-,\dots,-)$, et de telles signatures sont appelées *lorentziennes* de par leur usage en théorie de la relativité générale.

Cette propriété d'avoir exactement une valeur propre strictement positive est une incarnation combinatoire des relations de Hodge-Riemann en degrés $q \leqslant 1$, qui fournissent de manière similaire des formes bilinéaires ayant exactement une valeur propre strictement positive. Comme illustré dans les textes d'Omid Amini [3] et de Mathieu Piquerez [42], les applications combinatoires de ces relations de Hodge-Riemann découlant généralement de ce cas particulier de bas degré (voir par exemple l'article de survol de June Huh [27]), les polynômes complètement log-concaves (ou lorentziens) permettent ainsi d'extraire le sel combinatoire de ces constructions algébriques.

Bien qu'immédiate, la propriété suivante est la clé qui différencie les polynômes log-concaves des polynômes réels stables, qui n'ont pas d'analogue.

***Lemme 15.*** *Pour un polynôme $p$ homogène de degré $d \geqslant 3$, $p$ est log-concave en $z = a$ si et seulement si $D_a p$ est log-concave en $z = a$*

*Démonstration.* Cela découle immédiatement de la même identité d'Euler que celle utilisée dans le lemme précédent, stipulant que que $dp(z_1,\dots,z_n) = \sum_i z_i \partial_i p(z_1,\dots,z_n)$. □

Un dernier lemme permet d'additionner des polynômes log-concaves sous certaines conditions.

***Lemme 16.*** *Si $p_1$ et $p_2$ sont homogènes, à coefficients positifs, complètement log-concaves et s'il existe $b, c \in \mathbb{R}^n_{\geqslant 0}$ tels que $D_b p_1 = D_c p_2 \neq 0$, alors $p_1 + p_2$ est complètement log-concave.*

*Démonstration.* Par le lemme 14, il suffit de vérifier que la hessienne $\nabla^2(p_1 + p_2)_{|z=a}$ a exactement une valeur propre positive pour tout $a \in \mathbb{R}^n_{\geqslant 0}$. On note comme avant $P_1 = \nabla^2(p_1)_{|z=a}$ et $P_2 = \nabla^2(p_2)_{|z=a}$.

Comme $D_b p_1 = D_c p_2$, $p_1$ et $p_2$ ont le même degré, et on a $P_1 b = P_2 c$ puisque pour tout $i = 1, \dots, n$,

$$(P_1 b)_i = (\partial_i D_b p_1)_{|z=a} = (\partial_i D_c p_2)_{|z=a} = (P_2 b)_i.$$

Comme $D_b p_1 = D_c p_2 \neq 0$, $P_1 b = P_2 c$ sont non nuls et ont des coefficients positifs puisque c'est le cas pour $p_1$, $p_2$, $b$ et $c$. Donc $P_1$ et $P_2$ sont toutes deux des formes quadratiques négatives sur $(P_1 b)^\perp = (P_2 c)^\perp$ qui sont des sous-espaces de dimension $n-1$. Il en résulte que $P_1 + P_2$ est également une forme quadratique négative sur un espace de dimension $n-1$, ce qui conclut. □

Nous avons maintenant tous les éléments pour prouver le théorème 13. L'idée est de descendre en degré via le lemme 15. Pour cela, il faut montrer que les dérivées directionnelles $D_a p$ sont log-concaves si les dérivées directionnelles $\partial_i p$ le sont. Cela sera garanti par le lemme 16, l'indécomposabilité et l'identité $\partial_i \partial_j = \partial_j \partial_i$.

*Démonstration du théorème* 13. Le théorème se prouve par récurrence sur le degré $d$. Pour $d = 2$, il n'y a rien à faire, ce qui fait la base de la récurrence. On suppose ensuite que le théorème est vrai pour tous les polynômes de degré $d-1$. Prenons un polynôme $p$ homogène de degré $d \geqslant 3$ satisfaisant les hypothèses du théorème, et regardons $D_{v_1} \cdots D_{v_k} p$ pour tous $v_1, \dots, v_k \in \mathbb{R}^k_{\geqslant 0}$ et $0 \leqslant k \leqslant d-2$. Si $k = 0$, par le lemme 15, $p$ est log-concave en $a$ si et seulement si $D_a p$ l'est, donc on ramène le cas $k = 0$ au cas $k = 1$.

Remarquons ensuite qu'une façon équivalente d'exprimer l'indécomposabilité d'un polynôme $p$ est que le graphe où les sommets sont les $i$ tels que $\partial_i p \neq 0$ et les arêtes sont les $i, j$ tels que $\partial_i \partial_j p \neq 0$ est connexe. Par indécomposabilité, on peut donc supposer, quitte à renuméroter, que pour tout $i$, $\partial_i p \neq 0$ (quitte à jeter les variables pour lesquelles la dérivées est nulle), et que pour tout $j \geqslant 2$, il existe $i < j$, tel que $\partial_j \partial_i p \neq 0$. De plus, $f := D_{v_1} \dots D_{v_{k-1}} p$ est indécomposable d'après la première hypothèse du théorème, l'indécomposabilité passant sans problème aux dérivées directionnelles.

On peut maintenant appliquer l'astuce mentionnée juste avant la preuve. Les notations sont un peu lourdes donc nous la montrons juste pour l'exemple $v_k = (1, 1, 0, \dots, 0)$, le cas général étant le même

argument appliqué inductivement. On a $D_{v_k} f = \partial_1 f + \partial_2 f$, et $\partial_1 f$ et $\partial_2 f$ sont log-concaves par récurrence. Par indécomposabilité de $f$, $\partial_1 \partial_2 f = \partial_2 \partial_1 f \neq 0$. Le lemme 16 permet alors de conclure que $p = D_{v_k} f$ est donc log-concave. □

**3.5. Le cas quadratique.** Le théorème 13 nous permettant de réduire l'analyse au cas des polynômes quadratiques. Ensuite, le premier cas à considérer est celui des matroïdes de rang 2, qui constitue le cas de base de la preuve du théorème 7.

