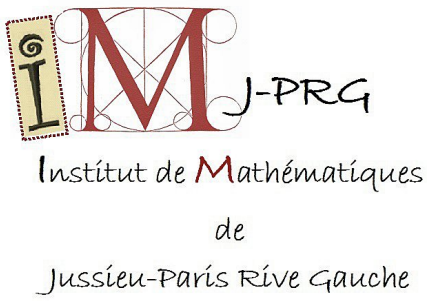
Rencontres du *t*ième type

Javier Fresán

IMJ-PRG, Sorbonne Université



Le problème des rencontres

Aujourd'hui, il s'agit de calculer la **probabilité qu'une permutation prise au hasard n'ait pas de point fixe**.

Mais à l'époque on formulait les choses un peu différemment...

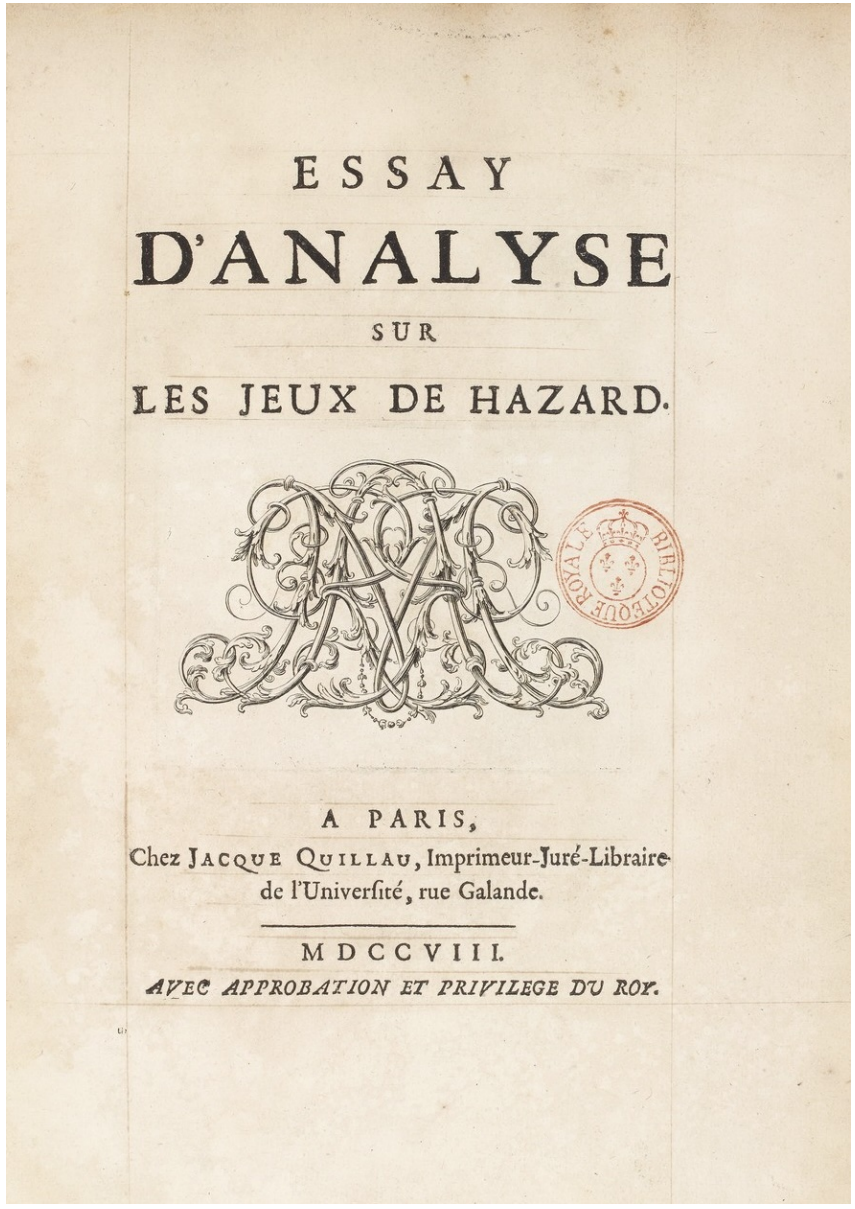
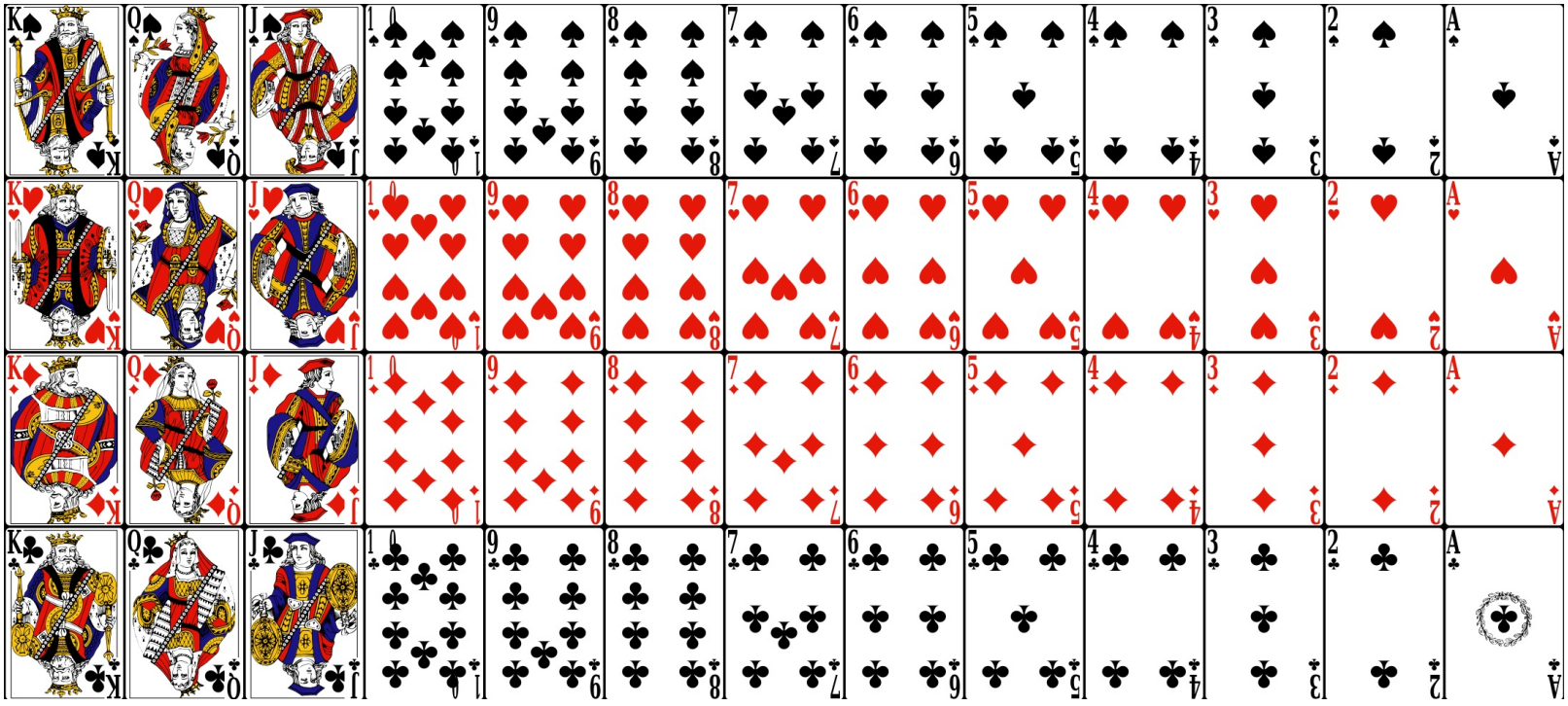


