Ecole Normale Supérieure

Polycopié de cours

Structures et algorithmes aléatoires

Auteur:
M. Lelarge
marc.lelarge@ens.fr

Rédacteur:
The Info Team

Version préliminaire, merci d'envoyer vos remarques à marc.lelarge@ens.fr

Contents

Part I

Probabilités discrètes

1 Evénements et probabilités

1.1 Application: vérifier les identités polynomiales

Question:

$$(x+1)(x-2)(x+3)(x-4)(x+5)(x-6) \equiv x^6 - 7x^3 + 25?$$

Soient deux polynômes $F(X)$ et $G(X)$, $F(X) = G(X)$?
Ecrire les polynômes sous forme canonique $\sum_i a_i X^i$.

Idée. Utiliser de l'aléa.

Algorithme. d = degré de F et G.
Choisit un entier $r \in \{1 \cdots 100d\}$, uniformément au hasard.
Calcul $F(r)$ et $G(r)$ en complexité $O(d)$.

- Si $F(r) \neq G(r)$, alors $F \neq G$.
- Si $F(r) = G(r)$, alors $F = G$.

L'algo se trompe si r est racine de $F(x) - G(x)$ qui est un polynôme de degré inférieur à d. Donc la probabilité que r soit une racine de ce polynôme (et donc que l'algorithme se trompe) est inférieure à $\frac{d}{100d} = \frac{1}{100}$.

1.2 Axiomes des probabilités

Définition 1.

Un espace de probabilité a 3 composantes :

1) Espace d'épreuves Ω

2) Famille d'ensembles $\mathcal{F} \subset \Omega$, tribu sur Ω, représente les événements.

3) Une probabilité $\mathbb{P} : \mathcal{F} \to \mathbb{R}$.

Exemple.
Modélisation de 2 lancers de pièce. $\Omega = \{(0,0),(0,1),(1,0),(1,1)\}$. L'événement le premier lancer donne pile est: $\{(0,0),(0,1)\}$ de probabilité: $\mathbb{P}(\{(0,0),(0,1)\}) = \frac{1}{2}$.
$\mathbb{P}(00) = \mathbb{P}(01) = \cdots = \frac{1}{4}$

Définition 2.

Une tribu sur Ω est une famille $\mathcal{F}$ de sous-ensembles de Ω tel que

1) Ω et $\emptyset$ sont dans $\mathcal{F}$.

2) $A \in \mathcal{F} \Rightarrow \bar{A} \in \mathcal{F}$

3) $(A_n)_{n\in\mathbb{N}} \in \mathcal{F}^{\mathbb{N}} \Rightarrow \bigcup_{n=1}^{\infty} A_n \in \mathcal{F}$

Définition 3.

Une (fonction de) probabilité $\mathbb{P} : \mathcal{F} \to \mathbb{R}$ satisfait

1) $\forall E \in \mathcal{F}$, $\mathbb{P}(E) \in [0,1]$

2) $\mathbb{P}(\Omega) = 1$

3) $(E_n, n \geq 1) \in \mathcal{F}$ deux à deux disjoints $\Rightarrow \mathbb{P}(\bigsqcup_{n=1}^{\infty} E_n) = \sum_{n=1}^{\infty} \mathbb{P}(A_n)$.

Remarque. • Dans ce cours, on se placera dans le cas des probabilités discrètes, c'est à dire Ω fini ou dénombrable. $\mathcal{F}$ est alors l'ensemble des sous-ensembles de Ω.

• On identifie les événements aux ensembles ainsi $E_1 \cap E_2 = E_1$ et E_2 se réalisent, $E_1 \cup E_2 = E_1$ ou E_2 se réalisent, $E_1 \setminus E_2 = E_1$ sans E_2.

Lemme 1.

- $\mathbb{P}(E_1 \cup E_2) = \mathbb{P}(E_1) + \mathbb{P}(E_2) - \mathbb{P}(E_1 \cap E_2)$
- $(E_n, n \geq 1) \quad \mathbb{P}(\bigcup_{n=1}^{\infty} E_n) \leq \sum_{n=1}^{\infty} \mathbb{P}(E_n)$.

On reprend l'exemple précédent: $\Omega = \{1 \cdots 100d\}$
On considère l'événement E: l'algorithme se trompe. $\mathbb{P}(E) \leq \frac{d}{100d} = \frac{1}{100}$.
Amélioration de l'algorithme :

• une solution consiste à tirer r entre 1 et 1000 d dans ce cas, $\mathbb{P}(E) \leq \frac{1}{1000}$.

• une autre solution consiste à itérer l'algorithme avec $100d$: On effectue un échantillonnage avec ou sans remplacement.

Dans le cas avec remplacement, si $F \neq G$, $\mathbb{P}$(se planter après k itérations) $\leq \frac{1}{100^k}$.

Définition 4 (Evénements indépendants**).**

- E et F sont idépendants $E \coprod F$ si $\mathbb{P}(E \cap F) = \mathbb{P}(E)\,\mathbb{P}(F)$.
- $(E_i)_{i \in \mathbb{N}}$ sont mutuellement indépendants si $\forall I \subset [\![1 \cdots k]\!]$
- $\mathbb{P}\left(\bigcap_{i \in I} E_i\right) = \prod_{i \in I} \mathbb{P}(E_i)$.

Pour considérer le cas avec remplacement, nous avons besoin d'introduire la notion de probabilité conditionnelle.

Définition 5.

La probabilité conditionnelle de l'événement E sachant F est $\mathbb{P}(E|F) = \frac{\mathbb{P}(E \cap F)}{\mathbb{P}(F)}$
Si $\mathbb{P}(F) = 0$, alors $\mathbb{P}(E \cap F) = 0$ et on prend $\mathbb{P}(E|F) = 0$

Remarque. $[E \coprod F$ et $\mathbb{P}(F) \neq 0] \Rightarrow \mathbb{P}(E|F) = \mathbb{P}(E)$.

Toujours dans l'exemple précédent, on considère maintenant le cas sans remplacement : soit E_i l'événement: à la i-ème itération, r_i est racine de $F(x) - G(x)$. On a alors pour $k \leq d + 1$:

$$\begin{aligned} \mathbb{P}(E_1 \cap E_2 \cdots \cap E_k) &= \mathbb{P}(E_1)\,\mathbb{P}(E_2|E_2)\,\mathbb{P}(E_3|E_1 \cap E_2) \cdots \mathbb{P}(E_k|E_1 \cap E_2 \cdots E_{k-1}) \\ &\leq \prod_{j=1}^{k} \frac{d-(j-1)}{100d-(j-1)} \end{aligned}$$

car $\mathbb{P}(E_j|E_1 \cap E_2 \cdots E_{j-1}) \leq \frac{d-(j-1)}{100d-(j-1)}$.
Que se passe-t-il pour $k = d + 1$? Quelle est alors le temps d'exécution de l'algorithme?

1.3 Application: Vérification d'un produit de matrice

On a 3 matrices $n \times n$, A, B, et C dans $\mathbb{Z}_2$. $AB = C$?

On multiplie A et B. Le nombre d'opérations requis est de $O(n^3)$ pour un algorithme naif et peut être amélioré à $O\left(n^{2,37}\right)$.

Algorithme. On choisit aléatoirement $\bar{r} = (r_1 \cdots r_n) \in \{0,1\}^n$ de manière uniforme. On calcule $A(B\bar{r})$ et $C\bar{r}$, ce qui nécessite $O\left(n^2\right)$ opérations.

Si $AB\bar{r} \neq C\bar{r}$, alors on retourne $AB \neq C$ sinon $AB = C$.

Proposition 1.
Si $AB \neq C$ et $\bar{r}$ est choisi de manière uniforme dans $\{0,1\}^n$, alors $\mathbb{P}(AB\bar{r} = C\bar{r}) \leq 1/2$.

Démonstration.
On définit la matrice D par: $D = AB - C \neq 0$. On a donc $AB\bar{r} = C\bar{r} \Leftrightarrow D\bar{r} = 0 \Rightarrow r_1 = -\frac{\sum_{j=2}^{n} d_{1j} r_j}{d_{11}}$

Théorème 1 (Loi des probabilités totales**).**
$E_1 \cdots E_n$ disjoints, $\bigsqcup_{i=1}^{n} E_i = \Omega$.
$\mathbb{P}(B) = \sum_{i=1}^{n} \mathbb{P}(B \cap E_i) = \sum_{i=1}^{n} \mathbb{P}(B|E_i)\,\mathbb{P}(E_i)$.

$$
\begin{aligned}
\mathbb{P}(AB\bar{r} = C\bar{r}) &= \sum_{\{x_2 \cdots x_n\} \in \{0,1\}^{n-1}} \mathbb{P}(D\bar{r} = 0, (r_2 \cdots r_n) = (x_2 \cdots x_n)) \\
&\leq \sum_{\{x_2 \cdots x_n\} \in \{0,1\}^{n-1}} \mathbb{P}\left(r_1 = -\frac{\sum_{j=2}^{n} d_{1j} x_j}{d_{11}}, (r_2 \cdots r_n) = (x_2 \cdots x_n)\right) \\
&= \sum_{\{x_2 \cdots x_n\} \in \{0,1\}^{n-1}} \mathbb{P}\left(r_1 = -\frac{\sum_{j=2}^{n} d_{1j} x_j}{d_{11}}\right) \mathbb{P}((r_2 \cdots r_n) = (x_2 \cdots x_n)) \\
&= \frac{1}{2}
\end{aligned}
$$

2 Variables aléatoires discrètes et espérance

2.1 Distribution de probabilité discrète

Soit $(\Omega, \mathcal{F}, \mathbb{P})$ un espace de probabilités. $\mathcal{X}$ un ensemble dénombrable.

Définition 6.

1) Une application $X : \Omega \longrightarrow \mathcal{X}$ est appelée **une variable aléatoire** (v.a.) à valeurs dans $\mathcal{X}$ si $\{X = x\} \in \mathcal{F}$ pour tout $x \in \mathcal{X}$.

2) Une suite de réels $(p(x), x \in \mathcal{X})$ telle que $0 \leq p(x) \leq 1$, $\sum_x p(x) = 1$ est appelée **distribution de probabilité sur** $\mathcal{X}$. Si la variable aléatoire X est telle que $\mathbb{P}(X \in A) = \sum_{x \in A} p(x)$ pour tout $A \subset \mathcal{X}$. On dit que $(p(x), x \in \mathcal{X})$ est la distribution de probabilité de X.

Définition 7.

1) Deux variables aléatoires X et Y sont indépendantes si et seulement si $\mathbb{P}((X = x) \cap (Y = y)) = \mathbb{P}(X = x)\,\mathbb{P}(Y = y)\,\forall x, y$

2) Les variables aléatoires $X_1, X_2, \cdots X_k$ sont mutuellement indépendantes si et seulement si pour tout $I \subset [\![1 \cdots k]\!]$ et pour tout x_i.
$\mathbb{P}\left(\bigcap_{i \in I} \{X_i = i\}\right) = \prod_{i \in I} \mathbb{P}(X_i = x_i)$.

Exemple.

1) La variable aléatoire de Bernoulli $Y = \begin{cases} 1 \text{ avec probabilité } p \\ 0 \text{ avec probabilité } 1-p \end{cases}$ $p \in [0,1]$

2) Distribution de Bernoulli d'ordre n et de paramètre p.
$h(x) = \sum_{i=1}^n x_i, x = (x_1, \cdots, x_n) \in \{0,1\}^n$ poids de Hamming.
$\mathcal{X} = \{0,1\}^n$ $p(x) = p^{h(x)}(1-p)^{n-h(x)}$ $p \in [0,1]$.

3) Distribution binomiale d'ordre n et de paramètre p.
$\mathcal{X} = \{1, \cdots, n\}$ $p(k) = \binom{k}{n} p^k (1-p)^{n-k}$ $0 \leq k \leq n$.

4) Distribution multinomiale (n, k, p) $p = (p_1, \cdots, p_k)$ distribution de probabilité sur $\{1, \cdots, k\}$.
$\mathcal{X} = \left\{(n_1, \cdots, n_k) \text{ tel que } \sum_{i=1}^k n_i = n, n_i \geq 0\right\}$. $p(n_1 \cdots n_k) = \frac{n!}{n_1! \cdots n_k!} p_1^{n_1} \cdots p_k^{n_k}$

2.2 Espérance

Définition 8.

Soit X une variable aléatoire à valeurs dans $\mathcal{X}$ et de distribution $(p(x), x \in \mathcal{X})$.
Soit $f : \mathcal{X} \longrightarrow \overline{\mathbb{R}}$. On définit l'espérance de la variable aléatoire $f(X)$, notée $\mathbb{E}[f(X)]$ par:

a) Si f ne prend que des valeurs non négatives $\mathbb{E}[f(X)] = \sum_{x \in \mathcal{X}} f(x)p(x)$.

b) Cas général : $f = f^+ - f^-$ avec

- $f^+(x) = \max(f(x), 0)$

- $f^-(x) = \max(-f(x), 0)$
- $|f| = f^+ + f^-$

b1) Si $\mathbb{E}[|f(X)|] < \infty$ on dit que f est intégrable $\mathbb{E}[f(X)] = \mathbb{E}[f^+(X)] - \mathbb{E}[f^-(X)] = \sum_{x\in\mathcal{X}} f(x)p(x) < \infty$.

b2) Si $\mathbb{E}[|f(X)|] = \infty$ et une des deux quantités $\mathbb{E}[f^+(X)]$ et $\mathbb{E}[f^-(X)]$ est infinie, $f(X)$ est sommable. $\mathbb{E}[f(X)] = \mathbb{E}[f^+(X)] - \mathbb{E}[f^-(X)]$.

b3) Si $\mathbb{E}[f^+(X)] = \mathbb{E}[f^-(X)] = \infty$, alors l'espérance n'existe pas.

Définition 9.

Si X est une variable aléatoire à valeurs dans $\mathcal{X} \subset \overline{\mathbb{R}}$, alors sa **moyenne** est $\mathbb{E}[X]$.

Définition 10.

Si X est une variable aléatoire à valeurs dans $\mathcal{X}$, et $\mathcal{P}$ est une proposition relative aux éléments x de $\mathcal{X}$. Si $\mathbb{P}(X \text{ vérifie } \mathcal{P}) = 1$, on dit que $\mathcal{P}$ est vérifiée pour X presque sûrement (p.s.).

