Logique à deux variables et Circuits booléens

Charles Paperman

LIAFA
Université Paris Diderot

FRec 2013

Introduction

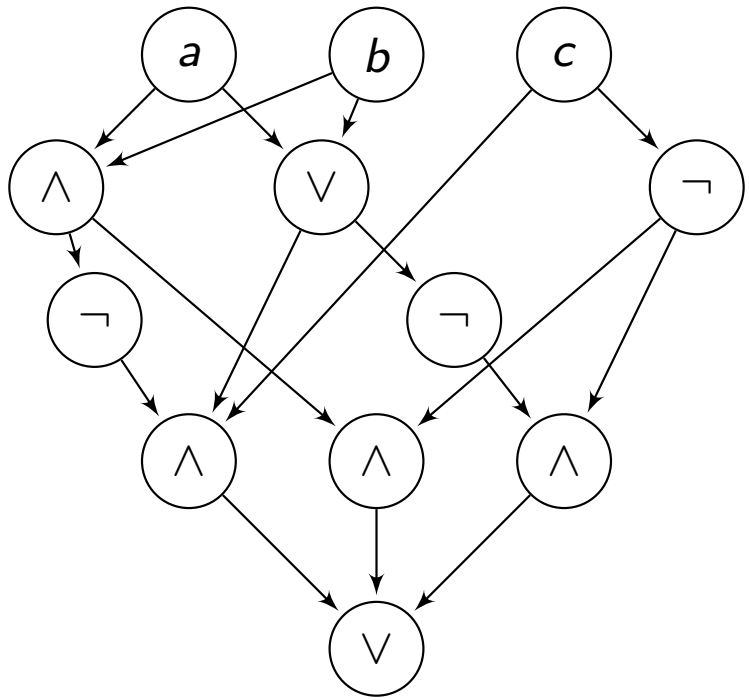
Plan:

1. Circuits booléens et complexité

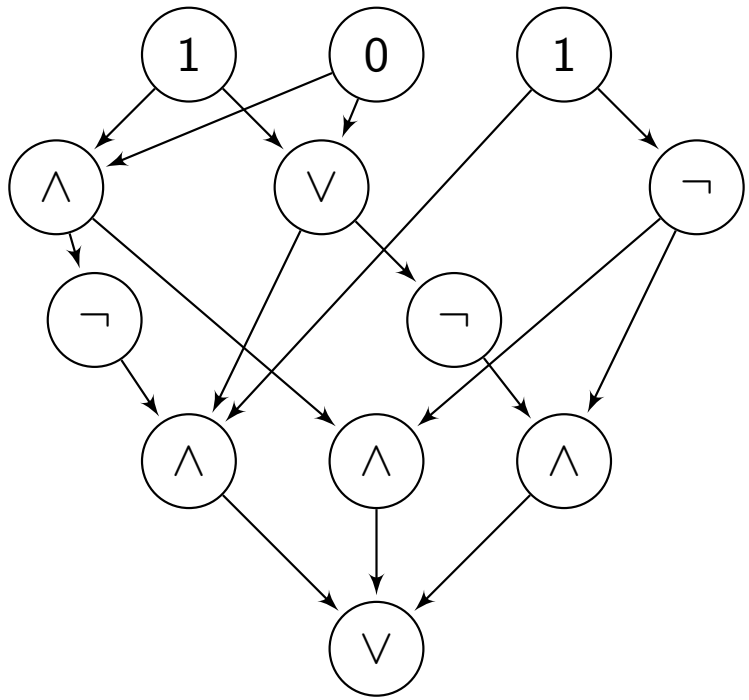
2. Logique du premier ordre.

