Normalisation quadratique dans les monoïdes

Patrick Dehornoy

LMNO (Caen) & IRIF (Paris)

Journées IRIF, octobre 2017

- Travail en commun avec Yves Guiraud, à partir d'une idée de Daan Krammer
- Un cadre général pour la construction de formes normales dans des monoïdes, englobant la normalisation de Garside
- Approche alternative par Viktoriya Ozornova et Alexander Hess

Plan :

- 1. Normalisation quadratique
- 2. Normalisation de classe (4,3) et règle du domino
- 3. Problème de terminaison

Plan :

- 1. Normalisation quadratique
- 2. Normalisation de classe (4,3) et règle du domino
- 3. Problème de terminaison

- Notation : S^* pour l'ensemble des mots sur S (monoïde libre),
  et $|$ pour la concaténation.

- Définition : Si M est un monoïde engendré par une famille S,
  une forme normale pour (M, S) est une section pour l'évaluation ev : $S^* \to M$.

Une forme normale NF est géodésique si

$$\forall w \ (\|\mathrm{NF}(\mathrm{ev}(w))\| \leqslant \|w\|).$$

- But (vague) : Étudier les formes normales géodésiques...

- Option technique : Travailler avec les mots
  - au lieu de NF : $M \to S^*$, considérer $N : S^* \to S^*$ où $N(w) = \mathrm{NF}(\mathrm{ev}(w))$.

- Exemple : M monoïde abélien libre de base S ; $<$ ordre total sur S ;
  $\mathrm{NF}(g) :=$ le représentant $<^{\mathrm{Lex}}$-nondécroissant de g ;
  $N^{\mathrm{Lex}}(w) :=$ le mot $<^{\mathrm{Lex}}$-nondécroissant obtenu par permutation des lettres de w.

• <u>Définition</u> : Une normalisation est une paire (S, N) avec $N : S^* \to S^*$ satisfaisant :
(i) $N(s) = s$ pour $s \in S$,
(ii) $\|N(w)\| = \|w\|$ pour tout w,
(iii) $N(u|v|w) = N(u|N(v)|w)$ pour tous u, v, w.
On dit que (S, N) est une normalisation pour un monoïde M si

$$M = \langle S \mid \{w = N(w) \mid w \in S^*\}\rangle^+.$$

• <u>Fait</u> : Si (S, N) est une normalisation pour M, on obtient une forme normale pour (M, S) en posant

$$\mathrm{NF}(g) = N(w) \text{ pour } w \text{ quelconque représentant } g.$$

Inversement, si NF est une forme normale pour (M, S) *et que les éléments de M ont une S-longueur unique* (i.e., M est gradué et les éléments de S ont degré 1), on obtient une normalisation (S, N) pour M en posant

$$N(w) = \mathrm{NF}(\mathrm{ev}(w)).$$

• <u>Exemple</u> : monoïde abélien libre et normalisation lexicographique.

• <u>Définition</u> : Si (S, N) est une normalisation, un élément e de S est N-neutre si

$$\forall w\ (N(w|e) = N(e|w) = N(w)|e).$$

On dit que (S, N) est une normalisation mod e pour M si e est N-neutre et

$$M = \langle S \mid \{w = N(w) \mid w \in S^*\} \cup \{e = 1\}\rangle^+.$$

• <u>Proposition</u> : *Si (S, N) est une normalisation mod e pour un monoïde M, on obtient une forme normale géodésique pour $(M, S\backslash\{e\})$ en posant*

$$NF(g) = \pi_e(N(w)) \quad \textit{pour } w \textit{ quelconque représentant } g,$$

où $\pi_e : S^* \to (S\backslash\{e\})^*$ est l'oubli de e.
Inversement, si NF est une forme normale géodésique sur (M, S), on obtient une normalisation $(S \cup \{e\}, N)$ mod e pour M en posant

$$N(w) = NF(ev(w))|e^m \quad \textit{avec } m = \|w\| - \|NF(ev(w))\|.$$

• <u>Exemple</u> : $M = B_n^+$, $S = \mathrm{Div}(\Delta_n)$, et

$$N(s_1|\cdots|s_p) = (s_1'|\cdots|s_q'|1|\cdots|1),$$

avec $(s_1'|\cdots|s_q')$ forme normale de Garside de $s_1 \cdots s_p$.
Id. pour tout monoïde M simplifiable à gauche et toute famille de Garside S de M.

• <u>Définition</u> : Une normalisation (S, N) est quadratique si
(i) Un mot w est N-normal (=fixe par N) ssi tout facteur de w de longueur 2 l'est,
(ii) On peut passer de w à $N(w)$ par une suite finie de normalisations de facteurs de longueur 2.

