La plus longue sous-suite croissante d'une permutation aléatoire

Valentin Féray

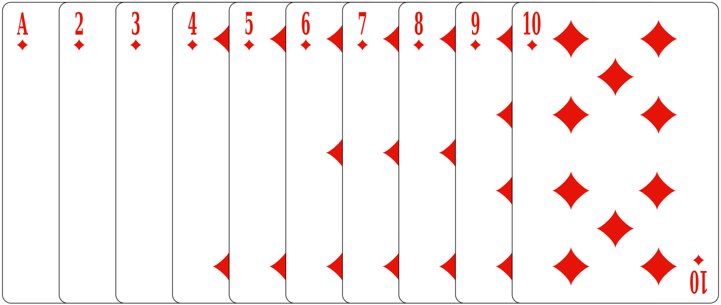
Institut für Mathematik, Universität Zürich

Mathematical Park
Institut Henri Poincaré, 9 novembre 2013

Universität Zürich[UZH]

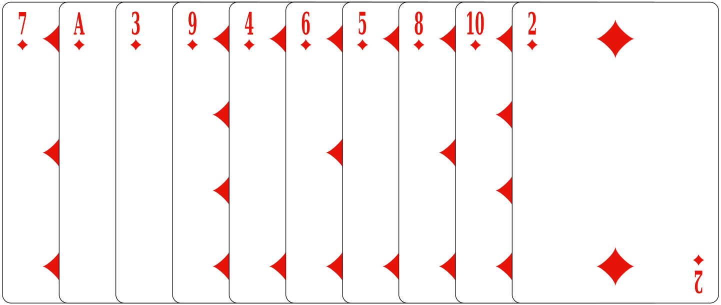
Trier des cartes

Considérons un jeu de cartes (simplifié) :



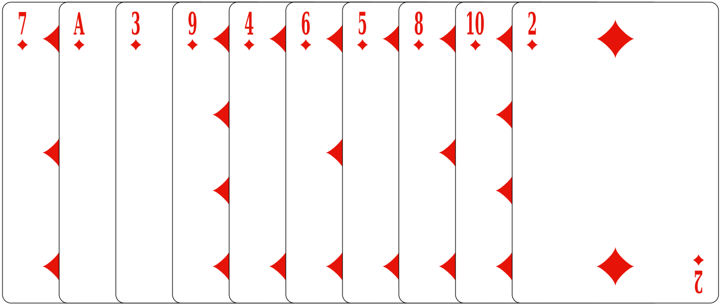
Trier des cartes

On mélange :



Trier des cartes

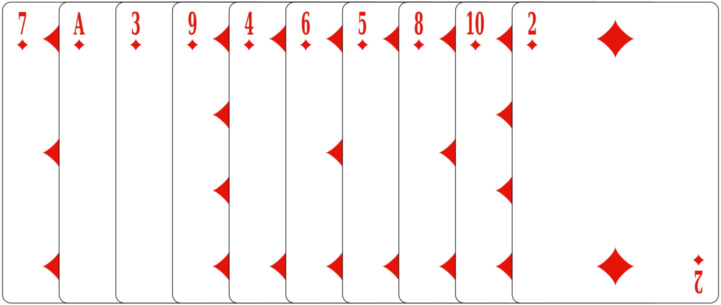
On mélange :



Combien de cartes faut-il déplacer pour trier le jeu ?

Trier des cartes

On mélange :



Simplifions les notations : le mélange ci-dessus est représenté par

7 1 3 9 4 6 5 8 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre.

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

1 3 9 4 6 5 7 8 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

1 3 9 4 6 5 7 8 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

1 3 9 4 6 5 7 8 10 2

1 3 4 6 5 7 8 9 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

1 3 9 4 6 5 7 8 10 2

1 3 4 6 5 7 8 9 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

1 3 9 4 6 5 7 8 10 2

1 3 4 6 5 7 8 9 10 2

1 3 4 5 6 7 8 9 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

1 3 9 4 6 5 7 8 10 2

1 3 4 6 5 7 8 9 10 2

1 3 4 5 6 7 8 9 10 2

Un example de tri

7 1 3 9 4 6 5 8 10 2

Idée : trouver un maximum de cartes déjà dans l'ordre, puis déplacer les autres cartes une à une.

7 1 3 9 4 6 5 8 10 2

1 3 9 4 6 5 7 8 10 2

1 3 4 6 5 7 8 9 10 2

1 3 4 5 6 7 8 9 10 2

1 2 3 4 5 6 7 8 9 10

Nombre d'étapes nécessaires

En remarquant qu'il y avait 6 cartes dans le bon ordre, on a pu trier en 10-6=4 étapes.

Nombre d'étapes nécessaires

En remarquant qu'il y avait 6 cartes dans le bon ordre, on a pu trier en 10-6=4 étapes.

Réciproquement, si on peut trier en 3 étapes, cela signifie que les 7 cartes non déplacées sont déjà dans le bon ordre au début.

Nombre d'étapes nécessaires

En remarquant qu'il y avait 6 cartes dans le bon ordre, on a pu trier en 10-6=4 étapes.

Réciproquement, si on peut trier en 3 étapes, cela signifie que les 7 cartes non déplacées sont déjà dans le bon ordre au début.

Conclusion : le nombre minimal de déplacements nécessaires pour trier un jeu est $n - r$,
où r est le nombre maximal de cartes déjà dans le bon ordre.

Reformulation mathématique

Definition

Une permutation d'un entier $n \geq 1$ est une liste d'entiers entre 1 et n où chaque entier apparaît exactement une fois.

Exemple : 2 5 7 3 1 4 8 6 est une permutation de 8.

Reformulation mathématique

Definition

Une permutation d'un entier $n \geq 1$ est une liste d'entiers entre 1 et n où chaque entier apparaît exactement une fois.

Exemple : 2 5 7 3 1 4 8 6 est une permutation de 8.

Objet	Formalisation mathématique
Jeu mélangé à n cartes	Permutation de n

Reformulation mathématique

Definition

Une permutation d'un entier $n \geq 1$ est une liste d'entiers entre 1 et n où chaque entier apparaît exactement une fois.

Exemple : 2 5 7 3 1 4 8 6 est une permutation de 8.

Objet	Formalisation mathématique
Jeu mélangé à n cartes	Permutation de n
certaines cartes du jeu	sous-suite

Reformulation mathématique

Definition

Une permutation d'un entier $n \geq 1$ est une liste d'entiers entre 1 et n où chaque entier apparaît exactement une fois.

Exemple : 2 5 7 3 1 4 8 6 est une permutation de 8.

Objet	Formalisation mathématique
Jeu mélangé à n cartes	Permutation de n
certaines cartes du jeu	sous-suite
dans le bon ordre	croissant

Reformulation mathématique

Definition

Une permutation d'un entier $n \geq 1$ est une liste d'entiers entre 1 et n où chaque entier apparaît exactement une fois.

Exemple : 2 5 7 3 1 4 8 6 est une permutation de 8.

Objet	Formalisation mathématique
Jeu mélangé à n cartes	Permutation de n
certaines cartes du jeu	sous-suite
dans le bon ordre	croissant

Proposition

Le nombre minimal de "déplacements" *nécessaires pour trier une permutation p est $n - r(p)$, où $r(p)$ est la longueur de la plus longue sous-suite croissante de p.*

Notre problème

Mais à quoi ressemble en général la longueur $r(p)$ de la plus longue sous suite croissante d'une grande permutation p ?

- Est-ce que c'est plutôt proche de n (i.e. le plus souvent on peut trouver une sous-suite croissante qui prend presque tous les nombres) ?

Notre problème

Mais à quoi ressemble en général la longueur $r(p)$ de la plus longue sous suite croissante d'une grande permutation p ?