3. Un Théorème *à la Crane Beach*

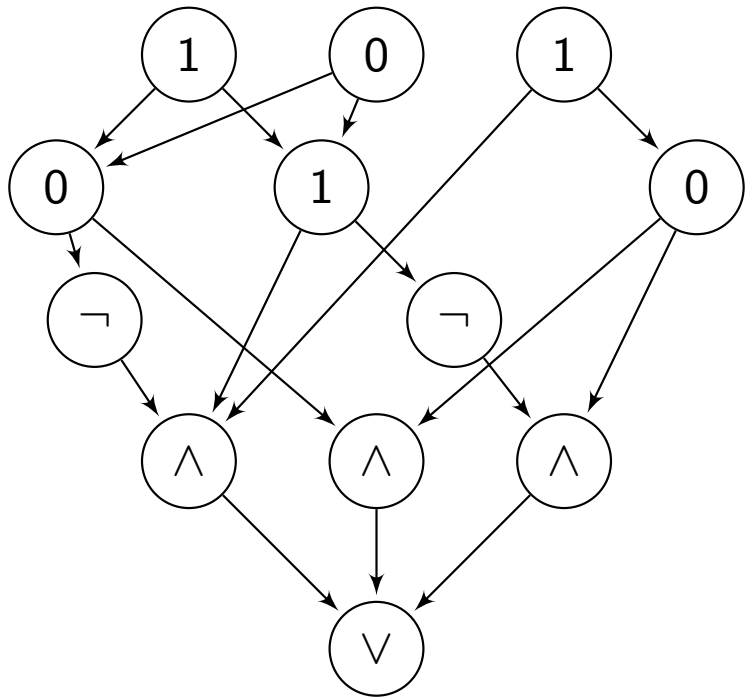
Un exemple de circuit



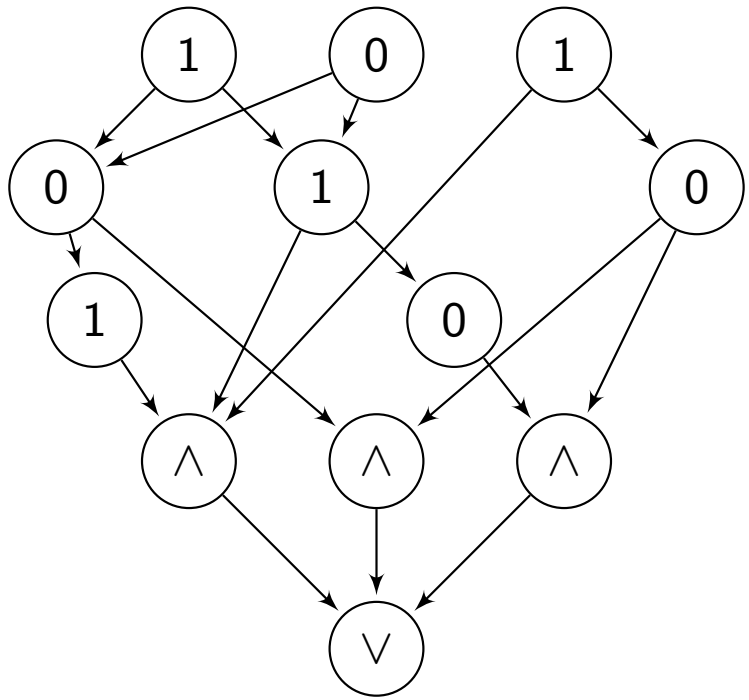
Un exemple de circuit



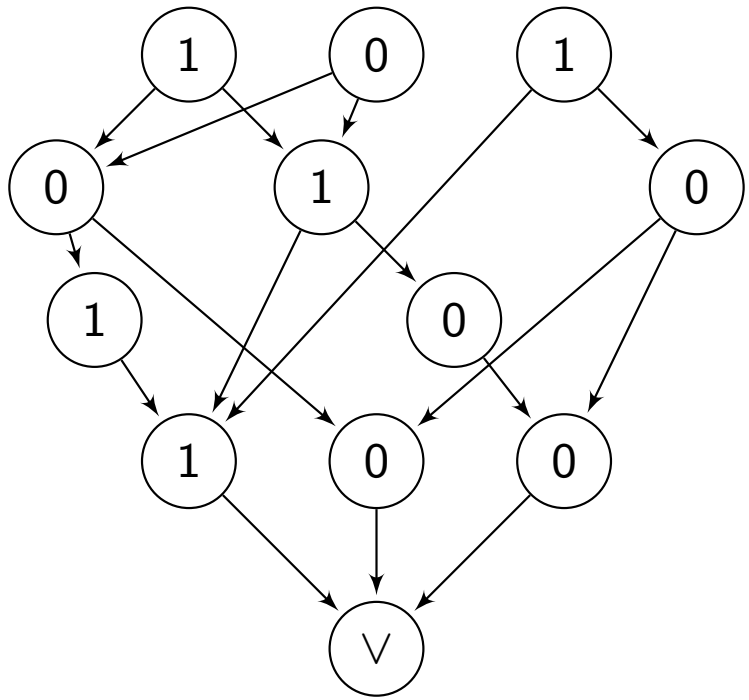
Un exemple de circuit



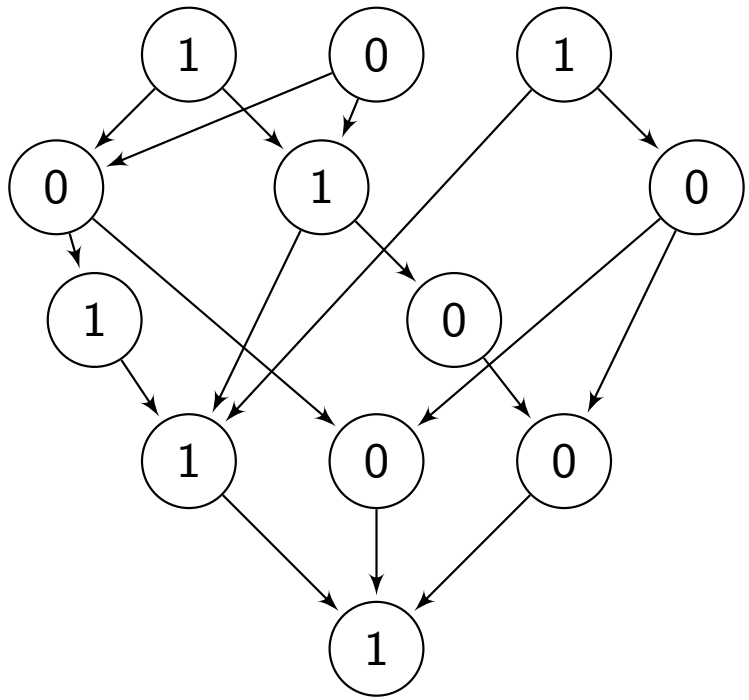
Un exemple de circuit



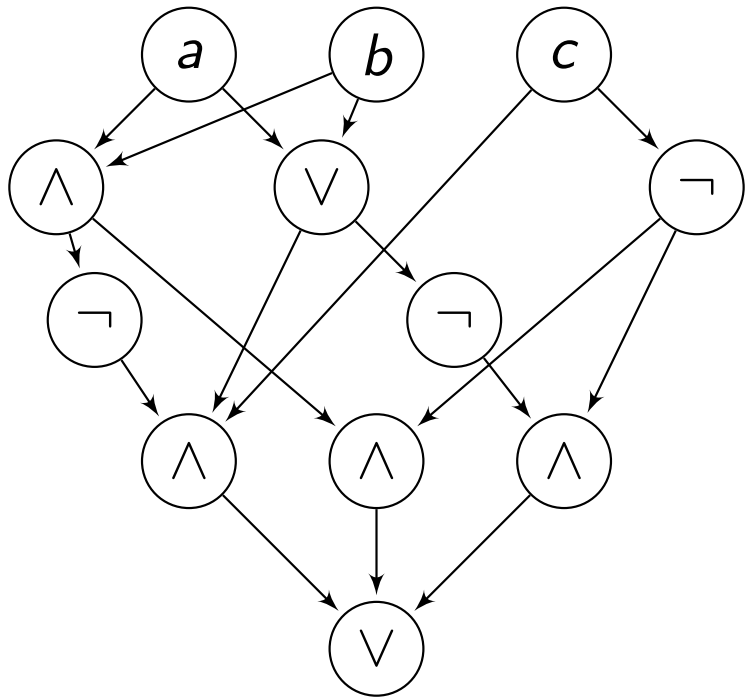
Un exemple de circuit



Un exemple de circuit

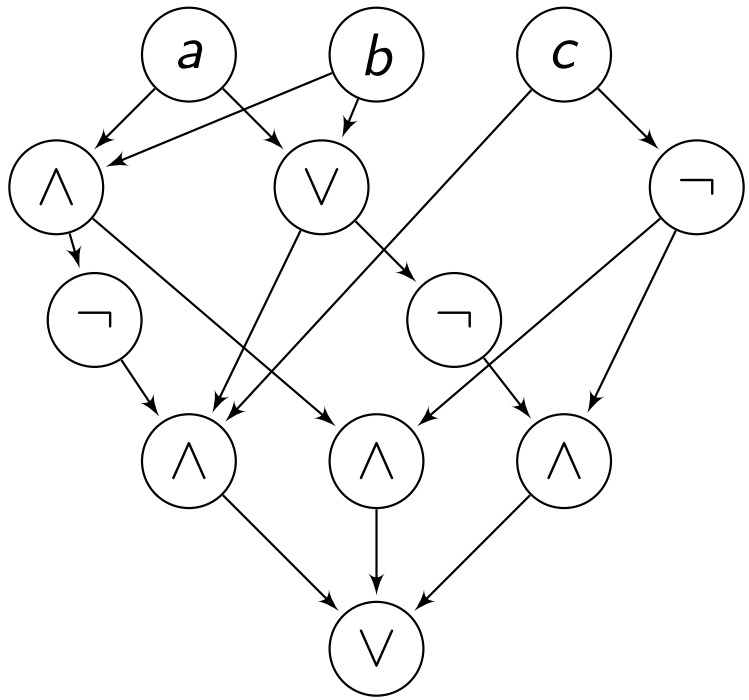


Un exemple de circuit



Mots acceptés : abc de $\{0,1\}^3$ tels que $a \oplus b = c$.

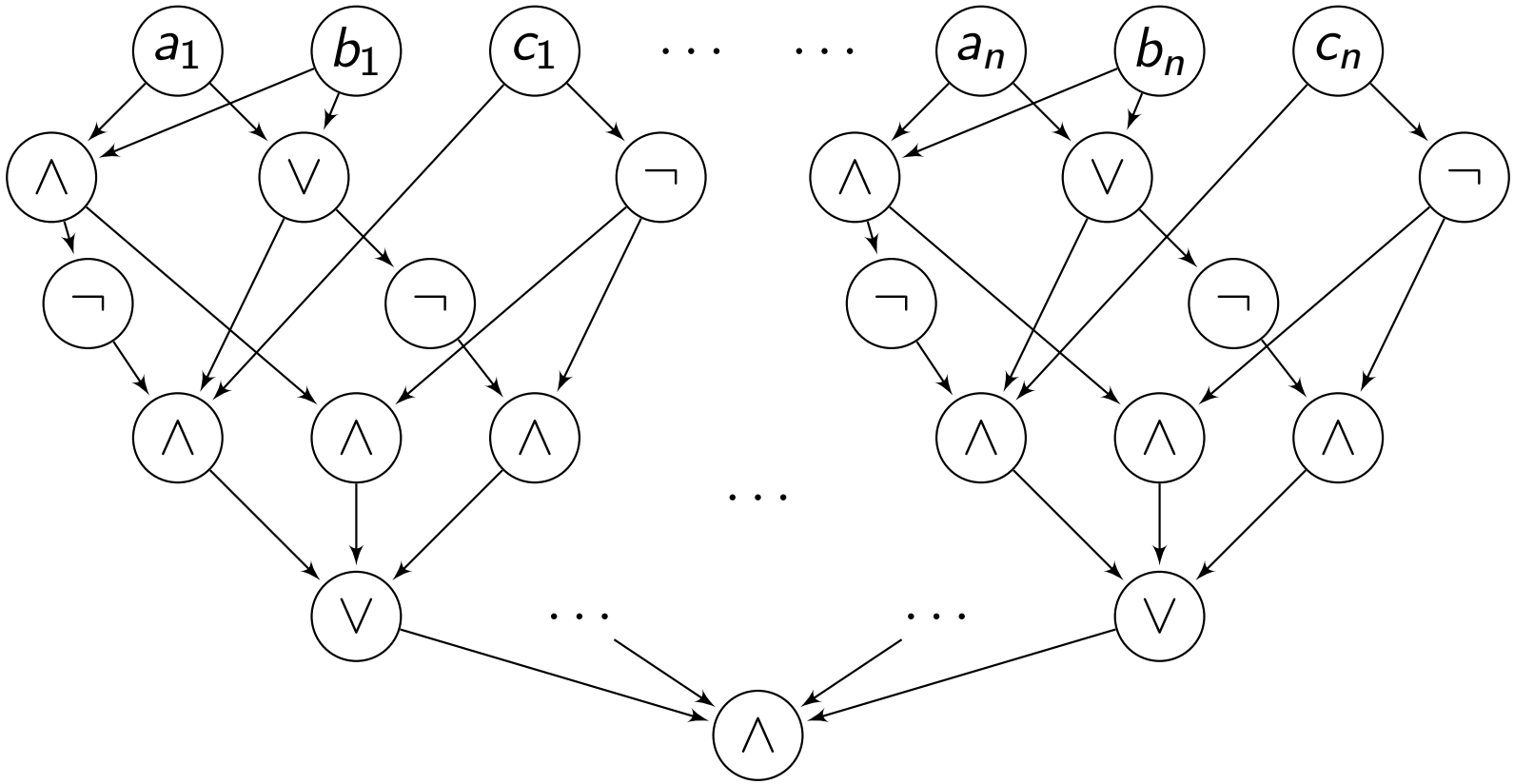
Un exemple de circuit



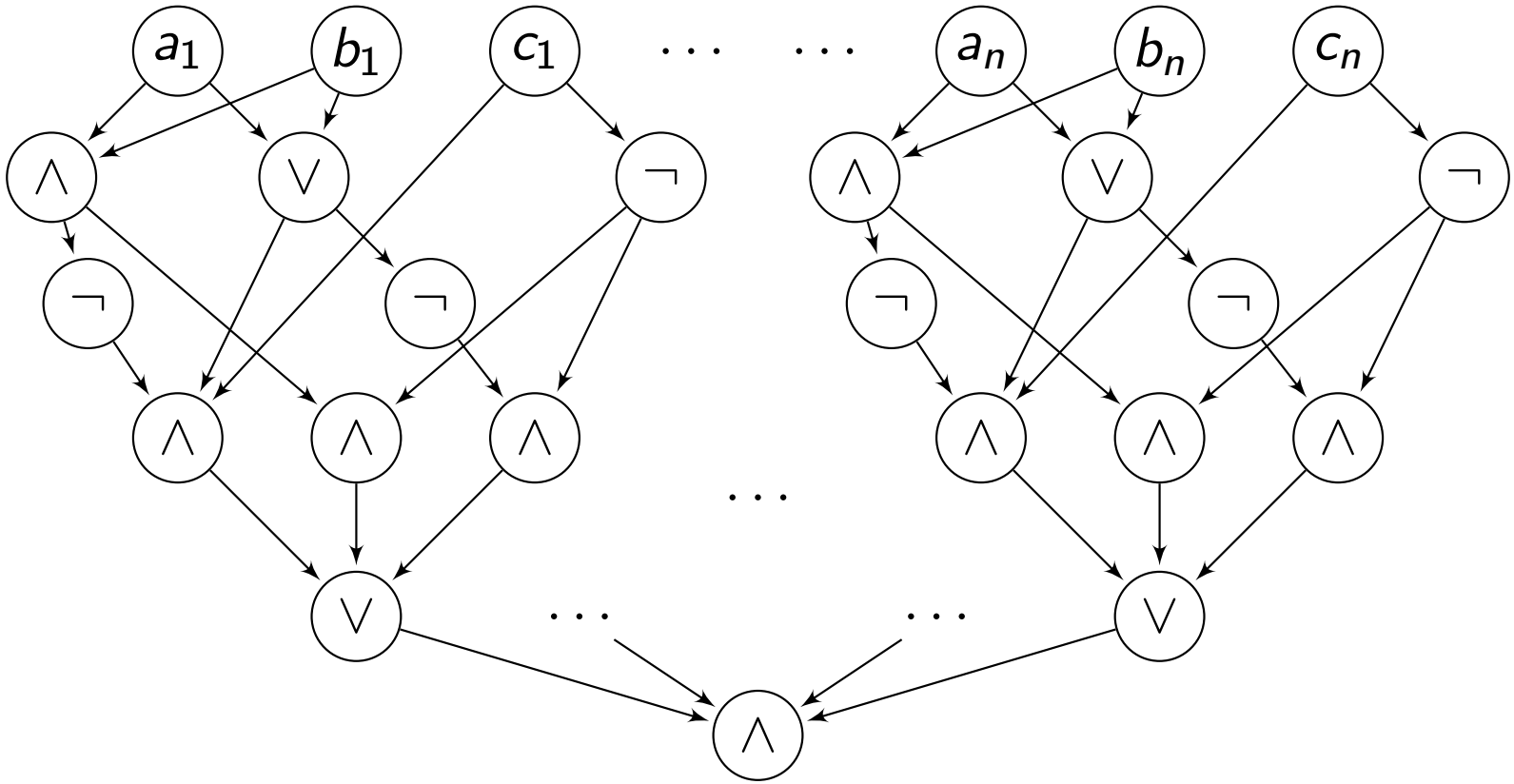
Mots acceptés : abc de $\{0,1\}^3$ tels que $a \oplus b = c$.

