$\mathbf{FO}^2[<, \mathbf{MOD}] = \mathbf{QDA}$

Luc Dartois, travail conjoint avec Charles Paperman

Réunion FRec, Juin 2012

Introduction

- La logique $\mathbf{FO}^2[<, \mathbf{MOD}]$
- Définition de la Quasi-variété

$\mathbf{FO}^2[<, \mathbf{MOD}] \subseteq \mathbf{QDA}$

- Automate stable
- Alphabet enrichi et mots bien formés

$\mathbf{QDA} \subseteq \mathbf{FO}^2[<, \mathbf{MOD}]$

- Congruence modulo d
- Passage par les jeux d'Ehrenfeucht-Fraïssé
- Relations de Green sur le semigroupe stable

Conclusion

La logique $\mathbf{FO}^2[<, \mathbf{MOD}]$

- On appelle $\mathbf{FO}^2[<]$ le fragment de logique du premier ordre où l'on ne s'autorise que deux variables.
  Exemple: Soit
  $\varphi = \exists x \exists y \Big(a(x) \wedge b(y) \wedge (x < y) \wedge (\exists x \; a(x) \wedge (y < x)) \Big)$.
  Le langage associé est $L(\varphi) = A^* a A^* b A^* a A^*$.

La logique $\mathbf{FO}^2[<, \mathbf{MOD}]$

- On appelle $\mathbf{FO}^2[<]$ le fragment de logique du premier ordre où l'on ne s'autorise que deux variables.
  Exemple: Soit
  $\varphi = \exists x \exists y \Big(a(x) \wedge b(y) \wedge (x < y) \wedge (\exists x \; a(x) \wedge (y < x)) \Big)$.
  Le langage associé est $L(\varphi) = A^* a A^* b A^* a A^*$.

- Les prédicats modulaires
  - $MOD_i^d(x)$, prédicat unaire vrai aux positions égales à i mod d.
  - D_i^d, constante vraie si le mot a une longueur égale à i mod d.

  Par exemple, la formule $\psi = \exists x (a(x) \wedge MOD_0^3(x) \wedge D_1^3)$ appartient à $\mathbf{FO}^2[<, \mathbf{MOD}]$. Le langage associé est $L(\psi) = (A^3)^* a (A^3)^*$.

Indice de Stabilité et Quasi-variété

On appelle timbre un morphisme d'un monoïde libre finiment engendré sur un monoïde fini.

Définition

Soit $h : A^* \to M$ un timbre.
L'indice de stabilité d'un timbre est le plus petit entier s tel que $h(A^s) = h(A^{2s})$.

L'ensemble $h(A^s)$ est appelé le semigroupe stable de h.

Indice de Stabilité et Quasi-variété

On appelle timbre un morphisme d'un monoïde libre finiment engendré sur un monoïde fini.

Définition

Soit $h : A^* \to M$ un timbre.
L'indice de stabilité d'un timbre est le plus petit entier s tel que $h(A^s) = h(A^{2s})$.

L'ensemble $h(A^s)$ est appelé le semigroupe stable de h.

- ### Quasi-variété

  Soit $\mathbf{V}$ une variété de monoïdes.
  Alors l'ensemble des timbres h tels que leur semigroupe stable est dans $\mathbf{V}$ forme une *lm*-variété de timbres, notée $\mathbf{QV}$.

La variété **DA**

- Variété **DA**
  La variété **DA** est la variété des monoïdes dont les $\mathcal{D}$-classes régulières sont des semigroupes apériodiques.
  Elle est caractérisée par l'équation

$$(xyz)^\omega = (xyz)^\omega y (xyz)^\omega$$

La variété **DA**

- Variété **DA**
  La variété **DA** est la variété des monoïdes dont les $\mathcal{D}$-classes régulières sont des semigroupes apériodiques.
  Elle est caractérisée par l'équation

$$(xyz)^\omega = (xyz)^\omega y (xyz)^\omega$$

- Théorème [TW98]
  Pour tout alphabet A, on a $\mathbf{FO}^2[<](A^*) = \mathcal{DA}(A^*)$.

k-automates

- **Définition**
  Soit $\mathcal{A} = (Q, A, \cdot)$ un automate déterministe et $k > 0$.
  Le k-automate de $\mathcal{A}$ est l'automate déterministe $\mathcal{A}_k = (Q, A^k, \cdot^k)$ où $q \cdot^k a_1 \dots a_k = (..(q \cdot a_1) \cdot a_2) \dots \cdot a_k)$.

