Sur les systèmes de formes normales pour représenter efficacement des fonctions multi-valuées

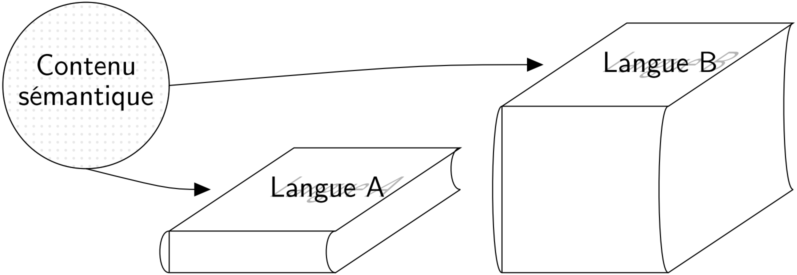
Pierre Mercuriali
sous la direction de
Miguel Couceiro & Romain Péchoux
Équipes Orpailleur & Mocqua

Loria
Laboratoire lorrain de recherche en informatique et ses applications

UNIVERSITÉ DE LORRAINE

Représentations

Représentations différentes pour un même contenu sémantique :



- Mesures d'efficacité : temps, espace, etc.
- Algorithmes (synthèse, simplification)
- Circuits : [Jukna, 2012]

Fonctions Booléennes et clones Booléens

Définition (Fonction Booléenne)

$f \ : \ \{0,1\}^n \to \{0,1\}$

Exemple

Projections $\pi_i^{(n)}$, médiane $\mathtt{m}(x,y,z) = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$

Définition (Composition de classes de fonctions)

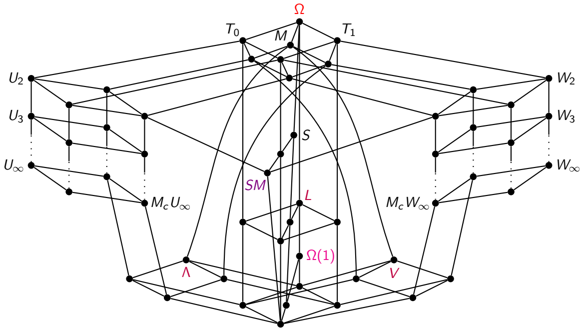
$\mathcal{I} \circ \mathcal{J} = \{f(g_1, \ldots, g_n) \mid f \in \mathcal{I}, g_i \in \mathcal{J} \text{ d'arité } m\}$

Définition (Clone Booléen)

Classe $\mathcal{C}$ de fonctions Booléennes telle que

- $\mathcal{C} \circ \mathcal{C} = \mathcal{C}$
- $\{\pi_i^{(n)} \mid n \in \mathbb{N}, i \leq n\} \subseteq \mathcal{C}$

Treillis de Post ([Post, 1941])



- Ω, clone de toutes les fonctions Booléennes
- Ω(1), littéraux et constantes
- Λ, conjonctions, et V, disjonctions, et L, fonctions affines
- SM, fonctions auto-duales et monotones

Factorisation de clones

[Couceiro et al., 2006]

- Description exhaustive de la factorisation de clones Booléens
- Factorisations irréductibles du clone des fonctions Booléennes
- Certaines factorisations correspondent à des systèmes usuels
  - Structure séquentielle $\rightarrow$ notion de forme normale

Exemple

- DNF : $\Omega = V_c \circ \Lambda_c \circ I^*$ et CNF : $\Omega = \Lambda_c \circ V_c \circ I^*$
- PNF : $\Omega = L_c \circ \Lambda_c \circ I$ et PNF^d : $\Omega = L_c \circ V_c \circ I$
- MNF : $\Omega = SM \circ \Omega(1)$

Motivation

MNF : *Median normal form*, basée sur la médiane

Théorème ([Couceiro et al., 2006])

- DNF, CNF, PNF, PNF^d incomparables
- MNF strictement plus efficace que les DNF, CNF, PNF, PNF^d

Contraintes fortes :

- Arité des connecteurs fixée
- Factorisations irréductibles

Question

Et si on relâche ces contraintes ?

