Lois logiques de (non)-convergence pour les permutations aléatoires

Valentin Féray, Université de Lorraine

Journées ALÉA 2023

Quelques notations

S_n : ensemble des permutations de taille n ;
$x \in_u E$: x est un élément uniforme de l'ensemble E (supposé fini) ;
$\#\mathrm{cyc}(\sigma)$: nombre de cycles de la permutation σ (y compris les points fixes) ;
$\#\mathrm{inv}(\sigma)$: nombre d'inversions de la permutation σ ;
$\sigma \models \varphi$: la permutation σ satisfait la propriété φ ;
$\mathrm{Av}(\tau)$ (resp. $\mathrm{Av}_n(\tau)$) : ensemble des permutations (resp. permutations de taille n) évitant le motif τ.
$\log^*(n)$: l'entier k minimal tel que $\underbrace{\log \cdots \log}_{k \text{ itérations}}(n) < 2$.

1 Introduction

1.1 Problématique

Modèles classiques de permutations aléatoires :

- uniformes : $\boldsymbol{\sigma}_n \in_u S_n$;
- biaisées, en particulier permutations d'Ewens et de Mallows :

$$\mathbb{P}^E_\theta(\sigma) \propto \theta^{\#\mathrm{cyc}(\sigma)}, \qquad \mathbb{P}^M_q(\sigma) \propto q^{\#\mathrm{inv}(\sigma)};$$

- uniformes avec contraintes : $\sigma_n \in_u \mathcal{C}_n$, pour un certain sous-ensemble $\mathcal{C}_n$ de S_n. En particulier, $\mathcal{C}_n$ peut être un ensemble de permutations évitant un ou plusieurs motifs.

Problèmes classiques :

- déterminer $\lim_{n\to\infty} \mathbb{P}[\sigma_n \models \varphi]$ pour certaines propriétés φ (par exemple, il est très classique qu'une permutation aléatoire uniforme n'a pas de point fixe avec probabilité asymptotiquement $1/e$) ;
- comportement asymptotique de certaines statistiques (par exemple le nombre de cycles, d'inversions ou de descentes, ou taille de la plus longue sous-suite croissante) ;
- « forme limite » (*permutons*).

Ici, on va seulement regarder la première question (et même seulement l'existence de la limite), mais pour un *grand ensemble de propriétés φ simultanément*. Plus précisément, on considère les propriétés φ *logiques du premier ordre*, i.e. qui peuvent s'écrire avec les symboles

$$\exists, \forall, \neg, \wedge, \vee, \underbrace{x, y, z, \ldots}_{\text{variables}}, =, <_P, <_V,$$

où :

- les variables représentent des entiers entre 1 et n ;
- $<_P$ est l'ordre naturel sur les entiers, $x <_V y$ est la relation $\sigma(x) < \sigma(y)$ ($<_P$ compare les *positions*, $<_V$ compare les *valeurs*) ;
- les quantificateurs $\exists$, $\forall$ portent uniquement sur des variables (pas sur des ensembles de variables !).

Exemples de propriétés du premier ordre :

- σ contient une sous-suite croissante de longueur 3 :
$$\exists x, y, z : (x <_P y <_P z) \wedge (x <_V y <_V z). \tag{1}$$
- σ contient une « adjacence » (i tel que $\sigma(i+1) = \sigma(i) + 1$) :
$$\exists x, y : (x <_P y) \wedge (x <_V y) \wedge \big(\neg \exists z : (x <_P z <_P y)\big) \wedge \big(\neg \exists t : (x <_V t <_V y)\big). \tag{2}$$
- « σ est de taille paire » ou « σ a un point fixe » ne sont pas des propriétés du premier ordre (voir exercice 4.1).

On peut maintenant introduire la notion de *loi de convergence*, centrale dans ce cours.

Definition 1.1. Un suite de permutations aléatoires σ_n satisfait une loi de convergence si, pour toute propriété φ du premier ordre, la limite $\lim \mathbb{P}[\sigma_n \models \varphi]$ existe.

Variante : à la place des relations $<_P$, $<_V$, on pourrait utiliser la relation R définie par $xRy \Leftrightarrow \sigma(x) = y$. Cela donnerait un autre ensemble de propriétés du premier ordre, (par exemple « σ contient un point fixe » est facilement exprimable dans ce cadre : $\exists x : xRx$), et donc une autre notion de loi de convergence. Il existe des résultats dans ce cadre, mais je ne les discuterai pas dans ce cours.