Théorème 2 (Linéarité**).**

Soient f, g deux fonctions de $\mathcal{X}$ dans $\mathbb{R}$ tel que $f(X)$ et $g(X)$ soient intégrables. $a, b \in \mathbb{R}$, alors $af(X) + bg(X)$ est intégrable et $\mathbb{E}[af(X) + bg(X)] = a\mathbb{E}[f(X)] + b\mathbb{E}[g(X)]$. Cette égalité vaut également lorsque f et g sont non-négatives et $a, b \geq 0$.

Théorème 3 (Monotonie**).**

Soient f, g: $\mathcal{X} \longrightarrow \overline{\mathbb{R}}$ tel que $f(X)$ et $g(X)$ admettent une espérance. Si $f(X) \leq g(X)$ presque sûrement alors $\mathbb{E}[f(X)] \leq \mathbb{E}[g(X)]$.

Théorème 4 (Inégalité de Jensen**).**

Soit φ une fonction convexe définie sur un intervalle $I \subset \mathbb{R}$ contenant toutes les valeurs possibles d'une variable aléatoire X à valeur dans $\mathbb{R}$.

Alors si X et $\varphi(X)$ sont intégrables, $\varphi(\mathbb{E}[X]) \leq \mathbb{E}[\varphi(X)]$.

Démonstration.

$\forall x_0 \in \overset{\circ}{I}, \exists \alpha$ tel que $\varphi(x) \leq \varphi(x_0) + \alpha(x - x_0)$.

Si X est une constante déterministe, ok. Sinon, $\mathbb{E}[X] \in \overset{\circ}{I}$ et donc pour $x_0 = \mathbb{E}[X]$, on a $\varphi(X) \leq \varphi(\mathbb{E}[X]) + \alpha(X - \mathbb{E}[X])$. On conclut en prenant l'espérance.

2.3 Distribution géométrique et le problème du collecteur de coupons

Définition 11.

Soit $\mathcal{X} = \mathbb{N}^*$. X est une variable aléatoire géométrique de paramètre p si $\mathbb{P}(X = n) = (1-p)^{n-1}p$.

Lemme 2 (Propriété sans mémoire**).**

$\mathbb{P}(X = n + k \text{ sachant que } X > k) = \mathbb{P}(X = n)$ *pour tout* $n \geq 0$.

Démonstration.
Pour $n > 0$, on a:

$$\begin{aligned}\mathbb{P}(X = n+k | X > k) &= \frac{\mathbb{P}(X = n+k)}{\mathbb{P}(X > k)} \\ &= \frac{(1-p)^{n+k-1}p}{\sum_{i=k}^{\infty}(1-p)^i p} = (1-p)^{n-1}p,\end{aligned}$$

où on a utilisé: $\sum_{i=k}^{\infty} x^i = \frac{x^k}{1-x}$.

Lemme 3.
Soit X une variable aléatoire à valeurs non négatives. Alors, $\mathbb{E}[X] = \sum_{i=1}^{\infty}\mathbb{P}(X \geq i)$.

Calcul de la moyenne d'une variable aléatoire géométrique de paramètre p.
$\mathbb{P}(X \geq i) = (1-p)^{i-1}$, donc $\mathbb{E}[X] = \sum(1-p)^{i-1} = \frac{1}{p}$.

Exemple.
n types de coupons à collecter. Chaque boîte contient un coupon. Combien faut-il ouvrir de boîtes en moyenne pour avoir au moins un coupon de chaque type?

Soit X la variable aléatoire égale au nombre de boîtes à ouvrir.

Soit X_i la variable aléatoire comptant le nombre de boîtes ouvertes quand on a pour la première fois $i-1$ coupons différents. On a donc $X_1 = 0$, $X_2 = 1$.

De plus, $X = \sum_{i=1}^{n} X_i$ où X_i est une v.a. géométrique de paramètre $p_i = 1 - \frac{i-1}{n}$. On a donc $\mathbb{E}[X_i] = \frac{1}{p_i}$ et par linéarité: $\mathbb{E}[X] = n\sum_{i=1}^{n}\frac{1}{i}$.

Quand $n \to \infty$, on trouve donc $\mathbb{E}[X(n)] = n\ln(n) + O(n)$.

2.4 Application : temps d'exécution de Quicksort

Algorithme. Entrée : Liste $S = \{x_1, \cdots, x_n\}$.
Sortie : Liste triée

1) Si S a un ou zéro élément, retourner S. Sinon, continuer
2) Choisir un élément x de S comme pivot.
3) Comparer tous les éléments à x et créer deux listes S_1 et S_2 d'éléments respectivement plus grands et plus petits que x.
4) Appliquer Quicksort à S_1 et S_2.
5) Retourner la concaténation des listes S_1 et S_2 triées.

Proposition 2.
On suppose que chaque fois, le pivot est choisi aléatoirement de manière uniforme parmi toutes les possibilités et de manière indépendantes des autres choix. Alors pour toute entrée, le nombre moyen de comparaisons est $2n\log(n) + \mathcal{O}(n)$.

Démonstration.
Soient $(y_1, \cdots, y_n)$ les mêmes valeurs que $(x_1, \cdots, x_n)$ mais triées. Pour $i < j$, on définit la v.a. $X_{ij} = \begin{cases} 1 \text{ si } y_i \text{ et } y_j \text{ sont comparées pendant l'exécution de l'algorithme} \\ 0 \text{ sinon} \end{cases}$. Le nombre total de comparaisons est alors: $X = \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} X_{ij}$.

y_i et y_j sont comparées si et seulement si y_i ou y_j est le premier pivot choisi dans l'ensemble $Y^{ij} = \{y_i, y_{i+1}, \cdots, y_{j-1}, y_j\}$.

Au moment où l'algorithme choisit pour la première fois un pivot dans cet ensemble, le choix

est fait de manière uniforme et donc $\mathbb{P}(y_i \text{ et } y_j \text{ sont comparées }) = \mathbb{P}(X_{ij} = 1) = \frac{2}{j-i+1}$

On a donc par linéarité: $\mathbb{E}[X] = \sum_i \sum_{j \geq i+1} \frac{2}{j-i+1} = (2n+1) \sum_{k=1}^{n} \frac{1}{k} - 4n$.

3 Moments et déviations

3.1 Inégalité de Markov

Sauf si cela est explicitement dit, on considère dans ce chapitre des variables aléatoires à valeurs réelles.

Théorème 5.
Soit X une variable aléatoire non négative, alors pour tout $a > 0$,
$\mathbb{P}(X > a) \leq \frac{\mathbb{E}[X]}{a}$

Démonstration.
$\mathbb{1}(X > a) \leq \frac{X}{a}$. Prendre l'espérance.

Exemple.
Si l'on effectue n tirages de pile ou face, majoration sur la probabilité d'obtenir au moins $\frac{3n}{4}$ piles ?
$X = \sum X_i$, $\mathbb{E}[X] = \frac{n}{2}$, donc $\mathbb{P}\left(X > \frac{3n}{4}\right) \leq \frac{\frac{n}{2}}{\frac{3n}{4}} = \frac{2}{3}$.

3.2 Variance et moments d'une variables aléatoire

Définition 12.

- Le k-ième moment de X est $\mathbb{E}[X^k]$.
- La **variance** de X est $\mathrm{Var}(X) = \mathbb{E}\left[(X - \mathbb{E}[X])^2\right] = \mathbb{E}\left[X^2\right] - \mathbb{E}[X]^2$.
- La **covariance** de deux variables aléatoires X et Y est $\mathrm{Cov}(X, Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])]$

Théorème 6.
Pour des variables aléatoires X et Y, $\mathrm{Var}(X + Y) = \mathrm{Var}(X) + \mathrm{Var}(Y) + 2\,\mathrm{Cov}(X, Y)$.

Théorème 7.
Soit Y et Z deux variables aléatoires indépendantes à valeurs dans $\mathcal{Y}$ et $\mathcal{Z}$ Soit $f : \mathcal{Y} \longrightarrow \mathbb{R}$ et $g : \mathcal{Z} \longrightarrow \mathbb{R}$ deux fonctions qui sont soit non-négatives, soit telles que $f(Y)$ et $g(Z)$ sont intégrables.
Alors dans le cas intégrable, $f(Y)g(Z)$ est aussi intégrable, et dans tous les cas $\mathbb{E}[f(Y)g(Z)] = \mathbb{E}[f(Y)]\,\mathbb{E}[g(Z)]$

Démonstration.
On traite le cas intégrable : soit $X = (Y, Z)$ et $h(X) = f(Y)g(Z)$ intégrable ?

$$\begin{aligned}
\mathbb{E}[|h(x)|] &= \sum_{y,z} |f(y)|\,|g(z)|\,\mathbb{P}(Y = y)\,\mathbb{P}(Z = z) \\
&= \left(\sum_{y} |f(y)|\,\mathbb{P}(Y = y)\right)\left(\sum_{z} |g(z)|\,\mathbb{P}(Z = z)\right) \\
&= \mathbb{E}[|f(Y)|]\,\mathbb{E}[|g(Z)|] < \infty
\end{aligned}$$

Théorème 8.
Si X et Y sont des variables aléatoires indépendantes, alors $\mathrm{Cov}(X, Y) = 0$ *et* $\mathrm{Var}(X + Y) = \mathrm{Var}(X) + \mathrm{Var}(Y)$.

Démonstration.

$$\begin{aligned}\mathrm{Cov}(X,Y) &= \mathbb{E}[(X-\mathbb{E}[X])(Y-\mathbb{E}[Y])] \\ &= \mathbb{E}[X-\mathbb{E}[X]]\,\mathbb{E}[Y-\mathbb{E}[Y]] = 0\end{aligned}$$

Exemple.
Calcul de la variance d'une variable aléatoire binomiale X. $Y \sim Ber(p)$ alors $\mathrm{Var}(Y) = \mathbb{E}\left[Y^2\right] - \mathbb{E}[Y]^2 = p(1-p)$ et donc $\mathrm{Var}(X) = np(1-p)$.

3.3 Inégalité de Chebychev

Théorème 9.
Soit X une variable aléatoire réelle, pour tout $a > 0$
$\mathbb{P}(|X - \mathbb{E}[X]| \geq a) \leq \frac{\mathrm{Var}(X)}{a^2}$.

Démonstration.
Inégalité de Markov appliquée à $(X - \mathbb{E}[X])^2$.

Exemple.

1) Loi faible des grands nombres :

Soient $X_1, X_2, \dots X_n$ des v.a. indépendantes identiquement distribuées (i.i.d.) de moyenne $\mathbb{E}[X_1] = m$ et de variance $\sigma^2 < \infty$. $S_n = X_1 + X_2 + \cdots + X_n$ est une variable aléatoire de moyenne nm et de variance $n\sigma^2$ donc on a $\mathbb{P}\left(\left|\frac{S_n}{n} - m\right| \geq \epsilon\right) \leq \frac{n\sigma^2}{(n\epsilon)^2} = \frac{1}{n}\frac{\sigma^2}{\epsilon^2}$.

On en déduit que $\lim_{x\to\infty} \mathbb{P}\left(\left|\frac{X_1+\cdots X_n}{n} - \mathbb{E}[X_1]\right| \geq \epsilon\right) = 0$. (LFGN).

2) Collecteur de coupons

Soit X le temps nécessaire pour avoir les n types de coupons.

$\mathbb{E}[X] = nH_n$ avec $H_n = \sum_{i=1}^n \frac{1}{i} = \ln n + O(1)$.

Par Markov, $\mathbb{P}(X \geq 2nH_n) \leq \frac{1}{2}$.

Par Chebychev $X = \sum_{i=1}^n X_i$ avec $X_i \sim \mathrm{Geom}\left(\frac{n-i+1}{n}\right)$

Lemme 4.
La variance d'une loi géométrique de paramètre p est $\frac{1-p}{p^2}$.

Démonstration.
Il faut calculer $\sum_{i=1}^\infty p(1-p)^i i^2$. Pour cela on utilise la relation valable pour $0 < x < 1$, $\frac{1}{1-x} = \sum_{i=0}^\infty x^i$.

On a donc $\mathrm{Var}(X) = \sum_{i=1}^n \mathrm{Var}(X_i) \leq \sum_{i=1}^n \left(\frac{n}{n-i+1}\right)^2 \leq \frac{\pi^2 n^2}{6}$ car $\sum \frac{1}{i^2} = \frac{\pi^2}{6}$

Donc, $\mathbb{P}(|X - nH_n| \geq nH_n) \leq \frac{n^2\frac{\pi^2}{6}}{(nH_n)^2} = O\left(\frac{1}{\ln n^2}\right)$

Cette inégalité est meilleure que celle obtenue par Markov, cependant elle n'est pas très bonne!

En effet, après $n(\ln n + c)$ itérations, la probabilité que l'on n'ait pas le coupon i est

$\left(1 - \frac{1}{n}\right)^{n(\ln n + c)} < \mathbf{e}^{-(c+\ln n)} = \frac{1}{n\mathbf{e}^c}$

Donc, la probabilité qu'un coupon manque après $n(\ln n + c)$ itérations est inférieure à $\mathbf{e}^{-c}$.

Pour $c = \ln n$, cette probabilité est inférieure à $\mathbf{e}^{-c} = \frac{1}{n}$.

3.4 Application: un algorithme randomizé qui calcule la médiane

Soit S un ensemble de n éléments. La **médiane** de S est un élément m de S tel que au moins $\lfloor \frac{n}{2} \rfloor$ éléments de S sont inférieurs ou égaux à m et au moins $\lfloor \frac{n}{2} \rfloor + 1$ sont supérieurs ou égaux à m.

Idée. Echantilloner pour trouver deux éléments tels que

1) $d \leq m \leq u$

2) $C = \{s \in S \text{ tel que } d \leq s \leq u\}$ avec $|C| = \mathcal{O}\left(\frac{n}{\ln n}\right)$

L'algorithme $\left|\begin{array}{l}\text{compte le nombre d'éléments de} S \leq d \\ \text{trie } C\end{array}\right|$ en temps linéaire.
Le $\lfloor \frac{n}{2} \rfloor - l_d + 1$ ième élément de C trié est alors m.

Algorithme. Entrée : Un ensemble S de n éléments.
Sortie : L'élément median m de S.