Problèmes

Question

Comment mesurer l'efficacité d'un NFS ?
Comment comparer des NFSs ?

Question

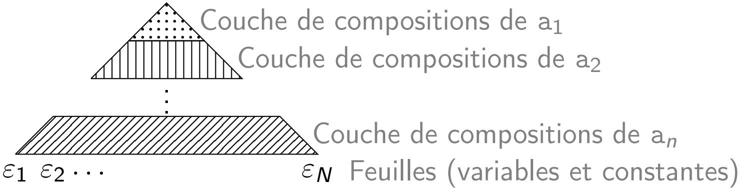
Existe-t-il des NFS minimaux ? Optimaux ?

Question

Dans un NFS, une formule donnée est-elle minimale ?
Quelle est la complexité de ce problème ?

Cadre typique : formules médianes dans le MNF.

Système de termes stratifiés



Définition (Système de formes normales)

Ensemble de termes stratifiés $T(a_1 \dots a_n)$, tel que

- $[T(a_1 \dots a_n)] = \Omega$, ($[T]$: interprétations)
- non-redondant

Exemple

DNF, $T(\vee \wedge \neg)$; CNF, $T(\wedge \vee \neg)$, etc.

Complexité d'un NFS

Définition (*Taille* d'un terme t)

$$|t| = \sum_{\alpha \in \Omega \setminus \{0,1,\neg\}} |t|_\alpha$$

Définition (*Complexité de f relativement à T*)

$$C_T(f) = \min\{|t| \colon t \in T,\ [t] = f\}$$

T un ensemble de termes, $f \in [T] \subseteq \Omega$

Exemple (Représentation de la médiane)

- $\mathtt{m}(x, y, z)$ dans $T(\mathtt{m}\neg)$: taille 1
- $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$ dans $T(\vee \wedge \neg)$: taille 5

Comparaison de NFSs

T, S deux ensembles de termes tels que $[S] \subseteq [T]$;

Définition ($T \preceq S$)

Il existe un polynôme $P \in \mathbb{N}[X]$ tel que
$\forall f \in [S],\ C_T(f) \leq P(C_S(f))$

Définition (Notations)

- Incomparabilité ($T \parallel S$) : $T \not\preceq S$ et $S \not\preceq T$
- Efficacité stricte ($T \prec S$) : $T \preceq S$ et $S \not\preceq T$
- Équivalence ($T \sim S$) : $T \preceq S$ et $S \preceq T$

Théorème ([Couceiro et al., 2006])

- $\forall \mathrm{A}, \mathrm{B} \in \{\mathrm{CNF}, \mathrm{DNF}, \mathrm{PNF}, \mathrm{PNF}^{\mathrm{d}}\}$, $\mathrm{A} \neq \mathrm{B} \rightarrow \mathrm{A} \parallel \mathrm{B}$
- $\mathrm{MNF} \prec \mathrm{CNF}, \mathrm{DNF}, \mathrm{PNF}, \mathrm{PNF}^{\mathrm{d}}$

Outil de comparaison de NFSs : réductions

Avec $A = T(\mathrm{a})$, et $B = T(\mathrm{b})$ tels que $[A] \subseteq [B]$

Définition (Réduction linéaire de A vers B)

$A \sqsupseteq B$ si il existe un terme $t \in T(b)$ tel que

$$\mathrm{a}(x_1, \ldots, x_n) \equiv t \quad \text{et} \quad \forall i, |t|_{x_i} = 1$$

Exemple (UNF $\sqsupseteq$ MNF)

Avec $\mathtt{u}(x_1, x_2, x_3) := (x_1 \vee x_2) \wedge x_3$:

$$\mathtt{u}(x_1, x_2, x_3) \equiv \mathtt{m}(\mathtt{m}(x_1, 1, x_2), 0, x_3)$$

Proposition

$$\sqsupseteq \; \subseteq \; \succeq$$

Réductions universelles quasi-linéaires

Définition

$A \sqsupseteq_\forall B$ si pour tout $j \in \{1, \ldots, n\}$, il existe $t_j \in T(\mathrm{b})$ tel que

$$\mathrm{a}(x_1, \ldots, x_n) \equiv t_j \quad \text{et} \quad |t_j|_{x_j} = 1$$