***Proposition 17.*** *Soit $M$ un matroïde de rang 2. Alors le polynôme quadratique*

$$g_M(y, z_1, \ldots, z_n) = \sum_{I \in \mathcal{I}} y^{2-|I|} \prod_{i \in I} z_i$$

*est complètement log-concave.*

*Démonstration.* Les matroïdes de rang 2 sont très simples. On peut supposer que chaque ensemble de taille 1 est indépendant, quitte à retirer les éléments non indépendants par eux-mêmes. Ensuite, les ensembles indépendants sont soit l'ensemble vide, soit les ensembles de taille 1, soit certains ensembles de taille 2. Si on considère comme équivalents deux éléments $i$ et $j$ si $\{i, j\}$ n'est *pas* indépendant (intuitivement ils correspondent à des vecteurs colinéaires), on peut partitionner l'ensemble des éléments via ces classes d'équivalence, et on voit facilement que les ensembles indépendants de taille 2 sont exactement ceux contenant deux éléments dans deux classes d'équivalence distinctes.

Définissons une matrice $B$ telle que $B_{ij} = 1$ si $i$ et $j$ ne sont pas équivalents et 0 sinon. La matrice $B$ s'écrit par blocs

$$B = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \ldots & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \ldots & \mathbf{1} \\ & & \ddots & \mathbf{1} \\ \mathbf{1} & \ldots & \mathbf{1} & \mathbf{0} \end{pmatrix} = \mathbf{1} - \begin{pmatrix} \mathbf{1} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \ldots & \mathbf{0} \\ & & \ddots & \mathbf{0} \\ \mathbf{0} & \ldots & \mathbf{0} & \mathbf{1} \end{pmatrix},$$

où $\mathbf{1}$ et $\mathbf{0}$ sont respectivement des (sous-)matrices remplies de 1 et de 0.

La matrice hessienne de $g_M$ est alors

$$Q := \nabla^2 g_M = \begin{pmatrix} n(n-1) & (n-1)\mathbf{1} \\ (n-1)\mathbf{1} & B \end{pmatrix}.$$

Si on note $a$ le vecteur $(1, 0, \dots, 0)$, on vérifie facilement l'inégalité $a^T Q a > 0$. On va montrer la log-concavité de $g_M$ en $a$, ce qui implique la log-concavité dans tout l'orthant positif parce que la hessienne ne dépend pas de $a$. Par le même calcul que dans la preuve du lemme 14, cela revient à montrer que $Q' = a^T Q a \cdot Q - (Qa)(Qa)^T$ est négative. On obtient

$$Q'_{|a^\perp} = (n-1)(nB-(n-1)\mathbf{1}) = (n-1)\cdot \left( \mathbf{1} - n \begin{pmatrix} \mathbf{1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \dots & \mathbf{0} \\ & & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{1} \end{pmatrix} \right).$$

Or, pour tout vecteur $x$,

$$\begin{aligned} Q'_{|a^\perp}(x) &= (n-1)\Big( \sum_i x_i^2 - n \sum_i \Big( \sum_{j \in P_i} x_j \Big)^2 \Big) \\ &= (n-1)\Big( \sum_i \sum_{j \in P_i} x_j^2 - n \sum_i \Big( \sum_{j \in P_i} x_j \Big)^2 \Big) \leqslant 0, \end{aligned}$$

en utilisant Cauchy-Schwarz et le fait qu'il y a au plus $n$ blocs dans $B$. □

On peut maintenant conclure la preuve du théorème 7

*Démonstration du théorème* 7. Par le théorème 13, il suffit de tester l'indécomposabilité de tous les polynômes $\partial^\alpha g_M$ pour $|\alpha| \leqslant d-2$ et la log-concavité des polynômes $\partial^\alpha g_M$ pour $|\alpha| = d-2$. On décompose $\alpha = \alpha_1 + \alpha_2$ où $\partial^{\alpha_2} = \partial_y^k$. Ensuite, si $\alpha_1$ contient le même indice plusieurs fois, le polynôme est nul, donc on peut considérer que $\alpha_1$ est la fonction indicatrice d'un ensemble $J$. De manière similaire, si $J$ n'est pas un ensemble indépendant, $\partial^{\alpha_1}$ est nul, et on voit alors que $\partial^{\alpha_1} g_M$ est exactement le polynôme $g_{M/J}$ du matroïde où l'on a contracté $J$. Par les bornes sur les tailles des $\alpha$, les matroïdes $M/J$ sont de rang au moins 2, et donc le variable $y$ apparaît dans un

monôme avec tous les éléments de $M/J$ qui ne sont pas des boucles. Cela prouve l'indécomposabilité.

La log-concavité des polynômes $\partial^\alpha g_M$ pour $|\alpha| = d-2$ découle alors du fait que qu'il s'agit des polynômes $g'_M$ pour des matroïdes $M' = M \setminus J$ où l'on a tronqué la taille des ensembles indépendants pour qu'il soient de taille au plus 2. Ce sont donc des matroïdes de rang 2, et la proposition 17 permet de conclure. □

## 4. Complexes simpliciaux et théorème local-global pour l'expansion en grande dimension

Revenons maintenant au problème de compter les bases de matroïdes, que nous avons réduit au problème de borner la seconde valeur propre (en valeur absolue) de la marche aléatoire d'échange de bases. Nous commençons par un exemple pour illustrer l'application des polynômes log-concaves à ce problème.