1. Choisir un ensemble R de $\lceil n^{\frac{3}{4}} \rceil$ éléments de S (choix de manière indépendante et avec remplacement pour simplifier l'analyse).
2. trier R.
3. Prendre d le $\lfloor \frac{n^{\frac{3}{4}}}{2} - \sqrt{n} \rfloor$ plus petit élément de R trié
4. Prendre u le $\lceil \frac{n^{\frac{3}{4}}}{2} + \sqrt{n} \rfloor$ plus petit élément de R trié
5. Comparer tous les éléments de S à d et à u et calculer $C = \{x \in S \text{ tel que } d \leq x \leq u\}$, $l_d = |\{x \in S, x < d\}|$ et $l_u = |\{x \in S, x > u\}|$.
6. Si $l_d > \frac{n}{2}$ ou $l_u > \frac{n}{2}$, alors ERREUR.
7. Si $|C| \leq 4n^{\frac{3}{4}}$ alors trier C sinon ERREUR.
8. Sortir le $\lfloor \frac{n}{2} \rfloor - l_d + 1$ ième élément de C trié.

Démonstration (Analyse de l'algorithme**).**

On suppose que $\sqrt{n}$, $n^{3/4}$ sont entiers et que les éléments de S sont tous différents et que n est impair.

L'algorithme termine en temps linéaire et soit retourne la bonne réponse soit retourne ERREUR.

$\mathcal{E}_1 : Y_1 = |\{r \in R \text{ tel que } r \leq m\}| < \frac{1}{2}n^{\frac{3}{4}} - \sqrt{n}$
$\mathcal{E}_2 : Y_2 = |\{r \in R \text{ tel que } r \geq m\}| < \frac{1}{2}n^{\frac{3}{4}} - \sqrt{n}$
$\mathcal{E}_3 : |C| > 4n^{\frac{3}{4}}$.
L'algorithme retourne ERREUR si et seulement si $\mathcal{E}_1$, $\mathcal{E}_2$ ou $\mathcal{E}_3$ se produit.

Lemme 5.
$\left|\mathbb{P}(\mathcal{E}_1) \leq \frac{1}{4}n^{\frac{-1}{4}}.\right.$

Démonstration.
$X_i = \begin{cases} 1 \text{ si le ième échantillon } \leq m \\ 0 \text{ sinon} \end{cases}$. Les X_i sont i.i.d. et $\mathbb{P}(X_i = 1) = \frac{\frac{n-1}{2}+1}{n} = \frac{1}{2} + \frac{1}{2n}$.

L'événement $\mathcal{E}_1$ correspond à: $Y_1 = \sum_{i=1}^{n^{\frac{3}{4}}} X_i < \frac{1}{2}n^{3/4} - \sqrt{n}$.

$$\begin{aligned}\mathrm{Var}\left(Y_1\right) &= n^{\frac{3}{4}}\left(\frac{1}{2}+\frac{1}{2n}\right)\left(\frac{1}{2}-\frac{1}{2n}\right)\\ &= \frac{n^{\frac{3}{4}}}{4}-\frac{1}{4n^{\frac{5}{4}}}<\frac{n^{\frac{3}{4}}}{4}\end{aligned}$$

Par Chebychev,

$$\begin{aligned}\mathbb{P}\left(\mathcal{E}_1\right) &\leq \mathbb{P}\left(\left|Y_1-\mathbb{E}\left[Y_1\right]\right|>\sqrt{n}\right)\\ &\leq \frac{\mathrm{Var}\left(Y_1\right)}{n}<\frac{1}{4}n^{\frac{-1}{4}}\end{aligned}$$

Lemme 6.
$\mathbb{P}\left(\mathcal{E}_3\right)\leq\frac{1}{2}n^{\frac{-1}{4}}$.

Soit $\mathcal{E}_{3,1}$ l'événement $2n^{\frac{3}{4}}$ éléments de $C\geq m$ et $\mathcal{E}_{3,2}$ l'événement $2n^{\frac{3}{4}}$ éléments de $C\leq m$.

Si $\mathcal{E}_{3,1}$ se produit, alors u dans S trié était au moins $\frac{n}{2}+2n^{\frac{3}{4}}$ et donc R avait au moins $\frac{n^{\frac{3}{4}}}{2}-\sqrt{n}$ éléments parmi les $\frac{n}{2}-2n^{\frac{3}{4}}$ plus grands éléments de S.

$X_i=\begin{cases}1 \text{ si le ième échantillon est parmi les } \frac{n}{2}-2^{\frac{3}{4}} \text{ plus grands de } S\\ 0 \text{ sinon}\end{cases}$

$X=\sum X_i$, $\mathbb{E}\left[X\right]=\frac{1}{2}n^{3/4}-2\sqrt{n}$ et $\mathrm{Var}\left(X\right)=n^{\frac{3}{4}}(\frac{1}{2}-2n^{\frac{-1}{4}})(\frac{1}{2}+2n^{\frac{-1}{4}})<\frac{n^{3/4}}{4}$.

Donc, $\mathbb{P}\left(\mathcal{E}_{3,1}\right)\leq\mathbb{P}\left(\left|X-\mathbb{E}\left[X\right]\right|\geq\sqrt{n}\right)\leq\frac{\mathrm{Var}(X)}{n}<\frac{n^{-1/4}}{4}$.

Au final, la probabilité que l'algorithme retourne ERREUR est inférieure à $n^{-1/4}$.

4 Fonction génératrice et borne de Chernoff

4.1 Fonction génératrice

$f(X) = f_1(X) + if_2(X)$ avec f_1 et f_2 des fonctions de X dans $\mathbb{R}$ et $i = \sqrt{-1}$.
$f(X)$ est intégrable si et seulement si f_1 et f_2 le sont. $\mathbb{E}[f(X)] = \mathbb{E}[f_1(X)] + i\mathbb{E}[f_2(X)]$

Définition 13.
Soit X une variable aléatoire à valeurs dans $\mathbb{N}$. On appelle **fonction génératrice** de X l'application $g_X : \{s \in \mathbb{C} \text{ tel que } |s| \leq 1\} \to \mathbb{C}$ définie par $g_X(s) = \mathbb{E}\left[s^X\right] = \sum_{n=0}^{\infty} s^n \mathbb{P}(X = n)$.

Exemple.

- Soit X une variable aléatoire de Poisson de paramètre λ: $\mathbb{P}(X = k) = \frac{\lambda^k}{k!}\mathbf{e}^{-\lambda}$. Alors $g_X(s) = \mathbf{e}^{\lambda(s-1)}$.
- Soit X une variable aléatoire de loi binomiale Bin(n,p). $g_X(s) = (ps + 1 - p)^n$.

Théorème 10.
Soient X et Y deux variables aléatoires indépendantes à valeurs dans $\mathbb{N}$ et de fonctions génératrices g_X et g_Y. Alors $X + Y$ a pour fonction génératrice $g_{X+Y}(s) = g_X(s)g_Y(s)$.

Théorème 11 (Somme aléatoire)**.**
Soit $N, X_1, \cdots, X_n$ une famille de variables aléatoires indépendantes à valeurs dans $\mathbb{N}$. Les $X_i, i \geq 1$ sont i.i.d. de fonction génératrice $g_X(s)$. N a pour fonction génératrice $g_N(s)$.
$\Sigma = X_1 + \cdots + X_N$ ($\Sigma = 0$ si $N = 0$) a pour fonction génératrice $g_\Sigma(s) = g_N(g_X(s))$

Démonstration.
$g_S(s) = \mathbb{E}\left[s^\Sigma\right] = \mathbb{E}\left[s^{X_1+\cdots+X_N}\right]$
$s^{X_1+\cdots+X_N} = \sum_{n=1}^{\infty} s^{X_1+\cdots+X_n}\mathbb{1}(N = n)$
Par linéarité de l'espérance :

$$\begin{aligned} g_\Sigma(s) &= \sum_{k=1}^{\infty} \mathbb{E}\left[\mathbb{1}(N = k)s^{X_1+\cdots+X_k}\right] \\ &= \sum_{k=1}^{\infty} \mathbb{P}(N = k) \prod_{i=1}^{k} \mathbb{E}\left[s^{X_i}\right] \\ &= \sum_{k=1}^{\infty} \mathbb{P}(N = k)\, g_X(s)^k. \end{aligned}$$

4.2 Dérivées successives et moments

Le rayon de convergence de la série entière est strictement positif (≥ 1) car $\sum \mathbb{P}(X = n) = 1$. On peut dériver la fonction génératrice et

- ${g'}_X(s) = \sum_{n=1}^{\infty} n\mathbb{P}(X = n)\, s^{n-1}$
- ${g''}_X(s) = \sum_{n=2}^{\infty} n(n-1)\mathbb{P}(X = n)\, s^{n-2}$

Supposons $R > 1$. Si X est intégrable, alors

- $\mathbb{E}[X] = {g'}_X(1)$

- ${g''}_X(1) = \mathbb{E}[X(X-1)]$
- $\mathbb{E}\left[X^2\right] = {g''}_X(1) + {g'}_X(1)$

Théorème 12.

i) Soit $g : \begin{array}{c}[0,1] \longrightarrow \mathbb{R} \\ x \mapsto \mathbb{E}\left[x^X\right]\end{array}$ *où X est une variable aléatoire à valeurs dans $\mathbb{N}$. Alors g est non décroissante et convexe. De plus, si $\mathbb{P}(X=0) < 1$, alors g est strictement croissante, et si $\mathbb{P}(X \leq 1) < 1$, elle est strictement convexe.*

ii) Supposons $\mathbb{P}(X \leq 1) < 1$.

- *Si $\mathbb{E}[X] \leq 1$, alors l'équation $x = g(x)$ a une unique solution $x \in [0,1]$ qui est $x = 1$.*
- *Si $\mathbb{E}[X] > 1$, alors elle a deux solutions dans $[0,1]$ qui sont $x = 1$ et $x = \beta \in (0,1)$*

Démonstration.

- ${g'}_X(x) = \sum_{n=1}^{\infty} n\mathbb{P}(X=n)\, x^{n-1}$, or $x \in [0,1]$ donc g est non décroissante.
- ${g''}_X(x) = \sum_{n=2}^{\infty} n(n-1)\mathbb{P}(X=n)\, x^{n-2}$ avec $x \in [0,1]$, donc g est convexe.
- Pour que ${g'}_X(x)$ s'annule, il faut $\mathbb{P}(X=n) = 0\ \forall n \geq 1$ donc $\mathbb{P}(X=0) = 1$.
- Pour que $g''_X(x)$ s'annule, il faut que $\mathbb{P}(X=n) = 0\ \forall n \geq 2$.

Donc si $\mathbb{P}(X=0) + \mathbb{P}(X=1) < 1$, g' et $g'' > 0$ et g est strictement croissante et strictement convexe.

On a une caractérisation de la loi par la fonction génératrice. La fonction génératrice caractérise la distribution d'une variable aléatoire à valeurs dans $\mathbb{N}$. (unicité du développement en série entière autour de l'origine).

Théorème 13.

Si X_1 et X_2 sont deux variables aléatoires de Poisson de paramètres λ_1 et λ_2 indépendantes. Alors $X_1 + X_2$ est une variable aléatoire de Poisson de paramètre $\lambda_1 + \lambda_2$.

Démonstration.
$g_{X_1+X_2}(s) = \mathbf{e}^{(\lambda_1+\lambda_2)(s-1)}$.

Exemple (Processus de branchement**).**
Soit une suite de variables aléatoires $(X_n)_{n\in\mathbb{N}}$ de premier terme X_0 et définie par $X_{n+1} = \begin{cases} \sum_{i=1}^{X_n} Z_i^{(n)} \text{ si } X_n \geq 1 \\ 0 \text{ si } X_n = 0 \end{cases}$ où $Z_i^{(n)}$ $n \geq 0$ et $i \geq 1$ sont des variables aléatoires i.i.d. de fonction génératrice g_Z et de moyenne finie.

La probabilité d'extinction $P_e = \mathbb{P}\left(\bigcup_{n=0}^{\infty}\{X_n = 0\}\right) = \lim_{n\to\infty}\mathbb{P}(X_n = 0)$ car $\{X_n = 0\} \subset \{X_{n+1} = 0\}$.

Soit φ_n la fonction génératrice de X_n. $\varphi_{n+1}(s) = \varphi_n(g_Z(s)) = \varphi_0(\underbrace{g_Z \circ \cdots \circ g_Z}_{n+1 \text{ fois}})(s)$

Si $X_0 = 1$, alors $\varphi_0(s) = s$ et donc $\varphi_{n+1}(s) = g_Z(\varphi_n(s))$.

$\mathbb{P}(X_n = 0) = \varphi_n(0)$ donc $\mathbb{P}(X_{n+1} = 0) = g_Z(\mathbb{P}(X_n = 0))$ donc en passant à la limite, $P_e = g_Z(P_e)$.

Par le Théorème 13, on a

- Si $\mathbb{E}[Z] \leq 1$, alors $P_e = 1$
- Si $\mathbb{E}[z] > 1$, alors $p_e = \beta < 1$ car $p_e = \lim_{n\to\infty} x_n$ où $x_n = \mathbb{P}(X_n = 0) = g_Z(x_{n-1})$ et $x_0 = 0$ (limite croissante).

4.3 Borne de Chernoff

On applique l'inégalité de Markov à $\mathbf{e}^{tX}$.

Pour tout $t \geq 0$, $\mathbb{P}(X \geq a) = \mathbb{P}\left(\mathbf{e}^{tX} \geq \mathbf{e}^{ta}\right) \leq \frac{\mathbb{E}\left[\mathbf{e}^{tX}\right]}{\mathbf{e}^{ta}}$.
En particulier

- $\mathbb{P}(X \geq a) \leq \inf_{t>0} \frac{\mathbb{E}\left[\mathbf{e}^{tX}\right]}{\mathbf{e}^{ta}}$
- $\mathbb{P}(X \leq a) \leq \inf_{t<0} \frac{\mathbb{E}\left[\mathbf{e}^{tX}\right]}{\mathbf{e}^{ta}}$

Théorème 14.