- Est-ce que c'est plutôt proche de n (i.e. le plus souvent on peut trouver une sous-suite croissante qui prend presque tous les nombres) ?
- Est-ce que ça reste constant (i.e. c'est rare d'avoir une sous-suite croissante plus grande que 10, par exemple) ?

Notre problème

Mais à quoi ressemble en général la longueur $r(p)$ de la plus longue sous suite croissante d'une grande permutation p ?

- Est-ce que c'est plutôt proche de n (i.e. le plus souvent on peut trouver une sous-suite croissante qui prend presque tous les nombres) ?
- Est-ce que ça reste constant (i.e. c'est rare d'avoir une sous-suite croissante plus grande que 10, par exemple) ?
- Entre les deux ?

Notre problème

Mais à quoi ressemble en général la longueur $r(p)$ de la plus longue sous suite croissante d'une grande permutation p ?

- Est-ce que c'est plutôt proche de n (i.e. le plus souvent on peut trouver une sous-suite croissante qui prend presque tous les nombres) ?
- Est-ce que ça reste constant (i.e. c'est rare d'avoir une sous-suite croissante plus grande que 10, par exemple) ?
- Entre les deux ?

Problème

Prenons une permutation p de taille n au hasard. Quelle est la moyenne de $r(p)$?

Notre problème

Mais à quoi ressemble en général la longueur $r(p)$ de la plus longue sous suite croissante d'une grande permutation p ?

- Est-ce que c'est plutôt proche de n (i.e. le plus souvent on peut trouver une sous-suite croissante qui prend presque tous les nombres) ?
- Est-ce que ça reste constant (i.e. c'est rare d'avoir une sous-suite croissante plus grande que 10, par exemple) ?
- Entre les deux ?

Problème

Prenons une permutation p de taille n au hasard. Quelle est la moyenne de $r(p)$?
Est-ce que $r(p)$ est proche de sa moyenne ?

Notre problème

Mais à quoi ressemble en général la longueur $r(p)$ de la plus longue sous suite croissante d'une grande permutation p ?

- Est-ce que c'est plutôt proche de n (i.e. le plus souvent on peut trouver une sous-suite croissante qui prend presque tous les nombres) ?
- Est-ce que ça reste constant (i.e. c'est rare d'avoir une sous-suite croissante plus grande que 10, par exemple) ?
- Entre les deux ?

Problème

Prenons une permutation p de taille n au hasard. Quelle est la moyenne de $r(p)$?
Est-ce que $r(p)$ est proche de sa moyenne ?

Pour des modèles de tris adaptés aux ordinateurs, cette question est fondamentale !

3 résultats

Proposition La moyenne $E(r(p))$ de $r(p)$ vérifie

$$E(r(p)) \geq \sqrt{n}.$$

3 résultats

Proposition La moyenne $E(r(p))$ de $r(p)$ vérifie

$$E(r(p)) \geq \sqrt{n}.$$

Proposition Avec très forte probabilité,

$$r(p) < 3\sqrt{n}$$

3 résultats

Proposition La moyenne $E(r(p))$ de $r(p)$ vérifie

$$E(r(p)) \geq \sqrt{n}.$$

Proposition Avec très forte probabilité,

$$r(p) < 3\sqrt{n}$$

Proposition Il existe un nombre C telle que, avec forte probabilité,

$$r(p) \approx C\sqrt{n}$$

3 résultats

Proposition La moyenne $E(r(p))$ de $r(p)$ vérifie

$$E(r(p)) \geq \sqrt{n}.$$

$\rightarrow$ principe des tiroirs.

Proposition Avec très forte probabilité,

$$r(p) < 3\sqrt{n}$$

$\rightarrow$ méthode du premier moment.

Proposition Il existe un nombre C telle que, avec forte probabilité,

$$r(p) \approx C\sqrt{n}$$

$\rightarrow$ points aléatoires, lemme sous-additif.

Valeurs possibles pour $r(p)$

$r(p)$ peut prendre toutes les valeurs entre 1 et n.

Valeurs possibles pour $r(p)$

$r(p)$ peut prendre toutes les valeurs entre 1 et n.

- Seule permutation avec $r(p) = 1$;

$$n\ (n-1)\ (n-2)\ (n-3)\ \ldots\ 4\ 3\ 2\ 1.$$

Valeurs possibles pour $r(p)$

$r(p)$ peut prendre toutes les valeurs entre 1 et n.

- Seule permutation avec $r(p) = 1$;

$$n \ (n-1) \ (n-2) \ (n-3) \ \dots \ 4 \ 3 \ 2 \ 1.$$

- Exemple de permutation avec $r(p) = 2$;

$$(n-1) \ n \ (n-3) \ (n-2) \dots \ 3 \ 4 \ 1 \ 2.$$

Valeurs possibles pour $r(p)$

$r(p)$ peut prendre toutes les valeurs entre 1 et n.

- Seule permutation avec $r(p) = 1$;

$$n\ (n-1)\ (n-2)\ (n-3)\ \dots\ 4\ 3\ 2\ 1.$$

- Exemple de permutation avec $r(p) = 2$;

$$(n-1)\ n\ (n-3)\ (n-2) \dots\ 3\ 4\ 1\ 2.$$

- ...
- Seule permutation avec $r(p) = n$;

$$1\ 2\ 3\ 4\ \dots\ (n-3)\ (n-2)\ (n-1)\ n.$$

Valeurs possibles pour $r(p)$

$r(p)$ peut prendre toutes les valeurs entre 1 et n.

- Seule permutation avec $r(p) = 1$;

$$n\ (n-1)\ (n-2)\ (n-3)\ \dots\ 4\ 3\ 2\ 1.$$

- Exemple de permutation avec $r(p) = 2$;

$$(n-1)\ n\ (n-3)\ (n-2) \dots\ 3\ 4\ 1\ 2.$$

- ...
- Seule permutation avec $r(p) = n$;

$$1\ 2\ 3\ 4\ \dots\ (n-3)\ (n-2)\ (n-1)\ n.$$

Remarque : si $r(p)$ est petit, alors on a une grande sous-suite décroissante.

Un lien entre sous-suites croissantes et décroissantes

Plus précisément, on va montrer le résultat suivant

Théorème d'Erdős-Szekeres (1935)

Soit p une permutation de n. Notons

- $r(p)$ la longueur de la plus longue sous-suite croissante de p ;
- $s(p)$ la longueur de la plus longue sous-suite décroissante de p.

Alors

$$r(p) \cdot s(p) \geq n.$$

Un lien entre sous-suites croissantes et décroissantes

Plus précisément, on va montrer le résultat suivant

Théorème d'Erdős-Szekeres (1935)

Soit p une permutation de n. Notons

- $r(p)$ la longueur de la plus longue sous-suite croissante de p ;
- $s(p)$ la longueur de la plus longue sous-suite décroissante de p.

Alors

$$r(p) \cdot s(p) \geq n.$$

Démonstration dans quelques slides.

Avant : quel est le rapport avec notre problème sur $r(p)$?