Figure – Pierre Remond de Montmort, *Essay d'analyse sur les jeux de hazard*, première édition de 1708



PROBLÉMES DIVERS SUR LE JEU DU TREIZE.

EXPLICATION DU JEU.

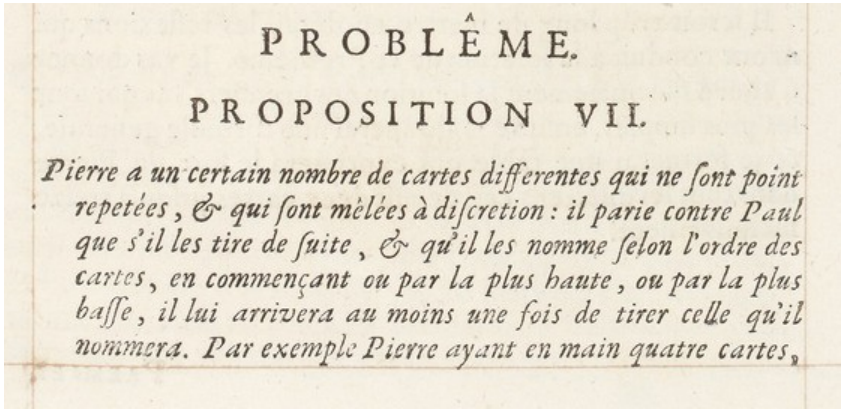
LEs Joueurs tirent d'abord à qui aura la main. Supposons que ce ſoit Pierre, & que le nombre des Joueurs ſoit tel qu'on voudra. Pierre ayant un jeu entier compoſé de cinquante-deux cartes mêlées à diſcretion, les tire l'une après l'autre. Nommant & prononçant un lorſqu'il tire la premiere carte, deux lorſqu'il tire la ſeconde, trois lorſqu'il tire la troiſiéme, & ainſi de ſuite juſqu'à la treiziéme qui eſt un Roy. Alors ſi dans toute cette ſuite de cartes il n'en a tiré aucune ſelon le rang qu'il les a nommées, il paye ce que chacun des Joueurs a mis au jeu, & cede la main à celui qui le ſuit à la droite.