Soient $X_1 \cdots X_n$ des variables aléatoires indépendantes. $\mathbb{P}(X_i = 1) = 1 - \mathbb{P}(X_i = 0) = p_i$
Soit $X = \sum_{i=1}^n X_i$ et $\mu = \mathbb{E}[X] = \sum p_i$.

i) Pour tout $\delta > 0$, $\mathbb{P}(X \geq (1+\delta)\mu) < \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu$.

ii) Pour $0 < \delta \leq 1$, $\mathbb{P}(X \geq (1+\delta)\mu) \leq e^{-\frac{\mu\delta^2}{3}}$

iii) Pour $R \geq 6\mu$, $\mathbb{P}(X \geq R) \leq 2^{-R}$

Démonstration.

Soit $M_{X_i}(t) = \mathbb{E}\left[\mathbf{e}^{tX_i}\right] = 1 + p_i(\mathbf{e}^t - 1) \leq \mathbf{e}^{p_i(\mathbf{e}^t-1)}$
$M_X(t) = \mathbb{E}\left[\mathbf{e}^{tX}\right] = \prod_{i=1}^n \mathbb{E}\left[\mathbf{e}^{tX_i}\right] \leq \prod_{i=1}^n \mathbf{e}^{p_i(\mathbf{e}^t-1)} = \mathbf{e}^{\mu(\mathbf{e}^t-1)}$.

$$\begin{aligned}
\mathbb{P}(X \geq (1+\delta)\mu) &= \mathbb{P}\left(\mathbf{e}^{tX} \geq \mathbf{e}^{t(1+\delta)\mu}\right) \\
&\leq \frac{\mathbb{E}\left[\mathbf{e}^{tX}\right]}{\mathbf{e}^{t(1+\delta)\mu}} \\
&\leq \frac{\mathbf{e}^{\mu(\mathbf{e}^t-1)}}{\mathbf{e}^{t(1+\delta)\mu}}
\end{aligned}$$

Pour tout $\delta > 0$, on peut poser $t = \ln(1+\delta) > 0$ et on obtient (i).
Pour obtenir (ii), on montre que pour $0 < \delta \leq 1$ on a $\frac{\mathbf{e}^\delta}{(1+\delta)^{1+\delta}} \leq \mathbf{e}^{-\frac{\delta^2}{3}}$.
Pour (iii), soit $R = (1+\delta)\mu$, alors pour $R > 6\mu \Rightarrow \delta \geq 5$ et par (i)

$$\begin{aligned}
\mathbb{P}(X \geq (1+\delta)\mu) &\leq \left(\frac{\mathbf{e}^\delta}{(1+\delta)^{(1+\delta)}}\right)^\mu \\
&\leq \left(\frac{e}{1+\delta}\right)^{(1+\delta)\mu} \\
&\leq \left(\frac{e}{6}\right)^R \leq 2^{-R}.
\end{aligned}$$

Dans le cas symétrique, on obtient de meilleurs bornes.

Théorème 15.

Soit $X_1 \cdots X_n$ des variables aléatoires indépendantes et identiquement distribuées. $\mathbb{P}(X_i = 1) = \mathbb{P}(X_i = -1) = \frac{1}{2}$.

$X = \sum_{i=1}^{n} X_i$, *alors* $\forall a > 0$, $\mathbb{P}(X \geq a) \leq e^{-\frac{a^2}{2n}}$

Démonstration.

$\forall t \geq 0$, $\mathbb{E}\left[\mathbf{e}^{tX_i}\right] = \frac{1}{2}\mathbf{e}^{-t} + \frac{1}{2}\mathbf{e}^{t} = \sum_i \frac{t^{2i}}{(2i)!} \leq \mathbf{e}^{\frac{t^2}{2}}$

$\mathbb{E}\left[\mathbf{e}^{tX}\right] = \prod_{i=1}^{n} \mathbb{E}\left[\mathbf{e}^{tX_i}\right] \leq \mathbf{e}^{t^2 \frac{n}{2}}$

$\mathbb{P}(X \geq a) \leq \frac{\mathbb{E}\left[\mathbf{e}^{tX}\right]}{\mathbf{e}^{ta}} \leq \mathbf{e}^{t^2 \frac{n}{2} - ta}$ et on prend $t = a/n$.

Corollaire 1.

$\forall a > 0$ $\mathbb{P}(|X| \geq a) \leq 2e^{-\frac{a^2}{2n}}$

Si $Y_i = \frac{X_i+1}{2}$, $Y = \sum Y_i = \frac{X}{2} + \frac{n}{2} = \frac{X}{2} + \mu$ où $\mu = \mathbb{E}[Y]$.

$\forall > 0$ $\mathbb{P}(Y \geq \mu + a) = \mathbb{P}(X \geq 2a) \leq \mathbf{e}^{-4\frac{a^2}{2n}}$

Corollaire 2.

Soient Y_i *des variables i.i.d.,* $\mathbb{P}(Y_i = 1) = \mathbb{P}(Y_i = 0) = \frac{1}{2}$

$Y = \sum_i Y_i$, $\mu = \mathbb{E}[[]\, Y] = \frac{n}{2}$

i) $\forall a \geq 0$, $\mathbb{P}(Y \geq \mu + a) \leq e^{-\frac{2a^2}{n}}$

ii) $\forall \delta > 0$, $\mathbb{P}(Y \geq (1+\delta)\mu) \leq e^{-\delta^2 \mu}$

5 Des boules et des urnes

5.1 Le paradoxe des anniversaires

Question. Quel est le nombre de personnes que l'on doit réunir pour avoir plus d'une chance sur deux pour que 2 personnes du groupe aient leur anniversaire le même jour ?
Réponse: 23

Soit m personnes et n anniversaires possibles, ($n = 365$).

Question. Probabilité que les m personnes aient des anniversaires tous différents ?

$$\begin{aligned}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{m-1}{n}\right) &= \prod_{j=1}^{m-1}\left(1-\frac{j}{m}\right)\\ &\simeq \prod_{j=1}^{m-1}\mathbf{e}^{-\frac{j}{n}} \text{ si } \frac{j}{m}=o(1)\\ &= \exp\left(-\sum_{j=1}^{m-1}\frac{j}{n}\right)\\ &\simeq \exp\left(-\frac{m^2}{2n}\right)\end{aligned}$$

Donc on cherche $\frac{m^2}{2n} = \ln 2 \Leftrightarrow m = \sqrt{2n\ln(2)}$. Pour $n = 365$, on trouve $m = 22,49$.

5.2 Des boules et des urnes

Modèle: m boules jetées dans n urnes de manière indépendante et uniforme. On appelle **charge d'une urne** le nombre de boules de la urne.

Question. Quelle est la distribution des boules dans les urnes? Quelle est la charge maximale?

Lemme 7.
Quand $m = n$, la probabilité que la charge maximale soit $\geq \frac{3\ln(n)}{\ln(\ln(n))}$ est au plus $\frac{1}{n}$ pour n suffisament grand.

Démonstration.
La probabilité que l'urne 1 reçoive plus de M boules $\leq \binom{n}{M}\left(\frac{1}{n}\right)^M$.
$\binom{n}{M}\frac{1}{n^M} \leq \frac{1}{M!} \leq \left(\frac{e}{M}\right)^M$
Donc pour, $M > \frac{3\ln(n)}{\ln(\ln(n))}$, on a

$$\begin{aligned}n\left(\frac{e}{M}\right)^M &\leq n\left(\frac{e\ln\ln n}{3\ln n}\right)^{3\ln n/\ln\ln n}\\ &\leq \mathbf{e}^{\ln n}\left(\mathbf{e}^{\ln\ln\ln n-\ln\ln n}\right)^{3\ln n/\ln\ln n}\\ &= \mathbf{e}^{-2\ln n+3\ln n\frac{\ln\ln\ln n}{\ln\ln n}} \leq \mathbf{e}^{-\ln n} = \frac{1}{n}.\end{aligned}$$

Application (Bucket sort, Tri par paquets**).**
Soient $n = 2^m$ éléments à trier, tirés uniformément dans $[0, 2^k)$, $k \geq m$.
Le tri se fait en 2 étapes :

1) On place les éléments dans n boîtes. La j-ième boîte contient tous les éléments dont les m premiers digits correspondent au nombre $j-1$. Temps $O(n)$

   ex : Pour $n = 2^{10}$, dans la 4e boîte, on aura tous les éléments dont les 10 premiers digits sont: 0000000011

2) Chaque boîte est triée en utilisant un algorithme quadratique en temps.

On retourne la concaténation des listes triées. Soit X_j le nombre d'éléments qui tombent dans la j-ième boite, le temps pour trier est $\leq cX_j^2$ pour une constante c.

$$\begin{aligned}\mathbb{E}\left[\sum_{i=1}^{n} cX_j^2\right] &= c\sum_{i=1}^{n}\mathbb{E}\left[X_j^2\right] \\ &= nc\mathbb{E}\left[X_1^2\right] \\ &= cn\left(\frac{n(n-1)}{n^2}+1\right) = \left(2-\frac{1}{n}\right)cn,\end{aligned}$$

car X_1 est une Binomial Binom $(n, 1/n)$

Donc le tri est linéaire en moyenne.

5.3 Limite de la loi binomiale

Dans le modèle à m boules et n urnes. Soit p_r la probabilité que l'urne 1 ait r boules.

$$p_r = \binom{m}{r}\left(\frac{1}{n}\right)^r\left(1-\frac{1}{n}\right)^{m-r}$$

C'est la loi binomiale Binom $\left(m, \frac{1}{n}\right)$

Théorème 16.

Soit $X_n \sim \text{Binom}\,(n, p(n))$ *avec* $\lim_{n\to\infty} np(n) = \lambda$, *alors*

$$\lim_{n\to\infty}\mathbb{P}\left(X_n = k\right) = \boldsymbol{e}^{-\lambda}\frac{\lambda^k}{k!}$$

Démonstration.

$$\begin{aligned}\mathbb{P}\left(X_n = k\right) &= \binom{n}{k}p^k(1-p)^{n-k} \\ &\leq \frac{n^k}{k!}p^k\frac{(1-p)^n}{(1-p)^k} \\ &\leq \frac{(np)^k}{k!}\frac{\mathbf{e}^{-pn}}{(1-pk)} \\ &\geq \frac{(n-k+1)^k}{k!}p^k(1-p)^n \\ &\geq \frac{((n-k+1)p)^k}{k!}\mathbf{e}^{-pn}(1-p^2)^n \\ &\geq \mathbf{e}^{-pn}\frac{((n-k+1)p)^k}{k!}(1-p^2n)\end{aligned}$$

On a utilisé $e^x(1-x^2) \leq 1+x$ pour $|x| \leq 1$ pour passer de la 4-ème à la 5-ème ligne.

5.4 Approximation de Poisson

Soient m boules jetées dans n boites indépendamment et uniformément au hasard.

- $X_i^{(m)}$ est le nombre de boules dans la i-ème boite $1 \leq i \leq n$
- $\left(Y_i^{(m)}, 1 \leq i \leq n\right)$ sont des variables aléatoires de Poisson indépendantes de moyenne $\frac{m}{n}$

Théorème 17.

La distribution du vecteur $\left(Y_1^{(m)}, \cdots, Y_n^{(m)}\right)$ conditionné à $\sum_{i=1}^n Y_i^{(m)} = k$ est la même que celle du vecteur $\left(X_1^{(k)}, \cdots, X_n^{(k)}\right)$ pour toute valeur de m.

Démonstration.
Soit un vecteur $(k_1, \cdots, k_n)$ tel que $\sum k_i = k$.

$$\mathbb{P}\left(\left(X_1^{(k)}, \cdots, X_n^{(k)}\right) = (k_1, \cdots, k_n)\right) = \frac{k!}{k_1! \cdots k_n! n^k}$$

$$\begin{aligned}
\mathbb{P}\left(\left(Y_1^{(m)}, \cdots, Y_n^{(m)}\right) = (k_1, \cdots, k_n) \,|\, \sum_{i=1}^n Y_i^{(m)} = k\right) &= \frac{\mathbb{P}\left(Y_1^{(m)} = k_1 \cdots Y_n^{(m)} = k_n\right)}{\mathbb{P}\left(\sum_{i=1}^n Y_i^{(m)} = k\right)} \\
&= \frac{\prod_{i=1}^n \mathbb{P}\left(Y_i^{(m)} = k_i\right)}{\mathbf{e}^{-m}\frac{m^k}{k!}} \\
&= \prod_{i=1}^n \frac{\mathbf{e}^{-\frac{m}{n}}}{k_i!}\left(\frac{m}{n}\right)^{k_i} \frac{k!}{\mathbf{e}^{-m} m^k}.
\end{aligned}$$

Théorème 18.

Soit $f(x_1, \cdots, x_n)$ une fonction à valeurs positives ou nulles. Alors

$$\mathbb{E}\left[f\left(X_1^{(m)}, \cdots, X_n^{(m)}\right)\right] \leq e\sqrt{m}\mathbb{E}\left[f\left(Y_1^{(m)}, \cdots, Y_n^{(m)}\right)\right]$$

Démonstration.

$$\begin{aligned}
\mathbb{E}\left[f\left(Y_1^{(m)}, \cdots, Y_n^{(m)}\right)\right] &= \sum_{k=1}^{\infty} \mathbb{E}\left[f\left(Y_1^{(m)}, \cdots, Y_n^{(m)}\right) \,|\, \sum_{i=1}^n Y_i^{(m)} = k\right] \mathbb{P}\left(\sum_{i=1}^n Y_i^{(m)} = k\right) \\
&\geq \mathbb{E}\left[f\left(Y_1^{(m)}, \cdots, Y_n^{(m)}\right) \,|\, \sum_{i=1}^n Y_i^{(m)} = m\right] \frac{m^m \mathbf{e}^{-m}}{m!} \\
&\geq \mathbb{E}\left[f\left(X_1^{(m)}, \cdots, X_n^{(m)}\right)\right] \frac{1}{e\sqrt{m}}
\end{aligned}$$

car $m! < e\sqrt{m}\left(\frac{m}{e}\right)^m$.

On dira que le scenario correspondant au cas où le nombre de balles dans les boites sont de variables de Poisson indépendante de moyenne m/n correspond au cas Poisson tandis que le scenario où m boules sont jetées dans n boites correspond au cas exact.

Lemme 8.

Quand n boules sont jetées indépendamment et uniformément au hasard dans n boites (i.e. $n = m$), la charge maximale est au moins $\frac{\ln(n)}{\ln(\ln(n))}$ avec une probabilité au moins $1 - \frac{1}{n}$ pour n assez grand.