Le théorème d'Erdős-Szekeres et $E(r(p))$

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

Le théorème d'Erdős-Szekeres et $E(r(p))$

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

Rappel : pour tout réels positifs a, b,

$$\frac{a+b}{2} \geq \sqrt{a \cdot b}.$$

En effet, $\frac{1}{2}\left(\sqrt{a} - \sqrt{b}\right)^2 = \frac{a+b}{2} - \sqrt{a \cdot b} \geq 0.$

Le théorème d'Erdős-Szekeres et $E(r(p))$

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

Rappel : pour tout réels positifs a, b,

$$\frac{a+b}{2} \geq \sqrt{a \cdot b}.$$

Donc pour toute permutation p

$$\frac{r(p)+s(p)}{2} \geq \sqrt{r(p) \cdot s(p)} \geq \sqrt{n}.$$

Le théorème d'Erdős-Szekeres et $E(r(p))$

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

Rappel : pour tout réels positifs a, b,

$$\frac{a+b}{2} \geq \sqrt{a \cdot b}.$$

Donc pour toute permutation p

$$\frac{r(p)+s(p)}{2} \geq \sqrt{r(p) \cdot s(p)} \geq \sqrt{n}.$$

Prenons la moyenne

$$E\left(\frac{r(p)+s(p)}{2}\right) = \frac{E(r(p))+E(s(p))}{2} \geq \sqrt{n}.$$

Le théorème d'Erdős-Szekeres et $E(r(p))$ (suite)

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

$$\frac{E(r(p)) + E(s(p))}{2} \geq \sqrt{n}.$$

Le théorème d'Erdős-Szekeres et $E(r(p))$ (suite)

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

$$\frac{E(r(p)) + E(s(p))}{2} \geq \sqrt{n}.$$

Or,

$$E(r(p)) = E(s(p)).$$

Le théorème d'Erdős-Szekeres et $E(r(p))$ (suite)

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

$$\frac{E(r(p)) + E(s(p))}{2} \geq \sqrt{n}.$$

Or,

$$E(r(p)) = E(s(p)).$$

En effet, Si $\bar{p}$ est la permutation p lue de droite à gauche, alors

$$s(\bar{p}) = r(p)$$

Exemple : $p = 2\ 3\ 1\ 5\ 4$, $\quad \bar{p} = 4\ 5\ 1\ 3\ 2$.

Le théorème d'Erdős-Szekeres et $E(r(p))$ (suite)

Lemme

Le théorème d'Erdős-Szekeres implique

$$E(r(p)) \geq \sqrt{n}$$

$$\frac{E(r(p)) + E(s(p))}{2} \geq \sqrt{n}.$$

Or,

$$E(r(p)) = E(s(p)).$$

En effet, Si $\bar{p}$ est la permutation p lue de droite à gauche, alors

$$s(\bar{p}) = r(p)$$

Exemple : $p = 2\ 3\ 1\ 5\ 4, \quad \bar{p} = 4\ 5\ 1\ 3\ 2.$

Conclusion: $E(r(p)) \geq \sqrt{n}$

Principe des tiroirs

Pour montrer le théorème d'Erdős-Szekeres, nous allons utiliser :

Principe des tiroirs

Principe des tiroirs

Pour montrer le théorème d'Erdős-Szekeres, nous allons utiliser :

Principe des tiroirs

Si on range 11 chaussettes dans 10 tiroirs, alors il existe au moins 1 tiroir qui contient au moins 2 chaussettes.

Principe des tiroirs

Pour montrer le théorème d'Erdős-Szekeres, nous allons utiliser :

Principe des tiroirs

Si on range $k+1$ chaussettes dans k tiroirs, alors il existe au moins 1 tiroir qui contient au moins 2 chaussettes.

Principe des tiroirs

Pour montrer le théorème d'Erdős-Szekeres, nous allons utiliser :

Principe des tiroirs

Si on range $k \cdot \ell + 1$ chaussettes dans k tiroirs, alors il existe au moins 1 tiroir qui contient au moins $\ell + 1$ chaussettes.

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que
$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

Démonstration : Considérons les nombres
$$0 = \{0 \cdot x\}, \{x\}, \{2 \cdot x\}, \dots, \{(n-1) \cdot x\}, \{n \cdot x\}$$

Ici, $\{y\}$ désigne la partie fractionnaire de y
$$\text{exemple : } \{2,573\} = 0,573.$$

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

Démonstration : Considérons les nombres

$$0 = \{0 \cdot x\}, \{x\}, \{2 \cdot x\}, \dots, \{(n-1) \cdot x\}, \{n \cdot x\}$$

et plaçons-les dans les "tiroirs"

$$\left[0, \frac{1}{n}\right[, \left[\frac{1}{n}, \frac{2}{n}\right[, \dots, \left[\frac{n-1}{n}, 1\right[.$$

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

Démonstration : Considérons les nombres

$$0 = \{0 \cdot x\}, \{x\}, \{2 \cdot x\}, \dots, \{(n-1) \cdot x\}, \{n \cdot x\}$$

et plaçons-les dans les "tiroirs"

$$\left[0, \frac{1}{n}\right[, \left[\frac{1}{n}, \frac{2}{n}\right[, \dots, \left[\frac{n-1}{n}, 1\right[.$$

D'après le principe des tiroirs, il y a deux nombres $\{i \cdot x\}$ et $\{j \cdot x\}$ dans le même tiroir.

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que
$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

Démonstration : Considérons les nombres
$$0 = \{0 \cdot x\}, \{x\}, \{2 \cdot x\}, \dots, \{(n-1) \cdot x\}, \{n \cdot x\}$$
et plaçons-les dans les "tiroirs"
$$\left[0, \frac{1}{n}\right[, \left[\frac{1}{n}, \frac{2}{n}\right[, \dots, \left[\frac{n-1}{n}, 1\right[.$$
D'après le principe des tiroirs, il y a deux nombres $\{i \cdot x\}$ et $\{j \cdot x\}$ dans le même tiroir. En particulier,
$$\left| \{i \cdot x\} - \{j \cdot x\} \right| \leq \frac{1}{n}$$

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

On vient de montrer qu'il existe i et j entre 0 et n tel que

$$\big| \{i \cdot x\} - \{j \cdot x\} \big| \leq \frac{1}{n}.$$

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

On vient de montrer qu'il existe i et j entre 0 et n tel que

$$\left| \{i \cdot x\} - \{j \cdot x\} \right| \leq \frac{1}{n}.$$

Donc il existe un entier p tel que

$$\left| (i \cdot x - j \cdot x) - p \right| \leq \frac{1}{n}.$$

Principe des tiroirs (exemple)

Proposition (approximabilité d'un réel par un rationnel)

Soit x un nombre réel et n un entier. Alors il existe un nombre rationel p/q avec $q \leq n$ tel que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}$$

On vient de montrer qu'il existe i et j entre 0 et n tel que

$$\left| \{i \cdot x\} - \{j \cdot x\} \right| \leq \frac{1}{n}.$$

Donc il existe un entier p tel que

$$\left| (i \cdot x - j \cdot x) - p \right| \leq \frac{1}{n}.$$

Posons $q = i - j$:

$$\left| q \cdot x - p \right| \leq \frac{1}{n} \text{ et donc } \left| x - \frac{p}{q} \right| \leq \frac{1}{n \cdot q}.$$

Principe des tiroirs (retour à notre problème)

Théorème d'Erdős-Szekeres (1935)

Soit p une permutation de n. Notons

- $r(p)$ la longueur de la plus longue sous-suite croissante de p ;
- $s(p)$ la longueur de la plus longue sous-suite décroissante de p.

Alors

$$r(p) \cdot s(p) \geq n.$$

Démonstration par le principe des tiroirs

Soit p une permutation de n. Notons a_i la longueur de la plus-longue sous-suite croissante commençant en position i.

Exemple :

$$\begin{array}{lcccccccccc} p: & 5 & 9 & 2 & 4 & 1 & 10 & 3 & 7 & 6 & 8 \\ a_i: & 3 & & & & & & & & & \end{array}$$

Démonstration par le principe des tiroirs

Soit p une permutation de n. Notons a_i la longueur de la plus-longue sous-suite croissante commençant en position i.