• <u>Exemple</u> : (S, N^{Lex}) est quadratique : un mot est $<^{\mathrm{Lex}}$-nondécroissant ssi tout facteur de longueur 2 l'est, et on peut passer de w à $N^{\mathrm{Lex}}(w)$ en échangeant des lettres adjacentes.

• <u>Exemple</u> : (S, N^{Gar}) est quadratique : un mot est S-normal ssi tout facteur de longueur 2 l'est, et on peut passer de w à $N^{\mathrm{Gar}}(w)$ en normalisant des lettres adjacentes : règle du domino.

• <u>Remarque</u> : (i) n'entraîne pas (ii), et (ii) n'entraîne pas (i).

- Notation : Pour (S, N) normalisation quadratique :

  $\overline{N} := N \upharpoonright S^{[2]}$,
  $\overline{N}_i := \overline{N}$ appliqué en position $i, i+1$ (à un mot de longueur $\geqslant i+1$),
  $\overline{N}_{i_1|\cdots|i_m} := \overline{N}_{i_m} \circ \cdots \circ \overline{N}_{i_1}$,
  $\overline{N}_{121\ldots[c]} := \overline{N}_{1|2|1|\ldots}$, longueur c.

- Si (S, N) est quadratique, alors, pour tout mot w,
  il existe une suite de positions u vérifiant $N(w) = \overline{N}_u(w)$.

En particulier, pour $\|w\| = 3$, les possibilités sont $u = 121\ldots[c]$ ou $u = 212\ldots[c]$.

- Définition : Une normalisation quadratique (S, N) est de classe à gauche c si

$$\forall w \in S^{[3]} \ (N(w) = \overline{N}_{121\ldots[c]}(w)).$$

... classe à droite c ... $\overline{N}_{212\ldots[c]}(w))$ ...
... classe (c, c') pour classe à gauche c et classe à droite c'.

- Exemple : (S, N^{Lex}) est de classe $(3, 3)$:

$$\forall w \in S^{[3]} \ (N^{\mathrm{Lex}}(w) = \overline{N}_{121}(w) = \overline{N}_{212}(w)).$$

- Exemple : (S, N^{Gar}) est de classe $(4, 3)$:

$$\forall w \in S^{[3]} \ (N^{\mathrm{Gar}}(w) = \overline{N}_{1212}(w) = \overline{N}_{212}(w)).$$

- Exemple : (S, N_*^{Lex}) est de classe $(3 + \lfloor \log_2(\#S) \rfloor, 3 + \lfloor \log_2(\#S) \rfloor)$:

$$N^{\mathrm{Lex}}(s|t) := t|s \text{ pour } s > t, \qquad \text{et } s|t \text{ sinon,}$$

$$N_*^{\mathrm{Lex}}(s|t) := \lceil (s+t)/2 \rceil | \lfloor (s+t)/2 \rfloor \text{ pour } s > t, \qquad \text{et } s|t \text{ sinon.}$$

- Lemme : Si (S, N) est de classe à gauche c, alors
  - (S, N) est de classe à gauche c' pour tout $c' \geqslant c$;
  - (S, N) est de classe à droite c'' pour tout $c'' \geqslant c + 1$.

- Démonstration :

  D'abord $\overline{N}_{121\ldots[c]}(w) = \overline{N}_{121\ldots[c+1]}(w)$.

  Ensuite $N(w) = N(\overline{N}_2(w) = \overline{N}_{121\ldots[c]}(\overline{N}_2(w)) = \overline{N}_{212\ldots[c+1]}(w)$. □

- Lemme : Une normalisation (S, N) est de classe à gauche c ssi $\overline{N}$ vérifie

$$\overline{N}_{121\ldots[c]} = \overline{N}_{121\ldots[c+1]} = \overline{N}_{212\ldots[c+1]}.$$

Une normalisation (S, N) est de classe (c, c) ssi $\overline{N}$ vérifie

$$\overline{N}_{121\ldots[c]} = \overline{N}_{212\ldots[c]}.$$

Plan :

- 1. Normalisation quadratique
- 2. Normalisation de classe (4,3) et règle du domino
- 3. Problème de terminaison

• Lemme : Une normalisation quadratique (S, N) est de classe $(4, 3)$ ssi la règle du domino est valide pour (S, N) :

$$\begin{tikzcd} \cdot \arrow[r, "s'_1"] \arrow[d, "t_0"'] & \cdot \arrow[r, "s'_2"] \arrow[d, "t_1"] & \cdot \arrow[d, "t_2"] \\ \cdot \arrow[r, "s_1"'] & \cdot \arrow[r, "s_2"'] & \cdot \end{tikzcd}$$

où $\xrightarrow{\;s\;}\xrightarrow{\;t\;}$ signifie «$s|t$ est N-normal».