Mais s'il lui arrive dans la ſuite des treize cartes, de tirer la carte qu'il nomme, par exemple de tirer un as dans le temps qu'il nomme un, ou un deux dans le temps qu'il nomme deux, ou un trois dans le temps qu'il nomme trois, &c. il prend tout ce qui eſt au jeu, & recommence comme auparavant, nommant un, enſuite deux, &c.

L'avantage eſt fort conſiderable à ce Jeu en faveur de celui qui a la main, & ceux qui le jouent ſouvent peuvent s'en appercevoir par pratique; mais il eſt extrémement difficile de déterminer cet avantage: l'Analyſe y pourroit conduire, mais cette route ſeroit extrémement longue, & je trouve qu'il faudroit reſoudre plus de mille égalités pour déterminer tous les cas poſſibles de ce Jeu. On en pourroit plutôt eſperer la ſolution en conſiderant tous les arrangemens poſſibles des cinquante-deux cartes, & découvrant comme l'on a fait pour le Pharaon, & comme l'on fera dans le Problême ſuivant pour le jeu de la Baſſette, quelque loi uniforme, qui des cas ſimples conduiſe à des cas plus compoſés, & fourniſſe ainſi une ſolution generale. Je ne donnerai point ici la ſolution de ce Problême, mais en ſa place en voici deux qui y ont beaucoup de raport, & dont la ſolution pourra faciliter celle du jeu du Treize à ceux d'entre mes Lecteurs qui voudront ſe donner la peine d'en faire la recherche.

Explication du jeu du treize

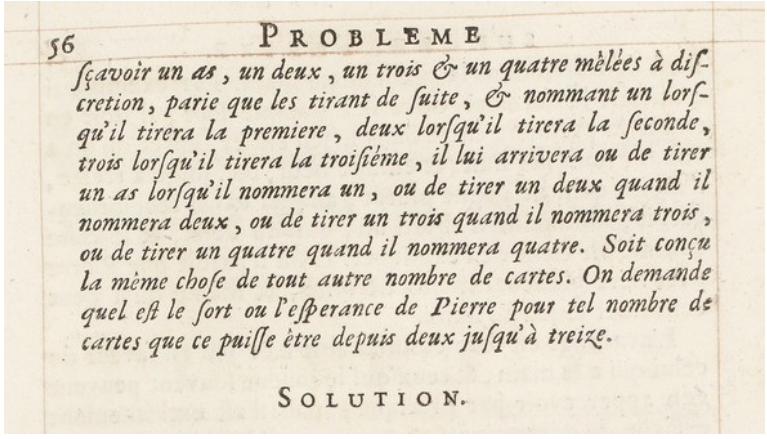
Les jouers tirent d'abord à qui aura la main. Supposons que ce soit Pierre, et que le nombre de jouers soit tel qu'on voudra. Pierre ayant un jeu entier composé de cinquante-deux cartes mêlées à discrétion, les tire l'une après l'autre. Nommant et prononçant un lorsqu'il tire la première carte, deux lorsqu'il tire la seconde, trois lorsqu'il tire la troisième, et ainsi de suite jusqu'à la treizième qui est un roi. Alors si dans toute cette suite de cartes il n'en a tiré aucune selon le rang qu'il les a nommées, il paye ce que chacun des jouers a mis au jeu, et cède la main à celui qui le suit à la droite. Mais s'il lui arrive dans la suite des treize cartes, de tirer la carte qu'il nomme, par exemple de tirer un as dans le temps qu'il nomme un, ou un deux dans le temps qu'il nomme deux, ou un temps dans le temps qu'il nomme trois, etc. il prend tout ce qui est au jeu, et recommence comme auparavant, nommant un, ensuite deux, etc.



PROBLÊME.

PROPOSITION VII.

Pierre a un certain nombre de cartes differentes qui ne ſont point repetées, & qui ſont mêlées à diſcretion : il parie contre Paul que s'il les tire de ſuite, & qu'il les nomme ſelon l'ordre des cartes, en commençant ou par la plus haute, ou par la plus baſſe, il lui arrivera au moins une fois de tirer celle qu'il nommera. Par exemple Pierre ayant en main quatre cartes,



ſçavoir un as, un deux, un trois & un quatre mêlées à diſcretion, parie que les tirant de ſuite, & nommant un lorſqu'il tirera la premiere, deux lorſqu'il tirera la ſeconde, trois lorſqu'il tirera la troiſiéme, il lui arrivera ou de tirer un as lorſqu'il nommera un, ou de tirer un deux quand il nommera deux, ou de tirer un trois quand il nommera trois, ou de tirer un quatre quand il nommera quatre. Soit conçu la même choſe de tout autre nombre de cartes. On demande quel eſt le ſort ou l'eſperance de Pierre pour tel nombre de cartes que ce puiſſe être depuis deux juſqu'à treize.