Exemple (MNF $\sqsupseteq_\forall$ UNF)

$$\mathtt{m}(x_1, x_2, x_3) \equiv \mathtt{u}(\mathtt{u}(x_1, 0, x_2), \mathtt{u}(x_1, x_2, x_3), 1)$$
$$\mathtt{m}(x_1, x_2, x_3) \equiv \mathtt{u}(\mathtt{u}(x_2, 0, x_3), \mathtt{u}(x_2, x_3, x_1), 1)$$
$$\mathtt{m}(x_1, x_2, x_3) \equiv \mathtt{u}(\mathtt{u}(x_3, 0, x_1), \mathtt{u}(x_3, x_1, x_2), 1)$$

Réductions existentielles quasi-linéaires

Définition

$A \sqsupseteq_\exists B$ s'il existe $t \in T(\mathrm{b})$ tel que

$$\mathrm{a}(x_1, \ldots, x_n) \equiv t \quad \text{et} \quad \exists j \in \{1, \ldots, n\}, |t|_{x_j} = 1$$

Exemple (SNF $\sqsupseteq_\exists$ MNF)

Avec $\mathtt{s}(x_1, x_2, x_3) := (x_1 \wedge x_2) \vee (\neg x_1 \wedge x_3)$:

$$\mathtt{s}(x_1, x_2, x_3) \equiv \mathtt{m}(\mathtt{m}(x_1, 0, x_2), 1, \mathtt{m}(\neg x_1, 0, x_3))$$

Remarque

$$\sqsupseteq \subset \sqsupseteq_\forall \subset \sqsupseteq_\exists$$

Propriétés des réductions

Théorème (Mercuriali et al., TCS 2020)

$$\sqsupseteq_\forall \subseteq \succeq$$

Théorème

$$\mathsf{MNF} \sim \mathsf{MNF}_5$$

Preuve :

$$\mathtt{m}(x_1, x_2, x_3) = \mathtt{m}_5(0, 1, x_1, x_2, x_3)$$

$$\mathtt{m}_5(x_1, x_2, x_3, x_4, x_5) = \mathtt{m}(\mathtt{m}(\mathtt{m}(x_2, x_3, x_4), x_4, x_5), \mathtt{m}(x_2, x_3, x_5), x_1)$$

Preuve de l'inclusion $\sqsupseteq_\forall \subseteq \succeq$

Proposition (Mercuriali et al., TCS 2020)

Si $A = T(\mathtt{a})$ et $B = T(\mathtt{b})$ alors

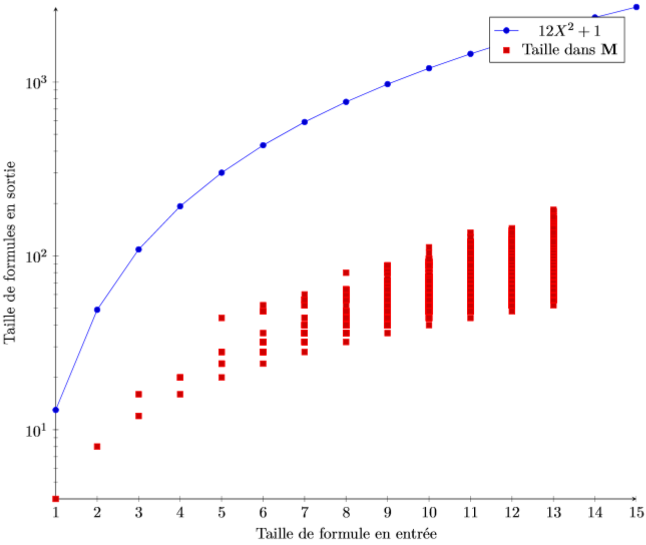
$$\forall f \in [A], \quad C_B(f) \leq nk(C_A(f))^q + 1$$

où $n := \mathrm{ar}(\mathtt{b})$, $k := \max_i\{|t_i|_{\mathtt{b}}\}$, et $q := \max_{i,j}\{|t_i|_{x_j}\}$