Démonstration.
On considère le cas Poisson : Le nombre de boules dans les boites sont des variables aléatoires de Poisson indépendantes de moyenne $\frac{m}{n} = 1$ ici.

$\mathbb{P}$(boite 1 a une charge $\geq M$ dans le cas Poisson) $\geq \frac{1}{eM!}$

$$\begin{aligned} \mathbb{P}\,(\text{ aucune des boites dans le cas Poisson n'a une charge } \geq M) &\leq \left(1 - \frac{1}{eM!}\right)^n \\ &\leq \mathbf{e}^{-\frac{n}{eM!}} \end{aligned}$$

Il suffit de montrer que pour $M = \frac{\ln(n)}{\ln(\ln(n))}$, on a $\mathbf{e}^{-\frac{n}{eM!}} \leq \frac{1}{n^2}$ car $\mathbb{P}$(aucune boite n'a une charge $\geq M$ dans le cas exact) $\leq \frac{e\sqrt{n}}{n^2} \leq \frac{1}{n}$

6 Martingales

6.1 Introduction

Définition 14.

Une suite de variables aléatoires $Z_0, Z_1, \cdots, Z_n$ est une **martingale** par rapport à $X_0, X_1, \cdots, X_n$ si pour tout $n \geq 0$, on a

- Z_n est une fonction de $X_0, X_1, \cdots, X_n$
- $\mathbb{E}[|Z_n|] < \infty$
- $\mathbb{E}[Z_{n+1}|X_0, X_1, \cdots, X_n] = Z_n$

Une suite de variables aléatoires $Z_0, Z_1, \cdots, Z_n$ est appelée **martingale** si $\mathbb{E}[|Z_n|] =< \infty$ et $\mathbb{E}[Z_{n+1}|Z_0, Z_1, \cdots, Z_n] = Z_n$.

Exemple.

Soit $(X_i)_{1 \leq i \leq n}$ une suite de variables aléatoires indépendantes et de moyenne $\mathbb{E}[X_i] = 0$. Alors $Z_n = \sum_{i=1}^{n} X_i$ est une martingale car:

$$\begin{aligned} \mathbb{E}[Z_{n+1}|Z_0, Z_1, \cdots, Z_n] &= \mathbb{E}[X_1 + X_2 + \cdots + X_{n+1}|X_1, \cdots, X_n] \\ &= Z_n + \mathbb{E}[X_n + 1|X_1, \ldots, X_n] \\ &= Z_n \end{aligned}$$

Construction générique

Soient $X_0, X_1, \ldots, X_n$ des variables aléatoires et Y tel que $\mathbb{E}[|Y|] < \infty$.
$Z_i = \mathbb{E}[Y|X_0, X_1, \cdots, X_i]$ pour $i \in \{1, \cdots, n\}$ est une martingale par rapport à $X_0, \ldots, X_n$.

Exemple.

Soit $G \sim G(n, p)$. $m = \binom{n}{2}$ arêtes possibles $e_1, \cdots, e_m$

$$X_i = \begin{cases} 1 \text{ si } e_i \text{ est dans } G \\ 0 \text{ sinon} \end{cases}$$

$Y = F(G) =$ taille du plus grand ensemble stable de G.
$Z_0 = \mathbb{E}[F(G)]$
$Z_i = \mathbb{E}[F(G)|X_1, \cdots, X_i]$, $i \in \{1, \cdots, m\}$.
$Z_m = F(G)$.

Exemple.

$n = m = 3$, $p = \frac{1}{2}$, $f(G) = \chi(G)$ le nombre chromatique de G. `dessin à ajouter!`
$\mathbb{E}[f(G)|X_1 = 0] = 1.75$
$\mathbb{E}[f(G)|X_1 = 1] = 2.25$

6.2 Inégalités pour des Martingales

Théorème 19 (Inégalité d'Azuma - Hoeffding**).**

Soit $X_0, \cdots, X_n$ une martingale tel que $|X_k - X_{k-1}| \leq c_k$ presque sûrement. Alors pour tout $t \geq 0$ et $\lambda > 0$,

$$\mathbb{P}(|X_t - X_0| \leq \lambda) \leq 2\boldsymbol{e}^{-\frac{\lambda^2}{2\sum_{k<1}^{t} c_k^2}}$$

Démonstration.

Soit $Y_i = X_i - X_{i-1}$, $i \in \{1, \cdots, t\}$, $|Y_i| \leq c_i$.
$\mathbb{E}[Y_i|X_0, \cdots, X_{i-1}] = 0$ car X est une martingale.

$Y_i = -c_i \frac{1-\frac{Y_i}{c_i}}{2} + c_i \frac{1+\frac{Y_i}{c_i}}{2}$.

On obtient par convexité: $e^{\alpha Y_i} \leq \frac{1-\frac{Y_i}{c_i}}{2} e^{-\alpha c_i} + \frac{1+\frac{Y_i}{c_i}}{2} e^{\alpha c_i} = \frac{e^{\alpha c_i}+e^{-\alpha c_i}}{2} + \frac{Y_i}{2c_i}\left(e^{\alpha c_i} - e^{-\alpha c_i}\right)$.

$\mathbb{E}\left[e^{\alpha Y_i} | X_0, \cdots, X_{i-1}\right] \leq \frac{e^{\alpha c_i}+e^{-\alpha c_i}}{2} \leq e^{\frac{(\alpha c_i)^2}{2}}$.

$$\begin{aligned}
\mathbb{E}\left[e^{\alpha(X_t - X_0)}\right] &= \mathbb{E}\left[\prod_{i=1}^{t-1} e^{\alpha Y_i}\right] \\
&= \mathbb{E}\left[\prod_{i=1}^{t-2} e^{\alpha Y_i} \mathbb{E}\left[e^{\alpha Y_t} | X_0, \cdots, X_{t-1}\right]\right] \\
&\leq \mathbb{E}\left[\prod_{i=1}^{t-2} e^{\alpha Y_i}\right] \mathbf{e}^{\alpha^2 \frac{c_k^2}{2}} \\
&\leq e^{\alpha^2 \sum_{k=1}^{t} \frac{c_k^2}{2}}
\end{aligned}$$

$$\begin{aligned}
\mathbb{P}\left(X_t - X_0 \geq \lambda\right) &= \mathbb{P}\left(e^{\alpha(X_t - Y_0)} \geq e^{\alpha\lambda}\right) \\
&\leq \frac{\mathbb{E}\left[e^{\alpha(X_t - Y_0)}\right]}{e^{\alpha\lambda}} \\
&\leq e^{\alpha^2 \sum_{k=1}^{t} \frac{c_k^2}{2} - \alpha\lambda} \\
&\leq e^{-\frac{\lambda^2}{2}\sum c_k^2}
\end{aligned}$$

pour $\alpha = \frac{\lambda}{\sum c_k^2}$.

6.3 Applications

6.3.1 Boules et urnes

m boules sont jetées dans n urnes de manière uniforme et indépendante.

- X_i = boite dans laquelle la i-ème boule tombe.
- F = nombres de boites vides à la fin. $\mathbb{E}[F] = Z_0 = n\left(1 - \frac{1}{n}\right)^m$
- $Z_i = \mathbb{E}[F | X_1, \cdots, X_i]$ est une martingale.
- On peut écrire $F = f(X_1, \ldots, X_m)$ avec $|f(x_1, \ldots, x_i, \cdots, x_m) - f(x_1, \cdots, y_i, \ldots x_m)| \leq 1$

Soit f_i la fonction correspondant au cas où la i-ème boule n'a pas été ajoutée, $f_i(x_1, \cdots x_m) = f(x_1, \cdots, x_{i-1}, *, x_{i+1}, \cdots, x_m)$ ne dépend donc pas de x_i. On a alors: $f_i(X_1, \ldots, X_m) - 1 \leq F \leq f_i(X_1, \ldots, X_m) + 1$. Donc en passant à l'espérance:

$\mathbb{E}[f_i(\underline{X}) | X_1, \cdots, X_{i-1}] - 1 \leq Z_{i-1} \leq \mathbb{E}[f_i(\underline{X}) | X_1, \cdots, X_{i-1}] + 1$.

$\mathbb{E}[f_i(\underline{X}) | X_1, \cdots, X_i] - 1 \leq Z_i \leq \mathbb{E}[f_i(\underline{X}) | X_1, \cdots, X_i] + 1$

$|Z_i - Z_{i-1}| \leq 2$.

$\mathbb{P}\left(|F - \mathbb{E}[F]| \leq \epsilon\right) \leq 2e^{-\frac{\epsilon^2}{8m}}$

7 La transition de phase des graphes d'Erdős-Rényi

Soit $n \in \mathbb{N}$ et $0 \leq p \leq 1$, $G(n,p)$ est un espace de probabilité sur les graphes à n sommets $\{1, \cdots, n\}$ déterminé par $\mathbb{P}\left(\{i,j\}_{i \neq j} \in G\right) = p$ et ces événements sont indépendants.

Nous allons étudié les propriétés de ces graphes lorsque n tend vers l'infini et dans le **régime** $p = \frac{c}{n}$, où c est une constante indépendante de n.

Par exemple, le degré du sommet 1 suit une loi binomiale $\text{Bin}\left(n-1, \frac{c}{n}\right) \simeq_{n \to \infty} \text{Poi}(c)$ (loi de Poisson)

Notation.
Soit $C(v)$ la composante contenant v. $|C(v)|$ est sa taille.
$L_1 = \max_v |C(v)|$, $L_2 =$ deuxième plus grande.

7.1 Trois processus

- Processus de branchement Poissonien
  - Paramètre : c
  - Z_t iid $\sim \text{Poi}(c)$
  - $Y_t := \begin{cases} Y_0 = 1 \\ Y_t = Y_{t-1} + Z_t - 1 \end{cases}$ (Taille du bord de l'arbre après t itérations).
  - $T = \min\{t, Y_t = 0\}$ $T = \infty$ si $Y_t > 0 \forall t$. (Taille de l'arbre).
- Processus de branchement binomial
  - Paramètres $m \in \mathbb{N}$ et $p \in [0,1]$.
  - Z_t iid $\sim \text{Bin}(m,p)$
  - $Y_t := \begin{cases} Y_0 = 1 \\ Y_t = Y_{t-1} + Z_t - 1 \end{cases}$
  - $T = \min\{t, Y_t = 0\}$
- Processus de branchement du graphe
  - Paramètres n et $p \in [0,1]$
  - $Z_1, \cdots, Z_n$, $Z_t \sim \text{Bin}(N_{t-1}, p)$
  - $Y_t := \begin{cases} Y_0 = 1 \\ Y_t = Y_{t-1} + Z_t - 1 \end{cases}$
  - N_t, $t \geq 0$ est défini par $\begin{cases} N_0 = n-1 \\ N_t = N_{t-1} - Z_t = n - t - Y_t \end{cases}$
  - $T = \min\{t, Y_t = 0\}$ $1 \leq T \leq n$.

7.2 Etude de $T_c^{Po} = T$

On considère le processus de branchement Poissonien.

Théorème 20.

- *Si $c \leq 1$, T est fini presque sûrement*
- *Si $c > 1$, T est infini avec probabilité y où $y > 0$, $e^{-cy} = 1 - y$.*

Démonstration.
Ce Théorème a déjà été démontré au Chapitre 4 (cf. probabilité d'extinction). Autre version:

- Si $c \geq 1$, alors $z = 1 - y = \mathbb{P}(T < \infty)$.

$$z = \sum_{i=0}^{\infty} \mathbb{P}(Z_1 = i)\, z^i = \sum_{i=0}^{\infty} e^{-c} \frac{c^i z^i}{i!} = e^{c(z-1)}$$

7.3 Le processus d'exploration

Les sommets sont soit vivants, soit morts, soit neutres. Les vivants sont mis dans une file.

$t = 0$ v est vivant, tous les autres sont neutres.

A chaque instant t, on retire un sommet vivant w de la file et on regarde toutes les arêtes $\{w, w'\}$ où w' est neutre. w est maintenant mort et les w' neutres voisins de w (possiblement vide) deviennent vivants et sont ajoutés en fin de file. Le processus s'arrête quand la file est vide. Soit T ce temps. Au temps T, tous les sommets sont neutres ou morts et l'ensemble des morts est $C(v)$, an particulier $T = |C(v)|$.

- Z_t le nombre de sommets ajoutés à la file au temps t.
- Y_t est la taille de la file à l'instant t. $Y_t = Y_{t-1} - 1 + Z_t$.
- N_t est le nombre de sommets neutres au temps t. $\begin{cases} N_0 = n - 1 \\ N_t = n - Y_t - t = N_{t-1} - Z_t \end{cases}$
- $Z_t \sim \text{Bin}(N_{t-1}, p) \sim \text{Bin}(n - (t-1) - Y_{t-1}, p)$.

Comme $N_1 = N_{t-1} - Z_t$, on a $N_t \sim \text{Bin}(N_t, 1-p)$. Par récurrence, $N_t \sim \text{Bin}(n-1, (1-p)^t)$, $0 \leq t \leq n$. Si $T = t$, alors $N_t = n - t$.

Proposition 3.
Dans $G(n,p)$,

$$\mathbb{P}(|C(v)| = t) \leq \mathbb{P}\left(\text{Bin}\left(n-1, (1-p)^t\right) = n - t\right)$$

7.4 Comparaison des processus sur le graphe et branchement de Poisson

On rappelle que $p = \frac{c}{n}$. Comme vu au chapitre 5, $Z_1 \sim \text{Bin}\left(n-1, \frac{c}{n}\right) \simeq \text{Poi}(c)$ de même pour Z_t tant que $n - N_t = o(n)$.