**4.1. Un exemple illustratif.** Considérons le polynôme symétrique $p = \sum_{1 \leqslant i < j \leqslant 4} x_i x_j$, qui est le polynôme des bases d'un matroïde sur 4 éléments où tous les ensembles de deux éléments distincts sont des bases. La marche d'échange des bases sur ce matroïde considère une base, en retire un élément puis en remet un. Elle commence donc par « descendre » dans le matroïde avant de « remonter », et on l'appelle marche *bas-haut*. De manière similaire, on peut définir une marche *haut-bas* qui part d'un ensemble indépendant de taille 1, ajoute un élément puis en retire un pour revenir à une taille 1. Cette marche haut-bas a pour matrice de transition

$$M = \begin{pmatrix} 1/2 & 1/6 & 1/6 & 1/6 \\ 1/6 & 1/2 & 1/6 & 1/6 \\ 1/6 & 1/6 & 1/2 & 1/6 \\ 1/6 & 1/6 & 1/6 & 1/2 \end{pmatrix}.$$

En effet, partant d'un élément $i$, la probabilité de monter à $ij$ est de $1/3$ pour chaque $j \neq i$, puis celle de redescendre à $j$ est de $1/2$. La probabilité de rester en $i$ au final est de $3 \cdot 1/3 \cdot 1/2 = 1/2$.

Comparons cette matrice avec la matrice hessienne de $p$, qui est

$$P = \nabla^2 p = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

On observe que $M = \mathrm{Id}\,/2 + 1/2(P/3)$. La marche haut-bas est donc exactement celle obtenue lorsqu'on rend paresseuse (cf. section 2.2) la matrice de transition associée à $\nabla^2 p/3$. Et la propriété de log-concavité de $p$ a le versant spectral suivant sur $M$ : comme $p$ est log-concave, $P$ a exactement une valeur propre positive, et donc c'est aussi le cas pour $P/3$. Il s'ensuit que la seconde valeur propre de $M = \mathrm{Id}\,/2 + 1/2(P/3)$ a pour valeur au plus $1/2$. Le trou spectral est donc constant, et la marche est paresseuse, et ainsi la marche aléatoire se mélange très vite.

La matrice $M$ étant la matrice de la marche haut-bas, elle peut s'écrire $M = 1/6 \cdot AA^T$ où la matrice $A$, de taille $4 \times 6$, est la matrice

$$A_{i,jk} = \begin{cases} 1 & \text{si } i \in \{j,k\}, \\ 0 & \text{sinon.} \end{cases}$$

C'est la marche bas-haut qui nous intéresse, et non la marche haut-bas. Mais il est facile de voir que celle-ci s'écrit $M' = 1/6 \cdot A^T A$. Elle a donc les mêmes valeurs propres que $M$, et donc le même trou spectral (absolu) ! Nous voyons bien ici comment la propriété de log-concavité intervient pour obtenir un mélange rapide de la marche d'échange des bases.

**4.2. Complexes simpliciaux.** Cet exemple ne se généralise pas facilement aux matroïdes de rang supérieur. En effet, en général la matrice hessienne du polynômes des bases d'un matroïde ne contrôle pas la marche d'échange des bases, mais seulement une version *locale* : en considérant un ensemble indépendant $S$ du matroïde, la matrice hessienne de la dérivée $\partial^S g_M$ décrit (à un changement d'échelle près) une marche aléatoire consistant à rajouter et à enlever des éléments à un ensemble indépendant qui contient $S$. L'ingrédient manquant est donc une façon de recoller l'expansion de ces marches locales pour

obtenir une borne sur la marche globale. Il se trouve que l'étude de telles propriétés locales-globales d'expansion, qui généralisent de façon très subtile les propriétés d'expansion dans les graphes que nous avons esquissées dans au paragraphe 2.2, a été l'objet d'une très forte attention dans les quinze dernières années, et nous renvoyons à l'article de survol de Lubotzky [39] pour un aperçu (déjà un peu daté) du sujet. Cela fait appel à des techniques venant de l'étude des *expanseurs en grande dimension*, dont nous commençons par introduire le langage.

Un *complexe simplicial* $\Delta$ est un ensemble de sous-ensembles de $\{1,\dots,n\}$, stable par inclusion, c'est-à-dire que si $T$ est un élément de $\Delta$, tous ses sous-ensembles $S \subseteq T$ sont également dans $\Delta$. Il est *pur* de dimension $d-1$ si tous les sous-ensembles maximaux sont de taille $d$. Il est immédiat de voir que les ensembles indépendants d'un matroïde forment un complexe simplicial de dimension $r-1$, où $r$ est le rang. Pour un complexe simplicial $\Delta$, on note $\Delta(k)$ l'ensemble des *simplexes* de dimension $k-1$ : $\Delta(k) = \{S \in \Delta \mid |S| = k\}$, et pour tout $S \in \Delta$, on définit un autre complexe, le *lien* $\mathrm{link}_S(\Delta)$ qui correspond aux différentes façons de compléter un ensemble $S$ en restant dans $\Delta$, c'est-à-dire $\mathrm{link}_S(\Delta) := \{T \subseteq \{1,\dots,n\} \subseteq S \mid S \cup T \in \Delta\}$. Si l'on associe des poids $w(S)$ à chaque simplexe de dimension maximale $d$, qui représentent des probabilités, ces poids descendent récursivement aux dimensions inférieures en définissant pour $S \in \Delta(k)$, $w(S) = \sum_{S\subseteq T,|T|=k+1} w(T)$. On utilisera toujours, par la suite, des poids uniformes sur les simplexes de dimension maximale, qui représentent donc notre quête d'échantillonner de façon uniforme les bases d'un matroïde.

On peut maintenant associer un polynôme à tout complexe simplicial $\Delta$, pur de dimension $d$, avec des poids $w$ :

$$(\Delta, w) \longmapsto p = \sum_{T\in\Delta(d)} w(T) z^T.$$

Le complexe $\mathrm{link}_S(\Delta)$ a alors pour polynôme

$$(\mathrm{link}_S(\Delta), w) \longmapsto p = \sum_{\substack{T\in\Delta(d)\\ S\subseteq T}} w(T) z^{T\setminus S} = \partial^S f.$$

Dans ce langage, la marche d'échange de bases est la marche bas-haut qui part d'un simplexe de $\Delta(d)$ (où $d = \text{rang} - 1$), retire un élément au hasard pour arriver à un simplexe de $\Delta(d-1)$ puis en rajoute un au hasard (potentiellement le même) pour remonter à $\Delta(d-1)$. La formule définissant les poids récursivement a été spécifiquement conçue pour que les probabilités d'ajout et de soustraction soient gouvernées par les poids $w$. De manière similaire, on peut définir la marche *haut-bas* qui part de $\Delta(d-1)$, ajoute un élément puis en retire un pour revenir à $\Delta(d-1)$, et même définir de telles marches haut-bas et bas-haut pour pour chaque ensemble $\Delta(k)$ de simplexes de dimension $k$.