SOLUTION.

Un problème plus simple...

Pierre a un certain nombre de cartes différentes qui ne sont point répétées, et qui sont mêlées à discrétion : il parie contre Paul que s'il les tire de suite, et qu'il les nomme selon l'ordre des cartes, en commençant ou par la plus haute, ou par la plus basse, il lui arrivera au moins une fois de tirer celle qu'il nommera. Par exemple, Pierre ayant en main quatre cartes [...] Soit conçu la même chose de tout autre nombre de cartes. **On demande quel est le sort ou l'espérance de Pierre pour tel nombre de cartes** *que ce puisse être depuis deux jusqu'à treize.*

Théorème (Montmort, Bernoulli)

Soient $n \geq 1$ et $k \geq 0$ des entiers. La probabilité qu'une permutation $\sigma \in S_n$ ait k points fixes est égale à

$$\frac{1}{n!}|\{\sigma \in S_n \mid |\mathrm{Fix}(\sigma)| = k\}| = \frac{1}{k!}\sum_{j=0}^{n-k}\frac{(-1)^j}{j!}.$$

En particulier,

$$\lim_{n\to+\infty}\frac{|\{\sigma \in S_n \mid |\mathrm{Fix}(\sigma)| = k\}|}{n!} = \frac{1}{k!}\frac{1}{e}.$$

Démonstration

Soit D_m le nombre de *dérangements* dans S_m, c'est-à-dire des permutations sans point fixe. Alors

$$|\{\sigma \in S_n \mid |\mathrm{Fix}(\sigma)| = k\}| = \binom{n}{k} D_{n-k}$$

et il suffit de calculer D_{n-k}.

Posons $A_i = \{\sigma \in S_m \mid \sigma(i) = i\}$ pour $i = 1, \ldots, m$. Alors, par le principe d'inclusion-exclusion

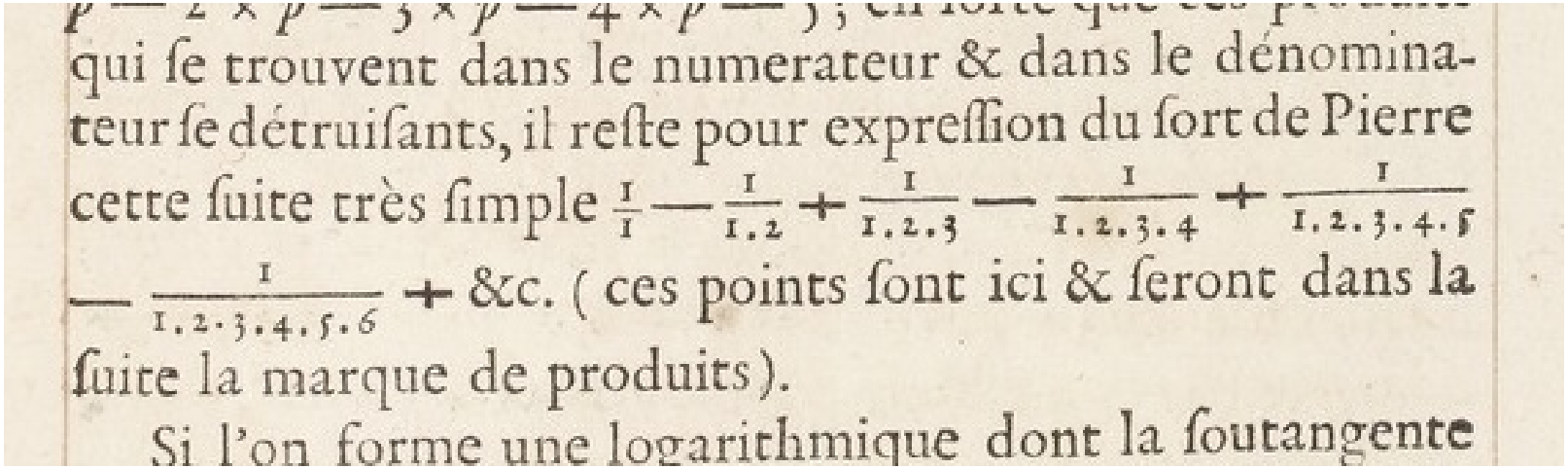
$$\begin{aligned} D_m &= |S_m| - |\bigcup_{i=1}^{m} A_i| \\ &= m! - \sum_{i=1}^{m} |A_i| + \sum_{1 \le i < j \le m} |A_i \cap A_j| - \cdots \\ &= m! - m(m-1)! + \binom{m}{2}(m-2)! - \cdots \\ &= m! \sum_{j=0}^{m} \frac{(-1)^j}{j!}. \end{aligned}$$

En mettant tout ensemble,

$$\frac{1}{n!}|\{\sigma \in S_n \mid |\mathrm{Fix}(\sigma)| = k\}| = \frac{1}{n!}\binom{n}{k} D_{n-k}$$

$$= \frac{1}{\cancel{n!}} \frac{\cancel{n!}}{\cancel{(n-k)!}k!} \cancel{(n-k)!} \sum_{j=0}^{n-k} \frac{(-1)^j}{j!},$$

ce qu'il fallait démontrer $\square$



qui ſe trouvent dans le numerateur & dans le dénominateur ſe détruiſants, il reſte pour expreſſion du ſort de Pierre cette ſuite très ſimple $\frac{1}{1} - \frac{1}{1.2} + \frac{1}{1.2.3} - \frac{1}{1.2.3.4} + \frac{1}{1.2.3.4.5} - \frac{1}{1.2.3.4.5.6}$ + &c. (ces points ſont ici & ſeront dans la ſuite la marque de produits).