k-automates

- **Définition**
  Soit $\mathcal{A} = (Q, A, \cdot)$ un automate déterministe et $k > 0$.
  Le k-automate de $\mathcal{A}$ est l'automate déterministe $\mathcal{A}_k = (Q, A^k, \cdot^k)$ où $q \cdot^k a_1 \dots a_k = (..(q \cdot a_1) \cdot a_2) \dots \cdot a_k)$.
  - Si $\varphi : A^* \to M$ est le timbre associé à $\mathcal{A}$, alors $\varphi_k : (A^k)^* \to \varphi((A^k)^*)$ est celui associé à $\mathcal{A}_k$.

k-automates

- **Définition**
  Soit $\mathcal{A} = (Q, A, \cdot)$ un automate déterministe et $k > 0$.
  Le k-automate de $\mathcal{A}$ est l'automate déterministe $\mathcal{A}_k = (Q, A^k, \cdot^k)$ où $q \cdot^k a_1 \dots a_k = (..(q \cdot a_1) \cdot a_2) \dots \cdot a_k)$.
  - Si $\varphi : A^* \to M$ est le timbre associé à $\mathcal{A}$, alors $\varphi_k : (A^k)^* \to \varphi((A^k)^*)$ est celui associé à $\mathcal{A}_k$.
- **Automate stable**
  Un automate déterministe sera dit *stable* si l'action de tout mot de deux lettres est équivalente à l'action d'une lettre, et inversement.

k-automates

- **Définition**
  Soit $\mathcal{A} = (Q, A, \cdot)$ un automate déterministe et $k > 0$.
  Le k-automate de $\mathcal{A}$ est l'automate déterministe $\mathcal{A}_k = (Q, A^k, \cdot^k)$ où $q \cdot^k a_1 \dots a_k = (..(q \cdot a_1) \cdot a_2) \dots \cdot a_k)$.
  - Si $\varphi : A^* \to M$ est le timbre associé à $\mathcal{A}$, alors $\varphi_k : (A^k)^* \to \varphi((A^k)^*)$ est celui associé à $\mathcal{A}_k$.
- **Automate stable**
  Un automate déterministe sera dit *stable* si l'action de tout mot de deux lettres est équivalente à l'action d'une lettre, et inversement.
  - Pour tout automate $\mathcal{A}$, il existe un entier k tel que $\mathcal{A}_k$ est stable.

Alphabet enrichi

- **Lemme (des restes chinois)**

  Soit L un langage de $\mathbf{FO}^2[<, \mathbf{MOD}]$.
  Alors il existe un entier d tel que $L \in \mathbf{FO}^2[<, \mathbf{MOD}_d]$.

Alphabet enrichi

- **Lemme (des restes chinois)**

  Soit L un langage de $\mathbf{FO}^2[<, \mathbf{MOD}]$.
  Alors il existe un entier d tel que $L \in \mathbf{FO}^2[<, \mathbf{MOD}_d]$.

- **Définition**

  Soit un alphabet A. On appelle $A_d = A \times \mathbb{Z}/d\mathbb{Z}$ l'alphabet enrichi de A, et $\pi : A_d^* \to A^*$ la projection canonique.

Alphabet enrichi

- **Lemme (des restes chinois)**

  Soit L un langage de $\mathbf{FO}^2[<, \mathbf{MOD}]$.
  Alors il existe un entier d tel que $L \in \mathbf{FO}^2[<, \mathbf{MOD}_d]$.

- **Définition**

  Soit un alphabet A. On appelle $A_d = A \times \mathbb{Z}/d\mathbb{Z}$ l'alphabet enrichi de A, et $\pi : A_d^* \to A^*$ la projection canonique.

- **Mots bien formés**

  Un mot enrichi $(a, i_0)(a_1, i_1)\dots(a_n, i_n)$ sera dit bien formé si, et seulement si, pour tout entier $0 \leqslant j \leqslant n$, $i_j \equiv j \bmod d$. On note K l'ensemble des mots bien formés.

Alphabet enrichi

- **Lemme (des restes chinois)**

  Soit L un langage de $\mathbf{FO}^2[<, \mathbf{MOD}]$.
  Alors il existe un entier d tel que $L \in \mathbf{FO}^2[<, \mathbf{MOD}_d]$.

- **Définition**

  Soit un alphabet A. On appelle $A_d = A \times \mathbb{Z}/d\mathbb{Z}$ l'alphabet enrichi de A, et $\pi : A_d^* \to A^*$ la projection canonique.