• Application : Si S est une famille de Garside, alors (S, N^{Gar}) est de classe $(4, 3)$,
… et même de classe $(3, 3)$ si la règle du domino 2 est aussi valide.
↑
vrai en particulier si S est bornée (i.e., s'il existe un Δ)

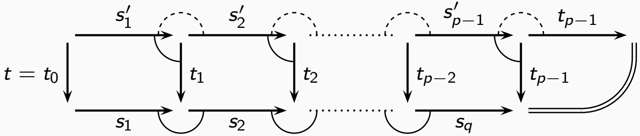
- Proposition : Si (S, N) est de classe $(4, 3)$, alors pour tout mot w de $S^{[p]}$, on a

$$N(w) = \overline{N}_{\delta_p}(w),$$

avec $\delta_2 = 1$, $\delta_3 = 212$, $\delta_4 = 323123$, $\delta_5 = 4342341234$, etc.

- Démonstration : Induction par la règle du domino,

$$N(t|w) = \overline{N}_{12\,\cdots\,(p-1)}(N(w)) :$$



□

• Théorème 1 : *Si* (S, N) *est de classe* $(4, 3)$*, alors la fonction* $\overline{N}$ *satisfait*

$$\overline{N}_{212} = \overline{N}_{1212} = \overline{N}_{2121}.$$

Réciproquement, si $F : S^{[2]} \to S^{[2]}$ *vérifie*

$$F_{212} = F_{1212} = F_{2121},$$

alors il existe une unique normalisation (S, N) *de classe* $(4, 3)$ *vérifiant* $\overline{N} = F$*.*

• Démonstration : calcul dans le monoïde d'Artin–Krammer associé à la "matrice de Cartan"

$$\begin{pmatrix} 1 & 4 & 2 & & & \\ 3 & 1 & 4 & \ddots & & \\ 2 & 3 & \ddots & \ddots & \ddots & \\ & \ddots & \ddots & \ddots & 4 & 2 \\ & & \ddots & 3 & 1 & 4 \\ & & & 2 & 3 & 1 \end{pmatrix}$$

□

• Remarque : Faux en général : il existe $F : S^{[2]} \to S^{[2]}$ vérifiant $F_{12121} = F_{21212}$ et ne pouvant être étendu en une normalisation (S, N) de classe vérifiant $\overline{N} = F$.

• Théorème 2 : *Si M est un monoïde simplifiable à gauche et S est une famille de Garside de M, alors (S, N^{Gar}) est de classe $(4,3)$ et est chargée à gauche.*

$$\uparrow$$

$$\forall s, t, s', t' \ (s'|t' = N^{Gar}(s|t) \Longrightarrow s \text{ divise } s' \text{ à gauche dans } M).$$

Réciproquement, si (S, N) est une normalisation de classe (4,3) chargée à gauche, alors S est une famille de Garside dans M et on a $N = N^{Gar}$.

• Démonstration : règle du domino + caractérisations des familles de Garside. $\square$

Plan :

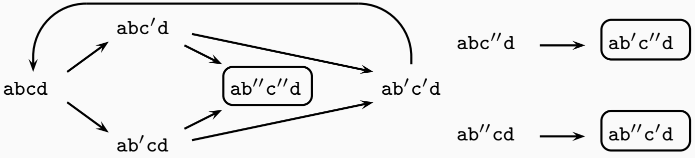
- 1. Normalisation quadratique
- 2. Normalisation de classe (4,3) et règle du domino
- 3. Problème de terminaison

- Normalisation (S, N) $\rightsquigarrow$ système de réécriture :
règles $s|t \to \overline{N}(s|t)$ quand $\overline{N}(s|t) \neq s|t$.

- Par construction : système normalisant : $\forall w\ \exists w'$normal $(w \to^* w')$,
et confluent : $\forall w, w', w''\ ((w \to^* w'$ et $w \to^* w'') \Rightarrow \exists w'''\ (w' \to^* w'''$ et $w'' \to^* w'''))$.
Mais, est-il terminant : <u>toute</u> suite de réécritures est-elle finie ?

- <u>Proposition</u> : *Il existe une normalisation de classe (4,4) non terminante.*

- Démonstration : $\mathtt{ab} \to \mathtt{ab'}$, $\mathtt{cd} \to \mathtt{c'd}$, $\mathtt{bc'} \to \mathtt{b''c''}$, $\mathtt{b'c} \to \mathtt{b''c''}$, $\mathtt{b'c'} \to \mathtt{bc}$.



$\square$

• Proposition : *Toute normalisation de classe (3,3) est terminante : toute suite de normalisations à partir d'un mot de longueur p a une longueur au plus $p(p-1)/2$.*

• Démonstration :

Claim : Si $\overline{N}_u(w)$ définit une suite de réécritures (donc t.q. deux mots consécutifs sont distincts), alors u est réduit (au sens des groupes de Coxeter).

Preuve par induction sur $\|u\|$.