Paramètres : profondeur 5, taille 8, arité 3.

Un exemple de famille de circuits



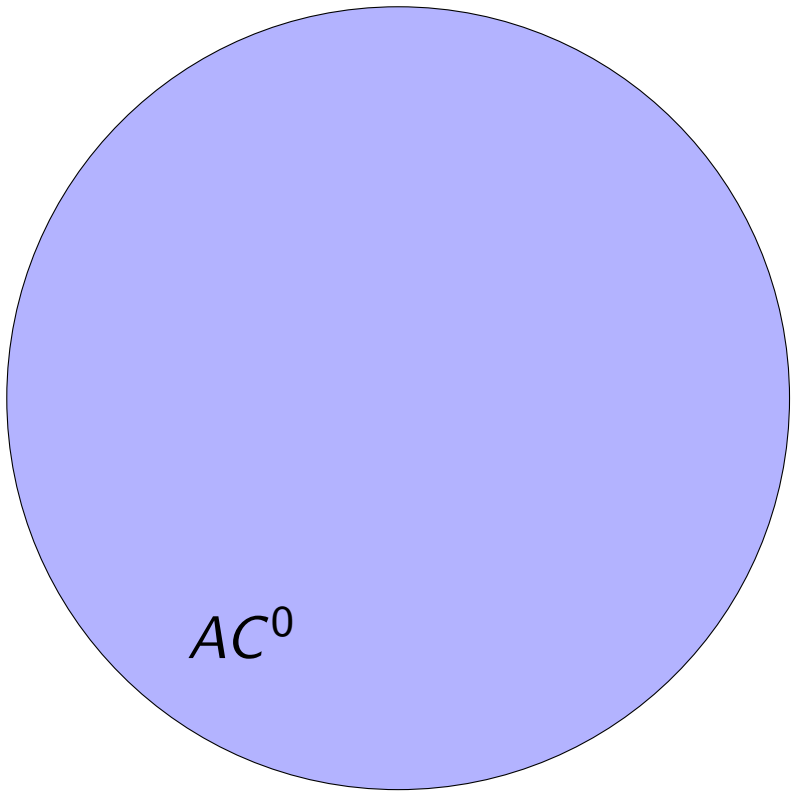
Un exemple de famille de circuits



Mots acceptés : $a_1 b_1 c_1 \cdots a_n b_n c_n$ de $\{0,1\}^{3n}$ tels que $a_i \oplus b_i = c_i$.

Paramètres : profondeur 6, taille $9n + 1$, arité n.

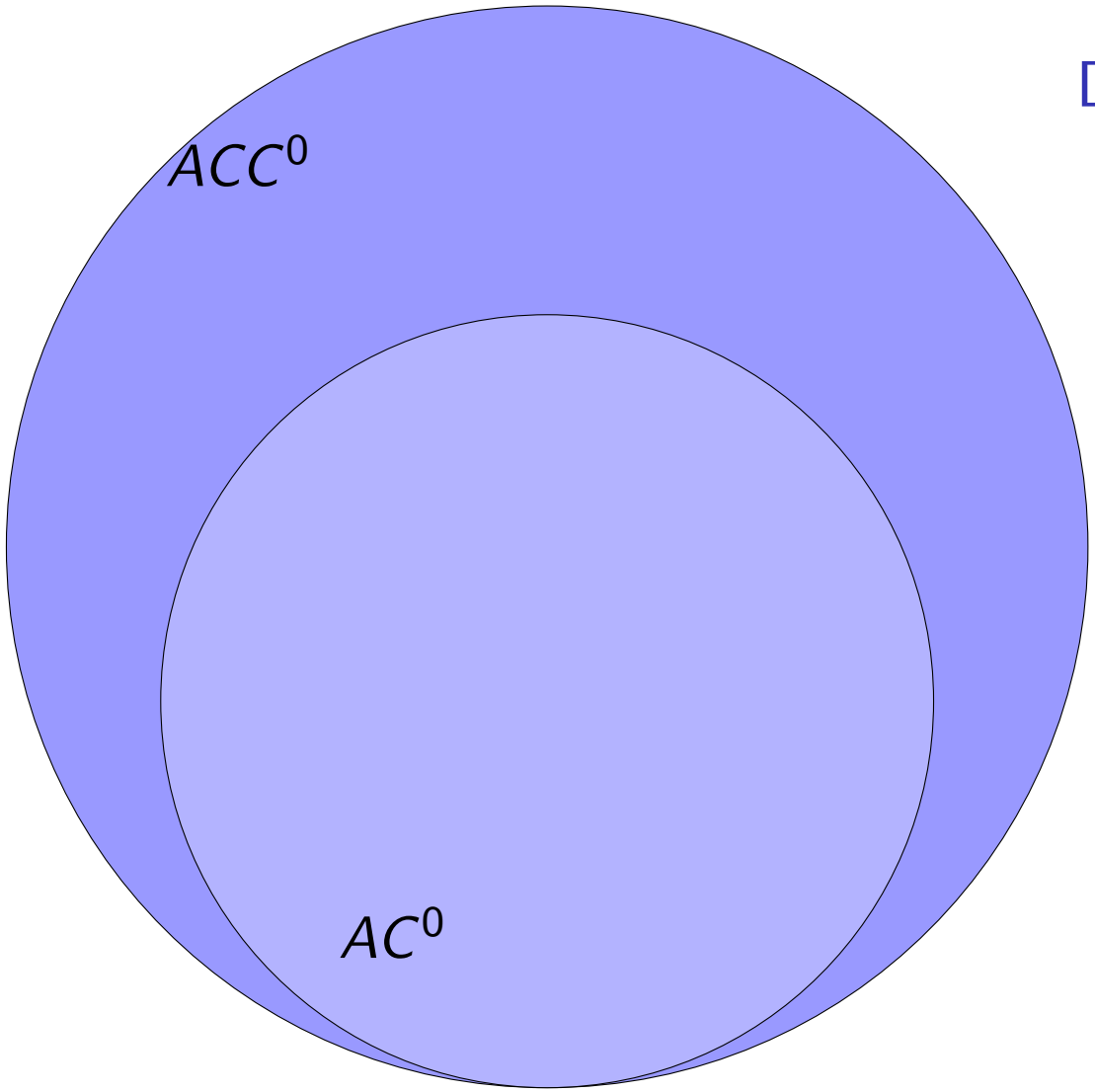
classes de complexité



Definition AC^0

- Portes $\wedge, \vee, \neg$
- nombre de portes polynomiales
- profondeur bornée

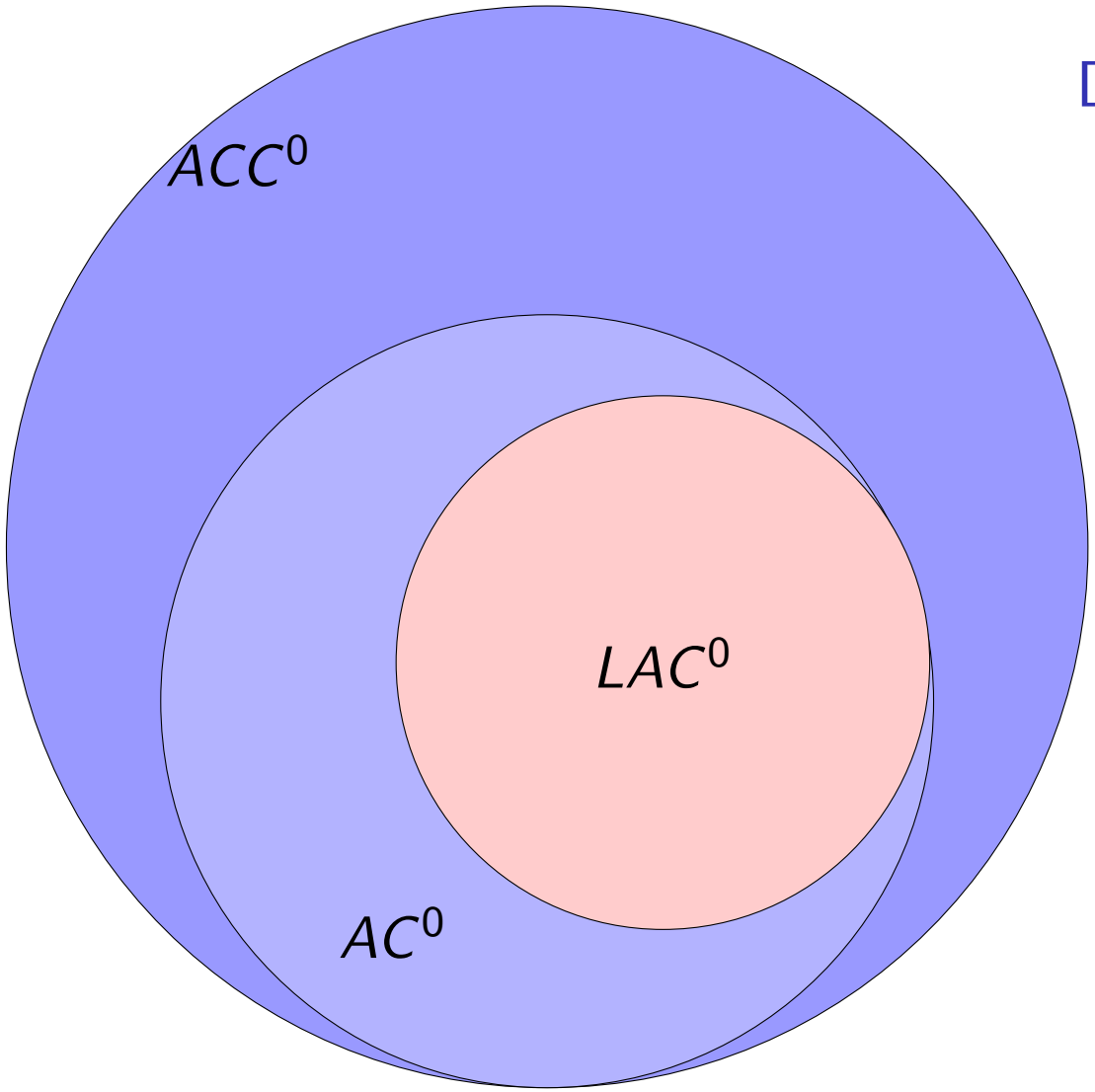
classes de complexité



Definition ACC^0

- Portes $\wedge, \vee, \neg$, **MOD**
- nombre de portes polynomiales
- profondeur bornée