- **Mots bien formés**

  Un mot enrichi $(a, i_0)(a_1, i_1)\dots(a_n, i_n)$ sera dit bien formé si, et seulement si, pour tout entier $0 \leqslant j \leqslant n$, $i_j \equiv j \bmod d$. On note K l'ensemble des mots bien formés.

  - Pour tout mot u de A^*, on note $\overline{u}$ l'unique mot bien formé de K tel que $\pi(\overline{u}) = u$.

Le langage des mots bien formés

- Le semigroupe de Brandt

  Soit $B_d = (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}) \cup \{\perp\}$ où $\perp$ est un zéro de B_d et pour tout entiers $i, j, k, l \in \mathbb{Z}/d\mathbb{Z}$,

$$(i,j).(k,l) = \begin{cases} (i,l) & \text{si } j = k \\ \perp & \text{sinon.} \end{cases}$$

Le langage des mots bien formés

- ## Le semigroupe de Brandt

  Soit $B_d = (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}) \cup \{\perp\}$ où $\perp$ est un zéro de B_d et pour tout entiers $i, j, k, l \in \mathbb{Z}/d\mathbb{Z}$,

$$(i,j).(k,l) = \begin{cases} (i,l) & \text{si } j = k \\ \perp & \text{sinon.} \end{cases}$$

- ## Propriété

  Le langages des mots bien formés K est reconnu par le semigroupe de Brandt par un timbre de $\mathbf{QJ_1}$.

Décalage des informations

- Théorème
  Soit d un entier positif, alors

$$\mathbf{FO}^2[<, \mathbf{MOD}_d](A^*) = \pi(\mathbf{FO}^2[<](A_d^*) \cap K)$$

Décalage des informations

- **Théorème**
  Soit d un entier positif, alors

$$\mathbf{FO}^2[<, \mathbf{MOD}_d](A^*) = \pi(\mathbf{FO}^2[<](A_d^*) \cap K)$$

  - 1. $\overline{MOD_i^d(x)} = \bigvee_{a \in A} (a, i)(x)$
  - 2. $\overline{a(x)} = \bigvee_{0 \leqslant i < d} (a, i)(x)$
  - 3. $\overline{D_i^d} = \exists x(\forall y, y \leqslant x \wedge \overline{MOD_i^d(x)})$

Décalage des informations

- **Théorème**
  Soit d un entier positif, alors

$$\mathbf{FO}^2[<, \mathbf{MOD}_d](A^*) = \pi(\mathbf{FO}^2[<](A_d^*) \cap K)$$

  - 1. $\overline{MOD_i^d(x)} = \bigvee_{a \in A} (a, i)(x)$
  - 2. $\overline{a(x)} = \bigvee_{0 \leqslant i < d} (a, i)(x)$
  - 3. $\overline{D_i^d} = \exists x(\forall y, y \leqslant x \wedge \overline{MOD_i^d(x)})$