1.2 Quelques résultats

Résultat "classique" sur le graphe aléatoire d'Erdős-Rényi $G(n,p)$ (n sommets, chaque paire est connectée par une arête avec probabilité p, indépendamment les unes des autres) :

Theorème 1.2. *Soit $p = cn^{-\alpha}$, $c > 0$, $\alpha \in [0,1]$. Alors*

- *Si $\alpha = 0$ (et $c < 1$), alors $G(n,p)$ satisfait une loi du 0-1 (i.e. une loi de convergence, et l'ensemble des limites possibles est $\{0,1\}$) [Glebskii–Kogan–Liagonskii–Talanov '69/Fagin '76] ;*
- *Si $\alpha = 1$, alors $G(n,p)$ satisfait une loi de convergence [Lynch, '92] ;*
- *Si $\alpha \in]0,1[\setminus \mathbb{Q}$, alors $G(n,p)$ satisfait une loi du 0-1 [Shelah–Spencer '88] ;*
- *Si $\alpha \in]0,1[\cap \mathbb{Q}$, alors $G(n,p)$ ne satisfait pas de loi de convergence [Shelah–Spencer '88].*

Pour les permutations de Mallows :

Theorème 1.3 (Foy-Woods, '90 pour le cas uniforme/ Müller–Skerman–Verstraaten, arXiv Fév. '23, pour q général)**.** *Soit $\sigma_{n,q}$ une permutation aléatoire de Mallows de taille n et paramètre q.*

- *Pour q fixe, $q \neq 1$, $\sigma_{n,q}$ satisfait une loi de convergence.*
- *Si $q = q(n)$ vérifie $1 - \frac{1}{\log^*(n)} \leq q \leq 1 + \frac{1}{\log^*(n)}$, alors $\sigma_{n,q}$ ne satisfait pas de loi de convergence.*

Pour les permutations évitant des motifs :

Theorème 1.4. — *Si $\sigma_n \in_u \mathrm{Av}_n(231, 312)$ (« permutations en couches »), alors σ_n satisfait une loi de convergence (Braunfeld, Kukla '22).*

- *Si $\sigma_n \in_u \mathrm{Av}_n(231)$, alors σ_n satisfait une loi de convergence (Albert–Bouvel–F.–Noy, arXiv Oct. '22).*

Il reste beaucoup à faire...

But du cours : expliquer les idées derrière la loi de convergence pour $\mathrm{Av}_n(231)$ (qui utilise de la combinatoire analytique et le théorème de Drmota–Lalley–Woods) et la non-convergence pour σ_n uniforme (méthode d'« arithmétisation » de Shelah et Spencer).

2 Loi de convergence pour $\mathrm{Av}(231)$

Cette partie est basée sur le preprint
Albert–Bouvel–F.–Noy, Convergence law for 231-avoiding permutations, arXiv Oct. '22,
qui s'inspire d'un article de Woods ('97) établissant une loi de convergence pour les arbres planaires enracinées uniformes à n sommets.

2.1 Préliminaire 1 : jeu d'Erhenfeucht Fraïssé

Definition 2.1. Si φ est une formule logique du premier ordre, on appelle *profondeur de quantificateur* (ou simplement *profondeur*) de φ, et on note $\mathrm{qd}(\varphi)$, le nombre maximal de quantificateurs imbriqués dans φ.

Par exemple, les formules (1) et (2) ont toutes les deux profondeur 3.
Par ailleurs, on note $\equiv_k$ la relation d'équivalence

$$\sigma \equiv_k \tau \;\Leftrightarrow\; \begin{array}{l}\sigma \text{ et } \tau \text{ satisfont les mêmes formules logiques} \\ \text{du premier ordre de profondeur} \leq k.\end{array}$$

Jeu d'Erhenfeucht-Fraïssé
La relation $\equiv_k$ a une interprétation très utile en terme de jeu combinatoire. Soit σ et τ deux permutations. Le jeu $\mathrm{EF}(\sigma, \tau; k)$ d'Erhenfeucht–Fraïssé est le jeu suivant :

- il y a deux joueurs Spoiler et Duplicator, le plateau de jeu est consitué des deux permutations σ et τ (vu comme des ensembles de points avec deux ordres totaux $(<_P^\sigma, <_V^\sigma)$ et $(<_P^\tau, <_V^\tau)$), et on joue k tours ;
- à chaque tour Spoiler commence et choisit un élément s_i dans σ **ou** t_i dans τ ;

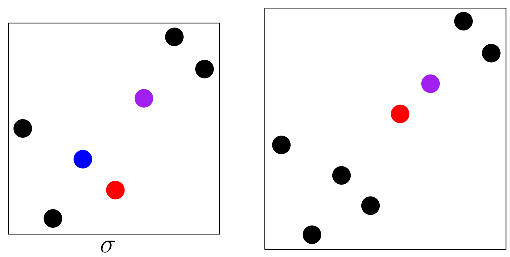
— Ensuite Duplicator choisit un élément dans l'autre permutation (s_i dans σ si Spoiler a choisi t_i dans τ, ou t_i dans τ si Spoiler a choisi s_i dans σ) ;

— A la fin des k tours, Duplicator gagne si, pour tout $i, j \leq k$, on a

$$s_i <_P^\sigma s_j \;\Leftrightarrow\; t_i <_P^\sigma t_j \text{ et } s_i <_V^\sigma s_j \;\Leftrightarrow\; t_i <_V^\sigma t_j.$$

Sinon, Spoiler a gagné.