Algorithme de conversion efficace :

- Conversion par récurrence de termes d'un NFS à un autre
- Minimisation de la taille des sous-termes déjà convertis
- Majoration polynomiale explicite

Exemple (Conversion entre MNF et MNF_5)



Restriction du champ de recherche

Théorème (Mercuriali et al., TCS 2020)

Si $T(\mathrm{a}_1 \ldots \mathrm{a}_n)$ est un NFS avec $n \geq 2$, alors $\forall i,\ [\mathrm{a}_i] \in V \cup L \cup \Lambda$

Exemple

$T(\wedge \vee \neg)$, $T(\vee \wedge \neg)$, $T(\oplus\wedge)$, $T(\oplus\vee)$.

Théorème (Mercuriali et al., TCS 2020)

Si $T(\mathrm{a}_1 \ldots \mathrm{a}_n)$ est un NFS et que $\forall i,\ [a_i] \in \Omega \backslash \Omega(1)$, alors $n \leq 2$

Ces résultats découlent en partie de la non-redondance.

NFS (monotone) optimal

Définition (NFS monotone)

$T(\mathtt{a}_1 \cdots \mathtt{a}_n)$ est dit *monotone* si tous les $[\mathtt{a}_i]$ sont des fonctions croissantes ou décroissantes en chaque argument

Exemple

$\mathsf{MNF} = T(\mathtt{m}\neg)$

Contre-exemple

$\mathsf{PNF} = T(\oplus\wedge)$

Définition (NFS monotone optimal)

- Minimal pour $\preceq$
- pour tout NFS monotone B, $A \prec B$

Optimalité du MNF

Théorème (Mercuriali et al., TCS 2020)

Le MNF est optimal parmi les NFSs monotones.

Principe de la preuve :

- Système de décomposition médiane

$$f(x_1, \ldots, x_n) \equiv \mathtt{m}(x_1, f(1, x_2, \ldots, x_n), f(0, x_2, \ldots, x_n))$$

- Algorithme pour produire des formes normales médianes
- L'algorithme permet d'obtenir des réductions universelles

NFSs optimaux

Théorème (Mercuriali et al., TCS 2020)

Les NFSs monotones de la forme $T(\mathrm{a})$ ou $T(\mathrm{a}\neg)$ sont optimaux.

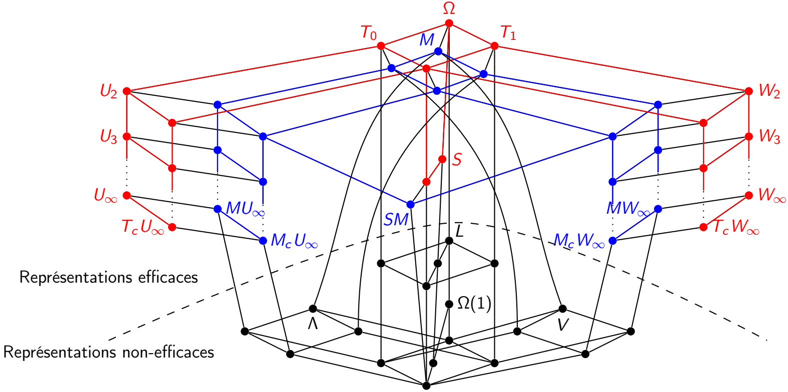
Principe de la preuve :

- Description exhaustive des compositions $\mathcal{C}_1 \circ \mathcal{C}_2 = \Omega$
- Démonstration "clone par clone"

Remarque

Pas besoin d'ajouter des connecteurs pour être optimal !