**4.3. Théorème local-global.** On veut maintenant démontrer le théorème suivant, où l'on choisira un ensemble de poids uniforme sur les simplexes de dimension maximale.

***Théorème 18.*** *Si $p = \sum_{T\in\Delta(d)} w(T)z^T$ est complètement log-concave, la matrice de transition pour la marche* bas-haut *de $\Delta(d)$ satisfait $\lambda_* = \max(\lambda_2, \lambda_n) \leqslant 1 - 1/d$.*

De façon concomitante aux travaux de [5], Kaufman et Oppenheim [33] ont démontré le théorème suivant qui fournit miraculeusement la pièce manquante du puzzle. On dit que $(\Delta, w)$ est un *expanseur spectral* $\lambda$-local si $\lambda_2(P_S) \leqslant \lambda$ pour tout $S \in \Delta$, où $P_S$ est la matrice définie par

$$(P_S)_{i,j} = \frac{w(S \cup i \cup j)}{w(S \cup i)} \quad \text{pour } i, j \notin S.$$

***Théorème 19*** **(Kaufman, Oppenheim** [33, Th. 1.4]**)**

*Si $(\Delta, w)$ est un expanseur spectral $\lambda$-local, alors la matrice de transition pour la marche bas-haut sur $\Delta(d)$ satisfait à :*

$$\lambda_* \leqslant 1 - \Big(\frac{1}{d} - \frac{d-1}{2}\lambda\Big).$$

Une force de ce théorème est qu'il permet d'analyser la marche aléatoire d'échanges de bases, qui est potentiellement très complexe, impliquant jusqu'à $n^r$ éléments et explorant tout le matroïde, en terme de marche aléatoires locales dans le voisinage de chaque

ensemble indépendant : en particulier la matrice $P_S$ n'a que $n^2$ entrées.

La proposition suivante permet alors de recoller tous les morceaux.

***Proposition 20.*** *Si $p = \sum_{T\in\Delta(d)} w(T)z^T$ est complètement log-concave, alors $(\Delta, w)$ est un expanseur spectral* 0*-local.*

*Démonstration.* Il suffit d'observer que $P_S$ est la matrice hessienne de $\partial^S p$ évaluée en $z = \mathbf{1}$, modulo la multiplication par une matrice diagonale à coefficients positifs pour rendre cette dernière stochastique. Par log-concavité de $p$, $P_S$ a donc exactement une valeur propre positive, ce qui est maintenu par la multiplication par une matrice diagonale à coefficients positifs, et donc $(\Delta, w)$ est bien un expanseur spectral 0-local. □

La réciproque de cette proposition est également vraie, nous renvoyons à [5] pour la preuve. On peut maintenant conclure.

*Démonstration du théorème* 1. Pour un système de poids uniforme sur $\Delta(d)$, le théorème 7 montre que le polynôme $p = \sum_{T\in\Delta(d)} z^T = \sum_{B\in\mathcal{B}(M)} \prod_{i\in B} z^i$ est complètement log-concave, et donc on peut appliquer la proposition 20 et le théorème 19 pour borner la seconde valeur propre de la marche d'échange des bases. La marche d'échange des bases est symétrique et connexe donc par la proposition 5, cela donne un algorithme efficace pour échantillonner uniformément des bases de matroïde. Avec le théorème 2 qui utilise cette échantillonnage pour compter les bases, nous obtenons enfin la preuve du théorème 1. □

***Remarque 4.*** La propriété lorentzienne des polynômes log-concaves ne donne a priori qu'un contrôle sur le trou spectral des marches $P_S$, et pas sur le trou spectral absolu. Mais comme illustré dans l'exemple, il se trouve que la marche d'échange des bases est naturellement paresseuse. De façon remarquable, le théorème 19 montre que les valeurs propres négatives des $P_S$ ne sont pas un obstacle pour trouver une borne sur le trou spectral absolu de la marche globale.

La preuve du théorème 19 n'est pas très difficile mais nous ne la détaillerons pas dans ces notes et renvoyons à [33] ou à [5, § 4] où le théorème est reprouvé. L'idée est que pour passer des marches locales indiquées par les $P_S$ à la marche globale que l'on veut contrôler, on procédera par récurrence en montant de dimension progressivement. Le cas de base de la récurrence est similaire à celui de l'exemple. Ensuite, on combinera deux outils. Le premier est la même observation que celle que nous avons faite dans l'exemple introductif : la marche haut-bas sur $\Delta(k)$ et la marche bas-haut sur $\Delta(k-1)$ ont les mêmes valeurs propres. L'autre outil est que la propriété d'expansion spectrale 0-locale permet de relier les valeurs propres de la marche bas-haut sur $\Delta(k)$ à celles de la marche haut-bas sur $\Delta(k)$. La combinaison de ses deux outils permet d'arriver à la conclusion sur la marche bas-haut des simplexes de dimension maximale et de conclure.

Pour un matroïde sur $n$ éléments et de rang $r$, l'algorithme d'échantillonnage utilise une marche aléatoire en $O(r\log(n^r/\varepsilon)) = O(r^2\log(n/\varepsilon))$ étapes. Peu après [5], une analyse plus fine a été proposée par Cryan, Guo et Mousa [13], puis dans le quatrième papier de la série sur les polynômes log-concaves [8], où les auteurs ont établi une borne $O(r\log(r/\varepsilon))$ qui est optimale. Notons que chaque étape de la marche aléatoire requiert d'échantillonner parmi les $n$ éléments du matroïde, donc la complexité de l'algorithme d'échantillonnage qui en résulte est $O(nr\log(r/\varepsilon))$.