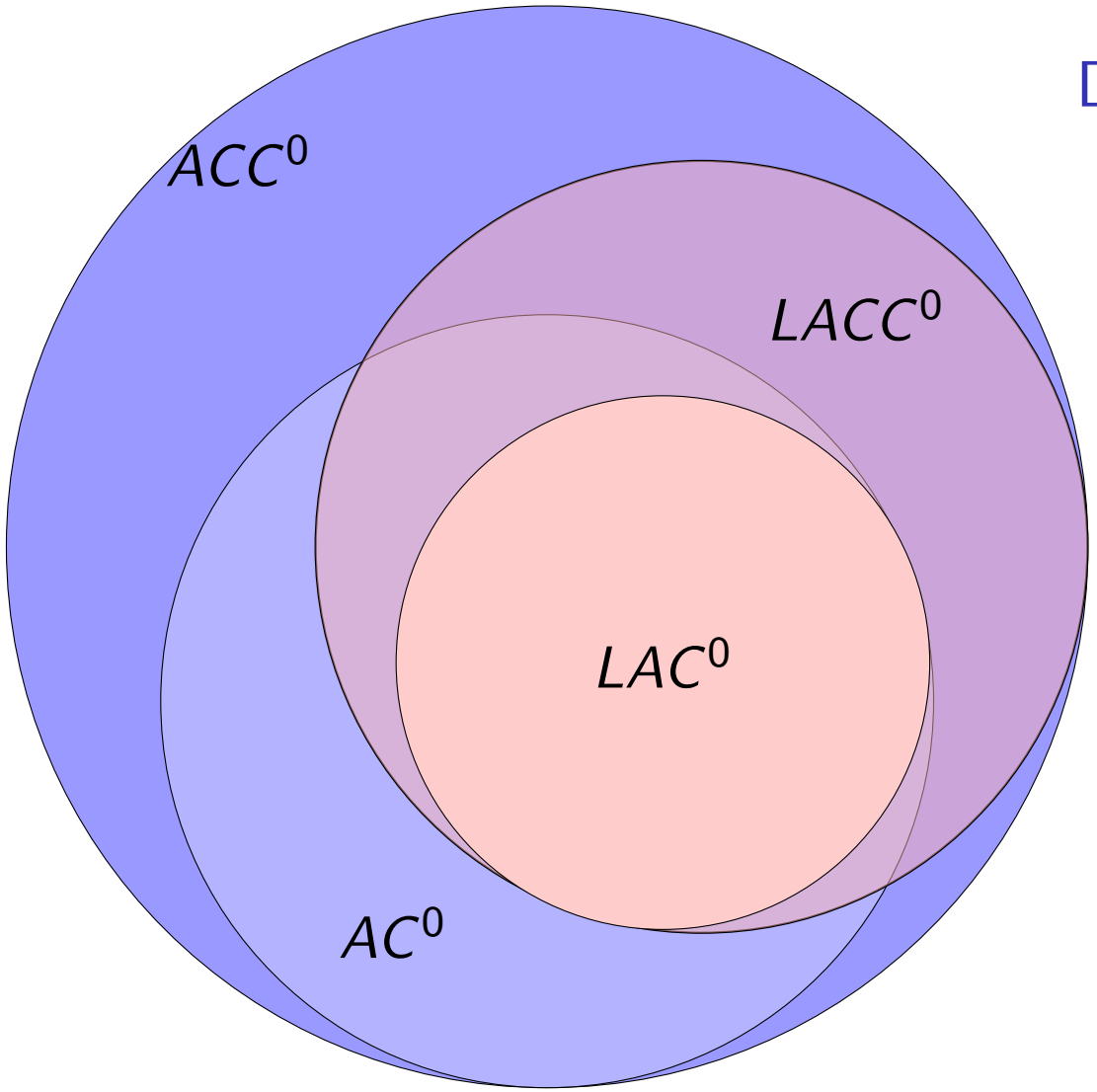
classes de complexité



Definition LAC^0

- Portes $\wedge, \vee, \neg$
- nombre de portes lineaires
- profondeur bornée

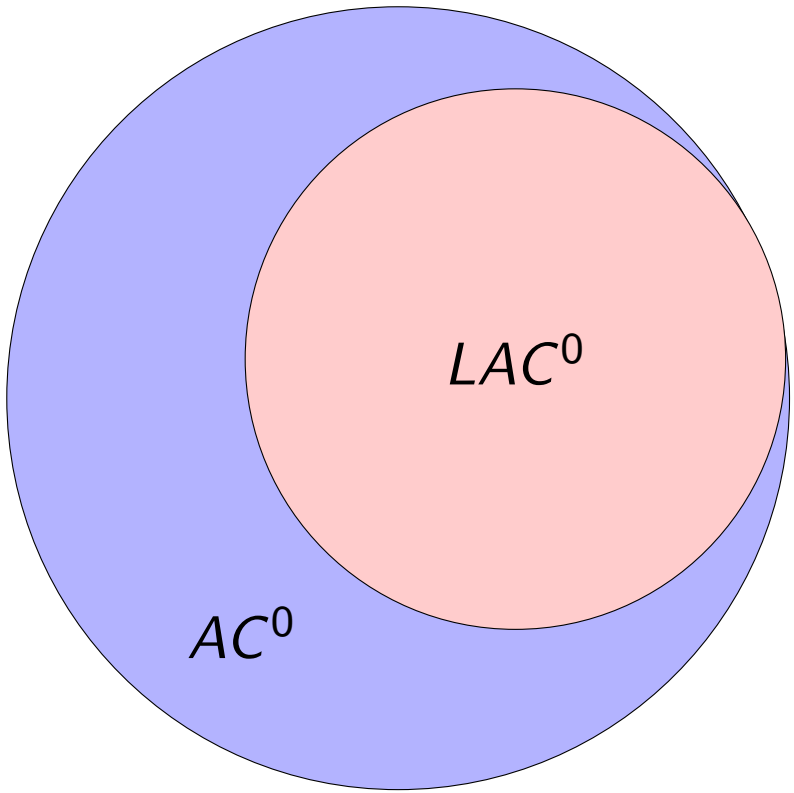
classes de complexité



Definition $LACC^0$

- Portes $\wedge, \vee, \neg$, **MOD**
- nombre de portes lineaires
- profondeur bornée

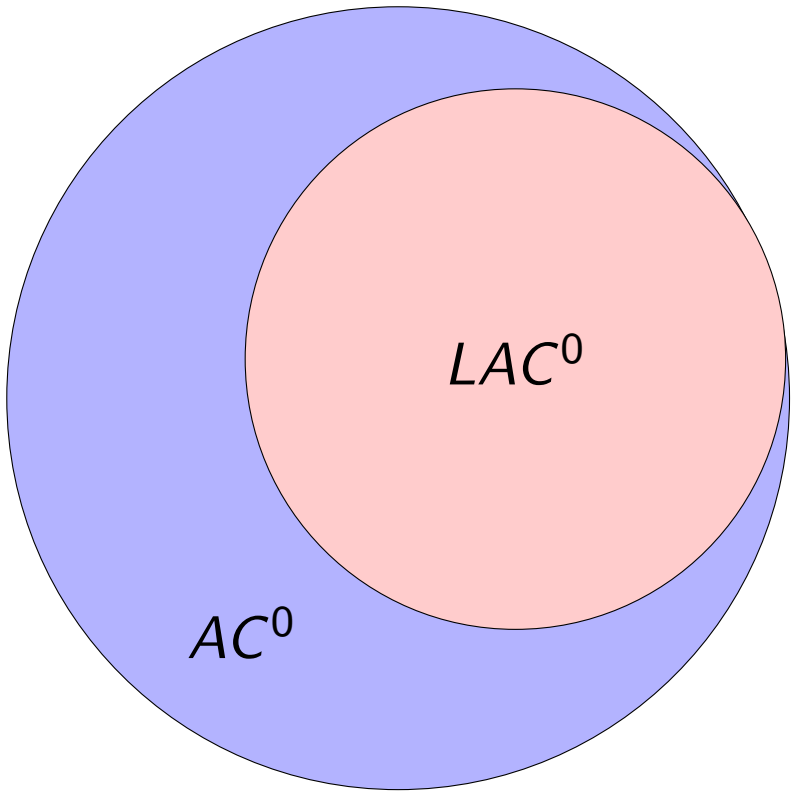
classes de complexité



Remarques

- AC^0 et LAC^0 sont séparées (fonction d'Ajitai, CR 96).
- Les langages réguliers de AC^0 sont connus (BCST 88).

classes de complexité



Remarques

- AC^0 et LAC^0 sont séparées (fonction d'Ajitai, CR 96).
- Les langages réguliers de AC^0 sont connus (BCST 88).

Question

Quels sont les langages réguliers de LAC^0 ?

Logique du premier ordre

Logique du premier ordre

- Modèle : mots finis sur alphabet fini.
  Exemple :

$$abaa = (\{0,1,2,3\}, \mathbf{a} = \{0,2,3\}, \mathbf{b} = \{1\}, \cdots)$$

- Logique:

$$\mathbf{FO}[P_1, \ldots, P_k] = \forall x \phi \mid \neg\phi \mid \psi \wedge \phi \mid a(x), b(x) \mid P_i(\vec{x})$$

  Exemple :

$$\varphi \equiv \forall x, y \ (y = x + 1 \wedge a(x)) \leftrightarrow b(y)) \wedge a(min) \wedge b(max)$$

$$L(\varphi) = (ab)^*$$

Fragment logique du premier ordre

$$\varphi \equiv \forall x, y\ (y = x + 1 \wedge a(x)) \leftrightarrow b(y)) \wedge a(min) \wedge b(max)$$

Plusieurs restrictions de **FO** sont possibles.

- $\mathbf{FO}_k$: formule de **FO** n'utilisant que k alternances de quantificateurs.
  Exemple :

  $\varphi \in \mathbf{FO}_0[min, max, +1]$ mais $L(\varphi) \notin \mathbf{FO}_0[min, max, \leq]$

Fragment logique du premier ordre

$$\varphi \equiv \forall x, y\ (y = x + 1 \wedge a(x)) \leftrightarrow b(y)) \wedge a(min) \wedge b(max)$$

Plusieurs restrictions de **FO** sont possibles.

- $\mathbf{FO}_k$: formule de **FO** n'utilisant que k alternances de quantificateurs.
  Exemple :

  $$\varphi \in \mathbf{FO}_0[min, max, +1] \text{ mais } L(\varphi) \notin \mathbf{FO}_0[min, max, \leq]$$

- $\mathbf{FO}^k$: formule de **FO** n'utilisant que k variables (avec réutilisation).
  Exemple :

  $$L(\varphi) \in \mathbf{FO}^2[+1] \text{ mais } L(\varphi) \notin \mathbf{FO}^2[\leq]$$

Classe de prédicats numériques

- Prédicat numérique : $P = (P_n)$ avec $P_n \subseteq \{0, \ldots, n\}^r$.
  Notations :
  L'ensemble des prédicats numériques : $\mathcal{N}$.
  L'ensemble des prédicats numériques d'arité au plus r: $\mathcal{N}_r$.