Exemple : on joue en 3 tours sur les deux permutations suivantes.



σ τ

Spoiler a une stratégie gagnante, qui exploite le fait que τ contient une adjacence, mais pas σ. En effet, Spoiler joue à ses deux premiers coups les points de τ formant l'adjacence (points rouge et violet à droite, peu importe dans quel ordre). Duplicator doit alors jouer deux points en position croissante, par exemple les points rouge et violet de gauche. Comme il n'y a pas d'adjacence dans σ, il ne peut pas les choisir à la fois consécutifs en position et en valeur. Dans notre exemple, ils ne sont pas consécutifs en valeur. Spoiler joue alors un point intermédiaire en valeur dans σ, par exemple le point bleu. Il n'y a pas de point intermédiaire en valeur dans τ entre les points rouges et violet, et Duplicator a perdu la partie.

Dans cet exemple, on a vu que l'existence d'une formule φ de profondeur 3 telle que $\sigma \not\models \varphi$ mais $\tau \models \varphi$ (rappelons que la formule logique (2),est une formule de profondeur 3 exprimant l'existence d'une adjacence) induit une stratégie gagnante pour Spoiler. Plus généralement, on peut montrer :

Theorème 2.2 (Fraïssé '54 – Ehrenfeucht '61)**.** Duplicator *a une stratégie gagnante pour le jeu* EF$(\sigma, \tau; k)$ *si et seulement si* $\sigma \equiv_k \tau$.

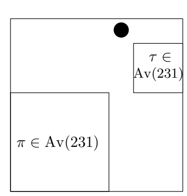
Une conséquence (pas totalement immédiate, mais importante pour nous) est que, quelque soit k *fixé*, il y a un nombre fini de classes d'équivalences pour $\equiv_k$. Ce théorème peut par ailleurs être utilisé pour montrer que certaines propriétés ne peuvent **pas** être représentées par une formule logique du premier ordre, voir l'exercice 4.1.

2.2 Préliminaire 2 : structure et énumération des permutations évitant 231

Definition 2.3. Une permutation σ contient le motif 231 s'il existe x, y, z tels que

$$x <_P y <_P z \text{ et } z <_V x <_V y.$$

Résultat classique. Une permutation σ non vide dans Av(231) se décompose de manière unique sous la forme suivante :

$H(\pi, \tau) :=$  .

σ

(Convention : Av(231) contient la permutation vide à 0 éléments.)

Conséquence : si $C(z)=\sum_{n\ge 0} c_n z^n$ est la série génératrice (ordinaire) de Av(231), on a

$$C(z) = 1 + z\,C(z)^2, \text{ et donc } C(z) = \frac{1-\sqrt{1-4z}}{2z}.$$

Donc $[z^n]C(z) = \mathrm{Cat}_n := \frac{1}{n+1}\binom{2n}{n}$ est le n-ième nombre de Catalan. Asymptotiquement, on a $c_n \sim \frac{4^n}{n^{3/2}\sqrt{\pi}}$.

2.3 Système raffiné

Lemme 2.4. *Soit $k \ge 1$. Si $\pi \equiv_k \pi'$ et $\tau \equiv_k \tau'$, alors $H(\pi,\tau) \equiv_k H(\pi',\tau')$.*

Idée de preuve. C'est une conséquence du théorème d'Erhenfeucht–Fraïssé : il est facile de construire une stratégie gagnante du jeu sur $\sigma := H(\pi,\tau)$ et $\sigma' := H(\pi',\tau')$ à partir de stratégies gagnantes sur π et π' d'un côté, et τ et τ' de l'autre. □

Ceci permet de raffiner l'équation $C(z) = 1 + zC(z)^2$ en un système tenant compte du type logique (i.e. de la classe d'équivalence pour $\equiv_k$). Soit $\mathcal{T}_k$ l'ensemble (fini, rappelons-le) des classes d'équivalence pour $\equiv_k$. Comme conséquence du lemme 2.4, l'application H induit une application de $\mathcal{T}_k \times \mathcal{T}_k$ dans $\mathcal{T}_k$, que l'on notera abusivement aussi H. Pour $t \in \mathcal{T}_k$ on note $\mathcal{C}_t$ l'ensemble des permutations de Av(231) de type t et $C_t(z)$ sa série génératrice. L'ensemble $\mathcal{T}_k$ contient un élément particulier $\varnothing$, correspondant au type de la permutation vide, qui est seule dans sa classe. On a alors : pour tout t dans $\mathcal{T}_k$,

$$C_t(z) = \delta_{t,\varnothing} + z \sum_{\substack{u,v \in \mathcal{T}_k \\ H(u,v)=t}} C_u(z)\,C_v(z). \tag{3}$$

C'est un système polynomial d'équations déterminant les série C_t.