Théorème 21.
Pour tout $c > 0$ et k fixé

$$\lim_{n\to\infty} \mathbb{P}\left(|C(v)| = k \text{ dans } G\left(n, \frac{c}{n}\right)\right) = \mathbb{P}\left(T_c^{Po} = k\right)$$

Démonstration.
Z_t^{Po}, T_c^{Po} sont les quantités associées au processus de branchement Poissonien et Z_t^{gr}, T^{gr} au processus de branchement du graphe.

$$\Gamma = \left\{ \vec{z} = (z_1, \cdots, z_k) \text{ tel que pour } y_n := \begin{cases} y_0 = 1 \\ y_t = y_{t-1} + z_t - 1 \end{cases} \text{ on ait } y_t > 0 \text{ pour } t < k \text{ et } y_k = 0 \right\}$$

$$\mathbb{P}(T^{gr} = k) = \sum_{\vec{z} \in \Gamma} \mathbb{P}(Z_i^{gr} = z_i \ 1 \leq i \leq k)$$

$$\mathbb{P}\left(T_c^{Po}=k\right)=\sum_{\vec{z}\in\Gamma}\mathbb{P}\left(Z_i^{Po}=z_i,\,1\leq i\leq k\right)$$

Pour $\vec{z}\in\Gamma$ fixé

$$\mathbb{P}\left(Z_i^{gr}=z_i,\,1\leq i\leq k\right)=\prod_{i=1}^{k}\mathbb{P}\left(\mathrm{Bin}\left(N_{i-1}^{gr},p\right)=z_i\right)\to\prod_{i=1}^{k}\mathbb{P}\left(Z_i^{Po}=z_i\right)$$

Théorème 22.

$$\forall c\ k\in\mathbb{N}\ \mathbb{P}\left(T_c^{Po}=k\right)=e^{-ck}\frac{(ck)^{k-1}}{k!}$$

Démonstration.
On a

$$\mathbb{P}\left(T_c^{Po}=k\right)=\lim_{n\to\infty}\mathbb{P}\left(|C(v)|=k\text{ dans }G\left(n,\frac{c}{n}\right)\right),$$

et on calcule la limite du terme de droite. Pour v fixé, il existe $\binom{n}{k-1}$ choix pour $C(v)\backslash\{v\}$ ensemble S. Pour un tel ensemble S, il y a une probabilité $O(p^k)=O(n^{-k})$ que $G(n,p)$ ait plus de $(k-1)$ arêtes.

Si $G(n,p)|_S$ a précisément $(k-1)$ arêtes, alors c'est un arbre.

Il y a k^{k-2} tels arbres, chacun ayant une probabilité $p^{k-1}(1-p)^{\binom{k}{2}-k+1}\sim p^{k-1}=c^{k-1}n^{1-k}$

Donc la probabilité que $G(n,p)$ restreint à S soit un graphe connecté est $\sim k^{k-2}c^{k-1}n^{1-k}$.

Pour que ce soit une composante, il ne faut pas d'arêtes entre $C(v)$ et son complément, probabilité $(1-p)^{k(n-k)}\sim e^{-ck}$.

$$\mathbb{P}\left(|C(v)|=k\right)\sim\binom{n}{k-1}k^{k-2}c^{k-1}n^{1-k}e^{-ck}\to e^{-ck}\frac{(ck)^{k-1}}{k!}$$

Théorème 23.

Pour tout u,

- $\mathbb{P}\left(T_{n,p}^{gr}\geq u\right)\leq\mathbb{P}\left(T_{n-1,p}^{bin}\geq u\right)$
- $\mathbb{P}\left(T_{n,p}^{gr}\geq u\right)\geq\mathbb{P}\left(T_{n-u,p}^{bin}\geq u\right)$

Démonstration.

7.5 Les régimes sous-critiques et sur-critiques

$p=\frac{c}{n}$.

- $c<1$. $\mathbb{P}\left(T_{n,p}^{gr}\geq u\right)\leq\mathbb{P}\left(T_{n-1,p}^{bin}\geq u\right)$ Par l'approximation de Poisson, $\mathbb{P}\left(|C(v)|\geq u\right)\leq(1+o(1))\mathbb{P}\left(T_c^{Po}\geq u\right)$

  Par Stirling : $\mathbb{P}\left(T_c^{Po}=k\right)\sim\frac{1}{\sqrt{2\pi}}k^{\frac{-3}{2}}c^{-1}\left(ce^{1-c}\right)^k$

  Comme $ce^{1-c}<1$, on a $\mathbb{P}\left(T_c^{Po}\geq u\right)<e^{-u(\alpha+o(1))}$ avec $\alpha=c-1-\ln c>0$.

  $u=K\ln n\Longrightarrow\mathbb{P}\left(|C(v)|\geq u\right)<n^{-(1+\epsilon)}$

  Donc $\mathbb{P}\left(\exists v,\,|C(v)|\geq u\right)\leq n^{-\epsilon}\to 0$ d'où $L_1=\mathcal{O}\left(\ln n\right)$ avec une probabilité tendant vers 1.

- $c > 1$. y solution > 0, $e^{-cy} = 1 - y$, δ petit, K grand. On définit $S = K \ln n$, $L^- = (y - \delta)n$ et $L^+ = (y + \delta)n$.

  $C(v)$ est dite $\begin{cases} \text{petite si } |C(v)| < S \\ \text{géante si } L^{-1} < |C(v)| < L^+ \\ \text{bizarre sinon} \end{cases}$

  - $C(v)$ est bizarre avec une probabilité $o\left(n^{-20}\right)$. n choix pour v. n choix pour $|C(v)|$. Il suffit de montrer que $\mathbb{P}\left(|C(v)| = t\right) = o\left(n^{-18}\right)$ pour t bizarre.

    D'après la Proposition 3, il suffit de borner $\mathbb{P}\left(\text{Bin}\left(n-1, 1-\left(1-\frac{c}{n}\right)^t\right) = t-1\right)$. $t \sim xn$. $1 - \left(1 - \frac{c}{n}\right)^t \sim 1 - e^{-cx} \neq x$ puis Chernoff.
  - $\alpha = \mathbb{P}\left(C(v) \text{ est petit}\right)$ $\mathbb{P}\left(T^{bin}_{n-s,p} \geq s\right) \leq 1 - \alpha \leq \mathbb{P}\left(T^{bin}_{n-1,p} \geq s\right)$. Comme $\mathbb{P}\left(T^{Po}_c \geq s\right) \sim \mathbb{P}\left(T^{Po}_c = \infty\right) \sim y$, on a: $C(v)$ est géante avec une probabilité $\sim y$.

  Donc le nombre moyen de sommets dans les composantes géantes $\sim ny$. Chaque composante géante a une taille entre $(y - \delta)n$ et $(y + \delta)n$. On veut une unique composante géante de taille $\sim yn$.

  On va utiliser la technique de l'arrosage.

  $p_1 = n^{\frac{-3}{2}}$. $G_1 \sim G(n, p_1)$ indépendant de $G \sim G(n, p)$ sur les mêmes sommets. $G^+ = G \cup G_1$. $G^+ \sim G(n, p^+)$ avec $p^+ = p + p_1 - pp_1$.

  Supposons que $G(n, p)$ a plus d'une composante géante. Soient V_1 et V_2 ensembles de sommets. $\Omega(n^2)$ paires $\{v_1, v_2\}$ $v_1 \in V_1$, $v_2 \in V_2$. Soit p_1 suffisamment grand pour qu'avec une probabilité $1 - o(1)$ une de ses paires est dans G, donc dans G^+. V_1 et V_2 sont connectés en une composante de taille $\geq 2y(1 - \delta)n \rightarrow$ bizarre. $p^+ \sim p = \frac{c}{n}$ probabilité pour que G^+ ait une composante bizarre $o\left(n^{-20}\right)$.

  Finallement, $L_1 \sim yn$ $L_2 \leq S = \mathcal{O}\left(\ln n\right)$

Part II

La méthode probabiliste

8 Introduction à la méthode probabiliste

8.1 Un premier exemple

Définition 15 (Nombre de Ramsey**).**

Le nombre de Ramsey $R(k,l)$ est le plus petit entier n tel que dans tout coloriage des arêtes du graphe complet sur n sommets K_n en rouge et bleu, il y a soit un K_k rouge soit un K_l bleu.

Ramsey (1929) a montré $R(k,l) < \infty \forall k,l$.

Proposition 4.

Si $\binom{n}{k}2^{1-\binom{k}{2}} < 1$*, alors* $R(k,k) > n$.

En particulier, $R(k,k) > \lfloor 2^{\frac{k}{2}} \rfloor$ *pour* $k \geq 3$.

Démonstration.

On considère un coloriage aléatoire des arêtes de K_n.

Pour tout ensemble R fixé de k sommets, on définit l'événement $A_R =$ { le sous-graphe induit par R est monochromatique}. On a $\mathbb{P}(A_R) = 2^{1-\binom{k}{2}}$.

Comme il y a $\binom{n}{k}$ choix possibles pour R, la probabilité qu'au moins un des A_R se produise est $\mathbb{P}(\bigcup_R A_R) \leq \binom{n}{k}2^{1-\binom{k}{2}} < 1$. Donc avec une probabilité > 0, aucun des A_R ne se produit et il existe un coloriage de K_n sans K_k monochromatique, c'est à dire $R(k,k) > n$.

Si $k \geq 3$ alors on prend $n = \lfloor 2^{\frac{k}{2}} \rfloor$ et on a: $\binom{n}{k}2^{1-\binom{k}{2}} < \frac{n^k}{k!}\frac{2^{1+\frac{k}{2}}}{2^{\frac{k}{2}}} < 1$. Donc $R(k,k) > \lfloor 2^{\frac{k}{2}} \rfloor$.

8.2 Théorie des graphes

Définition 16.

Un tournois sur un ensemble V de n joueurs est une orientation $T = (V,E)$ des arêtes du graphe complet sur l'ensemble des sommets V.

$\forall x,y \in V$, soit (x,y), soit (y,x) est dans E.

Interprétation : $(x,y) \in E \Leftrightarrow x \longrightarrow y \Leftrightarrow x$ bat y.

T a la propriété S_k si pour tout ensemble de k joueurs, il en existe un qui les bat tous.

Exemple.

$T_3 = (V,E)$.

$V = \{1,2,3\}$. $E = \{(1,2),(2,3),(3,1)\}$. T_3 a la propriété S_1.

Théorème 24.

Si $\binom{n}{k}(1-2^{-k})^{n-k} < 1$*, alors il existe un tournois sur* n *sommets ayant la propriété* S_k.

Démonstration.

On considère un tournois aléatoire sur $V = \{1,\cdots,n\}$, c'est à dire pour $1 \leq i < j \leq n$, on choisit indépendemment (i,j) ou (j,i) avec probabilité $\frac{1}{2}$ indépendamment des autres choix. Les $2^{\binom{n}{2}}$ tournois sont équiprobables.

Pour tout ensemble K de taille k dans V, on définit l'ensemble $A_K =$ { Il n'existe pas de sommet qui batte tous les membres de K}

$\mathbb{P}(A_K) = (1-2^{-k})^{n-k}$

$\mathbb{P}(\bigcup_K A_K) \leq \sum_K \mathbb{P}(A_K) = \binom{n}{k}(1-2^{-k})^{n-k} < 1$.

Définition 17.

Un **ensemble dominant** d'un graphe $G = (V,E)$ est un sous-ensemble $U \subset V$ tel que tout sommet $v \in V \setminus U$ a au moins un voisin dans U.

Théorème 25.

Soit $G = (V, E)$ un graphe à n sommets de degré minimal $\delta > 1$.
Alors G a un ensemble dominant d'au plus $\frac{n(1+ln(\delta+1))}{\delta+1}$ sommets.

Démonstration.

Soit $p \in [0, 1]$. On choisit $X \subset V$ en prenant chaque sommet de V avec une probabilité p de manière indépendante.

$Y = Y_X$ est l'ensemble aléatoire de tous les sommets dans $V \setminus X$ qui n'ont pas de voisin dans X.

Pour un sommet $v \in V$ fixé, $\mathbb{P}(v \in Y) = \mathbb{P}(\text{v et ses voisins ne sont pas dans X}) \leq (1-p)^{\delta+1}$.

$$\begin{aligned} \mathbb{E}|Y| &= \mathbb{E}\left[\sum_{v \in V} \mathbb{1}(v \in Y)\right] \\ &= \sum_{v \in V} \mathbb{P}(v \in Y) \leq n(1-p)^{\delta+1} \end{aligned}$$

L'ensemble $U = X \cup Y$ est un ensemble dominant. $\mathbb{E}|X| + |Y| \leq np + n(1-p)^{\delta+1}$.
Donc il existe une réalisation tel que $|X| + |Y_X| \leq np + n(1-p)^{\delta+1}$.
On optimise en p en utilisant que $1 - p \leq e^{-p}$.
$|U| \leq np + n\mathrm{e}^{-p(\delta+1)}$ minimal pour $p = \frac{ln(\delta+1)}{\delta+1}$.
$|U| \leq \frac{n(1+ln(\delta+1))}{\delta+1}$

8.3 Théorie des nombres

Définition 18.

Un sous-ensemble A d'un groupe abélien G est dit **sum-free** si $(A + A) \cap A = \emptyset$, c'est à dire $\forall a_1, a_2, a_3 \in A, a_1 + a_2 \neq a_3$.

Théorème 26.

Tout ensemble $B = \{b_1, \cdots, b_n\}$ de n entiers non nuls contient un sous-ensemble sum-free A de taille $|A| > \frac{1}{3}n$.

Démonstration.

Soit $p = 3k + 2$ un nombre premier tel que $p > 2max\,|b_i|$ (exo: montrer qu'un tel nombre premier existe!).

$C = \{k + 1, \cdots 2k + 1\}$. C est sum-free dans $\mathbb{Z}_p$.
$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}$.
Soit x un entier choisi uniformément dans $\{1, \ldots p-1\}$.
Soit $(d_i)_{i \in [\![1 \cdots n]\!]}$ tel que $d_i \equiv xb_i \mod p$ alors $0 \leq d_i < p$.
Pour i fixé, l'application de $\{1, \ldots p-1\}$ dans $\mathbb{Z}_p$ qui à x associe xb_i est bijective, donc $\mathbb{P}(d_i \in C) = \frac{|C|}{p-1} > \frac{1}{3}$.
En particulier, $\mathbb{E}[|\{b_i, d_i \in C\}|] > \frac{n}{3}$.
Donc $\exists x \in [\![1 \cdots p-1]\!]$ et $A \subset B$ avec $|A| > \frac{n}{3}$ tel que $xa \mod p \in C$, $\forall a \in A$.
A est sum-free car si $a_1 + a_2 = a_3$, alors $xa_1 + xa_2 \equiv xa_3 \mod p$, contredisant le fait que C soit sum-free dans $\mathbb{Z}_p$

8.4 Combinatoire

Définition 19.