Exemple :

$$\begin{array}{rcccccccccc} p: & 5 & \color{red}{9} & 2 & 4 & 1 & \color{red}{10} & 3 & 7 & 6 & 8 \\ a_i: & 3 & 2 & & & & & & & & \end{array}$$

Démonstration par le principe des tiroirs

Soit p une permutation de n. Notons a_i la longueur de la plus-longue sous-suite croissante commençant en position i.

Exemple :

$$\begin{array}{rcccccccccc} p: & 5 & 9 & 2 & 4 & 1 & 10 & 3 & 7 & 6 & 8 \\ a_i: & 3 & 2 & 4 & 3 & 4 & 1 & 3 & 2 & 2 & 1 \end{array}$$

Démonstration par le principe des tiroirs

Soit p une permutation de n. Notons a_i la longueur de la plus-longue sous-suite croissante commençant en position i.

Exemple :

$$\begin{array}{rcccccccccc} p: & 5 & 9 & 2 & 4 & 1 & 10 & 3 & 7 & 6 & 8 \\ a_i: & 3 & 2 & 4 & 3 & 4 & 1 & 3 & 2 & 2 & 1 \end{array}$$

Les valeurs de a_i sont entre 1 et $r(p)$ (ici $r(p) = 4$).

Démonstration par le principe des tiroirs

Soit p une permutation de n. Notons a_i la longueur de la plus-longue sous-suite croissante commençant en position i.

Exemple :

$$\begin{array}{lcccccccccc} p: & 5 & 9 & 2 & 4 & 1 & 10 & 3 & 7 & 6 & 8 \\ a_i: & 3 & 2 & 4 & 3 & 4 & 1 & 3 & 2 & 2 & 1 \end{array}$$

Les valeurs de a_i sont entre 1 et $r(p)$ (ici $r(p) = 4$).

Principe des tiroirs : il y a une valeur répétée au moins $\lceil n/r(p) \rceil$ fois (ici, 3 fois).

$\lceil x \rceil$: entier juste au-dessus de x.

Démonstration par le principe des tiroirs

Soit p une permutation de n. Notons a_i la longueur de la plus-longue sous-suite croissante commençant en position i.

Exemple :

$$\begin{array}{rcccccccccc} p: & 5 & 9 & 2 & 4 & 1 & 10 & 3 & 7 & 6 & 8 \\ a_i: & 3 & 2 & 4 & 3 & 4 & 1 & 3 & 2 & 2 & 1 \end{array}$$

Les valeurs de a_i sont entre 1 et $r(p)$ (ici $r(p) = 4$).

Principe des tiroirs : il y a une valeur répétée au moins $\lceil n/r(p) \rceil$ fois (ici, 3 fois).

Les nombres correspondant dans p forme une sous-suite décroissante.

Démonstration par le principe des tiroirs

Soit p une permutation de n. Notons a_i la longueur de la plus-longue sous-suite croissante commençant en position i.

Exemple :

$$\begin{array}{lcccccccccc} p: & 5 & 9 & 2 & 4 & 1 & 10 & 3 & 7 & 6 & 8 \\ a_i: & 3 & 2 & 4 & 3 & 4 & 1 & 3 & 2 & 2 & 1 \end{array}$$

Les valeurs de a_i sont entre 1 et $r(p)$ (ici $r(p) = 4$).

Principe des tiroirs : il y a une valeur répétée au moins $\lceil n/r(p) \rceil$ fois (ici, 3 fois).

Les nombres correspondant dans p forme une sous-suite décroissante. Donc

$$s(p) \geq \lceil n/r(p) \rceil \geq n/r(p). \quad \square$$

Transition

On vient de prouver avec le principe des tiroirs :

Proposition La moyenne $E(r(p))$ de $r(p)$ vérifie

$$E(r(p)) \geq \sqrt{n}.$$

Transition

On vient de prouver avec le principe des tiroirs :

Proposition La moyenne $E(r(p))$ de $r(p)$ vérifie

$$E(r(p)) \geq \sqrt{n}.$$

Prochaine partie :

Proposition Avec très forte probabilité,

$$r(p) < 3\sqrt{n}$$

en utilisant la méthode du premier moment.

Méthode du premier moment

Lemme

Soit X une variable aléatoire prenant des valeurs entières positives. Alors

$$P(X \neq 0) \leq E(X).$$

Méthode du premier moment

Lemme

Soit X une variable aléatoire prenant des valeurs entières positives. Alors

$$P(X \neq 0) \leq E(X).$$

Démonstration :

$$\begin{aligned} P(X \neq 0) &= && P(X = 1)+ && P(X = 2)+ && P(X = 3)+ && \cdots \\ E(X) &= 1 \cdot{} && P(X = 1)+ \; 2 \cdot{} && P(X = 2)+ \; 3 \cdot{} && P(X = 3)+ && \cdots \end{aligned}$$

d'où le résultat. $\square$

Exemple d'utilisation

Alice joue 10 grilles de 6 numéros au loto.
On suppose que la probabilité qu'une grille donnée soit gagnante (=au moins 3 bons numéros) est

$$1/1\,000.$$

Exemple d'utilisation

Alice joue 10 grilles de 6 numéros au loto.
On suppose que la probabilité qu'une grille donnée soit gagnante (=au moins 3 bons numéros) est

$$1/1\,000.$$

Alors la probabilité qu'Alice ait au moins 1 grille gagnante est

$$\leq 1/100.$$

Exemple d'utilisation

Alice joue 10 grilles de 6 numéros au loto.
On suppose que la probabilité qu'une grille donnée soit gagnante (=au moins 3 bons numéros) est

$$1/1\,000.$$

Alors la probabilité qu'Alice ait au moins 1 grille gagnante est

$$\leq 1/100.$$

Démonstration : notons $X_i = 1$ si la grille numéro i est gagnante, 0 sinon.
Par hypothèse,

$$E(X_i) = \frac{1}{1\,000}.$$

Exemple d'utilisation

Alice joue 10 grilles de 6 numéros au loto.
On suppose que la probabilité qu'une grille donnée soit gagnante (=au moins 3 bons numéros) est

$$1/1\,000.$$

Alors la probabilité qu'Alice ait au moins 1 grille gagnante est

$$\leq 1/100.$$

Démonstration : notons $X_i = 1$ si la grille numéro i est gagnante, 0 sinon. Par hypothèse,

$$E(X_i) = \frac{1}{1\,000}.$$

Le nombre de grilles gagnantes est $X = X_1 + \cdots + X_{10}$. Sa moyenne est

$$E(X) = E(X_1) + \cdots + E(X_{10}) = 1/100. \qquad \square$$

Retour aux sous-suites croissantes

On s'intéresse à

$$P(r(p) < 3\sqrt{n})$$

Retour aux sous-suites croissantes

On s'intéresse à

$$P(r(p) < 3\sqrt{n})$$

Retour aux sous-suites croissantes

On s'intéresse à

$$P(r(p) < 3\sqrt{n}) = 1 - P(r(p) \geq 3\sqrt{n})$$
$$= 1 - P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } \lceil 3\sqrt{n} \rceil \end{array} \right)$$

Notons $R = \lceil 3\sqrt{n} \rceil$. Exemple $n = 16$, $R = 12$,

$$p = \quad 11 \quad 3 \quad 15 \quad 1 \quad 9 \quad 5 \quad 8 \quad 4 \quad 10 \quad 16 \quad 12 \quad 2 \quad 6 \quad 13 \quad 7 \quad 14$$

Retour aux sous-suites croissantes

On s'intéresse à

$$\begin{aligned} P(r(p) < 3\sqrt{n}) &= 1 - P(r(p) \geq 3\sqrt{n}) \\ &= 1 - P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } \lceil 3\sqrt{n} \rceil \end{array} \right) \end{aligned}$$

Notons $R = \lceil 3\sqrt{n} \rceil$. Exemple $n = 16$, $R = 12$,

$$\begin{array}{lcccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

Je joue au loto : je choisis arbitrairement 12 flèches, est-ce que mes flèches correspondent à une sous suite croissante ?