2.4 Le théorème de Drmota–Lalley–Woods (d'après Flajolet–Sedgewick, '09)

Supposons que l'on a un système *polynomial non linéaire*

$$y_j = F_j(z; y_1, \dots, y_m), \qquad 0 \le j \le m,$$

où les y_j sont des séries entières en z, vérifiant les propriétés suivantes

positivité les coefficients des F_j sont positifs (ou nuls) ;

bien défini $\approx$ le système a une unique solution $y_j(z) = \sum_{n\ge 0} y_{j,n} z^n$ développable en série entière qui peut être obtenue par itération ;

irréducibilité le graphe de dépendance, ayant une arête $i \to j$ si y_i apparaît dans l'équation définissant y_j (i.e. si $\frac{\partial F_j}{\partial y_i}$), est fortement connexe ;

apériodicité au moins une des séries y_j est apériodique (dans le sens où son support $\{n : [z^n]y_j, \neq 0\}$ n'est pas contenu dans un sous-réseau $b + d\mathbb{Z}$ de $\mathbb{Z}$).

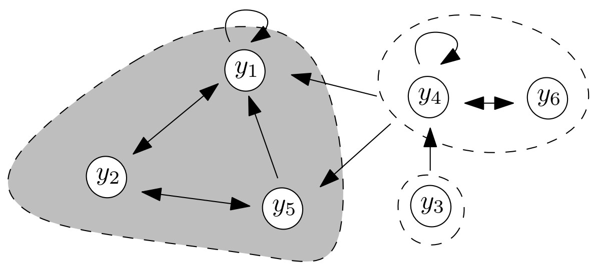
Alors toutes les séries y_j ont le même rayon de convergence $\rho < +\infty$ et, pour tout j, il existe $A_j > 0$ tel que

$$[z^n]y_j \sim A_j \rho^{-n} n^{-3/2}.$$

Pour illustrer la notion de graphe de dépendance, considérons le système

$$y_1 = 1 + zy_1y_4y_5 + zy_2^2; \quad y_2 = zy_1y_5; \quad y_3 = 1;$$
$$y_4 = 1 + zy_4 + z^2y_3y_6; \quad y_5 = z^2y_2^2y_4; \quad y_6 = zy_4^2.$$

Le graphe de dépendance correspondant est le suivant :



Les composantes fortement connexes sont indiquées en pointillé. En particulier, ce système ne vérifie pas l'hypothèse d'irréductibilité ci-dessus.

Remarque importante : le théorème peut être étendu à des systèmes où les F_j ne sont pas polynomiaux, mais holomorphes sur un domaine suffisamment grand (voir Drmota, '09).

2.5 Conclusion

Supposons que l'on puisse appliquer le théorème DLW au système (3).
Alors, pour tout type t, on aurait

$$[z^n]C_t(z) \sim A_t \rho^{-n} n^{-3/2}.$$

Comme $C(z) = \sum_t C_t(z)$, nécessairement $\rho = 1/4$. On aurait alors, pour $\sigma_n \in_u \mathrm{Av}_n(231)$,

$$\mathbb{P}\big(\sigma_n \text{ est de type } t\big) = \frac{[z^n]C_t(z)}{[z^n]C(z)} \to \frac{A_t}{\sqrt{\pi}}.$$

En particulier la limite existerait. Plus généralement, si φ est une propriété logique du premier ordre de profondeur k, il existe un sous-ensemble $\mathcal{T}_\varphi \subseteq \mathcal{T}_k$ tel que

$$\sigma \models \varphi \ \Leftrightarrow \sigma \in \bigcup_{t \in \mathcal{T}_\varphi} \mathcal{C}_t.$$

La quantité

$$\mathbb{P}\big(\sigma_n \models \varphi\big) = \sum_{t \in \mathcal{T}_\varphi} \mathbb{P}\big(\sigma_n \text{ est de type } t\big)$$

aurait donc toujours une limite, ce qui montrerait la loi de convergence pour $\sigma_n \in_u \mathrm{Av}_n(231)$.

Mais on ne peut pas appliquer le théorème DLW au système (3) car l'hypothèse d'irréductibilité n'est pas vérifiée (l'hypothèse d'apériodicité est elle vérifiée, voir ci-dessous). On peut cependant montrer que le graphe de dépendance a une unique composante fortement connexe terminale (en effet, partant de deux points u et v, il existe toujours un point w tel qu'il y ait une arête de u à w et de v à w ; il suffit de prendre $w = H(u, v)$).