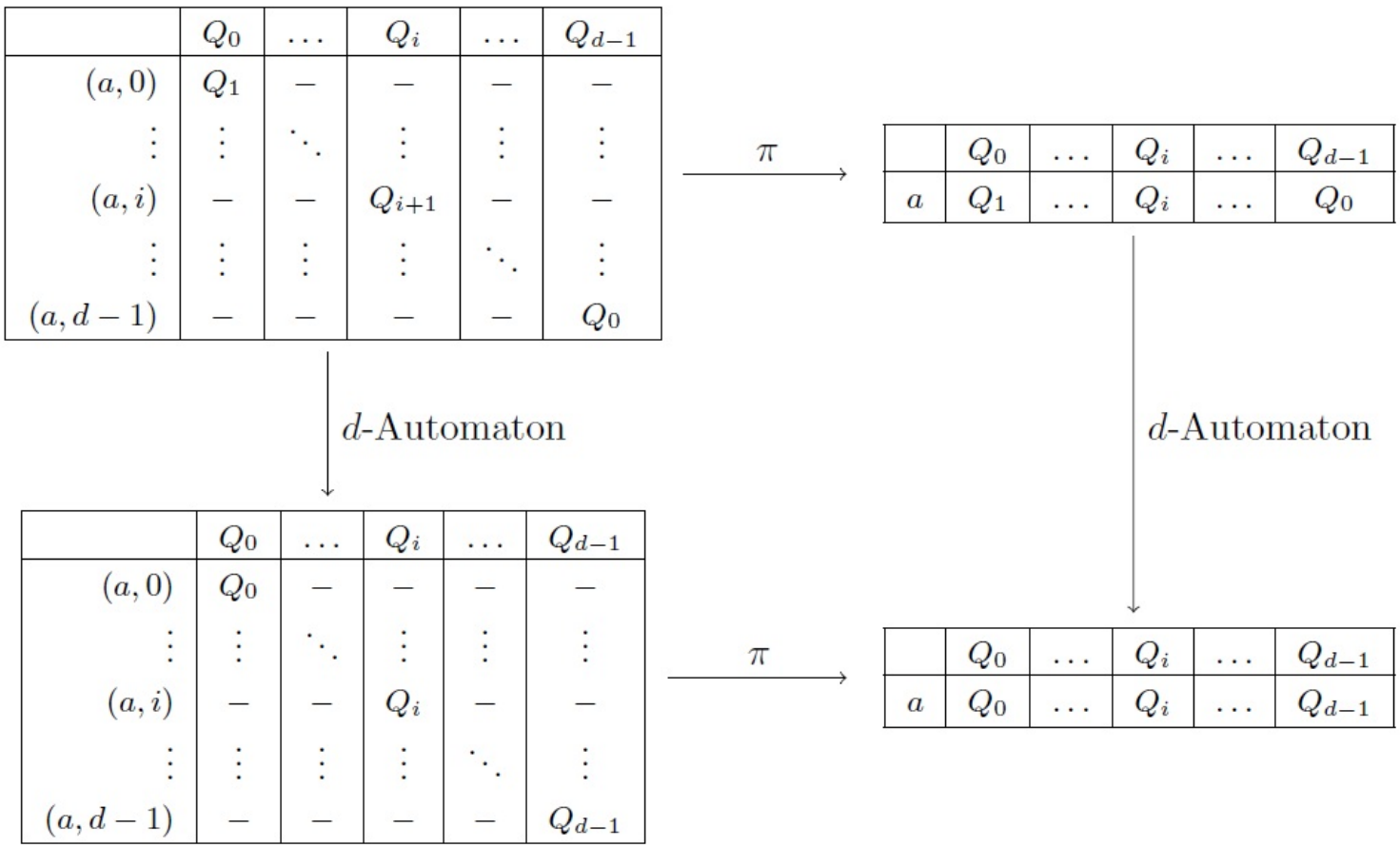
- **Lemme**
  Soit L un langage de $\mathcal{DA}(A_d^*)$. Alors le langage $L \cap K$ est dans $\mathcal{QDA}(A_d^*)$.

Première inclusion

- Théorème
  Soit L un langage définissable dans $\mathbf{FO}^2[<, \mathbf{MOD}]$. Alors son timbre syntaxique est dans **QDA**.

Première inclusion

- Théorème
  Soit L un langage définissable dans $\mathbf{FO}^2[<, \mathbf{MOD}]$. Alors son timbre syntaxique est dans **QDA**.
  -



- ## Décomposition gauche

  Soit $u \in A^*$ un mot, et a une lettre apparaissant dans u. La a-décomposition gauche de u est l'unique triplet (u_0, a, u_1) tel que $u = u_0 a u_1$ et a n'apparaît pas dans u_0.

- ## Décomposition gauche

  Soit $u \in A^*$ un mot, et a une lettre apparaissant dans u. La a-décomposition gauche de u est l'unique triplet (u_0, a, u_1) tel que $u = u_0 a u_1$ et a n'apparaît pas dans u_0.

- ## Relation $\equiv_n$

  Soient $u, v \in A^*$ deux mots. On a alors $u \equiv_0 v$.
  De plus, $u \equiv_n v$ si, et seulement si, les conditions suivantes sont satisfaites:

  1. $\alpha(u) = \alpha(v)$
     Et pour chaque a apparaissant dans u,
  2. si (u_0, a, u_1) est la a-décomposition gauche de u et (v_0, a, v_1) celle de v, alors $u_0 \equiv_n v_0$ et $u_1 \equiv_{n-1} v_1$.
  3. si (u_0, a, u_1) est la a-décomposition droite de u et (v_0, a, v_1) celle de v, alors $u_0 \equiv_{n-1} v_0$ et $u_1 \equiv_n v_1$.

- ## Décomposition gauche

  Soit $u \in A^*$ un mot, et a une lettre apparaissant dans u. La a-décomposition gauche de u est l'unique triplet (u_0, a, u_1) tel que $u = u_0 a u_1$ et a n'apparaît pas dans u_0.