Retour aux sous-suites croissantes

On s'intéresse à

$$\begin{aligned} P(r(p) < 3\sqrt{n}) &= 1 - P(r(p) \geq 3\sqrt{n}) \\ &= 1 - P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } \lceil 3\sqrt{n} \rceil \end{array} \right) \end{aligned}$$

Notons $R = \lceil 3\sqrt{n} \rceil$. Exemple $n = 16$, $R = 12$,

$$\begin{array}{cccccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

Je joue au loto : je choisis arbitrairement 12 flèches, est-ce que mes flèches correspondent à une sous suite croissante ?

Je vais jouer ainsi toutes les manières de positionner les 12 flèches :

- s'il y a une sous-suite croissante, je vais gagner au moins une fois ;
- sinon, je vais perdre à chaque fois.

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\begin{pmatrix} p \text{ contienne une sous-suite} \\ \text{croissante de longueur 12} \end{pmatrix} = P\begin{pmatrix} \text{je gagne} \\ \text{au "loto"} \end{pmatrix}$$

$$\leq \begin{pmatrix} \text{nombre de fois} \\ \text{où je joue} \end{pmatrix} \cdot \begin{pmatrix} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{pmatrix}$$

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\begin{pmatrix} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 12 \end{pmatrix} = P\begin{pmatrix} \text{je gagne} \\ \text{au "loto"} \end{pmatrix}$$

$$\leq \begin{pmatrix} \text{nombre de fois} \\ \text{où je joue} \end{pmatrix} \cdot \begin{pmatrix} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{pmatrix}$$

$$p = \begin{array}{cccccccccccccccc} 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

Rappel du jeu

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur 12} \end{array}\right) = P\left(\begin{array}{c} \text{je gagne} \\ \text{au "loto"} \end{array}\right)$$

$$\leq \left(\begin{array}{c} \text{nombre de fois} \\ \text{où je joue} \end{array}\right) \cdot \left(\begin{array}{c} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{array}\right)$$

$$\begin{array}{ccccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

- nombre de fois où je joue = nombre de choix de 12 flèches parmi 16 possibles =

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 12 \end{array}\right) = P\left(\begin{array}{c} \text{je gagne} \\ \text{au "loto"} \end{array}\right)$$

$$\leq \left(\begin{array}{c} \text{nombre de fois} \\ \text{où je joue} \end{array}\right) \cdot \left(\begin{array}{c} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{array}\right)$$

$$p = \begin{array}{cccccccccccccccc} 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

- nombre de fois où je joue = nombre de choix de 12 flèches parmi 16 possibles = $\binom{16}{12} = \frac{16!}{12! \cdot 4!}$.

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 12 \end{array}\right) = P\left(\begin{array}{c} \text{je gagne} \\ \text{au "loto"} \end{array}\right)$$
$$\leq \left(\begin{array}{c} \text{nombre de fois} \\ \text{où je joue} \end{array}\right) \cdot \left(\begin{array}{c} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{array}\right)$$

$$\begin{array}{cccccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

- nombre de fois où je joue = nombre de choix de 12 flèches parmi 16 possibles = $\binom{16}{12} = \frac{16!}{12! \cdot 4!}$.
- probabilité de gagner à un coup donné : correspond à prendre 12 nombres au hasard et voir s'ils sont dans le bon ordre.

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 12 \end{array}\right) = P\left(\begin{array}{c} \text{je gagne} \\ \text{au "loto"} \end{array}\right)$$

$$\leq \left(\begin{array}{c} \text{nombre de fois} \\ \text{où je joue} \end{array}\right) \cdot \left(\begin{array}{c} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{array}\right)$$

$$\begin{array}{cccccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

- nombre de fois où je joue = nombre de choix de 12 flèches parmi 16 possibles $= \binom{16}{12} = \frac{16!}{12! \cdot 4!}$.
- probabilité de gagner à un coup donné : correspond à prendre 12 nombres au hasard et voir s'ils sont dans le bon ordre. La proba est

$$\frac{1}{12}$$

proba que le premier soit le plus petit

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\begin{pmatrix} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 12 \end{pmatrix} = P\begin{pmatrix} \text{je gagne} \\ \text{au "loto"} \end{pmatrix}$$
$$\leq \begin{pmatrix} \text{nombre de fois} \\ \text{où je joue} \end{pmatrix} \cdot \begin{pmatrix} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{pmatrix}$$

$$\begin{array}{lcccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

- nombre de fois où je joue = nombre de choix de 12 flèches parmi 16 possibles = $\binom{16}{12} = \frac{16!}{12! \cdot 4!}$.
- probabilité de gagner à un coup donné : correspond à prendre 12 nombres au hasard et voir s'ils sont dans le bon ordre. La proba est

$$\frac{1}{12} \cdot \frac{1}{11}$$

proba que le deuxième soit le deuxième plus petit
sachant que le premier est le plus petit

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\left(\begin{array}{c}p \text{ contienne une sous-suite}\\ \text{croissante de longueur } 12\end{array}\right) = P\left(\begin{array}{c}\text{je gagne}\\ \text{au "loto"}\end{array}\right)$$

$$\leq \left(\begin{array}{c}\text{nombre de fois}\\ \text{où je joue}\end{array}\right) \cdot \left(\begin{array}{c}\text{probabilité que je}\\ \text{gagne à un coup donné}\end{array}\right)$$

$$\begin{array}{cccccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

- nombre de fois où je joue = nombre de choix de 12 flèches parmi 16 possibles $= \binom{16}{12} = \frac{16!}{12! \cdot 4!}$.
- probabilité de gagner à un coup donné : correspond à prendre 12 nombres au hasard et voir s'ils sont dans le bon ordre. La proba est

$$\frac{1}{12} \cdot \frac{1}{11} \cdot \frac{1}{10} \cdot \frac{1}{9} \cdots \frac{1}{2} \cdot \frac{1}{1}$$

Probabilité d'avoir une sous-suite croissante de longueur 12

$$P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 12 \end{array}\right) = P\left(\begin{array}{c} \text{je gagne} \\ \text{au "loto"} \end{array}\right)$$

$$\leq \left(\begin{array}{c} \text{nombre de fois} \\ \text{où je joue} \end{array}\right) \cdot \left(\begin{array}{c} \text{probabilité que je} \\ \text{gagne à un coup donné} \end{array}\right)$$

$$\begin{array}{cccccccccccccccccc} p = & 11 & 3 & 15 & 1 & 9 & 5 & 8 & 4 & 10 & 16 & 12 & 2 & 6 & 13 & 7 & 14 \\ & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & & & \uparrow & \uparrow & & \uparrow & \uparrow \end{array}$$

- nombre de fois où je joue = nombre de choix de 12 flèches parmi 16 possibles = $\binom{16}{12} = \frac{16!}{12! \cdot 4!}$.
- probabilité de gagner à un coup donné : correspond à prendre 12 nombres au hasard et voir s'ils sont dans le bon ordre. La proba est

$$\frac{1}{12} \cdot \frac{1}{11} \cdot \frac{1}{10} \cdot \frac{1}{9} \cdots \frac{1}{2} \cdot \frac{1}{1} = \frac{1}{12!}$$

Conclusion

Proposition

La probabilité qu'une permutation p de taille n aléatoire ait une sous-suite croissante de longueur $\lceil 3\sqrt{n} \rceil$ est inférieure à

$$\frac{n!}{(\lceil 3\sqrt{n} \rceil)!(n - \lceil 3\sqrt{n} \rceil)!} \cdot \frac{1}{(\lceil 3\sqrt{n} \rceil)!}$$