***Remarque 5.*** Comme on l'a vu tout au long de ce texte, la possibilité de pouvoir prendre des dérivées (directionnelles ou non) et de conserver la log-concavité est cruciale pour la théorie. Cependant, lorsqu'on considère des polynômes multi-affines, comme c'est le cas par exemple pour le polynôme des bases de matroïde, la complète log-concavité est une conséquence gratuite de la log-concavité. En effet, pour $p$ multi-affine et log-concave, on peut considérer $\lim_{\lambda\to\infty}\frac{1}{\lambda}p(\lambda z_1,\dots,z_n) = z_1\partial_1 p$ qui est log-concave (c'est une propriété fermée), et comme $p$ est multi-affine le terme $\partial_1 p$ n'a pas de variable en $z_1$. Pour que le produit de deux polynômes à variables disjointes soit log-concave, il faut que les deux polynômes le soient, et donc $\partial_1 p$ est log-concave.

On obtient ainsi immédiatement la log-concavité de toutes les dérivées partielles, et donc la complète log-concavité via le théorème 13.

***Remarque 6.*** La complète log-concavité des polynômes peut être généralisée de multiples façons pour capturer encore plus de phénomènes combinatoires. Une de ces généralisations est de considérer une log-concavité fractionnaire : on demande alors qu'il existe un $\alpha \in ]0,1]$ tel que la fonction $(z_1,\dots,z_n) \mapsto p(z_1^\alpha,\dots,z_n^\alpha)$ soit complètement log-concave. Cette généralisation a été mise à profit dans [2] pour obtenir des algorithmes de comptage approximés pour une classe encore plus large de problème. Une autre généralisation importante est obtenue en ne considérant la propriété de log-concavité que sur un cône $\mathcal{C}$ plus petit que l'orthant positif. La notion obtenue de polynômes $\mathcal{C}$-lorentziens a ainsi permis à Brändén et Leake [11] d'obtenir une nouvelle preuve de la log-concavité du polynôme chromatique des matroïdes, et a aussi mené à de nouveaux résultats sur l'expansion en grande dimension et l'échantillonnage [37]

## 5. Aparté : algorithmes de comptage exacts et permanent

Nous avons atteint notre objectif principal, mais en guise de conclusion nous proposons un aparté sur un autre aspect des algorithmes de comptage, où les polynômes log-concaves vont également nous être utiles. Comme on l'a vu, l'existence et l'efficacité de tels algorithmes de comptage sont intimement liés au problème d'échantillonner des éléments efficacement. De tels algorithmes d'échantillonnage sont, par essence, randomisés. Mais il n'y a pas de raison, a priori, pour que les algorithmes de comptage le soient, et on peut légitimement se demander s'il existe des algorithmes *déterministes* qui seraient tout aussi efficaces, par exemple pour notre problème de compter les bases de matroïdes. De façon plus générale, la question de l'utilisation du hasard et de quels algorithmes peuvent être dérandomisés, est une question centrale en informatique théorique. De façon étonnante, il y a désormais de bonnes raisons de penser que tous les algorithmes peuvent être dérandomisés, mais ce n'est à ce stade qu'une conjecture. Le livre récent d'Avi Wigderson [50] propose une introduction très accessible à ces problématiques.

Nous allons dans cette section nous intéresser à l'existence d'algorithmes déterministes pour un problème très proche de celui de compter les bases d'un matroïde. Notre objet d'étude principal est le *permanent* d'une matrice, qui est défini comme un déterminant mais sans les signes négatifs :

$$\mathrm{per}(A) = \sum_{\sigma \in S_n} \prod_i A_{i,\sigma(i)}.$$

Il ne faut pas se laisser tromper par la similitude apparente avec le déterminant. Le déterminant est un objet de nature géométrique (c'est un volume), qui s'appréhende très bien sous différents aspects et en particulier peut être calculé très efficacement par élimination gaussienne[(6)]. Le permanent, en revanche, ne s'interprète pas bien géométriquement, et son calcul est très difficile : même lorsque les entrées de $A$ sont 0 ou 1, calculer le permanent est $\#P$-complet [47], ce qui signifie qu'on ne peut pas, modulo les hypothèses classiques de la théorie de la complexité, le calculer en temps polynomial. Le meilleur algorithme connu, dû à Ryser [46], requiert $O(2^n n)$ opérations arithmétiques.

Nous avons déjà rencontré ce permanent de façon déguisée. Si l'on considère un graphe biparti $G = (V, U, E)$ où $|V| = |U|$, et sa matrice d'incidence $I_G$ dont l'entrée $ij$ est 1 si et seulement s'il y a une arête entre $v_i$ et $u_j$, le permanent $\mathrm{per}(I_G)$ compte toutes les bijections entre $V$ et $U$ réalisées par des arêtes, c'est-à-dire tous les couplages parfaits du graphe $G$. Ainsi, calculer un permanent revient à compter le nombre de bases dans l'intersection des deux matroïdes de partition $M_V$ et $M_U$. En général, les techniques du théorème 1 ne s'appliquent pas pour le problème d'intersection de bases qui est plus délicat que celui de compter les bases d'un seul matroïde, mais dans le cas particulier des couplages parfaits, un article célèbre de

(6) Le nombre d'opérations arithmétiques effectuées pendant une élimination gaussienne est clairement polynomial, mais une subtilité peu connue est que la taille des rationnels impliqués dans le calcul peut facilement exploser. Pour éviter cette explosion, il faut avoir recours à des techniques plus précises, voir par exemple l'algorithme de Bareiss [18, § 5.5].

Jerrum, Sinclair et Vigoda [30] fournit un analogue au théorème 1, c'est-à-dire un FPRAS pour le calcul du permanent.