Si l'on forme une logarithmique dont la ſoutangente

Figure – La solution chez Montmort : la probabilité que Pierre gagne au jeu de treize est $1 - D_n = 1 - \sum_{j=0}^{n} \frac{(-1)^j}{j!} = \sum_{j=1}^{n} \frac{(-1)^{j-1}}{j!}$.

D'un point de vue plus moderne, on formulerait l'énoncé limite dans le problème des rencontres comme suit :

Théorème

Soit $(X_n)_{n\geq 0}$ une suite de variables aléatoires avec X_n uniformément distribuée dans S_n. Alors, lorsque $n \to +\infty$, on a convergence en loi

$$|\mathrm{Fix}(X_n)| \longrightarrow \mathrm{Pois}(1),$$

où $\mathrm{Pois}(\lambda)$ est la loi de Poisson de paramètre λ (qui donne probabilité $\frac{\lambda^k}{k!}e^{-\lambda}$ à chaque entier $k \geq 0$).

Racines modulo p d'un polynôme

Soit $f \in \mathbb{Z}[X]$ un polynôme à coefficients entiers.

Pour chaque nombre premier p, on peut **réduire f modulo p et compter le nombre des racines** dans

$$\mathbb{Z}/p\mathbb{Z} = \{[0], [1], \ldots, [p-1]\}.$$

On le note

$$N_f(p) = \big|\{0 \leq x \leq p-1 \mid p \text{ divise } f(x)\}\big|.$$

Par exemple, prenons $f = X^4 - X - 1$. Ses premières valeurs sont :

x	$x^4 - x - 1$
0	-1
1	-1
2	13
3	7×11
4	251
5	619
6	1289
7	2393
8	61×67
9	6551
10	7×1427
11	14629
12	$17 \times 23 \times 53$

En regardant la table, on trouve les valeurs

p	2	3	5	7	11	13	17	19	$\cdots$
$N_f(p)$	0	0	0	1	1	1	2	0	$\cdots$

En fait, parmi les 1000 premiers nombres premiers, on trouve

375 fois la valeur $N_f(p) = 0$	$375/1000 \approx 3/8$
337 fois la valeur $N_f(p) = 1$	$337/1000 \approx 1/3$
253 fois la valeur $N_f(p) = 2$	$253/1000 \approx 1/4$
35 fois la valeur $N_f(p) = 4$	$35/1000 \approx 1/24$

Un théorème de Kronecker (1880)

Soit $f \in \mathbb{Z}[X]$ un polynôme à coefficients entiers de degré n.

Si f est irréductible, c'est-à-dire n'est pas un produit de polynômes de degré ≥ 1, alors f a exactement n racines complexes

$$\alpha_1, \ldots, \alpha_n.$$

En général, il n'y a pas de manière canonique d'en faire la liste et on est amené à considérer les permutations de $\{\alpha_1, \ldots, \alpha_n\}$.

Une permutation $\sigma \in S_n$ ne préserve pas nécessairement les relations algébriques entre les racines, c'est-à-dire les expressions

$$Q(\alpha_1, \ldots, \alpha_n) = 0$$

où $Q \in \mathbb{Z}[T_1, \ldots, T_n]$ est un polynôme en n variables.

Le **groupe de Galois de f** est le sous-ensemble $G \subset S_n$ formé des permutations σ telles que, pour tout $Q \in \mathbb{Z}[T_1, \ldots, T_n]$, on ait

$$Q(\alpha_1, \ldots, \alpha_n) = 0 \Longrightarrow Q(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0.$$

Par exemple, les racines de

$$f = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1$$

sont les 4 racines primitives cinquièmes de l'unité

$$\alpha_k = e^{\frac{2i\pi}{5}k} \quad k = 1, \ldots, 4$$

et la relation algébrique $\alpha_k = \alpha_1^k$ est seulement préservée par les permutations engendrées par le 4-cycle (1243).