Conclusion

Proposition

La probabilité qu'une permutation p de taille n aléatoire ait une sous-suite croissante de longueur $\lceil 3\sqrt{n}\rceil$ est inférieure *à*

$$\frac{n!}{(\lceil 3\sqrt{n}\rceil)!(n-\lceil 3\sqrt{n}\rceil)!}\cdot\frac{1}{(\lceil 3\sqrt{n}\rceil)!}$$

Lemme (équivalent de Stirling)

Pour calculer la limite ci-dessus, on peut remplacer $a!$ par $\sqrt{2\pi a}\left(\frac{a}{e}\right)^a$

Conclusion

Proposition

La probabilité qu'une permutation p de taille n aléatoire ait une sous-suite croissante de longueur $\lceil 3\sqrt{n} \rceil$ est inférieure à

$$\frac{n!}{(\lceil 3\sqrt{n} \rceil)!(n - \lceil 3\sqrt{n} \rceil)!} \cdot \frac{1}{(\lceil 3\sqrt{n} \rceil)!}$$

Lemme (équivalent de Stirling)

Pour calculer la limite ci-dessus, on peut remplacer $a!$ par $\sqrt{2\pi a}\left(\frac{a}{e}\right)^a$

Conclusion : le calcul donne

$$\lim_{n\to\infty} P\begin{pmatrix} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 3\sqrt{n} \end{pmatrix} = 0.$$

Conclusion

Proposition

La probabilité qu'une permutation p de taille n aléatoire ait une sous-suite croissante de longueur $\lceil 3\sqrt{n} \rceil$ est *inférieure* *à*

$$\frac{n!}{(\lceil 3\sqrt{n} \rceil)!(n - \lceil 3\sqrt{n} \rceil)!} \cdot \frac{1}{(\lceil 3\sqrt{n} \rceil)!}$$

Lemme (équivalent de Stirling)

Pour calculer la limite ci-dessus, on peut remplacer $a!$ par $\sqrt{2\pi a}\left(\frac{a}{e}\right)^a$

Conclusion : le calcul donne

$$\lim_{n\to\infty} P\left(\begin{array}{c} p \text{ contienne une sous-suite} \\ \text{croissante de longueur } 3\sqrt{n} \end{array} \right) = 0.$$

En d'autres termes, avec grande probabilité,

$$r(p) < 3\sqrt{n}.$$

Transition

On a montré

- $E(r(p)) \geq \sqrt{n}$;
- avec grande probabilité $r(p) < 3\sqrt{n}$

Transition

On a montré

- $E(r(p)) \geq \sqrt{n}$;
- avec grande probabilité $r(p) < 3\sqrt{n}$

On va maintenant "montrer"

Proposition Il existe un nombre C telle que, avec forte probabilité,

$$\lim_{n\to\infty} \frac{r(p)}{\sqrt{n}} = C.$$

Transition

On a montré

- $E(r(p)) \geq \sqrt{n}$;
- avec grande probabilité $r(p) < 3\sqrt{n}$

On va maintenant "montrer"

Proposition Il existe un nombre C telle que, avec forte probabilité,

$$\lim_{n\to\infty} \frac{r(p)}{\sqrt{n}} = C.$$

Ingrédient principal : lemme sous-additif.

Lemme sous-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \leq u_m + u_n.$$

Alors la suite $(\frac{u_n}{n})_{n\geq 1}$ a une limite.

Lemme sous-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \leq u_m + u_n.$$

Alors la suite $(\frac{u_n}{n})_{n\geq 1}$ a une limite.

Démonstration : Considérons le plus petit terme de la suite (u_n/n) :

$$\frac{u_k}{k} = \min_{n\geq 1} \frac{u_n}{n}.$$

⚠ Le minimum n'existe pas toujours. . . Mais supposons un instant qu'il existe.

Lemme sous-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \leq u_m + u_n.$$

Alors la suite $(\frac{u_n}{n})_{n\geq 1}$ a une limite.

Démonstration : Considérons le plus petit terme de la suite (u_n/n) :

$$\frac{u_k}{k} = \min_{n\geq 1} \frac{u_n}{n}.$$

Soit $n \geq 1$. Écrivons $n = qk + r$ (division de n par k). Alors

$$u_n \leq qu_k + u_r$$

Lemme sous-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \leq u_m + u_n.$$

Alors la suite $(\frac{u_n}{n})_{n\geq 1}$ a une limite.

Démonstration : Considérons le plus petit terme de la suite (u_n/n) :

$$\frac{u_k}{k} = \min_{n\geq 1} \frac{u_n}{n}.$$

Soit $n \geq 1$. Écrivons $n = qk + r$ (division de n par k). Alors

$$u_n \leq qu_k + u_r$$

$$\frac{u_k}{k} \leq \frac{u_n}{n} \leq \frac{q \cdot k}{n}\frac{u_k}{k} + \frac{u_r}{n}$$

Lemme sous-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \leq u_m + u_n.$$

Alors la suite $(\frac{u_n}{n})_{n\geq 1}$ a une limite.

Démonstration : Considérons le plus petit terme de la suite (u_n/n) :

$$\frac{u_k}{k} = \min_{n\geq 1} \frac{u_n}{n}.$$

Soit $n \geq 1$. Écrivons $n = qk + r$ (division de n par k). Alors

$$u_n \leq qu_k + u_r$$

$$\frac{u_k}{k} \leq \frac{u_n}{n} \leq \underbrace{\frac{q \cdot k}{n}}_{\to 1} \frac{u_k}{k} + \underbrace{\frac{u_r}{n}}_{\to 0}$$

Lemme sous-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \leq u_m + u_n.$$

Alors la suite $(\frac{u_n}{n})_{n\geq 1}$ a une limite.

Démonstration : Considérons le plus petit terme de la suite (u_n/n) :

$$\frac{u_k}{k} = \min_{n\geq 1} \frac{u_n}{n}.$$

Soit $n \geq 1$. Écrivons $n = qk + r$ (division de n par k). Alors

$$u_n \leq qu_k + u_r$$

$$\frac{u_k}{k} \leq \frac{u_n}{n} \leq \underbrace{\frac{q \cdot k}{n}}_{\to 1} \frac{u_k}{k} + \underbrace{\frac{u_r}{n}}_{\to 0}$$

théorème des gendarmes

$$\lim_{n\to\infty} \frac{u_n}{n} \text{ existe et vaut } \frac{u_k}{k}.$$

Lemme sous-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \leq u_m + u_n.$$

Alors la suite $(\frac{u_n}{n})_{n\geq 1}$ a une limite.

Démonstration : Considérons un petit terme de la suite (u_n/n) :

$$\frac{u_k}{k} \leq \inf_{n\geq 1} \frac{u_n}{n} + \varepsilon \qquad (\varepsilon > 0 \text{ fixé}).$$

Soit $n \geq 1$. Écrivons $n = qk + r$ (division de n par k). Alors

$$u_n \leq q u_k + u_r$$

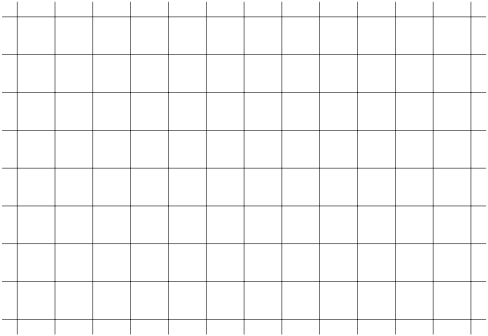
$$\inf \frac{u_n}{n} \leq \frac{u_n}{n} \leq \underbrace{\frac{q \cdot k}{n}}_{\to 1} \left(\inf \frac{u_n}{n} + \varepsilon\right) + \underbrace{\frac{u_r}{n}}_{\to 0}$$

théorème des gendarmes

$$\lim_{n\to\infty} \frac{u_n}{n} \text{ existe et vaut } \inf \frac{u_n}{n}.$$

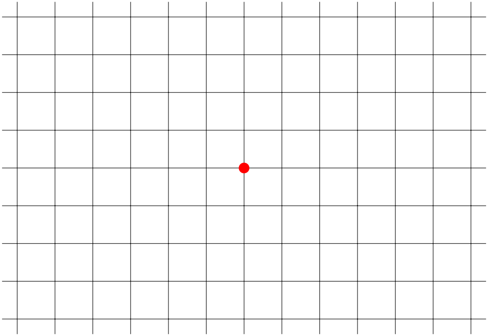
Lemme sous-additif (exemple d'application)