- P est uniforme s'il existe $Q \subseteq \mathbb{N}^r$ tel que $P_n = \{0, \ldots, n\}^r \cap Q$.
  Notation :
  L'ensemble des prédicats uniformes : $\mathcal{UN}$.

Exemples :
Prédicat d'arité 2 non uniforme : $x + y = max$.
Prédicat d'arité 3 uniforme : $x + y = z$.

Exemples et remarques

- On note $\overline{u}$ le miroir de u.
  Exemple:

$$baaaba = \overline{abaaab}$$

- Le langage miroir $L_M = \{u\overline{u} \mid u \in A^*\}$:

$$(\forall x, y \; x + y = max \rightarrow \bigvee_{a \in A} a(x) \wedge a(y)) \wedge max \equiv 0 \bmod 2$$

Exemples et remarques

- On note $\overline{u}$ le miroir de u.
  Exemple:

$$baaaba = \overline{abaaab}$$

- Le langage miroir $L_M = \{u\overline{u} \mid u \in A^*\}$:

$$(\forall x, y\ x + y = max \rightarrow \bigvee_{a \in A} a(x) \wedge a(y)) \wedge max \equiv 0 \bmod 2$$

- $L_M \in \mathbf{FO}^2[\mathcal{N}]$

- $\mathbf{FO}[\mathcal{N}] = \mathbf{FO}[\mathcal{UN}]$

Exemples et remarques

- On note $\overline{u}$ le miroir de u.
  Exemple:

$$baaaba = \overline{abaaab}$$

- Le langage miroir $L_M = \{u\overline{u} \mid u \in A^*\}$:

$$(\forall x, y\ x + y = max \rightarrow \bigvee_{a \in A} a(x) \wedge a(y)) \wedge max \equiv 0 \bmod 2$$

- On peut restreindre aux prédicats uniformes:

$$\exists z\ \forall x\ x \leq z \wedge$$
$$(\forall x, y\ x + y = z \rightarrow \bigvee_{a \in A} a(x) \wedge a(y)) \wedge z \equiv 0 \bmod 2$$

Exemples et remarques

- On note $\overline{u}$ le miroir de u.
  Exemple:

$$baaaba = \overline{abaaab}$$

- Le langage miroir $L_M = \{u\overline{u} \mid u \in A^*\}$:

$$\exists z\ \forall x\ x \leq z\ \wedge$$

$$(\forall x, y\ x + y = z \rightarrow \bigvee_{a \in A} a(x) \wedge a(y))\ \wedge\ z \equiv 0 \bmod 2$$

- A-t-on $L_M \in \mathbf{FO}^2[\mathcal{UN}]$?

Prédicats réguliers

Un prédicat P est régulier s'il est une combinaison booléenne de $x \leq y, x \equiv r \bmod q, x = y + k, min, max$.

Notation :
L'ensemble des prédicats réguliers : $\mathcal{REG}$.

Exemples :
Prédicat d'arité 1 non uniforme: $x = max - 3$.
Prédicat d'arité 2 uniforme: $x = y + 3$.

Prédicats réguliers

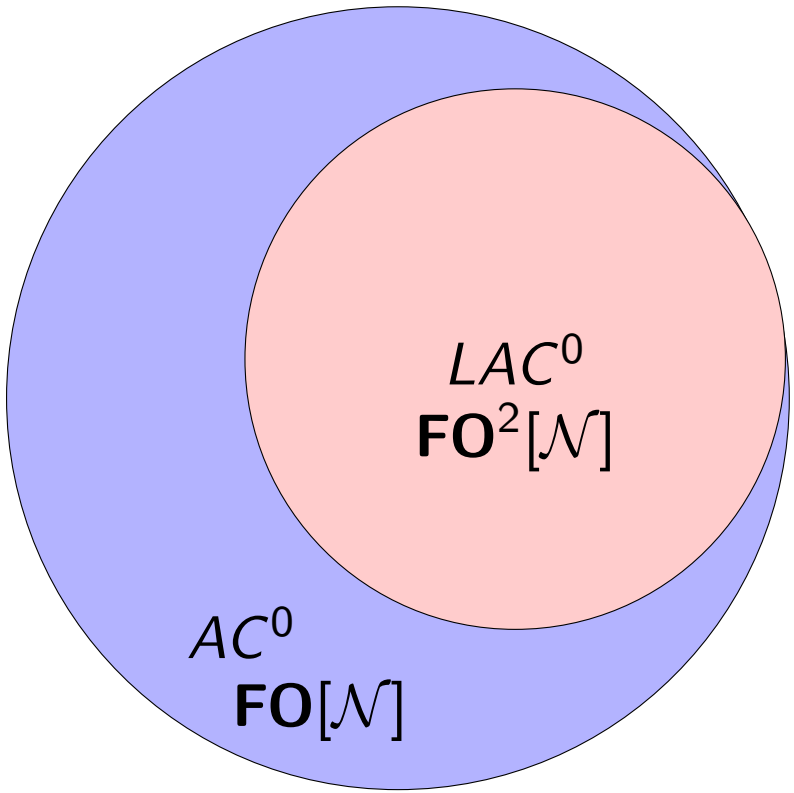
Les langages définissables dans $\mathbf{FO}[\mathcal{REG}]$ sont réguliers.

Théorème (Péladeau, 90)

Toute classe de prédicats numériques $\mathcal{C}$ telle que $\mathbf{FO}[\mathcal{C}] \subseteq \mathbf{REG}$ vérifie $\mathcal{C} \subseteq \mathcal{REG}$.

- $\mathbf{FO}[\mathcal{REG}] = \mathbf{FO}[\leq, MOD]$
- $\mathbf{FO}^2[\mathcal{REG}] = \mathbf{FO}^2[\leq, +1, MOD]$

Un peu de complexité descriptive



Equivalence logique/circuit

- $\mathbf{FO}[\mathcal{N}] = AC^0$
  (Immerman, 87)
- $\mathbf{FO}^2[\mathcal{N}] = LAC^0$
  (Koucký, Lautemann, Polczek, Thérien, 06)

Résultat classique

Théorème (BCST, 88)

$$\mathbf{FO}[\mathcal{N}] \cap REG = \mathbf{FO}[\mathcal{REG}]$$

Preuve

Les langages modulaires: $L_q \equiv \{u \in A^* \mid |u|_a \equiv 0 \bmod q\}$.

Proposition

- $\mathbf{FO}[\mathcal{REG}]$ est la plus grosse *lm*-variété qui ne contient pas les L_q.
- $\mathbf{FO}[\mathcal{N}] \cap REG$ est une *lm*-varieté.

Théorème (FSS[1] 84 ,Razborov 87)

Les langages L_q n'appartiennent pas à AC^0 ($\mathbf{FO}[\mathcal{N}]$).

[1] Furst, Saxe, Sipser

Et pour FO^2 ?

- Quelles caractérisations pour $\mathbf{FO}^2[\mathcal{REG}]$?
- Quels langages réguliers pour séparer $\mathbf{FO}^2[\mathcal{N}]$ et $\mathbf{FO}[\mathcal{N}]$?
- Peut-on prouver $\mathbf{FO}^2[\mathcal{N}] \cap REG = \mathbf{FO}^2[\mathcal{REG}]$?

$\mathbf{FO}^2[\mathcal{REG}]$

Théorème (Dartois Paperman)

$$\mathbf{FO}^2[\mathcal{REG}] = \mathbf{QLDA}$$

Corollaire

$\mathbf{FO}^2[\mathcal{REG}]$ est la plus grosse *lm*-variété qui ne contient pas les L_q et le langage $c^*(ac^*bc^*)^*$.

Corollaire

Si $c^*(ac^*bc^*)^*$ n'est pas définissable dans LAC^0 ($\mathbf{FO}^2[\mathcal{N}]$) alors:

$$\mathbf{FO}^2[\mathcal{N}] \cap REG = \mathbf{FO}^2[\mathcal{REG}].$$

Borne inférieure pour $c^*(ac^*bc^*)^*$

Méthodes classiques pour les bornes inférieures:

- Switching Lemma (Håstad, 87),
- Preuve de Rasborov: Approximation par des polynômes de faible degré,
- Complexité de la communication (Koucký, Pudlák, Thérien, 2004)

[2] Chandra, Fortune, Lipton

Borne inférieure pour $c^*(ac^*bc^*)^*$

Méthodes classiques pour les bornes inférieures:

- Switching Lemma (Håstad, 87),
- Preuve de Rasborov: Approximation par des polynômes de faible degré,
- Complexité de la communication (Koucký, Pudlák, Thérien, 2004)

Proposition(CFL[2] 85)

Pour tout ϵ, il existe une famille de circuits AC^0 qui calcule le langage $c^*(ac^*bc^*)^*$ avec $O(n^{1+\epsilon})$ portes.

[2]Chandra, Fortune, Lipton

Un théorème *à la Crane-Beach*

Deux définitions

Un prédicat uniforme d'arité 2 est de degré fini si chaque point a un nombre fini de voisins.

Notation :

L'ensemble des prédicats de degré fini : $\mathcal{F}$

Exemples :

- Les prédicats de degré borné $kx = y$, $x^k = y, \ldots$
- $\{(x, y) \mid x < y < 2x\}$

Co-exemples :

- L'ordre $x \leq y$.
- Le prédicat $BIT(x, y)$ tel que le y ème bit de x est un 1.

Deux définitions

Un langage L a une lettre neutre e si pour tout mot u, v,
$uev \in L \leftrightarrow uv \in L$

Notation :
Langages à lettre neutre: $\mathcal{NL}$

Exemples :

- Les langages L_q,
- Le langage $c^*(ac^*bc^*)^*$.

Un théorème *à la Crane-Beach*

Notation :

- L'ensemble des prédicats de degré fini : $\mathcal{F}$
- Langages à lettre neutre: $\mathcal{NL}$

Théorème

$$\mathbf{FO}^2[\leq, \mathcal{F}] \cap \mathcal{NL} = \mathbf{FO}^2[\leq] \cap \mathcal{NL}$$

Un théorème *à la Crane-Beach*

Notation :

- L'ensemble des prédicats de degré fini : $\mathcal{F}$
- Langages à lettre neutre: $\mathcal{NL}$

Théorème

$$\mathbf{FO}^2[\leq, \mathcal{F}] \cap \mathcal{NL} = \mathbf{FO}^2[\leq] \cap \mathcal{NL}$$

Corollaire

$$\mathbf{FO}^2[\leq, \mathcal{F}] \cap \mathit{REG} = \mathbf{FO}^2[\mathcal{REG}]$$

Questions autours de Crane Beach

Théorème (BILST[3], 2005)

$$\mathbf{FO}[\leq] \cap \mathcal{NL} \subsetneq \mathbf{FO}[\mathcal{N}] \cap \mathcal{NL}$$

Questions:

- $\mathbf{FO}[\leq, \mathcal{F}] \cap \mathcal{NL} = \mathbf{FO}[\leq] \cap \mathcal{NL}$?
- $\mathbf{FO}^2[\mathcal{N}] \cap \mathcal{NL} = \mathbf{FO}^2[\leq] \cap \mathcal{NL}$?

