Construction d'une formule non convergente

Valentin Féray
(following Shelah–Spencer '88
and Müller–Skerman–Verstraaten '23)

CNRS, Institut Élie Cartan de Lorraine (IECL)

Journées ALEA 2023
13-17 mars 2023

Expressivité de la logique du second ordre sur $(A,<)$

Considérons un ensemble A muni d'un ordre total $<$. On identifie les éléments de A avec $1,\dots,|A|$.

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

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

Expressivité de la logique du second ordre sur $(A,<)$

Considérons un ensemble A muni d'un ordre total $<$. On identifie les éléments de A avec $1, \dots, |A|$.

- 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 $y = 2 * x$;

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

Expressivité de la logique du second ordre sur $(A, <)$

Considérons un ensemble A muni d'un ordre total $<$. On identifie les éléments de A avec $1, \dots, |A|$.

- 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;

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

Expressivité de la logique du second ordre sur $(A,<)$ (suite)

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

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

Expressivité de la logique du second ordre sur $(A,<)$ (suite)

- 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 $y=\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{x \text{ fois}}$;

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

Expressivité de la logique du second ordre sur $(A,<)$ (suite)

- 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 $\ell = \log^*(|A|)$;

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

Expressivité de la logique du second ordre sur $(A,<)$ (suite)

- 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 $\log^*(|A|) \bmod 8 \in \{0,1,2,3\}$;

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

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!

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!

Lemma (Müller–Skerman–Verstraaten, '23, version simplifiée)

Avec probabilité tendant vers 1, *il existe* I^* *tel que* $\log(\log(n)) \le |C(I^*)| \le 2\log(\log(n))$.

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!

Lemma (Müller–Skerman–Verstraaten, '23, version simplifiée)

Avec probabilité tendant vers 1*, il existe* I^* *tel que* $\log(\log(n)) \le |C(I^*)| \le 2\log(\log(n))$*.*

Heuristique: Pour I donné, $\mathbb{E}(|C(I)|) = \Theta(|I|^3 n^{-2})$ et $|C(I)|$ est concentré autour de sa moyenne si $\mathbb{E}(|C(I)|) \to +\infty$. En prenant I^* de taille $(\frac{3}{2}\log(\log(n)))^{1/3} n^{2/3}$, cela prouve le lemme ! $\square$

Construction d'ensembles

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

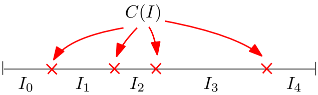
$$C(I) = \Big\{ i \in I : \sigma_n(i), \sigma_n(i)+1, \sigma_n(i)+2 \in \sigma_n(I) \Big\}.$$

Note : l'appartenance à l'ensemble $C(I)$ peut être décrite en logique du premier ordre!

Lemma (Müller–Skerman–Verstraaten, '23, version simplifiée)

Avec probabilité tendant vers 1*, il existe* I^* *tel que* $\log(\log(n)) \le |C(I^*)| \le 2\log(\log(n))$.

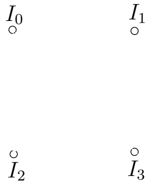
On considère aussi $S(I) = (I_0, \dots, I_k)$ les intervalles de $I \setminus C(I)$.



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 $S(J) = (J_1, \dots, J_M)$.

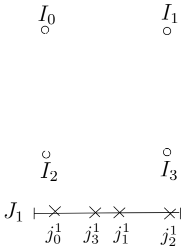
Penser à tous les I_h, J_m disjoints de taille $\approx n^{2/3}$.



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 tous les I_h, J_m disjoints de taille $\approx n^{2/3}$.

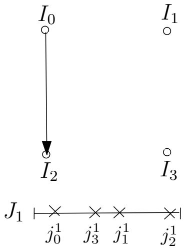
- Pour tout h, on cherche i dans I_h et j_h^1 dans J_1 tel que $\sigma_n(i) = \sigma_n(j_h^1) + 1$, tel que i soit minimal. En gros cela sélectionne pour chaque I_h, un élément j_h^1 uniformément au hasard dans J_1.



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 tous les I_h, J_m disjoints de taille $\approx n^{2/3}$.

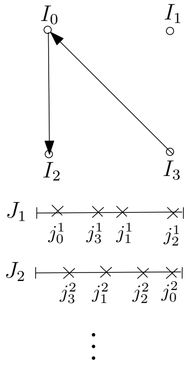
- Pour tout h, on cherche i dans I_h et j_h^1 dans J_1 tel que $\sigma_n(i) = \sigma_n(j_h^1) + 1$, tel que i soit minimal. En gros cela sélectionne pour chaque I_h, un élément j_h^1 uniformément au hasard dans J_1.
- On ordonne les ensembles I_h selon les valeurs de j_h^1, et on trace une arête du minimum vers le maximum. En gros, cela trace une arête dirigée uniformément au hasard dans l'ensemble de sommets $S(I)$.