Les algorithmes déterministes pour approximer le permanent sont considérablement moins bons : les meilleurs connus ne fournissent que des bornes d'approximation exponentielles. L'objectif de cette section est de démontrer le théorème suivant, et les polynômes log-concaves feront encore une apparition dans sa preuve.

***Théorème 21.*** *Pour une matrice $A$ de taille $n \times n$ et à entrées positives, il existe un algorithme polynomial qui calcule une $e^n$-approximation du permanent* $\mathrm{per}(A)$*, c'est-à-dire une quantité $P$ telle que*

$$P \cdot e^{-n} \leqslant \mathrm{per}(A) \leqslant P.$$

Ce théorème n'est pas le meilleur connu, l'état de l'art permettant une approximation à un facteur $(\sqrt{2})^n$ [7, 22], ce qui est également exponentiel. Trouver des algorithmes déterministes qui rivalisent avec les algorithmes randomisés pour approximer le permanent est l'un des problèmes ouverts les plus fondamentaux du domaine de la dérandomisation.

L'algorithme derrière le théorème 21 provient du théorème suivant, originellement formulé pour les polynômes stables et dû à Gurvits [20].

***Théorème 22.*** *Soit $p(z_1, \ldots, z_n)$ un polynôme complètement log-concave à coefficients positifs. Alors*

$$e^{-n} \inf_{z>0} \frac{p(z_1, \ldots, z_n)}{z_1 \ldots z_n} \leqslant \partial_1 \ldots \partial_n p_{|z=0} \leqslant \inf_{z>0} \frac{p(z_1, \ldots, z_n)}{z_1 \ldots z_n}.$$

L'intérêt algorithmique de ce problème est que la quantité

$$\inf_{z>0} \frac{p(z_1, \ldots, z_n)}{z_1 \cdots z_n},$$

appelée *capacité* de $p$, peut être calculée rapidement. En effet, on commence par effectuer un changement de variable $z_i = e^{y_i}$, qui est valide puisque $z > 0$, et le quotient s'écrit alors $p(e^{y_1}, \ldots, e^{y_n})/e^{y_1} \ldots e^{y_n}$.

Pour minimiser le quotient, on peut aussi bien minimiser son logarithme et il s'agit donc de minimiser

$$\log p(e^{y_1}, \dots, e^{y_n}) - \sum_i y_i.$$

C'est une fonction facile à minimiser parce qu'elle est convexe : c'est évident pour les $y_i$ qui sont des fonctions linéaires, mais également facile à voir pour le premier terme car la fonction log-sum-exp

$$(y_1, \dots, y_n) \longmapsto \log \sum_i a_i e^{\langle b_i, y_i \rangle}$$

est convexe pour des $a_i$ positifs.

Pour relier le théorème 22 au calcul du permanent, on considère le polynôme

$$p(z) = \prod_{i=1}^{n} \sum_{j=1}^{n} A_{i,j} z_j.$$

C'est un produit de polynômes complètement log-concaves (des formes linéaires à coefficients positifs). Un tel produit est toujours complètement log-concave, mais le prouver requiert un peu de travail sur les dérivées directionnelles. Cependant, dans ce cas précis, on peut utiliser le tour de passe-passe suivant : on commence par considérer le produit comme si les variables étaient disjointes. Le polynôme que l'on obtient étant multi-affine, il est complètement log-concave car il est log-concave (cf. remarque 5). On peut ensuite spécifier les variables comme il faut en préservant la log-concavité complète de par le lemme 6.

On observe alors que

$$\partial_1 \dots \partial_n p_{|z=0} = \mathrm{per}(A),$$

et donc le théorème 22 implique directement le théorème 21.

Avant de le démontrer, observons que le théorème 22 implique également immédiatement le résultat suivant, qui est une conjecture classique de van der Waerden datant de 1926 et qui n'a été résolue qu'en 1981 [15, 16]. Une matrice est *doublement stochastique* si la somme de chaque colonne et la somme de chaque ligne vaut 1.

***Théorème 23.*** *Si $A$ est une matrice positive doublement stochastique, alors* $\mathrm{per}(A) \geqslant e^{-n}$.

*Démonstration.* Il suffit de montrer que pour $A$ doublement stochastique, $\inf_{z>0}(p(z_1,\dots,z_n)/z_1\dots z_n) \geqslant 1$, où $p$ est le polynôme défini ci-dessus. Pour cela, on fera appel à l'inégalité arithmético-géométrique dans une version pondérée, qui énonce que pour tous $a_1,\dots,a_n \geqslant 0$ et $\lambda_1,\dots,\lambda_n \geqslant 0$ tels que $\sum \lambda_i = 1$, on a

$$\sum \lambda_i a_i \geqslant \prod_i a_i^{\lambda_i}.$$

On écrit alors

$$\begin{aligned} p(z_1,\dots,z_n) &= \prod_{i=1}^n \sum_{j=1}^n A_{i,j} z_j \\ &\geqslant \prod_{i=1}^n \prod_{j=1}^n z_j^{A_{i,j}} = \prod_{i=1}^n z_j^{\sum_{i=1}^n A_{i,j}} = \prod_{i=1}^n z_j. \end{aligned}$$ □

On passe maintenant à la preuve du théorème 22.

*Démonstration.* L'inégalité de droite est triviale et est valide pour tout polynôme à coefficients positifs. En effet, $\partial_1 \dots \partial_n p_{|z=0}$ est exactement le coefficient du monôme $z_1 \dots z_n$ dans $p$.

Ensuite, on considère le cas univarié qui servira de cas de base à une récurrence. Pour $p$ un polynôme positif log-concave en une seule variable $t$, $\log p$ est inférieur à sa dérivée et donc

$$\log p(t) \leqslant \log p(0) + t\,\frac{p'(0)}{p(0)}.$$

On prend $t = p(0)/p'(0)$, ce qui donne $\log p(t) \leqslant \log p(0) + 1$ et donc

$$\log(p(t)/t) \leqslant 1 + \log p(0) - \log(p(0)/p'(0)) = 1 + \log p'(0).$$

Ainsi, dans le cas univarié, on a $\frac{1}{e}\inf_{t>0}(p(t)/t) \geqslant p'(0)$.