[3] Barrington, Immerman, Lautemann, Schweikardt, Thérien

Conclusion

Théorème

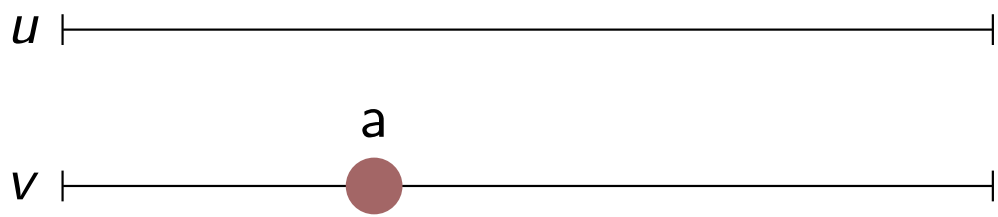
$$\mathbf{FO}^2[\leq, \mathcal{F}] \cap \mathcal{NL} = \mathbf{FO}^2[\leq] \cap \mathcal{NL}$$

Et maintenant :

- Peut-on généraliser à $\mathbf{FO}^2_k$? à $\mathbf{FO}$?
- Comment prouver $c^*(ac^*bc^*)^* \notin \mathbf{FO}^2[\mathcal{N}]$?
- Quels langages réguliers pour caractériser $LACC^0 = (\mathbf{FO} + MOD)^2[\mathcal{N}]$?