Situer les NFSs optimaux sur le treillis de Post



Résultat : Noir $\succ$ Bleu $\succeq$ Rouge

NFSs non-optimaux (généralisation)

$\mathcal{C}([\mathrm{a}])$: le clone généré par le connecteur a

Théorème (Mercuriali et al., TCS 2020)

Si $\mathcal{C}([\mathrm{a}]) = \Lambda_{\mathrm{c}}$, et $\mathcal{C}([\mathrm{b}]) = \bigvee_{\mathrm{c}}$, alors

$$T(\mathtt{ab}\neg) \sim \mathsf{CNF}$$

+ résultat similaire pour la DNF, PNF, PNF^d

Exemple

Utiliser $\wedge_5(x_1, x_2, x_3, x_4, x_5)$ ou $\wedge$ dans la DNF, CNF, etc. ne change pas l'efficacité des représentations

Résultats obtenus sur les NFSs

Question

Comment comparer des NFSs ?

- Calcul de l'efficacité d'un NFS
- Outil : réductions entre NFSs

Question

Existe-t-il des NFSs optimaux ?

- NFSs basés sur un seul connecteur non-trivial : plus efficaces
- NFSs monotones : équivalents à MNF
- MNF optimal parmi les NFSs monotones

Axiomatisation de la médiane

Domaine plus général : treillis (distributifs) et polynômes latticiels

$$
\begin{aligned}
&\mathtt{m}(x, y, z) \equiv \mathtt{m}(x, z, y) \equiv \mathtt{m}(z, x, y), && \text{(symétrie)}\\
&\mathtt{m}(x, x, y) \equiv x, && \text{(majorité)}\\
&\mathtt{m}(\mathtt{m}(x, u, v), \mathtt{m}(y, u, v), z) \equiv \mathtt{m}(\mathtt{m}(x, y, z), u, v), && \text{(distributivité)}\\
&\mathtt{m}(0, 1, x) \equiv x, &&
\end{aligned}
$$

Théorème (d'après [Birkhoff, 1940])

Le système ci-dessus est *correct* et *complet*.

Formes normales médianes minimales

Définition (Représentation structurelle)

$f \in T(\mathtt{m})$, $S_f = (n_0, \ldots, n_d) \in \mathbb{N}^d$ décroissante t.q.
n_i : nombre de médianes à profondeur $\leq i$

Cette représentation privilégie la parallélisation.

Définition (Ensemble de formes normales médianes minimales)

Pour $f \in T(\mathtt{m})$, $\{g \in T(\mathtt{m}) \mid g \equiv f, \forall g', S_g \leq_{lex} S_{g'}\}$

Exemple

$$\mathtt{m}(\mathtt{m}(x, x, y), y, z)$$

a pour ensemble de formes normales médianes minimales

$$\{\mathtt{m}(x, y, z), \mathtt{m}(x, z, y), \mathtt{m}(y, x, z), \mathtt{m}(y, z, x), \mathtt{m}(z, x, y), \mathtt{m}(z, y, x)\}$$

Problèmes similaires dans NP

Définition (PrimiSize (Taille d'implicant premier))

Entrée : $f \in T(\vee \wedge \neg)$, $k \in \mathbb{N}$;

Sortie : VRAI ssi f a un implicant premier de taille $\leq k$.

Définition (MinDNFSize (Taille de DNF))

Entrée : $f \in T(\vee \wedge \neg)$, $k \in \mathbb{N}$;

Sortie : VRAI ssi f a une DNF avec au plus k occurrences de variables.

Question

Une formule $f \in T(\mathtt{m})$ peut-elle être simplifiée ?

Problème complexe !

Simplification de formules médianes

Question

$f \in T(\mathtt{m})$ est-elle simplifiable ?

Sous-problème pour minorer la complexité :

Définition (MonotoneSmallmed)

Entrée : $f \in T(\mathtt{m}), S \in \mathbb{N}^n$;

Sortie : VRAI ssi $\exists g \equiv f$ telle que $S_g <_{lex} S$.

Théorème (Mercuriali et al., MVL 2019)

Monotone Smallmed appartient à la classe Σ_2^{P}.