Le théorème se déduit par récurrence sur le nombre de variables : on note $q(z_1,\dots,z_{n-1}) = \partial_n p_{|z_n=0}$, et on suppose que $q$ satisfait la conclusion du théorème par hypothèse de récurrence. On a donc

$$\partial_1 \dots \partial_n p_{|z=0} = \partial_1 \dots \partial_{n-1} q_{|z=0} \geqslant e^{-(n-1)} \inf_{z_1,\dots,z_{n-1}>0} \frac{q(z_1,\dots,z_{n-1})}{z_1 \dots z_{n-1}}.$$

Si on nomme $z_1^*, \dots z_{n-1}^*$ les points où l'infimum est atteint (si celui-ci n'est pas atteint, un même argument approximé avec des $\varepsilon$ et des $\delta$ fera l'affaire), on peut définir notre polynôme univarié $f(z_n) = p(z_1^*, \dots, z_{n-1}^*, z_n)$, et

$$q(z_1^*, \dots, z_{n-1}^*) = f'(0) \geqslant \frac{1}{e} \inf_{z_n > 0} \frac{f(z_n)}{z_n}.$$

Le théorème est prouvé en combinant ces inégalités. □

La première application des polynômes complètement log-concaves [6] a été de généraliser cette approche pour obtenir un algorithme déterministe permettant d'approximer le nombre de bases d'un matroïde, ou d'une intersection de matroïdes, à un facteur multiplicatif $2^{O(r)}$ près.

## Références


[1] K. Adiprasito, J. Huh & E. Katz – « Hodge theory for combinatorial geometries », *Annals of Mathematics. Second Series* **188** (2018), no. 2, p. 381–452.

[2] Y. Alimohammadi, N. Anari, K. Shiragur & T.-D. Vuong – « Fractionally log-concave and sector-stable polynomials: counting planar matchings and more », in *STOC '21—Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, ACM, New York, NY, 2021, p. 433–446.

[3] O. Amini – « Géométries combinatoires », in *Combinatoire et géométries exotiques*, Journées X-UPS, Les Éditions de l'École polytechnique, Palaiseau, 2025, ce volume.

[4] N. Anari, K. Liu, S. Oveis Gharan & C. Vinzant – « Log-concave polynomials III: Mason's ultra-log-concavity conjecture for independent sets of matroids », *Proceedings of the American Mathematical Society* **152** (2024), no. 5, p. 1969–1981.

[5] ———, « Log-concave polynomials II: High-dimensional walks and an FPRAS for counting bases of a matroid », *Annals of Mathematics. Second Series* **199** (2024), no. 1, p. 259–299.

[6] N. Anari, S. Oveis Gharan & C. Vinzant – « Log-concave polynomials, entropy, and a deterministic approximation algorithm for counting bases of matroids », in *59th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2018*, IEEE Computer Soc., Los Alamitos, CA, 2018, p. 35–46.

[7] N. Anari & A. Rezaei – « A tight analysis of Bethe approximation for permanent », in *2019 IEEE 60th Annual Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press, Los Alamitos, CA, 2019, p. 1434–1445.

[8] N. Anari, C. Vinzant, K. Liu, S. Oveis Gharan & T.-D. Vuong – « Log-concave polynomials IV: approximate exchange, tight mixing times, and near-optimal sampling of forests », in *STOC '21—Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, ACM, New York, 2021, p. 408–420.

[9] P. Brändén – « Polynomials with the half-plane property and matroid theory », *Advances in Mathematics* **216** (2007), no. 1, p. 302–320.

[10] P. Brändén & J. Huh – « Lorentzian polynomials », *Annals of Mathematics. Second Series* **192** (2020), no. 3, p. 821–891.

[11] P. Brändén & J. Leake – « Lorentzian polynomials on cones and the Heron-Rota-Welsh conjecture », 2021, arXiv:2110.00487.
[12] Y.-B. Choe, J. G. Oxley, A. D. Sokal & D. G. Wagner – « Homogeneous multivariate polynomials with the half-plane property », *Advances in Applied Mathematics* **32** (2004), no. 1-2, p. 88–187, Special issue on the Tutte polynomial.
[13] M. Cryan, H. Guo & G. Mousa – « Modified log-Sobolev inequalities for strongly log-concave distributions », *The Annals of Probability* **49** (2021), no. 1, p. 506–525.
[14] J. Edmonds – « Submodular functions, matroids, and certain polyhedra », in *Combinatorial optimization – Eureka, you shrink. Papers dedicated to Jack Edmonds. 5th international workshop, Aussois, France, March 5–9, 2001*, Springer, Berlin, 2003, p. 11–26.
[15] G. P. Egorychev – « The solution of van der Waerden's problem for permanents », *Advances in Mathematics* **42** (1981), no. 3, p. 299–305.
[16] D. I. Falikman – « Proof of the van der Waerden conjecture regarding the permanent of a doubly stochastic matrix », *Mathematical Notes* **29** (1981), p. 475–479.
[17] T. Feder & M. Mihail – « Balanced matroids », in *Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, 1992, p. 26–38.
[18] J. von zur Gathen & J. Gerhard – *Modern computer algebra*, 3e éd., Cambridge University Press, Cambridge, 2013.
[19] H. Guo & M. Jerrum – « A polynomial-time approximation algorithm for all-terminal network reliability », *SIAM Journal on Computing* **48** (2019), no. 3, p. 964–978.
[20] L. Gurvits – « Van der Waerden/Schrijver-Valiant like conjectures and stable (aka hyperbolic) homogeneous polynomials: one theorem for all », *Electronic Journal of Combinatorics* **15** (2008), no. 1, article no. 66 (26 pages).
[21] ———, « On multivariate Newton-like inequalities », in *Advances in combinatorial mathematics: Proceedings of the Waterloo Workshop in Computer Algebra 2008*, Springer, Berlin, 2009, p. 61–78.
[22] L. Gurvits & A. Samorodnitsky – « Bounds on the permanent and some applications », in *55th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2014*, IEEE Computer Soc., Los Alamitos, CA, 2014, p. 90–99.
[23] A. P. Heron – « Matroid polynomials », in *Combinatorics (Proc. Conf. Combinatorial Math., Math. Inst., Oxford, 1972)*, The Institute of Mathematics and Its Applications, Southend-on-Sea, 1972, p. 164–202.
[24] S. G. Hoggar – « Chromatic polynomials and logarithmic concavity », *Journal of Combinatorial Theory. Series B* **16** (1974), p. 248–254.
[25] S. Hoory, N. Linial & A. Wigderson – « Expander graphs and their applications », *American Mathematical Society. Bulletin. New Series* **43** (2006), no. 4, p. 439–561.
[26] J. Huh – « Milnor numbers of projective hypersurfaces and the chromatic polynomial of graphs », *Journal of the American Mathematical Society* **25** (2012), no. 3, p. 907–927.
[27] ———, « Combinatorial applications of the Hodge-Riemann relations », in *Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. IV. Invited lectures*, World Scientific Publications, Hackensack, NJ, 2018, p. 3093–3111.
[28] J. Huh & E. Katz – « Log-concavity of characteristic polynomials and the Bergman fan of matroids », *Mathematische Annalen* **354** (2012), no. 3, p. 1103–1116.
[29] M. Jerrum – *Counting, sampling and integrating: algorithms and complexity*, Lectures in Mathematics ETH Zürich, Birkhäuser Verlag, Basel, 2003.