- ## Relation $\equiv_n$

  Soient $u, v \in A^*$ deux mots. On a alors $u \equiv_0 v$.
  De plus, $u \equiv_n v$ si, et seulement si, les conditions suivantes sont satisfaites:

  1. $\alpha(u) = \alpha(v)$
     Et pour chaque a apparaissant dans u,
  2. si (u_0, a, u_1) est la a-décomposition gauche de u et (v_0, a, v_1) celle de v, alors $u_0 \equiv_n v_0$ et $u_1 \equiv_{n-1} v_1$.
  3. si (u_0, a, u_1) est la a-décomposition droite de u et (v_0, a, v_1) celle de v, alors $u_0 \equiv_{n-1} v_0$ et $u_1 \equiv_n v_1$.

  - Pour un entier d donné, on définit $u \equiv_n^d v$ si, et seulement si $\overline{u} \equiv_n \overline{v}$.

- ## Décomposition gauche

  Soit $u \in A^*$ un mot, et a une lettre apparaissant dans u. La a-décomposition gauche de u est l'unique triplet (u_0, a, u_1) tel que $u = u_0 a u_1$ et a n'apparaît pas dans u_0.

- ## Relation $\equiv_n$

  Soient $u, v \in A^*$ deux mots. On a alors $u \equiv_0 v$.
  De plus, $u \equiv_n v$ si, et seulement si, les conditions suivantes sont satisfaites:

  1. $\alpha(u) = \alpha(v)$
     Et pour chaque a apparaissant dans u,
  2. si (u_0, a, u_1) est la a-décomposition gauche de u et (v_0, a, v_1) celle de v, alors $u_0 \equiv_n v_0$ et $u_1 \equiv_{n-1} v_1$.
  3. si (u_0, a, u_1) est la a-décomposition droite de u et (v_0, a, v_1) celle de v, alors $u_0 \equiv_{n-1} v_0$ et $u_1 \equiv_n v_1$.

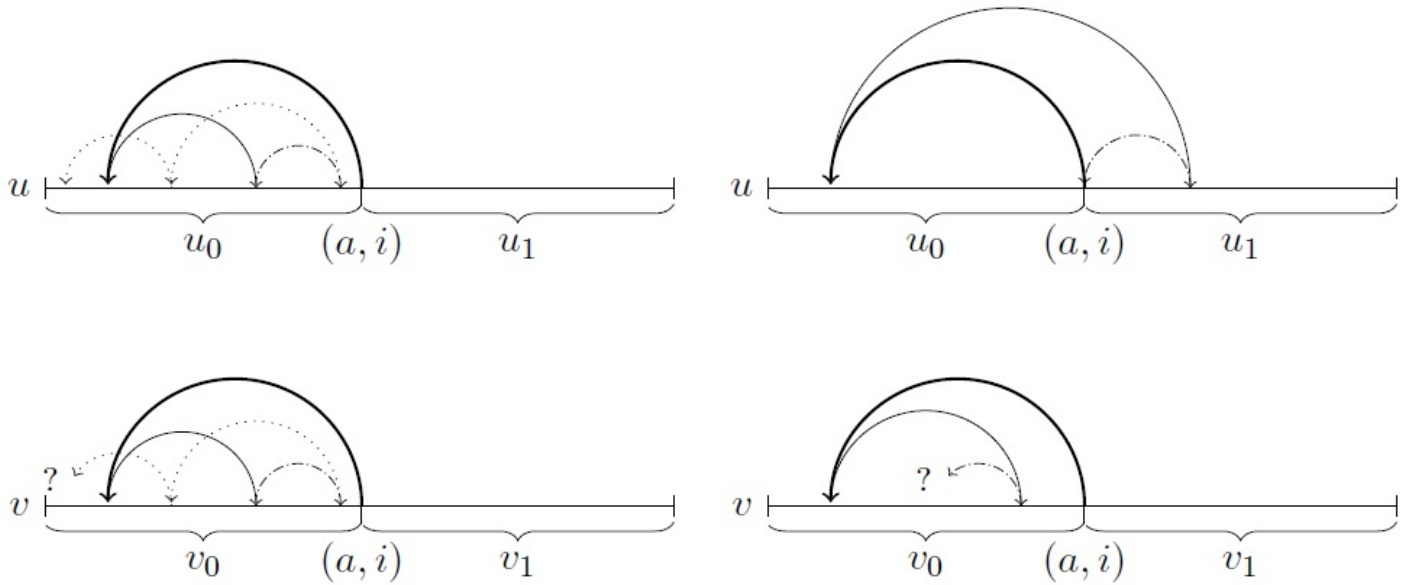
  - Pour un entier d donné, on définit $u \equiv_n^d v$ si, et seulement si $\overline{u} \equiv_n \overline{v}$.
  - Les relations $\equiv_n$ et $\equiv_n^d$ sont des congruences.