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

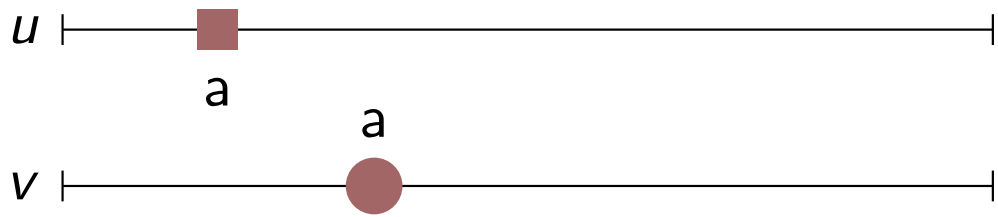


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

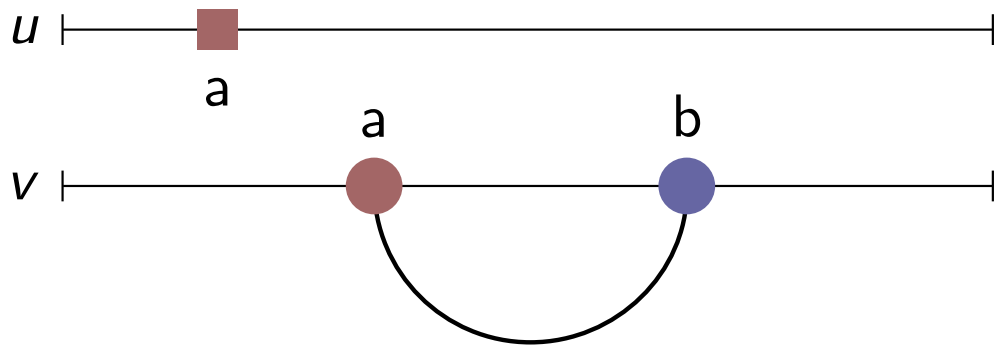


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

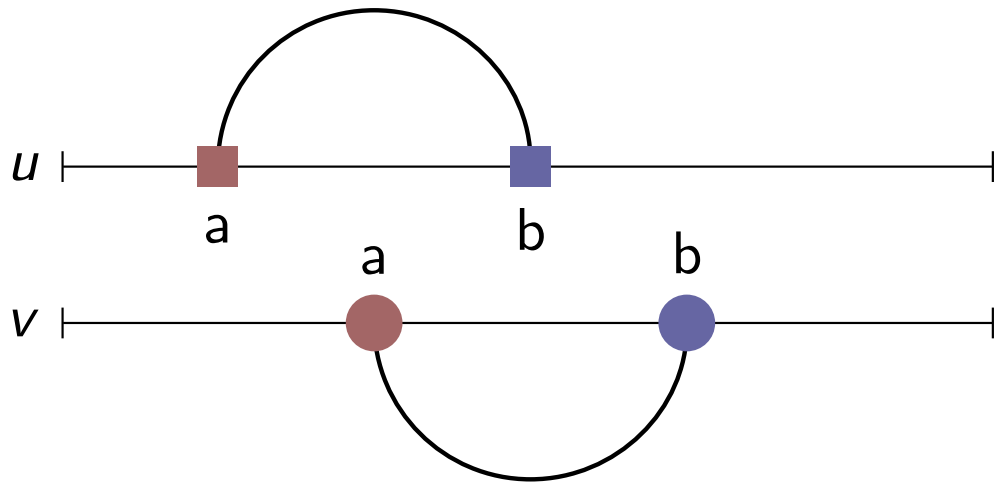


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

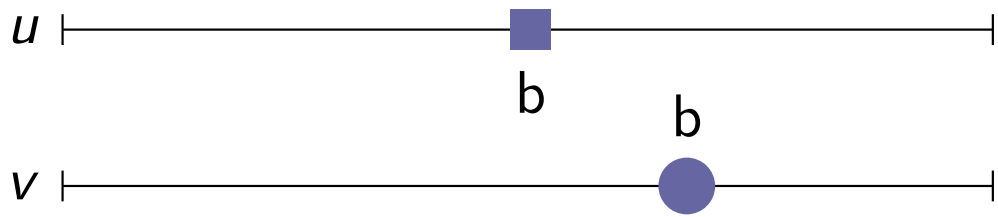


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

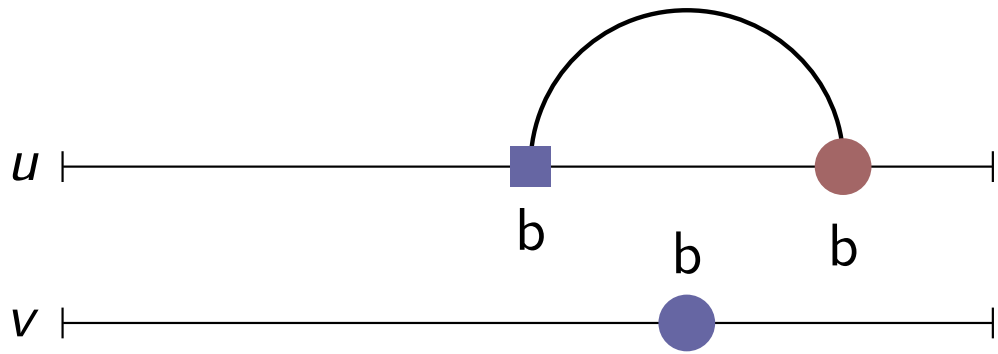


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

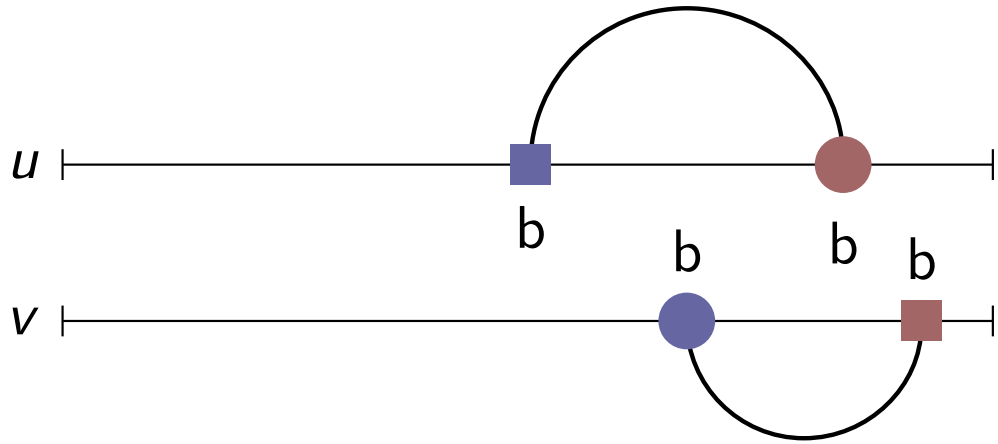


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

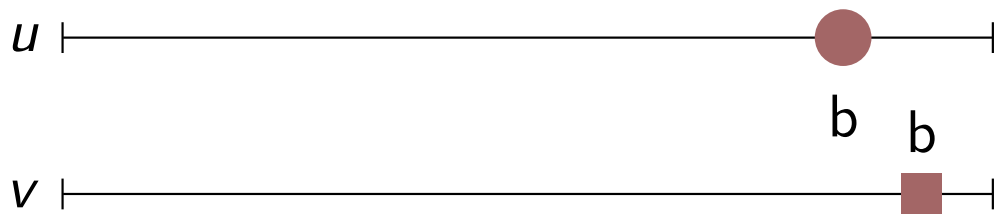


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

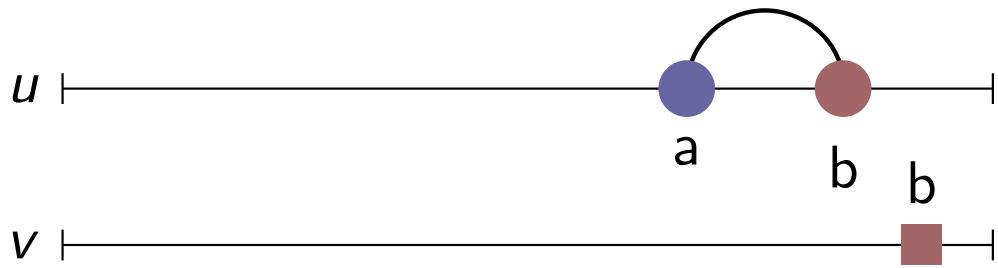


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

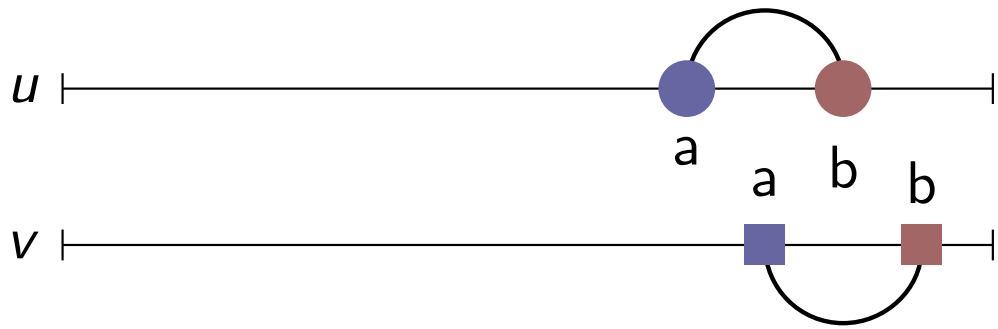


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

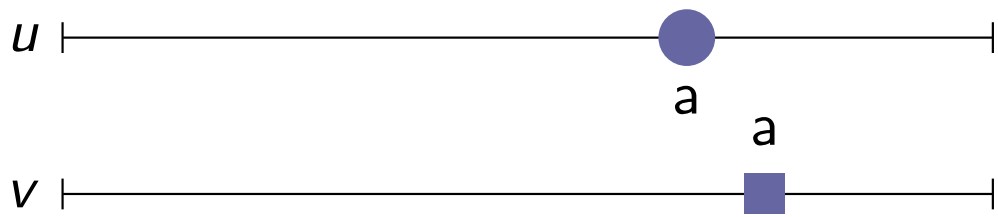


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

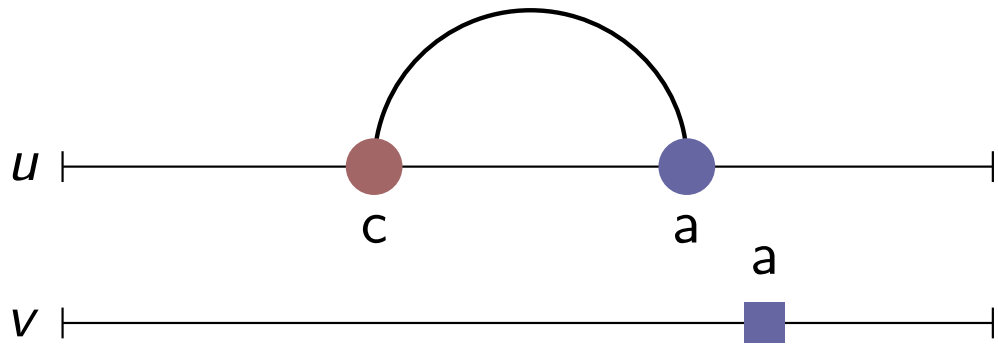


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

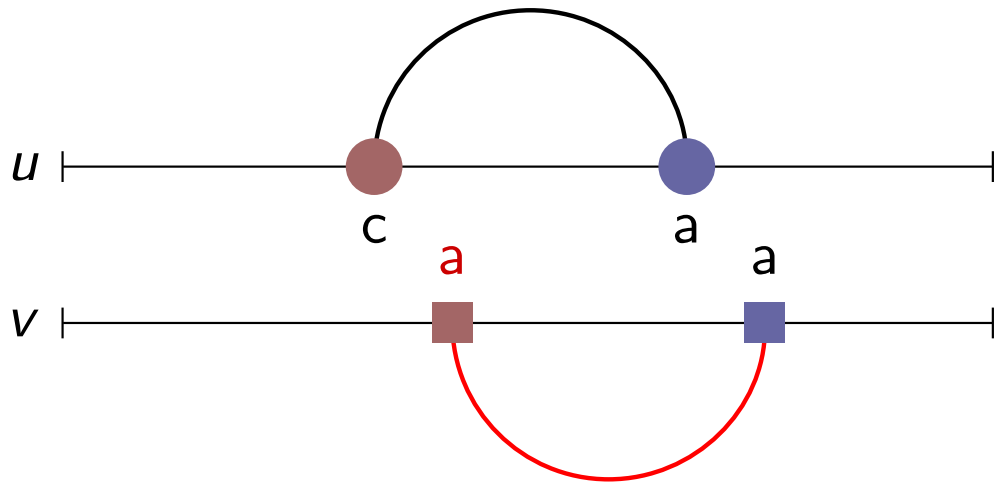


■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,



■ Duplicator

● Spoiler

Ingrédients de la preuve

Des jeux à deux jetons d'Ehrenfeucht-Fraïssé,

Théorème (Immerman 87)

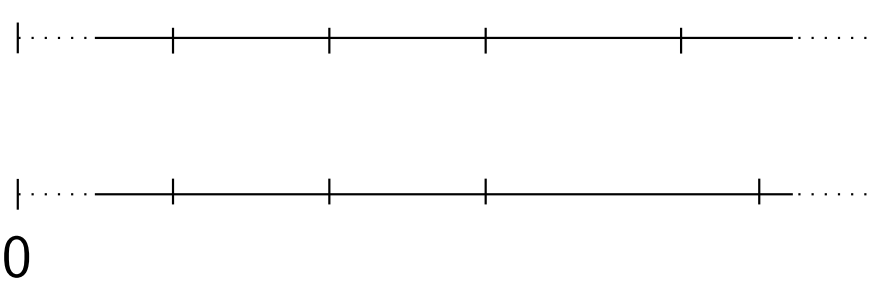
Un langage L est définissable dans $\mathbf{FO}^2_k[P_1, \ldots, P_t]$ si, et seulement si, pour tout couple $(u, v) \in L \times L^c$, Spoiler a un stratégie gagnante en k coups pour le jeux à deux jetons.

Schéma général

- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:

Schéma général

- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:



$u_1 u_2 u_3 \cdots u_n = u$

$v_1 v_1 v_3 \cdots v_p = v$

Schéma général

- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:

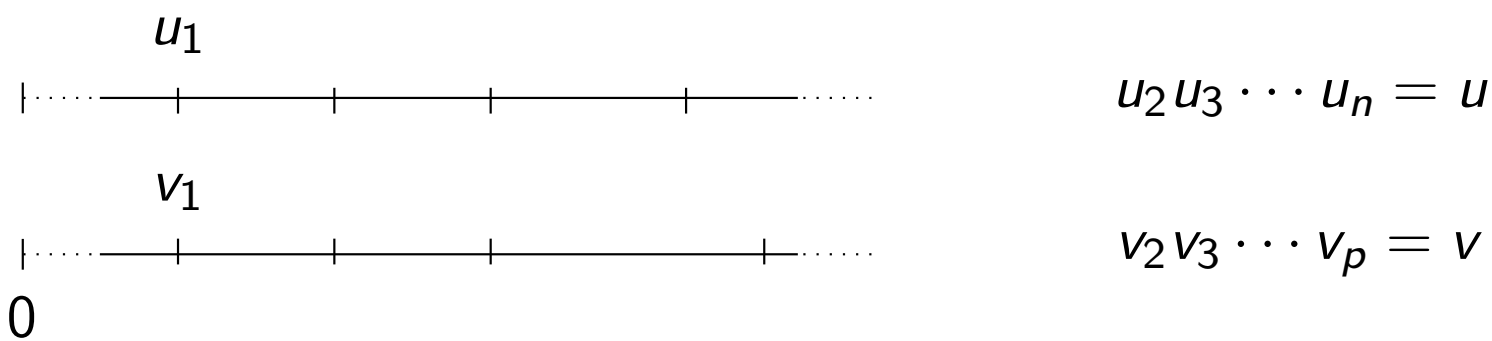
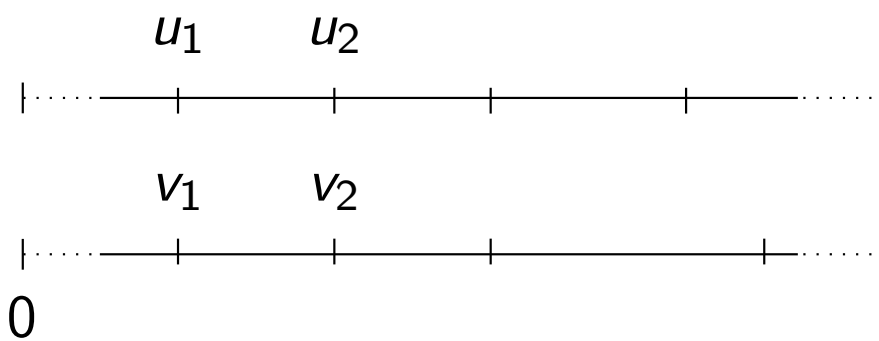


Schéma général

- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:



$u_3 \cdots u_n = u$

$v_3 \cdots v_p = v$

Schéma général

- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:

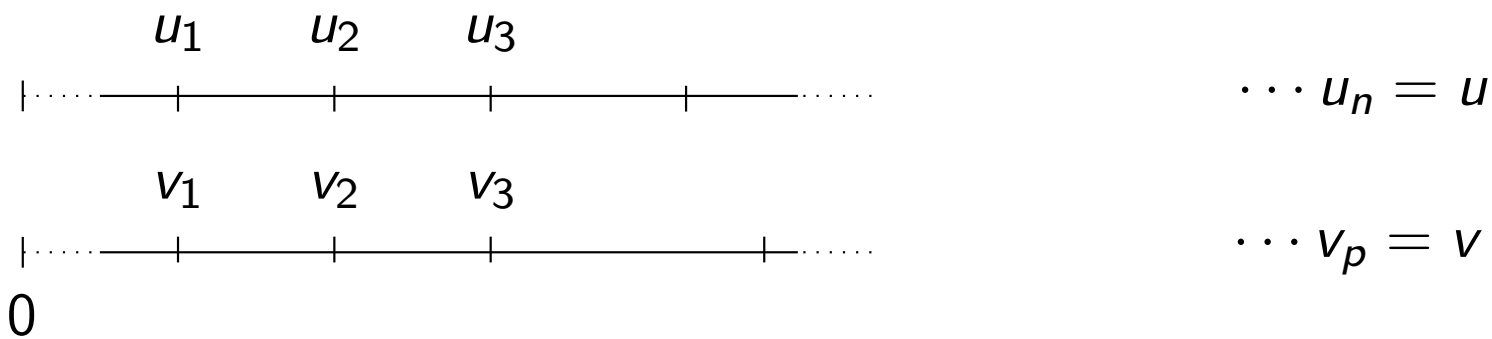


Schéma général

- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:

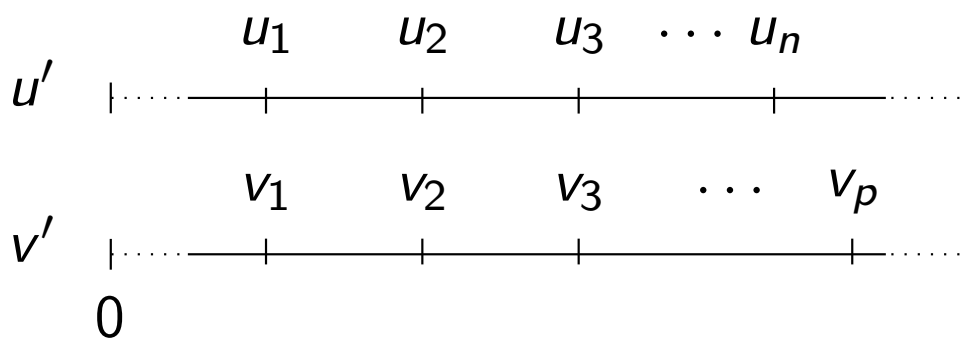


Schéma général

- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:

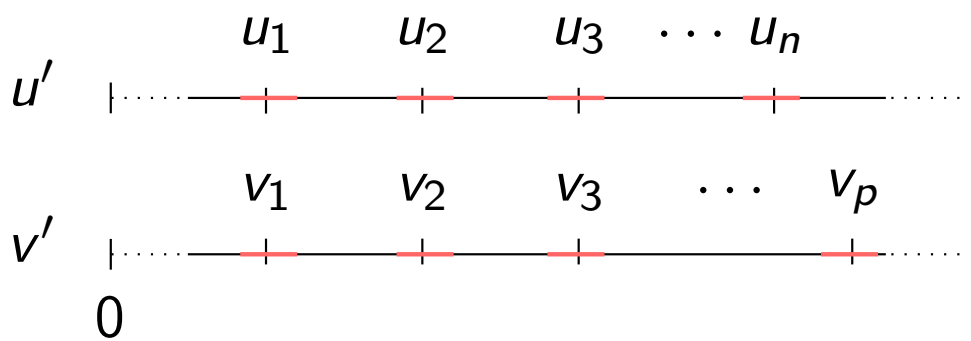
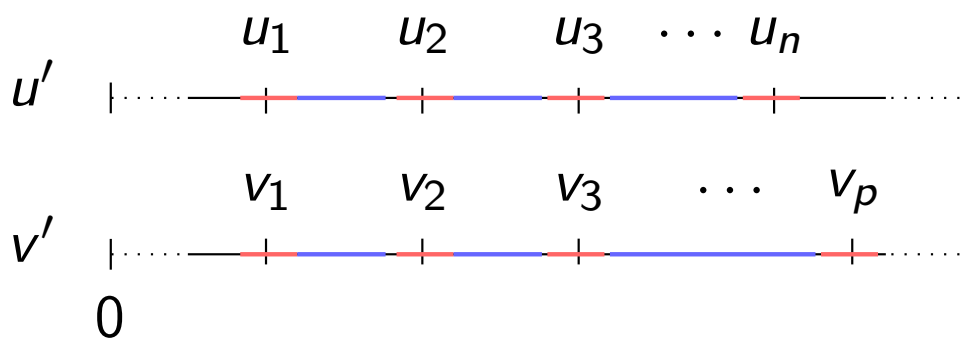
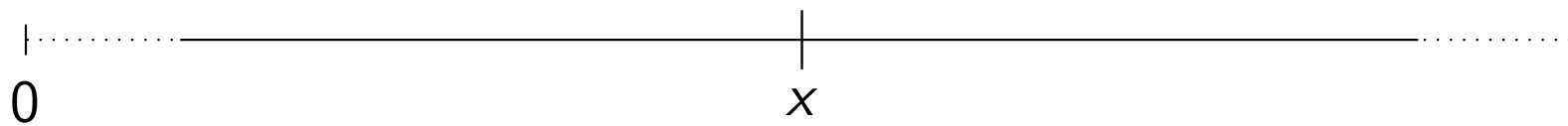


Schéma général

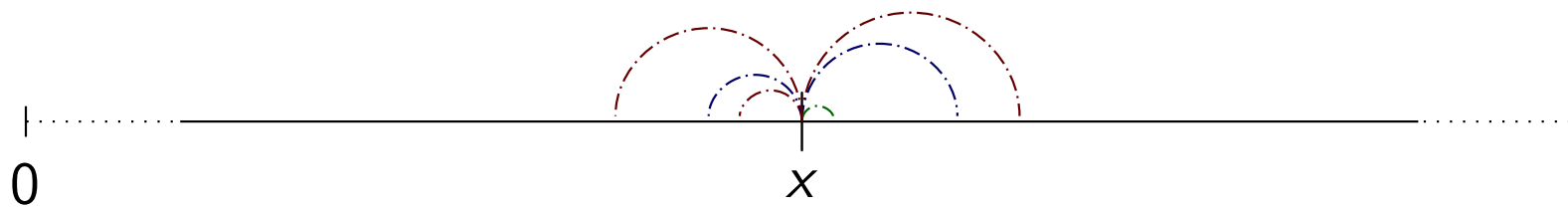
- On suppose par l'absurde qu'il existe $L \in \mathbf{FO}^2[P_1, \ldots, P_t] \cap \mathcal{NL}$ mais $L \notin \mathbf{FO}^2[\leq]$.
- Il existe donc $(u, v) \in L \times L^c$ tel que Spoiler a une stratégie gagnante sur (u, v) avec $P_1, \ldots, P_t$ mais Duplicateur a une stratégie gagnante sur (u, v) avec $\leq$.
- On trouve un ensemble de positions bien choisies de $\mathbb{N}$ telles que:



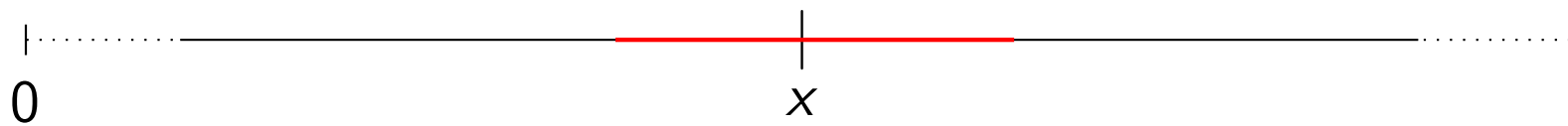
Voisinages



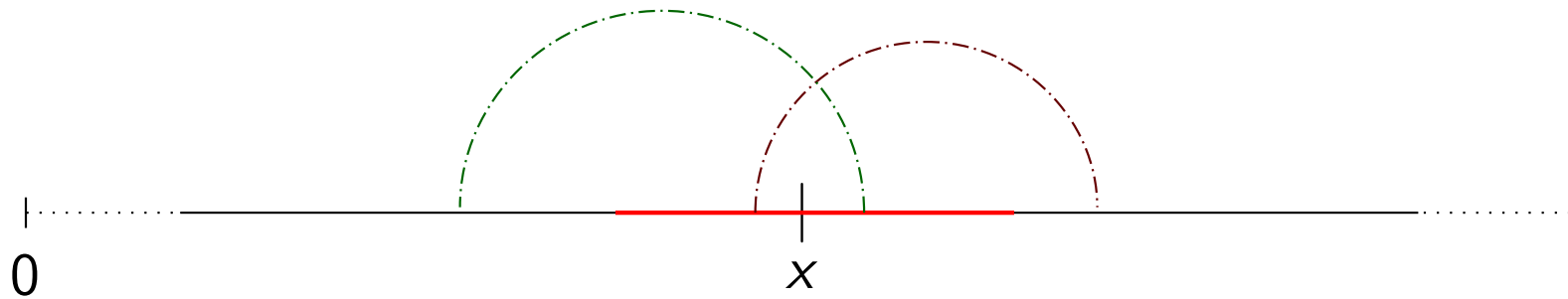
Voisinages



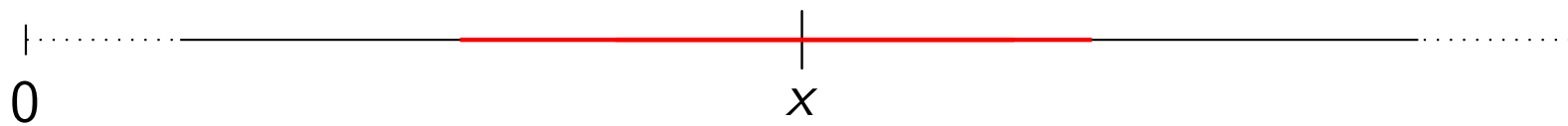
Voisinages



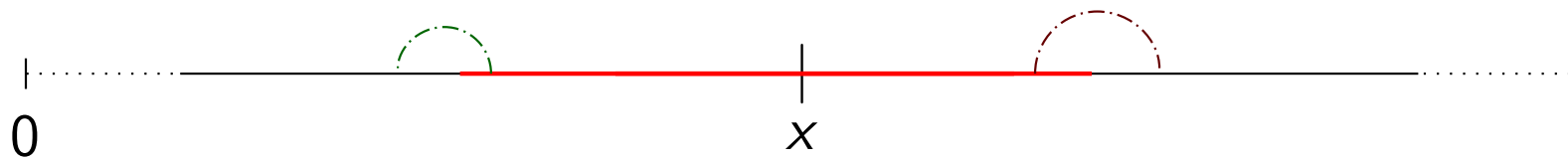
Voisinages



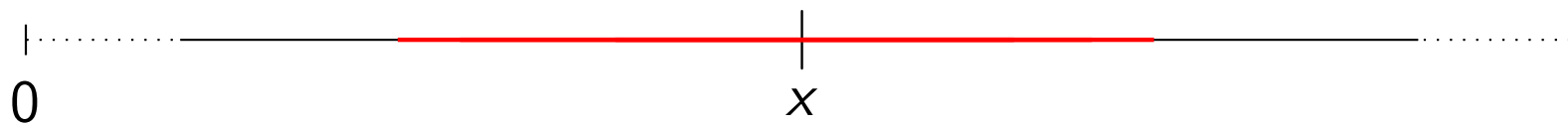
Voisinages



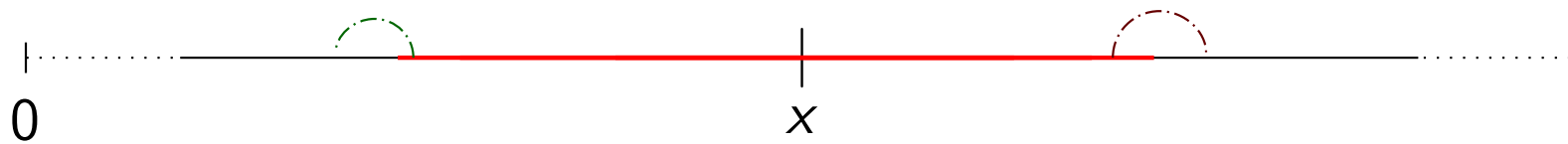
Voisinages



Voisinages



Voisinages



Voisinages