On va appliquer le théorème DLW en considérant les séries de cette composante terminale comme des inconnues et les autres comme des paramètres (ce n'est plus un système polynomial, car les séries « non terminales » ne sont pas des polynômes, il faut donc utiliser la version analytique du théorème, et vérifier que les séries « non terminales » ont un rayon de convergence strictement plus grand que 1/4). Pour les détails, voir Albert–Bouvel–F.–Noy, Convergence law for 231-avoiding permutations, arXiv Oct. '22.

Apériodicité : il faut vérifier qu'il y a au moins une série dans la composante fortement connexe terminale. Partons d'une permutation τ d'un type logique *terminal*, et posons $\sigma_0 = \tau$, $\sigma_{i+1} = H(\sigma_i, \varnothing)$. Le type de σ_i ne dépend plus de i à partir d'un certain rang (par un argument utilisant le jeu EF, similaire à celui de l'exercice 4.1). Ceci montre que $\mathcal{T}^*$ contient au moins un type apériodique et vérifie donc l'hypothèse d'apériodicité du théorème DLW.

3 Non-convergence pour les permutations aléatoires uniformes

Soit $\sigma_n \in_u S_n$. Le but de cette section est de construire une formule logique φ du premier ordre « non-convergente », i.e. telle que $\mathbb{P}(\sigma_n \models \varphi)$ ne converge pas quand n tend vers $+\infty$.

Cette partie est basée sur (une partie de) l'article
Müller–Skerman–Verstraaten, Logical limit laws for Mallows random permutations, arXiv Fév. '23
qui adapte au cadre des permutations la méthode d'arithmétisation développée par Shelah et Spencer pour $G(n, n^{-\alpha})$, $\alpha \in \mathbb{Q} \cap]0, 1[$.

3.1 Expressivité de la logique du deuxième ordre

Pour cela, on va utiliser la notion de formule logique du deuxième ordre : on peut maintenant quantifier non seulement sur des variables, mais sur des relations (de n'importe quelle arité) entre variables.

On va voir que cela permet d'exprimer des propriétés arithmétiques fines. Considérons un ensemble A muni d'une relation d'ordre total $<$ (par exemple l'ordre $<_P$ d'une permutation). On identifie les éléments de A avec 1,..., $|A|$. On peut alors exprimer les notions suivantes

— On peut exprimer (en logique du premier ordre) $x = 1$, $y = x + 1$, $x = |A|$, ...

$$y = x + 1 : \ (x < y) \wedge \big(\nexists z : \ x < z < y \big).$$

— On peut définir une relation $D(x, y)$ exprimant $y = 2 * x$;

$$\exists D : \ D(x, y) \Leftrightarrow \Big((x = 1) \wedge (y = 2) \Big) \vee \Big(\exists w, z : \ (x = w + 1) \wedge D(w, z) \wedge (y = z + 2) \Big).$$

— On peut alors exprimer, par exemple, que $|A|$ est pair ;

$$(\exists <, D \ \cdots) \wedge (\exists t : \ D(t, |A|)).$$

— On peut définir une relation $P(x,y)$ exprimant $y = 2^x$;

$$\exists P :\ P(x,y) \Leftrightarrow \Big((x=1) \wedge (y=2)\Big) \vee \Big(\exists w,z :\ (x=w+1) \wedge P(w,z) \wedge D(z,y)\Big).$$

— On peut définir une relation $T(x,y)$ exprimant $y = \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{x \text{ fois}}$;

$$\exists T :\ T(x,y) \Leftrightarrow \Big((x=1) \wedge (y=2)\Big) \vee \Big(\exists w,z :\ (x=w+1) \wedge T(w,z) \wedge P(z,y)\Big).$$

— On peut trouver $\ell = \log^*(|A|)$;

$$\exists \ell :\ \Big(\exists x :\ T(\ell,x)\Big) \wedge \Big(\forall m > \ell,\ \nexists y :\ T(m,y)\Big).$$

— On peut alors exprimer que $\log^*(|A|) \bmod 8 \in \{0,1,2,3\}$;

$$\exists D,P,T,\ell\ \cdots \wedge \Big(\exists x,y,z,t :\ D(x,y) \wedge D(y,z) \wedge D(z,t)\Big) \wedge \Big((\ell=t) \vee (\ell=t+1) \vee (\ell=t+2) \vee (\ell=t+3)\Big).$$

3.2 Émulation des formules du second ordre en logique du premier ordre

Les formules ci-dessus sont clairement non convergentes, mais ce ne sont pas des formules du premier ordre. L'idée est donc de construire, avec des formules du premier ordre, des ensembles et des relations sur ces ensembles, de telle sorte que toutes les relations possibles apparaissent avec probabilité tendant vers 1 (sur des ensembles de taille assez petits). On pourra ainsi remplacer la partie "deuxième ordre" des formules par quelque chose du premier ordre.