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 tous les I_h, J_m disjoints de taille $\approx n^{2/3}$.

- Pour tout h, on cherche i dans I_h et j_h^1 dans J_1 tel que $\sigma_n(i) = \sigma_n(j_h^1) + 1$, tel que i soit minimal. En gros cela 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, cela trace une arête dirigée uniformément au hasard dans l'ensemble de sommets $S(I)$.
- On recommence avec $(J_2, \dots, J_M)$.



Construction de relation binaire

On obtient un graphe dirigé $G(I, J)$ avec ensemble de sommets $S(I)$, ou de manière équivalente une relation R_J sur $S(I)$.

Note : R_J est exprimable en logique du premier ordre.

Construction de relation binaire

On obtient un graphe dirigé $G(I,J)$ avec ensemble de sommets $S(I)$, ou de manière équivalente une relation R_J sur $S(I)$.

Note : R_J est exprimable en logique du premier ordre.

Lemma (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

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

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

Heuristique : R_J est une relation aléatoire sur $S(I)$. En testant suffisamment de J, on en trouve un tel que $R_J = R$...

Construction de relation binaire

On obtient un graphe dirigé $G(I,J)$ avec ensemble de sommets $S(I)$, ou de manière équivalente une relation R_J sur $S(I)$.

Note : R_J est exprimable en logique du premier ordre.

Lemma (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

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

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

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

Construction de relation binaire

On obtient un graphe dirigé $G(I,J)$ avec ensemble de sommets $S(I)$, ou de manière équivalente une relation R_J sur $S(I)$.

Note : R_J est exprimable en logique du premier ordre.

Lemma (Müller–Skerman–Verstraaten, '23)

Pour tout $\varepsilon > 0$, avec probabilité tendant vers 1, σ_n vérifie la propriété suivante. Pour tout ensemble I avec $|S(I)| \le 2\log(\log(n))$ tel que

$$n^{1/2+\varepsilon} \le |I_1|, \ldots, |I_k| \le n^{1-\varepsilon},$$

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

Variante : si I et I' vérifie $|S(I)| \le |S(I')| \le 2\log(\log(n))$, 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 $S(I')$.

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

Les formules ARITH et PSEUDOMAX

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

- ARITH(ℓ_I, r_I) (l'ensemble $S(I)$ est "arithmétisable"):

  $\exists$ intervalles J_D, J_P, J_T tels que

  $$R_{J_D}, R_{J_P}, R_{J_T} \text{ définissent les relations } D, P, T \text{ sur } S(I).$$

Les formules ARITH et PSEUDOMAX

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

- $\mathrm{ARITH}(\ell_I, r_I)$ (l'ensemble $S(I)$ est "arithmétisable"):

  $\exists$ intervalles J_D, J_P, J_T tels que

  $$R_{J_D}, R_{J_P}, R_{J_T} \text{ définissent les relations } D, P, T \text{ sur } S(I).$$

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

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

Les formules ARITH et PSEUDOMAX

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

- ARITH(ℓ_I, r_I) (l'ensemble $S(I)$ est "arithmétisable"):

  $\exists$ intervalles J_D, J_P, J_T tels que

  $$R_{J_D}, R_{J_P}, R_{J_T} \text{ définissent les relations } D, P, T \text{ sur } S(I).$$

- PSEUDOMAX(ℓ_I, r_I) (pas d'ensemble $S(H)$ arithmétisable et certifié plus grand):

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

Heuristique (en oubliant les conditions en gris) : avec forte probabilité,

- tous les I tels que $|S(I)| \leq 2\log(\log(n))$ vérifie ARITH, en particulier le I^* du premier lemme.
- tous les I pseudo-maximaux vérifient

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

Heuristique pour la formule non convergente

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

Heuristique pour la formule non convergente

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

- 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
$$\log^*(|S(I)|) \in \{\log^*(n_j) - 2, \log^*(n_j) - 1, \log^*(n_j)\}.$$
Comme il existe avec forte probabilité au moins un I pseudo-maximal, φ est satisfaite. On a
$$\lim_{n_j \to +\infty} \mathbb{P}[\sigma_{n_j} \models \varphi] = 1.$$

Heuristique pour la formule non convergente

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

- 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
$$\log^*(|S(I)|) \in \{\log^*(n_j) - 2, \log^*(n_j) - 1, \log^*(n_j)\}.$$
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,
$$\log^*(|S(I)|) \in \{\log^*(n_k) - 2, \log^*(n_k) - 1, \log^*(n_k)\},$$
et donc φ n'est pas satisfaite. On a
$$\lim_{n_k \to +\infty} \mathbb{P}[\sigma_{n_k} \models \varphi] = 0. \quad \square$$