Théorème (Kronecker, 1880)

Soit $f \in \mathbb{Z}[X]$ un polynôme irréductible de degré n avec groupe de Galois G. Pour chaque entier $k \geq 0$, on a

$$\lim_{T \to +\infty} \frac{|\{p \leq T \text{ premier } \mid N_f(p) = k\}|}{|\{p \leq T \text{ premier}\}|} = \frac{|\{\sigma \in G \mid |\mathrm{Fix}(\sigma)| = k\}|}{|G|}$$

Par exemple, le polynôme $f = X^4 - X - 1$ a groupe de Galois S_4 et on trouve la limite

$$\lim_{T \to +\infty} \frac{|\{p \leq T \mid N_f(p) = 1\}|}{|\{p \leq T\}|} = \sum_{j=0}^{3} \frac{(-1)^j}{j!} = \frac{1}{3}.$$

lkeinen besonderen Affect besitzt, so resultirt, indem man sich die Gleichung ffür eine lineare Function von h Wurzeln gebildet denkt, die Relation

$$\sum_{k=1}^{k=n} k(k-1)\cdots(k-h+1)D_k = 1,$$

und diese ergiebt für die Dichtigkeit D_k den Werth

$$\frac{1}{k!}\sum_{\lambda}\frac{(-1)^{\lambda}}{\lambda!} \qquad (\lambda = 0, 1, \ldots n-k) \qquad (0! = 1),$$

welcher für grosse Werthe von n und relativ kleine von k nahezu gleich $\frac{1}{e}\cdot\frac{1}{k!}$ wird, und die Summe

$$\sum_{k=1}^{n}\frac{k}{e\cdot k!}$$

wird eben wieder gleich 1. Dagegen wird die Gesammtdichtigkeit der Primtheiler einer irreductibeln Function $F(x)$, die gleich Null gesetzt eine allgemeine Gleichung repräsentirt, für grössere Werthe des Grades n nahezu $\left(\left(1-\frac{1}{e}\right)\right.$ also etwa $\frac{7}{11}$.

Figure – Leopold Kronecker, *Sur l'irréductibilité des équations*, 1880

Si on avait fait nos expériences pour le polynôme

$$f = X^4 - X^2 - 1,$$

on aurait trouvé les statistiques

633 fois la valeur $N_f(p) = 0$	$633/1000 \approx 5/8$
251 fois la valeur $N_f(p) = 2$	$251/1000 \approx 1/4$
116 fois la valeur $N_f(p) = 4$	$116/1000 \approx 1/8,$

ce qui suggère que le groupe de Galois $G \subset S_4$ est d'ordre 8 au lieu de 24 (et en effet c'est le groupe D_8 des symétries du carré !).

Pseudopolynômes

Si $f \in \mathbb{Z}[X]$ est un polynôme à coefficients entiers, alors pour tous entiers $n \geq 0$ et $d \geq 1$

$$f(n+d) - f(n) \text{ est divisible par d.}$$

En effet, il suffit de le démontrer pour $f = X^k$, auquel cas

$$(n+d)^k - n^k = \sum_{j=1}^{k} \binom{k}{j} n^{k-j} d^j$$

par la formule du binôme. Au fond, c'est la raison pour laquelle la réduction modulo p d'un polynôme est bien définie...

Cette propriété ne caractérise pas les polynômes...

Définition (Hall, 1971)

Un pseudopolynôme est une suite $(a_n)_{n\geq 0}$ *de nombres entiers telle que* d *divise* $a_{n+d} - a_n$ *pour tous entiers* $n \geq 0$ *et* $d \geq 1$.

Il existe une infinité non dénombrable de pseudopolynômes qui ne proviennent pas de polynômes.

Pour en construire, on considère des suites de la forme

$$a_n = \sum_{k=0}^{n} \binom{n}{k} b_k,$$

où $(b_n)_{n\geq 0}$ est une suite d'entiers avec la propriété

$$\mathrm{ppcm}(1, \ldots, n) \text{ divise } b_n.$$

Hall démontre que $(a_n)_{n\geq 0}$ est alors un pseudopolynôme qui provient d'un polynôme si et seulement si $b_n = 0$ pour n grand.

Par exemple, pour $b_n = n!$, on trouve

$$a_n = n! \sum_{k=0}^{n} \frac{1}{k!} = \lfloor en! \rfloor$$

(la deuxième égalité est seulement vraie pour $n \geq 1$).

Grâce aux propriétés de congruence, le nombre de racines modulo p d'un pseudopolynôme $f(n) = a_n$ est bien défini :