3.2.1 Construction d'ensembles

Soit $I = [\![\ell_I, r_I]\!] \subset [n]$ un intervalle. On définit l'ensemble aléatoire

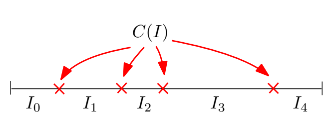
$$C(I) = \Big\{ i \in I : \sigma_n(i), \sigma_n(i)+1, \sigma_n(i)+2 \in \sigma_n(I) \Big\}.$$

Note : l'appartenance à l'ensemble $C(I)$ peut être décrite en logique du premier ordre ! (En particulier, on peut parler d'intervalle en logique du premier ordre, car un intervalle I est déterminé par deux éléments ℓ_I et r_I.)

Lemme 3.1 (Müller–Skerman–Verstraaten, '23, version simplifiée)**.** *Avec probabilité tendant vers* 1*, il existe* I^* *tel que* $\log(\log(n)) \leq |C(I^*)| \leq 2\log(\log(n))$.

Heuristique : Pour I donné, on peut montrer que $\mathbb{E}(|C(I)|) = \Theta(|I|^3 n^{-1})$ et que $|C(I)|$ est asymptotiquement concentré autour de sa moyenne. Pour prouver le lemme, il suffit de choisir un ensemble I^* de taille $(\frac{3}{2}\log(\log(n)))^{1/3} n^{2/3}$, (voir exercice 4.3) □

On considère aussi $S(I) = (I_0, \ldots, I_k)$ les intervalles de $I \setminus C(I)$. C'est sur l'ensemble $S(I)$ que l'on va construire des relations.



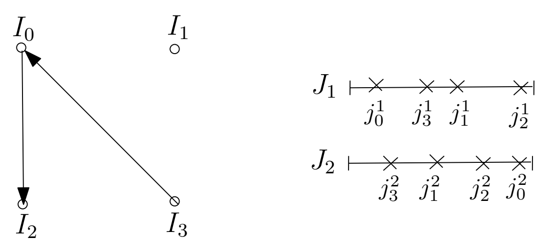
3.2.2 Construction de relations binaires

On va maintenant construire une relation (ou un graphe dirigé) sur $S(I) = (I_0, \dots, I_k)$, en utilisant un autre ensemble $S(J) = (J_1, \dots, J_M)$.

Penser à I, J disjoints de taille $n^{2/3}$.

- Pour tout h, on cherche i minimal dans I_h et j_h^1 dans J_1 tel que $\sigma_n(i) = \sigma_n(j_h) + 1$. Si I_h et J_1 sont de taille $\approx n^{2/3}$, il existe un tel i avec forte probabilité. En gros, cette construction sélectionne pour chaque I_h, un élément j_h^1 uniformément au hasard dans J_1.
- On ordonne les ensembles I_h selon les valeurs de j_h^1, et on trace une arête du minimum vers le maximum. En gros, cette construction trace une arête dirigée uniformément au hasard sur l'ensemble de sommets $S(I)$.
- On recommence avec $(J_2, \dots, J_M)$.

Voici une illustration schématique de cette construction. Dans ce cas, $k+1 = 4$, $M = 2$ (i.e. on a 4 sommets I_0, I_1, I_2 et I_3 et 2 intervalles J_1 et J_2), J_1 induit l'arête dirigée (I_0, I_2) et J_2 induit l'arête dirigée (I_3, I_0).



En général, on obtient un graphe dirigé $G(I, J)$ avec ensemble de sommets $S(I)$ (si une arête est répétée, on oublie la répétition). De manière équivalente, on peut voir ce graphe comme une relation (binaire anti-réflexive) R_J sur $S(I)$.

Note : le fait que I_h soit relié à I_k par R_J s'exprime en logique du premier ordre !

Lemme 3.2 (Müller–Skerman–Verstraaten, '23)**.** *Pour tout $\varepsilon > 0$, avec probabilité tendant vers 1, σ_n vérifie la propriété suivante. Pour tout ensemble I avec $|S(I)| \leq 2\log(\log(n))$ tel que*

$$n^{1/2+\varepsilon} \leq |I_1|, \dots, |I_k| \leq n^{1-\varepsilon} \tag{4}$$

et toute relation (binaire anti-réflexive) R sur $S(I)$, on peut trouver J tel que $R_J = R$.