On considère une feuille quadrillée



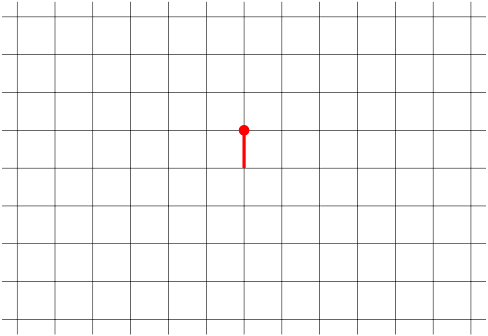
Lemme sous-additif (exemple d'application)

Un marcheur débute au point $(0,0)$.



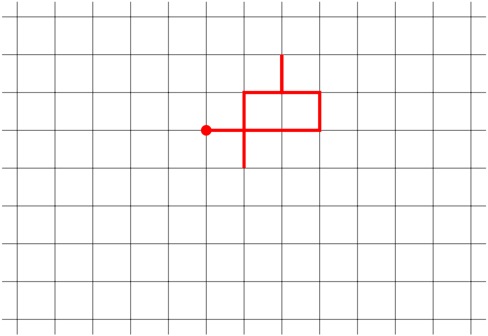
Lemme sous-additif (exemple d'application)

Il se déplace le long de la grille.



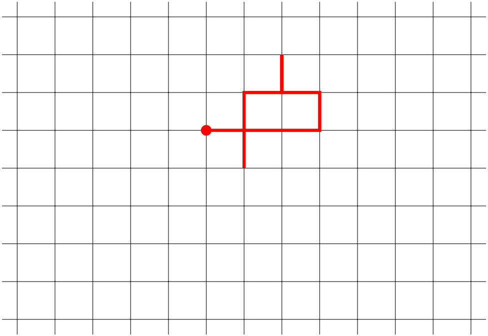
Lemme sous-additif (exemple d'application)

Combien de trajectoire de longueur n le marcheur peut-il faire ?



Lemme sous-additif (exemple d'application)

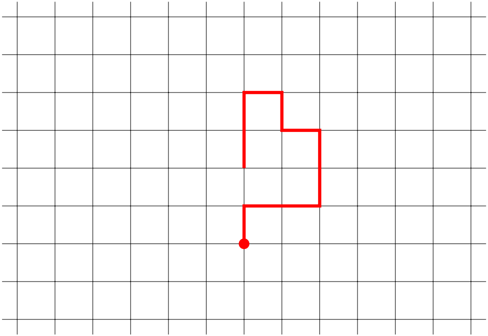
Combien de trajectoire de longueur n le marcheur peut-il faire ?



Facile ! 4 choix pour le premier pas, 4 choix pour le second, ...
Finalement 4^n marches.

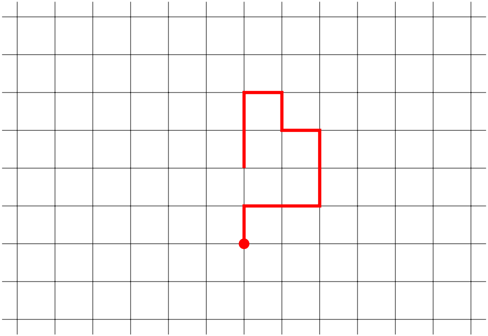
Lemme sous-additif (exemple d'application)

Et si le marcheur ne veut pas passer deux fois au même endroit ?



Lemme sous-additif (exemple d'application)

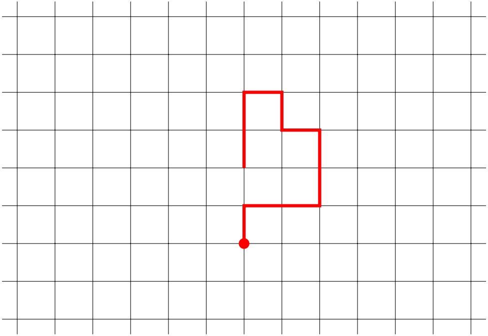
Et si le marcheur ne veut pas passer deux fois au même endroit ?



Difficile ! C'est un problème ouvert important !

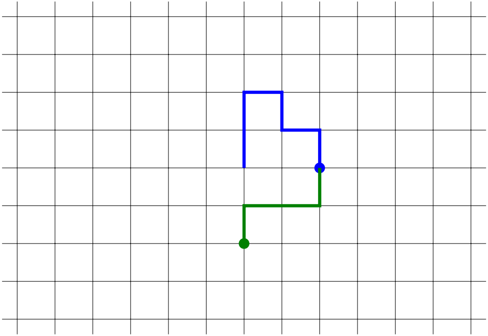
Lemme sous-additif (exemple d'application)

Notons u_n le nombre de marches auto-évitantes de longueur n commençant en $(0,0)$.



Lemme sous-additif (exemple d'application)

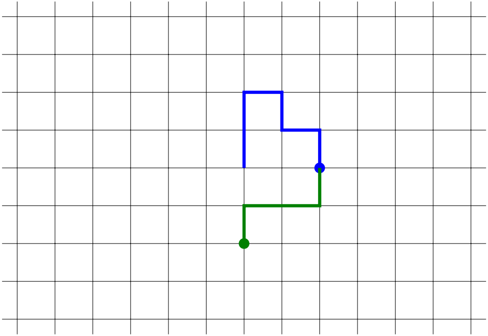
Notons u_n le nombre de marches auto-évitantes de longueur n commençant en $(0, 0)$.



pour tous $m, n \geq 0$, $u_{m+n} \leq u_m \cdot u_n$.

Lemme sous-additif (exemple d'application)

Notons u_n le nombre de marches auto-évitantes de longueur n commençant en $(0,0)$.



$$\text{pour tous } m, n \geq 0,\ u_{m+n} \leq u_m \cdot u_n.$$

Donc $\ln(u_n)$ est sous-additive et

$$\lim_{n\to\infty} \frac{\ln(u_n)}{n} \text{ existe.}$$

Lemme sur-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

$$u_{m+n} \geq u_m + u_n.$$

Alors, si la suite $(\frac{u_n}{n})_{n\geq 1}$ est bornée, elle a une limite.

Lemme sur-additif

Lemme (Fekete)

Soit $(u_n)_{n\geq 1}$ une suite de réels positifs. Supposons que pour tous entiers m et n,

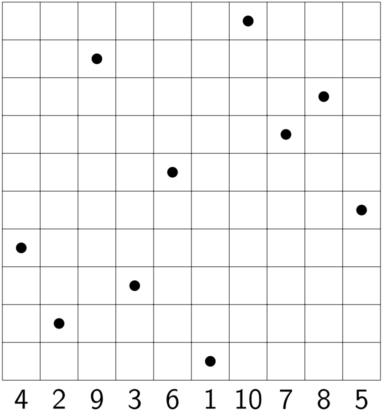
$$u_{m+n} \geq u_m + u_n.$$

Alors, si la suite $(\frac{u_n}{n})_{n\geq 1}$ est bornée, elle a une limite.