Supposons u réduit et $u|i$ non réduit.

Par le lemme de Matsumoto, il existe u' vérifiant $u \equiv_{121=212} u'|i$.

Alors $\overline{N}_{u|i}(w) = \overline{N}_{u'|i|i}(w)$, d'où $\overline{N}_{u|i}(w) = \overline{N}_u(w)$,

et $\overline{N}_{u|i}(w)$ ne définit pas une suite de réécritures.

Donc la longueur maximale d'une suite de réécritures est

$\leqslant$ la longueur maximale d'un mot réduit sur $1, \ldots, p-1$, soit $p(p-1)/2$. □

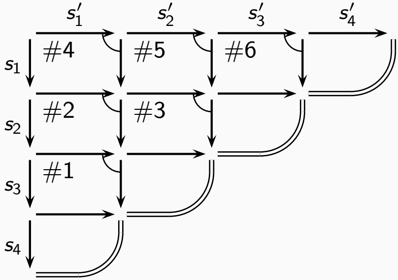
• <u>Théorème 3</u> : *Toute normalisation de classe (4,3) est terminante : toute suite de normalisations à partir d'un mot de longueur p a une longueur au plus $2^p - p - 1$.*

• <u>Remarque</u> : Le «monoïde de Coxeter-Krammer» est infini, donc on ne peut pas l'utiliser à la place du groupe symétrique.

• Démonstration :

Principe : À cause du domino, on progresse inévitablement vers la forme normale.

Cœur : Attacher à chaque mot d'une suite de réécritures un chemin dans une grille de normalisation du type suivant :



• Théorème 3 : *Toute normalisation de classe (4,3) est terminante : toute suite de normalisations à partir d'un mot de longueur p a une longueur au plus $2^p - p - 1$.*

• Démonstration (suite) :

Induction sur p. Supposons $w_0, w_1, w_2, \ldots$ suite de réécritures avec $\|w_0\| = p$.
On attache à w_i un chemin dans la grille pour la taille p,
i.e., on attache à chaque lettre une direction $\downarrow$ ou $\rightarrow$.
Pour $w = s_1|\cdots|s_p$, on part de $s_1{\downarrow}|s_2{\downarrow}|\cdots|s_{p-1}{\downarrow}|s_p{\rightarrow}$.
Quatre types de normalisations a priori possibles : $\rightarrow\rightarrow$, $\rightarrow\downarrow$, $\downarrow\downarrow$, $\downarrow\rightarrow$.
Or $\rightarrow\rightarrow$ et $\rightarrow\downarrow$ sont impossibles, car la règle du domino entraîne que
tous les sous-mots $\rightarrow\rightarrow$ et $\rightarrow\downarrow$ sont normaux.
Chaque $\downarrow\rightarrow$ fait traverser un carré de la grille, donc $\leqslant p(p-1)/2$ telles étapes.
Entre deux $\downarrow\rightarrow$, les $\downarrow\downarrow$ concernent des sous-mots de longueur $\leqslant p - 1$.
Donc, si $F(p) :=$ longueur maximale d'une suite de réécritures sur $S^{[p]}$,

$$F(p) \leqslant \frac{p(p-1)}{2} + \left(\frac{p(p-1)}{2} + 1\right) F(p-1).$$

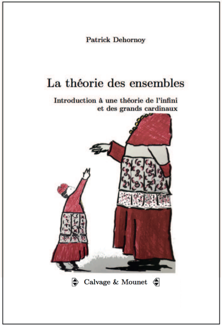
(et on peut être plus soigneux). □

• Corollaire 1 : *Toute normalisation Garside est terminante : toute suite de normalisations à partir d'un mot de longueur p a une longueur au plus $2^p - p - 1$.*

• Corollaire 2 : *Tout monoïde d'Artin–Tits finiment engendré a une présentation convergente finie.*

• Démonstration :
(D.–Dyer–Hohlweg) Tout monoïde d'Artin–Tits finiment engendré
admet une famille de Garside finie.
Si S est une famille de Garside pour un monoïde M,
alors M est présenté par les relations $s|t = N^{\mathrm{Gar}}(s|t)$ pour s, t dans S,
(et par les relations $s|t = st$ pour s, t, et st dans S).
Par le théorème, la normalisation associée est convergente. □

- P. Dehornoy, Y. Guiraud, *Quadratic normalisation in monoids*, Int. J. Alg. Comput. 26-5 (2016) 935-972
- A. Hess, V. Ozornova, *Factorability, string rewriting and discrete Morse theory* arXiv:1412.3025
- D. Krammer, *An asymmetric generalisation of Artin monoids*, Groups Complex. Cryptol. **5** (2013) 141–168.
- P. Dehornoy, La théorie des ensembles, Calvage & Mounet (2017)



//dehornoy.users.lmno.cnrs.fr/