Heuristique. R_J est une relation aléatoire sur $S(I)$, et les R_J correspondant à différents J sont indépendants. En testant suffisamment de J, on en trouve un tel que $R_J = R$... □

Variante importante : si I et I' vérifie $|S(I)| \leq |S(I')| \leq 2\log(\log(n))$ et

$$n^{1/2+\varepsilon} \leq |I_1|, \dots, |I_k|, |I'_1|, \dots, |I'_k| \leq n^{1-\varepsilon},$$

alors on peut trouver J telle que R_J (construite sur $S(I) \cup S(I')$) soit le graphe d'une injection de $S(I)$ dans $S(I')$ (i.e. tout élément de $S(I)$ est en relation avec exactement un élément de $S(I')$, et tout élément de $S(I')$ est en relation avec au plus un élément de $S(I)$).

Dans ce cas on écrit $|S(I)| \leq_{\text{CERT}} |S(I')|$ (c'est une formule logique du premier ordre !).

3.3 Les formules ARITH et PSEUDOMAX

On définit les formules logiques du *premier ordre* (avec des variables libres) suivantes :

— $\mathrm{ARITH}(\ell_I, r_I)$ ($S(I)$ est « arithmétisable ») :

$\exists$ intervalles J_D, J_P, J_T tels que $R_{J_D}, R_{J_P}, R_{J_T}$ correspondent aux relations D,P,T sur $S(I)$.

— $\mathrm{PSEUDOMAX}(\ell_I, r_I)$ (pas d'ensemble $S(H)$ arithmétisable et certifié plus grand) :

$$\forall H \ (|S(H)| \geq_{\mathrm{CERT}} |S(I)|) \Rightarrow (\neg\, \mathrm{ARITH}(\ell_H, r_H)).$$

Heuristique 3.3 (en oubliant la condition (4) dans le lemme 3.2)**.** *Avec probabilité tendant vers* 1*,*

— *tous les I tels que $|S(I)| \leq 2\log(\log(n))$ vérifie* ARITH*, en particulier le I^* du lemme 3.1 ;*

— *tous les I pseudo-maximaux vérifient*

$$|S(I)| \geq |S(I^*)| \geq \log(\log(n)).$$

3.4 Heuristique pour la formule non convergente

On considère la formule logique du premier ordre suivant (notons que, quand $\mathrm{ARITH}(\ell_I, r_I)$ est valide, on peut exprimer la condition $\log^*(|S(I)|) \bmod 8 \in \{0,1,2,3\}$ en logique du premier ordre) :

$$\varphi : \exists \ell_I, r_I,\ \mathrm{ARITH}(\ell_I, r_I) \wedge \mathrm{PSEUDOMAX}(\ell_I, r_I) \wedge \Big(\log^*(|S(I)|) \bmod 8 \in \{0,1,2,3\}\Big).$$

En admettant l'heuristique 3.3,

— Soit $n_j \to +\infty$ une suite telle que $\log^*(n_j) \bmod 8 \in \{2,3\}$. Avec probabilité tendant vers 1, tous les I pseudo-maximaux vérifient

$$\log^*(|S(I)|) \in \big\{\log^*(n_j) - 2, \log^*(n_j) - 1, \log^*(n_j)\big\}.$$

Comme il existe avec forte probabilité au moins un I pseudo-maximal, φ est satisfaite. On a

$$\lim_{n_j \to +\infty} \mathbb{P}[\sigma_{n_j} \models \varphi] = 1.$$

— Soit $n_k \to +\infty$ une suite telle que $\log^*(n_k) \bmod 8 \in \{6,7\}$. Avec probabilité tendant vers 1, pour tout I pseudo-maximal,

$$\log^*(|S(I)|) \in \big\{\log^*(n_k) - 2, \log^*(n_k) - 1, \log^*(n_k)\big\},$$

et donc φ n'est pas satisfaite. On a

$$\lim_{n_k \to +\infty} \mathbb{P}[\sigma_{n_k} \models \varphi] = 0.$$

On conclut que $\mathbb{P}[\sigma_n \models \varphi]$ n'admet pas de limite. $\square$

4 Exercices

Exercice 4.1 (Expressivité de la logique du premier ordre, voir Albert–Bouvel–F. '20).

1. Exprimer la propriété $\sigma(1) > \sigma(2)$ en logique du premier ordre ;
2. Une permutation de taille n est dite *simple* s'il n'existe pas d'intervalle I non trivial ($2 \leq |I| \leq n-1$) tel que $\sigma(I)$ soit un intervalle. Exprimer la propriété « σ est simple » en logique du premier ordre.
3. Soit $\omega_n = n\ n-1\ \cdots\ 1$ la permutation décroissante de taille n. Qui de Spoiler et Duplicator a une stratégie gagnante pour le jeu d'Erhenfeucht-Fraïssé à k tours sur (ω_n, ω_{n+1}) ?

   En déduire que la propriété « σ a un point fixe » n'est pas expressible en logique du premier ordre.