Démonstration : similaire au cas sous-additif.

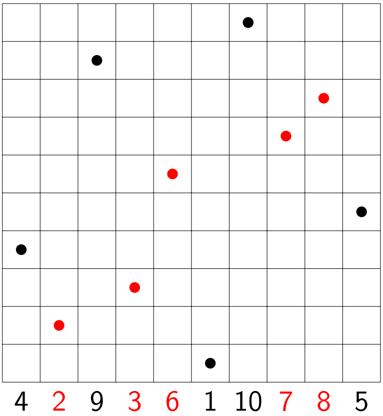
Permutations et points dans une grille

On peut représenter une permutation par des points dans une grille



Permutations et points dans une grille

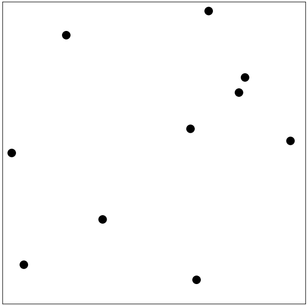
On peut représenter une permutation par des points dans une grille



sous-suite croissante = ensemble de points allant vers le Nord-Est

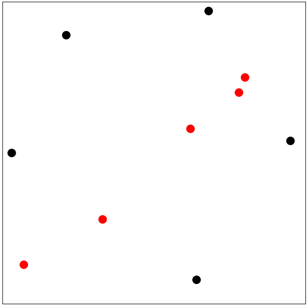
Points aléatoires

Au lieu de prendre une premutation aléatoire, on peut prendre n points au hasard dans un carré.



Points aléatoires

Au lieu de prendre une premutation aléatoire, on peut prendre n points au hasard dans un carré.



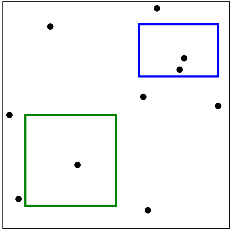
Problème

À quoi ressemble la taille du plus grand ensemble de points en direction Nord-Est?

Exactement la même question qu'étudier $r(p)$...

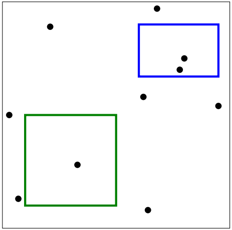
Poissonisation

Difficulté : ce qui se passe dans deux zones disjointes du carré n'est pas indépendant.



Poissonisation

Difficulté : ce qui se passe dans deux zones disjointes du carré n'est pas indépendant.

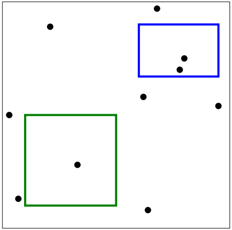


Solution : au lieu de prendre n points, on prend un nombre N aléatoire de points

$$P(N = k) = \frac{n^k}{k!} e^{-n}$$

Poissonisation

Difficulté : ce qui se passe dans deux zones disjointes du carré n'est pas indépendant.



Solution : au lieu de prendre n points, on prend un nombre N aléatoire de points

$$P(N = k) = \frac{n^k}{k!} e^{-n}$$

Miracle : N est "proche" de n et, maintenant ce qui se passe dans les rectangles bleu et vert est indépendant.

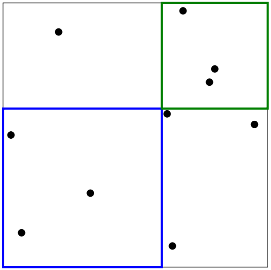
Sur additivité

Notons u_n la taille du plus grand sous-ensemble de points Nord-Est quand on prend environ n points au hasard dans un carré.
$u_n \approx r(p)$.

Sur additivité

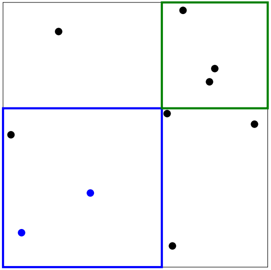
Notons u_n la taille du plus grand sous-ensemble de points Nord-Est quand on prend environ n points au hasard dans un carré.

Soit $n = (s+t)^2$.



Sur additivité

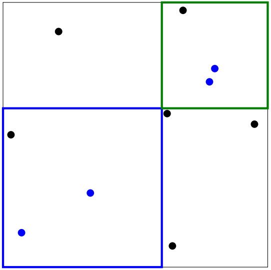
Notons u_n la taille du plus grand sous-ensemble de points Nord-Est quand on prend environ n points au hasard dans un carré.
Soit $n = (s+t)^2$.



- dans le rectangle bleu, on a environ s^2 points au hasard, donc u_{s^2} points en position Nord-Est.

Sur additivité

Notons u_n la taille du plus grand sous-ensemble de points Nord-Est quand on prend environ n points au hasard dans un carré.
Soit $n = (s+t)^2$.

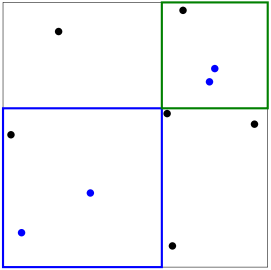


- dans le rectangle bleu, on a environ s^2 points au hasard, donc u_{s^2} points en position Nord-Est.
- dans le rectangle vert, on a environ t^2 points au hasard, donc u_{t^2} points en position Nord-Est.

Sur additivité

Notons u_n la taille du plus grand sous-ensemble de points Nord-Est quand on prend environ n points au hasard dans un carré.

Soit $n = (s+t)^2$.



- dans le rectangle bleu, on a environ s^2 points au hasard, donc u_{s^2} points en position Nord-Est.
- dans le rectangle vert, on a environ t^2 points au hasard, donc u_{t^2} points en position Nord-Est.

Conclusion : $u_{(s+t)^2} \geq u_{s^2} + u_{t^2}$.

Conclusion

- On a expliqué : u_{s^2} est sur-additif ;

Conclusion

- On a expliqué : u_{s^2} est sur-additif ;
- Comme $u_n \approx r(p)$, on a $u_{s^2} \leq 3\sqrt{s^2} = 3s$ avec grande probabilité ;

Conclusion

- On a expliqué : u_{s^2} est sur-additif ;
- Comme $u_n \approx r(p)$, on a $u_{s^2} \leq 3\sqrt{s^2} = 3s$ avec grande probabilité ;

En utilisant une version aléatoire du lemme sur-additif (Kingman, 1976), on obtient

$$\frac{u_{s^2}}{s} \text{ a une limite (avec forte probabilité)}$$

Conclusion

- On a expliqué : u_{s^2} est sur-additif ;
- Comme $u_n \approx r(p)$, on a $u_{s^2} \leq 3\sqrt{s^2} = 3s$ avec grande probabilité ;

En utilisant une version aléatoire du lemme sur-additif (Kingman, 1976), on obtient

$$\frac{u_{s^2}}{s} \text{ a une limite (avec forte probabilité)}$$

En posant $s = \sqrt{n}$ (on oublie ici que s était entier) et, en *dépoissonisant*, on en déduit que :

Proposition Il existe un nombre C telle que, avec forte probabilité,

$$r(p) \approx C\sqrt{n}.$$

3 résultats

Proposition La moyenne $E(r(p))$ de $r(p)$ vérifie

$$E(r(p)) \geq \sqrt{n}.$$

$\rightarrow$ principe des tiroirs.

Proposition Avec très forte probabilité,

$$r(p) < 3\sqrt{n}$$

$\rightarrow$ méthode du premier moment.

Proposition Il existe un nombre C telle que, avec forte probabilité,

$$r(p) \approx C\sqrt{n}$$

$\rightarrow$ points aléatoires, lemme sur-additif.