$$N_f(p) = |\{0 \leq n \leq p-1 \mid \ p \text{ divise } a_n\}|.$$

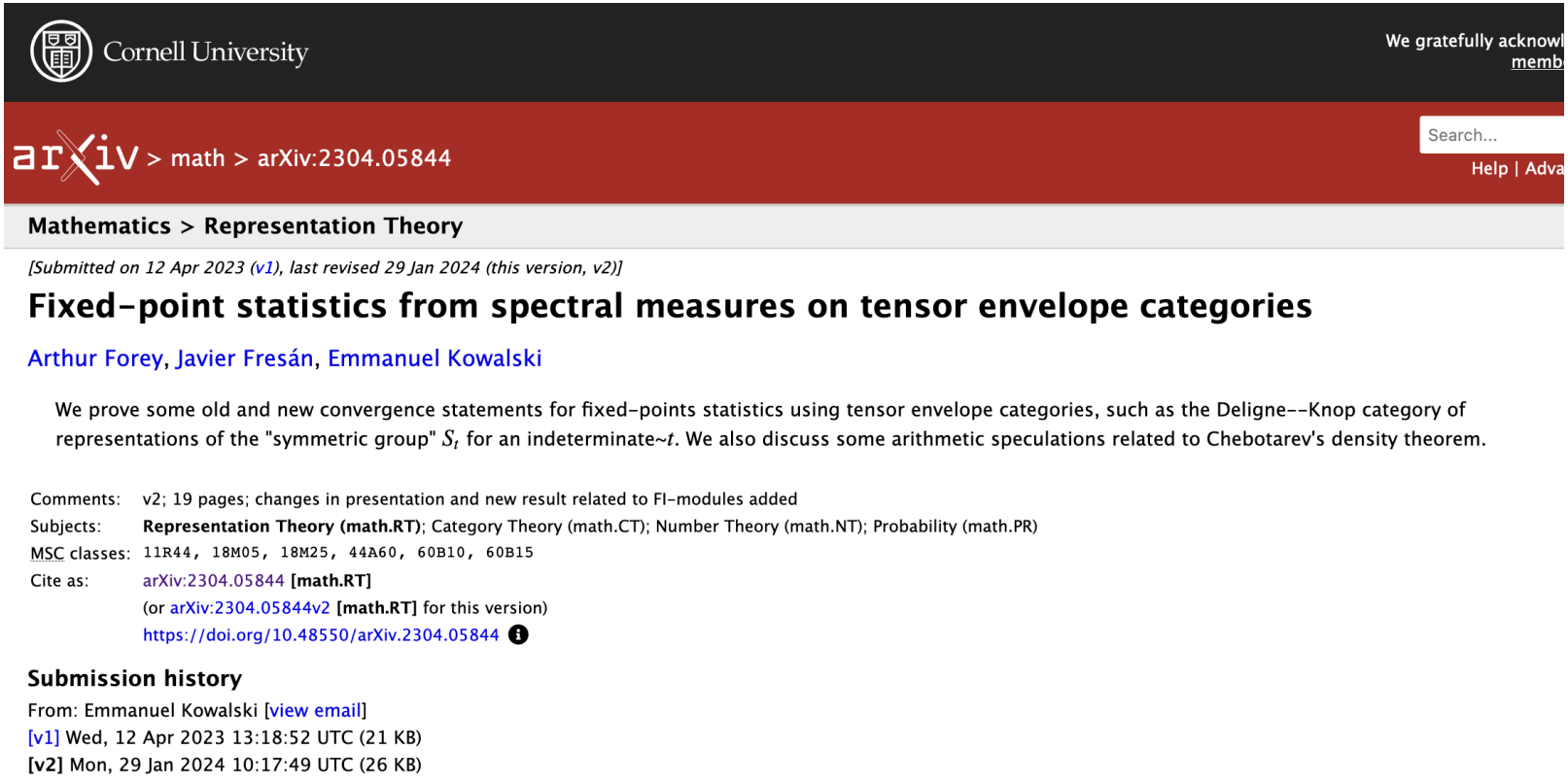
Par exemple, pour notre pseudopolynôme favori :

n	$\lfloor en! \rfloor$
0	1
1	2
2	5
3	2^4
4	5×13
5	2×163
6	19×103
7	$2^2 \times 5^2 \times 137$

Conjecture (Kowalski–Soundararajan)

Soit $f(n) = \lfloor en! \rfloor$. *Pour chaque entier* $k \geq 0$, *on a la limite*

$$\lim_{T \to +\infty} \frac{|\{p \leq T \mid N_f(p) = k\}|}{|\{p \leq T\}|} = \frac{1}{k!}\frac{1}{e}.$$



Cornell University

We gratefully acknowl
memb

arXiv > math > arXiv:2304.05844

Search...

Help | Adva

Mathematics > Representation Theory

[Submitted on 12 Apr 2023 (v1), last revised 29 Jan 2024 (this version, v2)]

Fixed-point statistics from spectral measures on tensor envelope categories

Arthur Forey, Javier Fresán, Emmanuel Kowalski

We prove some old and new convergence statements for fixed-points statistics using tensor envelope categories, such as the Deligne--Knop category of representations of the "symmetric group" S_t for an indeterminate~t. We also discuss some arithmetic speculations related to Chebotarev's density theorem.