Jeux d'Ehrenfeucht-Fraïssé

- **Théorème**
  Soient $u, v \in A^*$ deux mots. Si $u \not\equiv_n^d v$ alors il existe une formule de $\mathbf{FO}^2[<, \mathbf{MOD}_d]$ de profondeur de quantificateur au plus $n + |\alpha(\overline{u})|$ qui sépare u et v.

Jeux d'Ehrenfeucht-Fraïssé

- **Théorème**
  Soient $u, v \in A^*$ deux mots. Si $u \not\equiv_n^d v$ alors il existe une formule de $\mathbf{FO}^2[<, \mathbf{MOD}_d]$ de profondeur de quantificateur au plus $n + |\alpha(\overline{u})|$ qui sépare u et v.



-

Congruence et opérations algébriques

- Relations de Green sur le semigroupe stable

  Soit $h : A^* \to M$ un timbre et S son semigroupe stable. Pour tout x, y dans M, on définit :

$$x \leqslant_{\mathcal{R}_{st}} y \text{ si, et seulement si } xM \cap S \subseteq yM \cap S$$

Congruence et opérations algébriques

- Relations de Green sur le semigroupe stable

  Soit $h : A^* \to M$ un timbre et S son semigroupe stable. Pour tout x, y dans M, on définit :

  $$x \leqslant_{\mathcal{R}_{st}} y \text{ si, et seulement si } xM \cap S \subseteq yM \cap S$$

  - On définit également de la même façon $\leqslant_{\mathcal{L}_{st}}$, $\leqslant_{\mathcal{H}_{st}}$, et les relations $\mathcal{R}_{st}$, $\mathcal{L}_{st}$ et $\mathcal{H}_{st}$.

Les timbres *length faithful*

- Définition

  Soit $h : A^* \to M$ un timbre et S son semigroupe stable.
  h sera dit *length faithful* si, et seulement si, $h^{-1}(S^1) = (A^d)^*$.

Les timbres *length faithful*

- **Définition**
  Soit $h : A^* \to M$ un timbre et S son semigroupe stable.
  h sera dit *length faithful* si, et seulement si, $h^{-1}(S^1) = (A^d)^*$.

- **Propriété**
  Soit h un timbre et d son indice de stabilité. Alors le timbre

$$\begin{aligned} h' : A^* &\to M \times \mathbb{Z}/d\mathbb{Z} \\ u &\to (h(u), |u| \bmod d) \end{aligned}$$

  est length faithful.

- **Propriété**

  Soit $h : A^* \to M$ un timbre length faithful et soit S son semigroupe stable et soit $\mathcal{X} \in \{\mathcal{R}, \mathcal{L}, \mathcal{H}\}$.
  Alors la restriction de $\leqslant_{\mathcal{X}_{st}}$ (et $\mathcal{X}_{st}$) à S est exactement la relation de Green restreinte au semigroupe S.

- **Propriété**

  Soit $h : A^* \to M$ un timbre length faithful et soit S son semigroupe stable et soit $\mathcal{X} \in \{\mathcal{R}, \mathcal{L}, \mathcal{H}\}$.
  Alors la restriction de $\leqslant_{\mathcal{X}_{st}}$ (et $\mathcal{X}_{st}$) à S est exactement la relation de Green restreinte au semigroupe S.

- **Théorème**

  Soit $h : A^* \to M$ un timbre length faithful de **QDA** et soit d son indice de stabilité.
  Alors il existe un entier n tel que pour tout couple de mots u et v, si $u \equiv_n^d v$ alors $h(u) = h(v)$.

Conclusion et développements

- Décidabilité de $\mathbf{FO}^2[<, \mathbf{MOD}]$
- Dans la continuité d'autres résultats comme $\Sigma_1[<, MOD]$, $FO[<, MOD]$.

Conclusion et développements

- Décidabilité de $\mathbf{FO}^2[<, \mathbf{MOD}]$
- Dans la continuité d'autres résultats comme $\Sigma_1[<, MOD]$, $FO[<, MOD]$.
- Vers un théorème général?
- Piste: le théorème des catégories dérivées de Tilson.

Merci.