Un hypergraphe est une paire $H = (V, E)$ où V est un ensemble fini dont les éléments sont les sommets et E est une famille de sous-ensembles de V appelés les arêtes. Il est dit **n-uniforme** si chaque arête contient n sommets.

Définition 20.

> H est deux coloriable si il existe un coloriage de V tel qu'aucune arête ne soit monochromatique. On note $m(n)$ le nombre minimal possible d'arêtes d'un hypergraphe n-uniforme qui n'est pas deux coloriable.

Proposition 5.

> *Tout hypergraphe n-uniforme avec moins de 2^{n-1} arêtes est 2-coloriable, donc $m(n) \geq 2^{n-1}$.*

Démonstration.

Soit $H = (V, E)$ un hypergraphe n-uniforme ayant moins de 2^{n-1} arêtes. On considère un coloriage aléatoire de V en 2 couleurs. $\forall e \in E$, $A_e = \{e \text{ est monochromatique}\}$. $\mathbb{P}(A_e) = 2^{1-n}$

$\mathbb{P}(\bigcup_e A_e) \leq \sum_e \mathbb{P}(A_e) < 1$.

9 Linéarité de l'espérance

Soit σ une permutation aléatoire de $\{1, \cdots, n\}$ choisie uniformément. $X(\sigma)$ est le nombre de points fixes de σ. Voici un calcul simple de $\mathbb{E}[X(\sigma)]$.

$X = X_1 + \cdots + X_n$ $X_i = \mathbb{1}(\sigma(i) = i)$.

$\mathbb{E}[X_i] = \mathbb{P}(\sigma(i) = i) = \frac{1}{n}$. $\mathbb{E}[X] = 1$.

Théorème 27.

Il existe un tournois T avec n joueurs et au moins $n!2^{-(n-1)}$ chemins Harmiltoniens (qui visitent tous les sommets exactement une fois).

Démonstration.

Dans un tournoi aléatoire, soit X le nombre de chemins Harmiltoniens. Pour chaque permutation σ, on note $X_\sigma = \mathbb{1}(\sigma$ donne un chemin harmiltonien), c'est à dire

$(\sigma(i), \sigma(i+1)) \in T$ $1 \leq i < n$.

$X = \sum_\sigma X_\sigma$

$\mathbb{E}[X] = n!2^{-(n-1)}$.

9.1 Division de graphes

Théorème 28.

Soit $G = (V, E)$ un graphe à n sommets et e arêtes. Alors G contient un sous-graphe biparti avec au moins $\frac{e}{2}$ arêtes.

Démonstration.

Soit $T \subset V$ un sous-ensemble aléatoire avec $\mathbb{P}(x \in T) = \frac{1}{2}$ et des choix indépendants.

$\{x, y\}$ est traversante si exactement un des x, y est dans T.

L'ensemble des arêtes traversantes constitue un graphe biparti. Soit X le nombre d'arêtes traversantes. $X = \sum_{\{x,y\} \in E} X_{xy}$, où $X_{xy} = \mathbf{1}((x, y)$ est traversante).

Comme $\mathbb{E}[X_{xy}] = 1/2$, on a $\mathbb{E}[X] = \frac{e}{2}$.

9.2 Equilibrage de vecteurs

Théorème 29.

Soit $(v_1, \cdots, v_n) \in \mathbb{R}^{n^2}$ avec $\|v_i\| = 1$ où $\|v_i\|$ est la norme Euclidienne. Alors $\exists \epsilon_1 \cdots \epsilon_n = \pm 1$ tel que $|\epsilon_1 v_1 + \cdots + \epsilon_n v_n| \leq \sqrt{n}$ et $\exists \epsilon_1 \cdots \epsilon_n = \pm 1$ tel que $|\epsilon_1 v_1 + \cdots + \epsilon_n v_n| \geq \sqrt{n}$

Démonstration.

$\epsilon_1 \cdots \epsilon_n$ indépendants $\in \{-1, 1\}$.

$X = \|\epsilon_1 v_1 + \cdots + \epsilon_n v_n\|^2 = \sum_{i=1}^n \sum_{j=1}^n \epsilon_i \epsilon_j \langle v_i, v_j \rangle$

$\mathbb{E}[\epsilon_i \epsilon_j] = \mathbb{E}[\epsilon_i]\mathbb{E}[\epsilon_j] = 0$ pour $i \neq j$.

$\mathbb{E}[X] = \sum_{i=1}^n \langle v_i, v_i \rangle = n$.

Théorème 30.

Soit M une matrice d'éléments $a_{ij} = \pm 1$, $1 \leq i, j \leq n$.

$\exists x_i, y_j \in \{\pm 1\}$ $1 \leq i, j \leq n$ tel que $\sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i y_j \geq \left(\sqrt{\frac{2}{\pi}} + o(1)\right) n^{\frac{3}{2}}$.

Démonstration.

Soit $y_1 \cdots y_n = \pm 1$ choisis indépendament et uniformément.

$R_i = \sum_{j=1}^n a_{ij} y_j$ et $R_i = \sum_{j=1}^n \zeta_j$ avec $\zeta_j = \pm 1$ avec une probabilité $\frac{1}{2}$ et i.i.d.

Lemme 9.

Soit $S_n = \sum_{i=1}^n \zeta_i$ où $\zeta_i = \pm 1$ avec probabilité $1/2$. Alors $\mathbb{E}[|S_n|] = n2^{1-n}\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}$.

$\mathbb{E}[|R_i|] = \mathbb{E}[|\sum \zeta_j|] = n2^{1-n}\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor} = \left(\sqrt{\frac{2}{\pi}} + o(1)\right)\sqrt{n}$.
Soit $R = \sum_{i=1}^{n} |R_i|$. $\mathbb{E}[R] = \sum_{i=1}^{n} \mathbb{E}[|R_i|] = \left(\sqrt{\frac{2}{\pi}} + o(1)\right) n^{\frac{3}{2}}$.
Enfin on choisit x_i égale au signe de R_i.

Démonstration.
du Lemme 9 On a

$$|S_{n+1}| = \mathbf{1}(|S_n| = 0) + (1 - \mathbf{1}(|S_n| = 0))(|S_n| + \zeta_{n+1}),$$

donc

$$\mathbb{E}[|S_{n+1}|] = \mathbb{P}\left(|S_n| = 0\right) + \mathbb{E}[|S_n|],$$

et

$$\mathbb{P}\left(() \, |S_n| = 0\right) = \mathbf{1}(n = 2k)\binom{n}{k}\frac{1}{2^n}.$$

On a donc par induction:

$$\begin{aligned}
\mathbb{E}[|S_{n+1}|] &= \frac{1}{2^2 k}\binom{2k}{k} + 2k2^{1-2k}\binom{2k-1}{k-1} \\
&= 2^{-2k}(2k+1)\binom{2k}{k}. \\
\mathbb{E}[|S_n|] &= (2k-1)2^{2-2k}\binom{2k-2}{k-1} \\
&= 2^{1-2k}2k\binom{2k-1}{k-1}.
\end{aligned}$$

9.3 Altérations

Définition 21.
Le nombre de stabilité de G : $\alpha(G) \geq t \Leftrightarrow \exists t$ sommets sans arêtes entre eux.

Théorème 31.
Soit un graphe simple $G = (V, E)$ *ayant* n *sommets et* $\frac{nd}{2}$ *arêtes* $d \geq 1$. *Alors* $\alpha(G) \geq \frac{n}{2d}$.

Démonstration.
$S \subset V$ sous-ensemble aléatoire. $\mathbb{P}\left(v \in S\right) = p$ choisi de manière indépendante. Soit X le cardinal de S et Y le nombre d'arêtes dans le graphe induit par S ($G|_S$).
$\mathbb{E}[X] = np$. $\mathbb{E}[Y] = \sum_{i,j \in E} \mathbb{P}\left(i, j \in S\right) = \frac{nd}{2}p^2$
$\mathbb{E}[X - Y] = np - \frac{nd}{2}p^2$ maximal pour $p = \frac{1}{d}$ et alors $\mathbb{E}[X - Y] = \frac{n}{2d}$.
Donc $\exists S$ pour lequel le nombre de sommets moins le nombre d'arêtes est au moins $\frac{n}{2d}$. On choisit un sommet de chaque arête de S et on le retire. On obtient S^* avec au moins $\frac{n}{2d}$ sommets et S^* est un ensemble indépendant.

9.4 Altérations suite : Recoloriage

Rappel. $m(n) > m \Leftrightarrow$ étant donné un hypergraphe $H = (V, E)$ n-uniforme avec m arêtes, il existe un 2-coloriage de V tel qu'aucune arête ne soit monochromatique.

Théorème 32 (Radhakrishnan et Srinivasan 2000**).**
S'il existe $p \in [0, 1]$ *avec* $k(1-p)^n + k^2 p < 1$, *alors* $m(n) > 2^{n-1}k$

Corollaire 3.
$m(n) = \Omega\left(2^n \left(\frac{n}{\ln n}\right)^{\frac{1}{2}}\right)$.

Démonstration.

$1-p \leq \mathbf{e}^{-p}$ et $k\mathbf{e}^{-np}+k^2p$ qui est minimal en $p=\frac{\ln \frac{n}{k}}{n}$ on obtient alors $\frac{k^2}{n}(1+\ln \frac{n}{k})<1$ pour la condition du théorème. Celle-ci est donc vérifiée si $k=c\left(\frac{n}{\ln n}\right)^{\frac{1}{2}}$ pour $c<\sqrt{2}$ pour n suffisament grand.

Démonstration (Démonstration du théorème**).**

On fixe un hypergraphe $H=(V,E)$ avec $m=2^{n-1}k$ arêtes et p satisfaisant la condition.

Pour chaque $v \in V$, on effectue 2 tirages à pile ou face $\mathbb{P}(A_v=1)=\frac{1}{2}$ et $\mathbb{P}(B_v=1)=p$ et les sommets de V sont ordonnés aléatoirement.

On effectue un coloriage de V en deux étapes:

- 1-ère étape: on colorie $v \in V$ en rouge si $A_v=1$ et en bleu sinon. Ce coloriage est le premier coloriage. On définit $D=\{v \in V,\ v \text{ est dans une arête monochromatique}\}$.
- 2-ème étape: on considère les éléments de D à la suite dans l'ordre induit par celui de V.

  Quand d est considéré, on dit qu'il est encore dangereux s'il existe une arête $e \in E$ contenant d qui était monochromatique dans le premier coloriage et pour laquelle aucun sommet n'a encore changé de couleur.

  Si d n'est plus dangereux, on ne fait rien. Si d est encore dangereux, si $B_v=1$, on change de couleur. Sinon, on ne fait rien.

  On obtient ainsi le coloriage final.

On dit que l'algorithme échoue s'il existe une arête monochromatique dans le coloriage final. Nous allons borné la probabilité d'échec de l'algorithme par $k(1-p)^n+k^2p$.

On regarde l'événement $\mathcal{E}=\{\exists e \in E \text{ qui est rouge dans le coloriage final}\}$. La probabilité d'échec est alors inférieure à $2\mathbb{P}(\mathcal{E})$.

$e \in E$ peut être rouge dans le coloriage final de deux manières disjointes :

- Soit e est rouge dans le premier coloriage et reste rouge.
- Soit e n'est pas rouge dans le premier coloriage mais devient rouge à l'étape 2.

Soit A_e le premier événement et C_e le second. $\mathbb{P}(A_e)=2^{-n}(1-p)^n$ (2^{-n} est la probabilité que e sois rouge au départ et $(1-p)^n$ est la probabilité qu'il n'y ait pas de modification dans la deuxième étape). Remarquer qu'un sommet change de couleur au plus une fois.

Donc $2\sum_e \mathbb{P}(A_e)=k(1-p)^n$.

Borne pour $\mathbb{P}(C_e)$.

Pour $(e,f) \in E^2$, on dit que l'arête e en veut à l'arête f si

- $e \cap f=\{v\}$
- Dans le premier coloriage, f était bleu et dans le coloriage final e est rouge.
- Dans la 2e étape, v était le dernier sommet de e qui change de bleu en rouge.
- Quand v a changé de couleur, f était entièrement bleu.

On suppose que C_e se produit. Des sommets dans e ont changé de bleu à rouge, soit v le dernier sommet dans e qui passe de bleu à rouge. Donc v doit être dans une arête f qui est bleue au premier coloriage et encore bleue quand v est considéré. e et f ne peuvent pas avoir d'autres sommets en commun sinon un tel v' aurait changé de bleu à rouge avant v (car e est rouge dans le coloriage final). Donc quand C_e se produit, l'arête e en veut à un certain f. Soit B_{ef} l'événement e en veut à f. On a $\sum_e \mathbb{P}(C_e) \leq \sum_{e \neq f} \mathbb{P}(B_{ef})$. Comme il y a moins de $(2^{n-1}k)^2$ couples $e \neq f$, il suffit de prouver que $\mathbb{P}(B_{ef}) \leq 2^{1-2n}p$.

Soit e,f avec $e \cap f=\{v\}$. L'ordre sur V induit un ordre σ sur $e \cup f$. Soit i le nombre de $v' \in e$

avant v et j le nombre de $v' \in f$ avant v. On fixe l'ordre σ, c'est à dire i et j alors

$$\mathbb{P}\left(B_{ef}|\sigma\right) \leq \frac{p}{2} 2^{-n+1} (1-p)^j 2^{-n+1+i} \left(\frac{1+p}{2}\right)^i,$$

où les termes correspondent à:

- $p/2$ correspond à la probabilité que v soit d'abord bleu puis devienne rouge;
- 2^{-n+1} est la probabilité que tous les autres $v' \in f$ soient bleu;
- $(1-p)^j$ est la probabilité que pour les $v' \in f$ avant v $B_{v'} = 0$;
- 2^{-n+1+i} est la probabilité que $v' \in e$ après v sont rouges dans le premier coloriage;
- $\left(\frac{1+p}{2}\right)^i$ est la probabilité que $v' \in e$ avant v sont soit rouge soit bleu devenant rouge.