Comments: v2; 19 pages; changes in presentation and new result related to FI-modules added
Subjects: **Representation Theory (math.RT)**; Category Theory (math.CT); Number Theory (math.NT); Probability (math.PR)
MSC classes: 11R44, 18M05, 18M25, 44A60, 60B10, 60B15
Cite as: arXiv:2304.05844 **[math.RT]**
(or arXiv:2304.05844v2 **[math.RT]** for this version)
https://doi.org/10.48550/arXiv.2304.05844

Submission history

From: Emmanuel Kowalski [view email]
[v1] Wed, 12 Apr 2023 13:18:52 UTC (21 KB)
[v2] Mon, 29 Jan 2024 10:17:49 UTC (26 KB)

Figure – Arthur Forey, Javier Fresán, Emmanuel Kowalski, *Fixed-point statistics from spectral measures on tensor envelope categories*, 2023

Par la **méthode des moments**, pour démontrer la convergence en loi $|\mathrm{Fix}(X_n)| \to \mathrm{Pois}(1)$, il suffit de démontrer la convergence des suites des moments : pour tout $k \geq 1$,

$$\lim_{n \to +\infty} \frac{1}{n!} \sum_{\sigma \in S_n} |\mathrm{Fix}(\sigma)|^k = \frac{1}{e} \sum_{r=0}^{\infty} \frac{r^k}{r!}$$

Le côté gauche a une interprétation en termes des représentations du groupe symétrique S_n. Une **représentation** est un espace vectoriel complexe de dimension finie V muni d'endomorphismes

$$\varphi_\sigma \colon V \longrightarrow V, \quad \text{un pour chaque } \sigma \in S_n,$$

qui satisfont à $\varphi_{\sigma\tau} = \varphi_\sigma \circ \varphi_\tau$ et $\varphi_{\mathrm{Id}} = \mathrm{Id}_V$.

Par exemple, $V = \mathbb{C}^n$, avec les matrices de permutation

$$\varphi_\sigma(e_i) = e_{\sigma(i)}.$$

On l'appelle la représentation *standard* et on la note Std.

$V = \mathbb{C}$ avec tous les endomorphismes $\varphi_\sigma = \mathrm{Id}_V$. On l'appelle la représentation *triviale* et on la note $\mathbf{1}$.

Pour une représentation V, on peut chercher des sous-espaces vectoriels $W \subset V$ stables sous les endomorphismes φ_σ.

Par exemple, la droite $e_1 + \cdots + e_n \subset \mathbb{C}^n$ est stable sous les matrices de permutation φ_σ, qui y agissent trivialement :

$$\varphi_\sigma(e_1 + \cdots + e_n) = e_{\sigma(1)} + \cdots + e_{\sigma(n)} = e_1 + \cdots + e_n.$$

On dit que Std contient une copie de la représentation triviale $\mathbf{1}$. Plus est vrai : il existe un supplémentaire qui est aussi stable sous les endomorphismes φ_σ.

Pour chaque $k \geq 1$, l'espace vectoriel $(\mathbb{C}^n)^{\otimes k}$ est de dimension n^k, une base étant donnée par

$$e_{i_1} \otimes \cdots \otimes e_{i_k} \qquad \big(i_1, \ldots, i_k \in \{1, \ldots, n\}\big).$$

On définit une représentation de S_n en posant :

$$\begin{aligned} \varphi_\sigma(e_{i_1} \otimes \cdots \otimes e_{i_k}) &= \varphi_\sigma(e_{i_1}) \otimes \cdots \otimes \varphi_\sigma(e_{i_k}) \\ &= e_{\sigma(i_1)} \otimes \cdots \otimes e_{\sigma(i_k)} \end{aligned}$$

On la note $\mathrm{Std}^{\otimes k}$.

Proposition

$$\frac{1}{n!} \sum_{\sigma \in S_n} |\mathrm{Fix}(\sigma)|^k$$

est égal à la multiplicité de $\mathbf{1}$ *dans la représentation* $\mathrm{Std}^{\otimes k}$.

La suite dans le côté droit

$$\frac{1}{e}\sum_{r=0}^{\infty}\frac{r^k}{r!}$$

est célèbre en combinatoire sous le nom de **nombres de Bell**. C'est le nombre de partitions d'un ensemble à k éléments :

$$1, 2, 5, 15, 52, 203, 877, 4140, 21147, \ldots$$

Explication : les deux suites satisfont aux mêmes relations de récurrence $c_0 = 1$ et

$$c_{n+1} = \sum_{s=0}^{n}\binom{n}{s}c_s.$$

(Exercice !)

Pour une variable t, il n'existe pas de groupe symétrique S_t. Cependant, Deligne et Knop (2007) définissent ce que devraient être les représentations de S_t. Lorsque t est un entier $n \geq 1$, on retrouve à peu de choses près les représentations de S_n. Parmi ces représentations, il y a une représentation standard Std_t et une représentation triviale $\mathbf{1}_t$, et on peut démontrer l'égalité

$$\frac{1}{e}\sum_{r=0}^{\infty}\frac{r^k}{r!} = \text{multiplicité de } \mathbf{1}_t \text{ dans } \mathrm{Std}_t^{\otimes k}.$$

Question

Le pseudopolynôme $f(n) = \lfloor en! \rfloor$ a-t-il "groupe de Galois" S_t ?