Exercice 4.2 (Ensemble des limites possibles dans la loi de convergence pour Av(231)). Soit $\sigma_n \in_u \mathrm{Av}_n(231)$. On écrit $\sigma_n = H(\tau_n, \rho_n)$, où τ_n et ρ_n évitent 231 (leur taille est aléatoire).

1. Soit π une permutation évitant 231. Calculer

$$\lim_{n\to+\infty} \mathbb{P}(\tau_n = \pi) \text{ et } \lim_{n\to+\infty} \mathbb{P}(\rho_n = \pi).$$

2. On admet l'énoncé suivant : tout x dans $[0,1]$ peut s'écrire sous la forme $\sum_{k\geq 0} a_k 4^{-k-1}$ pour une certaine suite $(a_k)_{k\geq 0}$ vérifiant $0 \leq a_k \leq 2\,\mathrm{Cat}_k$. Montrer que l'ensemble

$$\Big\{ \lim_{n\to+\infty} \mathbb{P}(\sigma_n \models \varphi), \varphi \text{ propriété du premier ordre} \Big\}$$

   est dense dans $[0,1]$.

Exercice 4.3 (Un petit lemme sur les permutations aléatoires uniformes, Lemme 3.1). Soit σ_n une permutation aléatoire dans S_n. On appelle I^* l'intervalle $[\![1,k]\!]$ ($k \leq n$) et on pose

$$X_{n,k} = \#\big\{ j : j, j+1, j+2 \in \sigma_n(I^*) \big\}.$$

1. En supposant $n^{2/3} \ll k \ll n$, calculer asymptotiquement $\mathbb{E}(X_{n,k})$ et $\mathrm{Var}(X_{n,k})$;
2. Montrer que si on choisit $k = \big\lfloor (\frac{3}{2}\log(\log(n)))^{1/3} n^{2/3} \big\rfloor$, alors

$$\lim_{n\to+\infty} \mathbb{P}\Big[\log(\log(n)) \leq X_{n,k} \leq 2\log(\log(n)) \Big] = 1.$$

Références (par thème)

Théorie des modèles (jeu d'Erhenfeucht-Fraïssé)

[EF99] H.-D. Ebbinghaus and J. Flum. *Finite model theory.* Springer monographs in mathematics. Springer, 1999. 2nd ed.

Expressivité de la logique du premier ordre sur les permutations

[ABF20] M. Albert, M. Bouvel, and V. Féray. Two first-order logics of permutations. *J. Comb. Theory, Ser. A*, 171 :46, 2020. Id/No 105158.

Combinatoire analytique (théorème de Drmota-Lalley-Woods)

[Drm09] M. Drmota. *Random trees : an interplay between combinatorics and probability.* Springer, 2009.

[FS09] P. Flajolet and R. Sedgewick. *Analytic Combinatorics.* Cambridge University Press, 2009.

[Woo97] A. Woods. Coloring rules for finite trees, and probabilities of monadic second order sentences. *Random Struct. Alg.*, 10(4) :453–485, 1997.

Loi de 0-1, convergence ou non-convergence pour les graphes et arbres aléatoires

[Fag76] R. Fagin. Probabilities on finite models. *J. Symb. Log.*, 41 :50–58, 1976.

[GKLT69] Y. V. Glebskij, D. I. Kogan, M. I. Liogon'kij, and V. A. Talanov. Umfang und Anteil der Erfüllbarkeit von Formeln des engeren Prädikatenkalküls. *Kibernetika*, 1969(2) :17–27, 1969.

[Lyn92] J. F. Lynch. Probabilities of sentences about very sparse random graphs. *Random Struct. Algorithms*, 3(1) :33–53, 1992.

[SS88] S. Shelah and J. Spencer. Zero-one laws for sparse random graphs. *J. Am. Math. Soc.*, 1(1) :97–115, 1988.

[Woo97] A. Woods. Coloring rules for finite trees, and probabilities of monadic second order sentences. *Random Struct. Alg.*, 10(4) :453–485, 1997.

Loi de convergence ou non-convergence pour les permutations aléatoires

[ABFN22] M. Albert, M. Bouvel, V. Féray, and M. Noy. Convergence law for 231-avoiding permutations, 2022. preprint arXiv :2210.05537.

[BK22] S. Braunfeld and M. Kukla. Logical limit laws for layered permutations and related structures. *Enum. Combin. Appl.*, 2(4) :Article #S4PP2, 2022.

[FW90] J. Foy and A. Woods. Probabilities of sentences about two linear orderings. In *Feasible mathematics. A Mathematical Sciences Institute Workshop, Ithaca, NY, June 1989. Proceedings*, pages 181–193. Boston etc. : Birkhäuser, 1990.

[MSV23] T. Müller, F. Skerman, and T. W. Verstraaten. Logical limit laws for Mallows random permutations, 2023. preprint arXiv :2302.10148.