On a donc

$$\mathbb{P}\left(B_{ef}\right) \leq 2^{1-2n} p \mathbb{E}\left[(1+p)^i (1-p)^i\right],$$

où l'espérance est sur les choix de σ: $i(\sigma), j(\sigma)$. Le Lemme suivant finit donc la preuve:

Lemme 10.
$\mathbb{E}\left[(1+p)^i (1-p)^j\right] < 1$

10 La méthode du second moment

Rappel. $\mathrm{Var}(X) = \mathbb{E}\left[(X - \mathbb{E}[X])^2\right] = \sigma^2$. $\mathbb{E}[X] = \mu$.
Chebychev: $\mathbb{P}(|X - \mu| \geq \lambda\sigma) \leq \frac{1}{\lambda^2}$

Démonstration.
$\sigma^2 = \mathrm{Var}(X) = \mathbb{E}\left[(X-\mu)^2\right] \geq \lambda^2\sigma^2\mathbb{P}(|X - \mu| \geq \lambda\sigma)$

Si on a une décomposition $X = X_1 + \cdots + X_n$, alors $\mathrm{Var}(X) = \sum_{i=1}^n \mathrm{Var}(X_i) + \sum_{i\neq j} \mathrm{Cov}(X_i, X_j)$ où $\mathrm{Cov}(Y, Z) = \mathbb{E}[YZ] - \mathbb{E}[Y]\,\mathbb{E}[Z]$.

- Si $Y \coprod Z$, $\mathrm{Cov}(Y, Z) = 0$
- Si $X_i = \mathbb{1}(A_i)$, $p_i = \mathbb{P}(A_i) = \mathbb{E}[X_i]$. $\mathrm{Var}(X_i) = p_i(1 - p_i) \leq p_i = \mathbb{E}[X_i]$.
  $\mathrm{Var}(X) \leq \mathbb{E}[X] + \sum_{i\neq j} \mathrm{Cov}(X_i, X_j)$

10.1 Théorie des nombres

Soit $\nu(n)$ = nombre de nombres premiers qui divisent n (sans multiplicité).

Théorème 33 (Hardy Ramanujan (1920)**).**
Soit $\omega(n)$ une fonction tendant vers l'infini arbitrairement lentement. Alors le nombre de $x \in \{1, \cdots, n\}$ tel que $|\nu(x) - \ln(\ln(n))| > \omega(n)\sqrt{\ln(\ln(n))}$ est $o(n)$.

10.2 Remarques faciles

$X \geq 0$ à valeurs dans $\mathbb{N}$. Le but est de borner $\mathbb{P}(X = 0)$ étant donné $\mu = \mathbb{E}[X]$.
Si $\mu < 1$, $\mathbb{P}(X > 0) \leq \mathbb{E}[X]$
Si $\mathbb{E}[X]$ tend vers 0, alors $X = 0$ presque toujours.
Que se passe-t-il quand $\mathbb{E}[X]$ tend vers l'infini?

Théorème 34.
$\mathbb{P}(X = 0) \leq \frac{\mathrm{Var}(X)}{\mathbb{E}[X]^2}$.

Démonstration.
On applique Chebychev avec $\lambda = \frac{\mu}{\sigma}$.

Corollaire 4.
Si $\mathrm{Var}(X) = o\left(\mathbb{E}[X]^2\right)$, alors $X > 0$ presque toujours. C'est à dire $\mathbb{P}(X > 0) \to 1$.

$X = X_1 + \cdots + X_m$ avec $X_i = \mathbb{1}(A_i)$.
$i \sim j$ si $i \neq j$ et A_i et A_j ne sont pas indépendants.
$\Delta = \sum_{i\sim j} \mathbb{P}(A_i \cap A_j)$.
Si $i \sim j$, $\mathrm{Cov}(X_i, X_j) = \mathbb{E}[X_iX_j] - \mathbb{E}[X_i]\,\mathbb{E}[X_j] \leq \mathbb{E}[X_iX_j] = \mathbb{P}(A_i \cap A_j)$.
On a donc $\mathrm{Var}(X) \leq \mathbb{E}[X] + \Delta$.

Corollaire 5.
Si $\mathbb{E}[X] \to \infty$ et $\Delta = o(\mathbb{E}[X]^2)$ alors $X > 0$ presque toujours.

10.3 Graphes aléatoires

$G(n,p)$ est un graphe à n sommets où chaque paire de sommets est une arête avec une probabilité p de manière indépendante (cf Chapitre 7).

Définition 22.

- Une **propriété** P est une famille de graphes fermée pour les isomorphismes.
- Une fonction $r(n)$ est une fonction **seuil** pour une propriété P si :
  - Si $p(n) << r(n)$, alors $G(n,p(n))$ ne satisfait par P presque toujours.
  - Si $p(n) >> r(n)$, alors $G(n,p(n))$ satisfait P presque toujours.

Théorème 35.
Soit $\omega(G)$ = nombre de sommets dans une clique maximale de G. La propriété $\omega(G) \geq 4$ a pour fonction seuil $n^{-\frac{2}{3}}$.

Démonstration.
pour chaque ensemble S de 4 sommets dans $G(n,p)$. A_s = "S est une clique". $X_S = \mathbb{1}(A_S)$. $\mathbb{E}[X_S] = p^6$.
$X = \sum_{|S|=4} X_S$ = le nombre de 4 cliques dans G.
$\omega(G) \geq 4 \Leftrightarrow X > 0$.
$\mathbb{E}[X] = \sum_{|S|=4} \mathbb{E}[X_S] = \binom{n}{4} p^6 \sim \frac{n^4 p^6}{24}$

- Quand $p(n) << n^{-\frac{2}{3}}$, $\mathbb{E}[X] \to 0$ et $X = 0$ presque toujours.
- Si $p(n) >> n^{-\frac{2}{3}}$, $\mathbb{E}[X] \to \infty$

$\Delta = \sum_{S \sim T} \mathbb{P}(A_S \cap A_T)$. $S \sim T$ si $S \neq T$ et S et T partagent des arêtes donc $|S \cap T| = 2$ ou 3.

- Si $|S \cap T| = 2$, $\mathbb{P}(A_S \cap A_T) = \mathbb{P}(A_S)\,\mathbb{P}(A_T|A_S)$ et $\mathbb{P}(A_T|A_S) = p^5$.
- Si $|S \cap T| = 3$, $\mathbb{P}(A_T|A_S) = p^3$.

$\Delta = \sum_S \mathbb{P}(A_S) \sum_{T \sim S} \mathbb{P}(A_T|A_S)$.
$\Delta^* = \sum_{T \sim S} \mathbb{P}(A_T|A_S)$ où S est fixé. Δ^* ne dépend donc pas S et on a:
$\Delta = \sum_S \mathbb{P}(A_S)\,\Delta^* = \Delta^* \mathbb{E}[X]$.
Comme il y a $O(n^2)$ ensemble T tels que $|S \cap T| = 2$ et $O(n)$ ensembles T tels que $|S \cap T| = 3$, on a:
$\Delta^* = O(n^2 p^5) + O(np^3) = o(n^4 p^6) = o(\mathbb{E}[X])$.
$\Delta = o\left(\mathbb{E}[X]^2\right)$.
Donc $X > 0$ presque toujours.

11 Le lemme de Lovász

11.1 Le Lemme

Lemme 11.

Soit $A_1, \cdots, A_n$ des événements.

*Un graphe orienté $D = (V, E)$ sur l'ensemble des sommets $V = \{1, \cdots, n\}$ est appelé un **graphe de dépendance** pour les événements $A_1, \cdots, A_n$ si pour tout $1 \leq i \leq n$, A_i est mutuellement indépendant des événements $\{A_j, (i,j) \notin E\}$*

On suppoe que $D = (V, E)$ est un graphe de dépendance pour les événements A_i et qu'il existe des réels $x_1, \cdots, x_n$ tel que $0 \leq x_i < 1$ et $\mathbb{P}(A_i) \leq x_i \prod_{(i,j)\in E}(1 - x_j)$ Alors

$$\mathbb{P}\left(\bigcap_{i=1}^{n} \overline{A_i}\right) \geq \prod_{i=1}^{n}(1 - x_i) > 0$$

Démonstration.

On prouve par induction sur s que pour tout $S \subset \{1, \cdots, n\}$, $|S| = s < n$ et pour tout $i \notin S$, $\mathbb{P}\left(A_i | \bigcap_{j\in S} \overline{A_j}\right) \leq x_i$

Ok pour $s = 0$, on suppose que c'est vrai pour tout $s' < s$.
$|S| = s$. $S_1 = \{j \in S, (r,j) \in E\}$ $S_2 = S \setminus S_1$

$$\mathbb{P}\left(A_i | \bigcap_{j\in S} \overline{A_j}\right) = \frac{\mathbb{P}\left(A_i \cap \bigcap_{j\in S_1} \overline{A_j} | \bigcap_{l\in S_2} \overline{A_l}\right)}{\mathbb{P}\left(\bigcap_{j\in S_1} \overline{A_j} | \bigcap_{l\in S_2} \overline{A_l}\right)}$$

Numérateur A_i et $(A_l, l \in S_2)$ sont mutuellement indépendants donc

$$\begin{aligned}\mathbb{P}\left(A_i \cap \bigcap_{j\in S_1} \overline{A_j} | \bigcap_{l\in S_2} \overline{A_l}\right) &\leq \mathbb{P}\left(A_i | \bigcap_{l\in S_2} \overline{A_l}\right) \\ &= \mathbb{P}(A_i) \leq x_i \prod_{(i,j)\in E}(1 - x_j)\end{aligned}$$

Dénominateur, on utilise l'induction $S_1 = \{j_1, \cdots, j_r\}$
Pour $r = 0$, alors le dénominateur vaut 1. ok. Sinon $|S_2| < |S|$ et

$$\begin{aligned}\mathbb{P}\left(\bigcap_{j\in S_1} \overline{A_j} | \bigcap_{l\in S_2} \overline{A_l}\right) &= \left(1 - \mathbb{P}\left(A_{j_1} | \bigcap_{l\in S_2} \overline{A_l}\right)\right) \\ &\quad \left(1 - \mathbb{P}\left(A_{j_2} | \overline{A_{j_1}} \cap \bigcap_{l\in S_2} \overline{A_l}\right)\right) \\ &\cdots \quad \left(1 - \mathbb{P}\left(A_{j_r} | \overline{A_{j_1}} \cap \cdots \cap \overline{A_{j_{r-1}}} \cap \bigcap_{l\in S_2} \overline{A_l}\right)\right) \\ &\geq (1 - x_{j_1})(1 - x_{j_2}) \cdots (1 - x_{j_r}) \\ &\geq \prod_{(i,j)\in E}(1 - x_j)\end{aligned}$$

Donc $\mathbb{P}\left(A_i | \bigcap_{j\in S} \overline{A_j}\right) \leq x_i$

$$\begin{aligned}\mathbb{P}\left(\bigcap_{i=1}^{n}\overline{A_i}\right) &= \left(1-\mathbb{P}\left(A_1\right)\right)\left(1-\mathbb{P}\left(A_2|\overline{A_1}\right)\right)\cdots\left(1-\mathbb{P}\left(A_n|\bigcap_{j=1}^{n-1}\overline{A_j}\right)\right)\\ &\geq \prod_{i=1}^{n}(1-x_i)\end{aligned}$$

Corollaire 6.

Cas symétrique $A_1,\cdots,A_n$ des événements tels que chaque A_i est mutuellement indépendant de l'ensemble des autres événements sauf au plus d d'entre eux et $\mathbb{P}\left(A_i\right)\leq p$
Si $ep(d+1)\leq 1$, alors $\mathbb{P}\left(\bigcap_{i=1}^{n}\overline{A_i}\right)>0$

Démonstration.
Si $d=0$, ok. Sinon, le graphe de dépendance $D=(V,E)$ a un degré maximal d: $|\{i,(i,j)\in E\}|\leq d$.
On prend alors $x_i=\frac{1}{d+1}<1$ et on utilise $\left(1-\frac{1}{d+1}\right)^d>\frac{1}{e}$

11.2 Applications

Rappel. Un hypergraphe $H=(V,E)$ est 2-coloriable s'il existe un coloriage de V en 2 couleurs tel qu'aucune arête $f\in E$ ne soit monochromatique.

Théorème 36.

Soit $H=(V,E)$ un hypergraphe tel que toute arête ait au moins k éléments et intersecte au plus d autres arêtes. Si $e(d+1)\leq 2^{k-1}$, alors H est 2-coloriable.

Démonstration.
Soit un coloriage aléatoire de H. $f\in E$, $A_f=\{f \text{ est monochromatique}\}$
$\mathbb{P}\left(A_f\right)=\frac{2}{2^{|f|}}\leq\frac{1}{2^{k-1}}$ et A_f est mutuellement indépendant des $A_{f'}$, $f\cap f^{'}=\emptyset$. Donc le corollaire s'applique

Proposition 6.

Pour $k\geq 9$, tout hypergraphe k-uniforme, k-régulier est 2 coloriable

Démonstration.
Une arête f contient k sommets, chacun étant incident à k arêtes, donc f intersecte au plus $d=k(k-1)$ autres arêtes.
On a alors $e(k(k-1)+1)\leq 2^{k-1}$ pour $k\geq 9$.

Application (Problème de k-SAT**).**
Soit x,y des variables booléennes.
$\bar{x}$ est la négation de x, $x\wedge y$ est la conjonction de x et y, $x\vee y$ est la disjonction de x et y.
k,m entiers ≥ 0 $x_1,\cdots,x_m\in\{0,1\}$ clause de k termes $\bigvee_{j=1}^{k}y_j$ $y_j\in\{x_1,\bar{x}_1,x_2,\bar{x}_2,\cdots,x_m,\bar{x}_m\}$
Expression du problème de k-SAT: Toute conjonction de clauses à k termes $\bigwedge_{i=1}^{m}\bigvee_{j=1}^{k}y_{ij}$ $y_{ij}\in\{x_1,\bar{x}_1,x_2,\bar{x}_2,\cdots,x_m,\bar{x}_m\}$
On suppose qu'aucune clause ne contient x_i et $\bar{x}_i$

Proposition 7.

Si aucune variable n'apparaît dans plus de $T=\frac{2^k}{4k}$ clauses, alors il existe une solution au problème de satisfiabilité.

Démonstration.
On tire au hasard des variables $x_1,\cdots,x_n$.

On note $E_i = \{$ la clause i n'est pas vérifiée $\}$.
$\mathbb{P}(E_i) = 2^{-k} = p$
Le graphe de dépendance a un degré borné par $d = k(T-1) = 2^{k-2} - k$ et $ep(d+1) = e2^{-k}(2^{k-2} - k) < 1$.