[30] M. Jerrum, A. Sinclair & E. Vigoda – « A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries », *Journal of the ACM* **51** (2004), no. 4, p. 671–697.
[31] M. R. Jerrum, L. G. Valiant & V. V. Vazirani – « Random generation of combinatorial structures from a uniform distribution », *Theoretical Computer Science* **43** (1986), no. 2-3, p. 169–188.
[32] D. R. Karger – « A randomized fully polynomial time approximation scheme for the all terminal network reliability problem », in *Proceedings of the twenty-seventh annual ACM Symposium on Theory of Computing*, ACM, New York, NY, 1995, p. 11–17.
[33] T. Kaufman & I. Oppenheim – « High order random walks: beyond spectral gap », *Combinatorica. An International Journal on Combinatorics and the Theory of Computing* **40** (2020), no. 2, p. 245–281.
[34] A. Krause & D. Golovin – « Submodular function maximization », in *Tractability*, Cambridge University Press, Cambridge, 2014, p. 71–104.
[35] J. B. Kruskal, Jr. – « On the shortest spanning subtree of a graph and the traveling salesman problem », *Proceedings of the American Mathematical Society* **7** (1956), p. 48–50.
[36] G. Laman – « On graphs and rigidity of plane skeletal structures », *Journal of Engineering Mathematics* **4** (1970), p. 331–340.
[37] J. Leake, K. Lindberg & S. O. Gharan – « Optimal trickle-down theorems for path complexes via C-Lorentzian polynomials with applications to sampling and log-concave sequences », 2025, `arXiv:2503.01005`.
[38] D. A. Levin & Y. Peres – *Markov chains and mixing times*, 2e éd., American Mathematical Society, Providence, RI, 2017.
[39] A. Lubotzky – « High dimensional expanders », in *Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. I. Plenary lectures*, World Scientific Publications, Hackensack, NJ, 2018, p. 705–730.
[40] J. H. Mason – « Matroids: unimodal conjectures and Motzkin's theorem », in *Combinatorics (Proc. Conf. Combinatorial Math., Math. Inst., Oxford, 1972)*, The Institute of Mathematics and Its Applications, Southend-on-Sea, 1972, p. 207–220.
[41] M. Mitzenmacher & E. Upfal – *Probability and computing. Randomization and probabilistic techniques in algorithms and data analysis*, 2e éd., Cambridge University Press, Cambridge, 2017.
[42] M. Piquerez – « Algèbres et volumes des polytopes », in *Combinatoire et géométries exotiques*, Journées X-UPS, Les Éditions de l'École polytechnique, Palaiseau, 2025, ce volume.
[43] J. S. Provan & M. O. Ball – « The complexity of counting cuts and of computing the probability that a graph is connected », *SIAM Journal on Computing* **12** (1983), no. 4, p. 777–788.
[44] R. C. Read – « An introduction to chromatic polynomials », *Journal of Combinatorial Theory* **4** (1968), p. 52–71.
[45] G.-C. Rota – « Combinatorial theory, old and new », in *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3*, Gauthier-Villars Éditeur, Paris, 1971, p. 229–233.
[46] H. J. Ryser – *Combinatorial mathematics*, The Carus Mathematical Monographs, vol. 14, Mathematical Association of America, 1963.
[47] L. G. Valiant – « The complexity of enumeration and reliability problems », *SIAM Journal on Computing* **8** (1979), no. 3, p. 410–421.

[48] D. J. A. Welsh – « Combinatorial problems in matroid theory », in *Combinatorial Mathematics and its Applications (Proc. Conf., Oxford, 1969)*, Academic Press, London-New York, 1971, p. 291–306.
[49] H. Whitney – « On the abstract properties of linear dependence », *American Journal of Mathematics* **57** (1935), no. 3, p. 509–533.
[50] A. Wigderson – *Mathematics and computation. A theory revolutionizing technology and science*, Princeton University Press, Princeton, NJ, 2019.

Arnaud de Mesmay, LIGM Laboratoire Informatique Gaspard Monge Univ Gustave Eiffel, CNRS, LIGM, F-77454 Marne-la-Vallée, France
*E-mail :* `arnaud.de-mesmay@univ-eiffel.fr`
*Url :* `https://monge.univ-mlv.fr/~demesma/`