- $\Sigma_2^{\mathrm{P}} = \{x \ : \ \exists c_1 \forall c_2 F(x, c_1, c_2)\}$, contient NP
- c_1,c_2 certificats de tailles polynomiales en la taille de x
- F fonction calculable en temps polynomial

Représentations de fonctions monotones

Proposition

$\exists f \in T(\mathtt{m}), f' \in T(\mathtt{m}\neg)$, tels que

- $f \equiv f'$
- $|f'| < |f|$

Exemple

- $f = \mathrm{m}(y, \mathrm{m}(u, v, t), \mathrm{m}(x, z, \mathrm{m}(u, v, t)))$
- $f' = \mathrm{m}(x, \mathrm{m}(\neg x, y, z), \mathrm{m}(u, v, t))$

Contributions

Question

Comment comparer des NFSs en fonction de leur efficacité ?

- Outil : réductions linéaires

Question

Existence et détermination de NFSs optimaux.

- NFSs optimaux ne nécessitent qu'un seul connecteur
- MNF optimale parmi les NFS monotones

Question

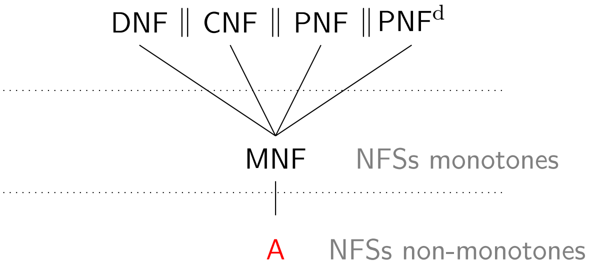
Dans un NFS, une formule donnée est-elle minimale ?

Application au MNF :

- Algorithmes explicites, problème modérément intractable

Conjecture

Pour un NFS non-monotone A de la forme $T(\mathrm{a})$ ou $T(\mathrm{a}\neg)$:



- Candidat : fonction de "Shannon" :

$$s(x, y, z) = (x \wedge y) \vee (\neg x \wedge z)$$

- Analogue au système de décomposition médiane

Ouvertures

Question (Efficacité des NFSs pour des fonctions multi-valuées)

Que dire des NFSs sur un ensemble $|L| > 2$?

- Cardinalité de l'ensemble des clones sur L : continuum
- Quelle description exhaustive de la composition de classes ?

Question (Circuits stratifiés)

A-t-on des résultats analogues sur les circuits stratifiés ?

- Différence : sharing
- [Jukna, 2012] : résultats de complexité, mais sans stratification
- [Amarù et al., 2018] : Minimisation expérimentale de circuits

Merci pour votre attention !

Publications

Journaux :

- MVL 2019 [Couceiro, Mercuriali, Péchoux, Saffidine]
- TCS 2020 [Couceiro, Lehtonen, Mercuriali, Péchoux]

Conférence :

- ISMVL 2017 [Couceiro, Mercuriali, Péchoux, Saffidine]

Workshops :

- LFA 2017 [Couceiro, Mercuriali, Péchoux]
- DICE 2018 [Couceiro, Lehtonen, Mercuriali, Péchoux, Soeken]

Bibliographie I

Amarù, L., Testa, E., Couceiro, M., Zografos, O., De Micheli, G., and Soeken, M. (2018).
Majority logic synthesis.
In *ICCAD 2018 - IEEE/ACM International Conference on Computer-Aided Design*, San Diego, United States.

Birkhoff, G. (1940).
Lattice theory, volume 25.
American Mathematical Soc.

Couceiro, M., Foldes, S., and Lehtonen, E. (2006).
Composition of Post classes and normal forms of Boolean functions.
Discrete mathematics, 306(24) :3223–3243.

Bibliographie II

Jukna, S. (2012).
Boolean function complexity : advances and frontiers, volume 27.
Springer Science & Business Media.

Post, E. L. (1941).
The Two-Valued Iterative Systems of Mathematical Logic.(AM-5), volume 5.
Princeton University Press.