Sur l'efficacité des systèmes de formes normales de fonctions Booléennes

Miguel Couceiro, Pierre Mercuriali, Romain Péchoux

Sur l'efficacité des systèmes de formes normales de fonctions Booléennes

On the efficiency of normal form systems of Boolean functions

M. Couceiro[1] P. Mercuriali[1] R. Péchoux[1]
[1] LORIA (CNRS - inria Nancy G.E. - Univ. Lorraine)
{miguel.couceiro, pierre.mercuriali, romain.pechoux}@loria.fr

Résumé :

Dans cet article, nous comparons différentes représentations des fonctions Booléennes à l'aide de systèmes de formes normales. Nous étendons les travaux de [3] sur l'étude asymptotique de l'efficacité des représentations produites par des systèmes de formes normales (*Normal Form Systems*–NFSs). Nous identifions certaines propriétés, comme l'associativité, la linéarité, la quasi-linéarité et la symétrie, qui nous permettent de comparer l'efficacité des NFSs correspondantes. Nous illustrons ces résultats en comparant des NFSs usuelles telles que la DNF, CNF, les représentations polynomiales, ainsi que la forme normale médiane (MNF) et celle dite de Sheffer (SNF). Nous obtenons en particulier que les NFSs générés par un seul connecteur sont polynomialement aussi efficace que ceux générés par plusieurs. La MNF, quand à elle, est aussi efficace que n'importe quel autre système.

Mots-clés :

Fonctions Booléennes, formes normales, médiane, représentations structurelles, représentations efficaces

Abstract:

In this paper we compare various normal form representations of Boolean functions. We extend the study of [3] pertaining to the comparison of the asymptotic efficiency of representations produced by normal form systems (NFSs). We identify some properties, such as associativity, linearity, quasi-linearity and symmetry, that allow the efficiency of the corresponding NFSs to be compared. We illustrate these results by comparing well-known NFSs such as the DNF, CNF, polynomial (PNF) representations, as well as the Median Normal Form (MNF) and Sheffer Normal Form (SNF). We obtain in particular that NFSs generated by a single connective are polynomially as efficient as those generated by several connectives. As for the MNF, it is as efficient as any other NFS.

Keywords:

Boolean functions, normal forms, median, structural representations, efficient representations

1 Introduction

Trouver des représentations en forme normale de fonctions Booléennes efficaces, ainsi que des procédures optimales pour construire ces représentations, demeure un sujet d'intérêt en ingénierie de circuits, ainsi qu'en fouille de données et en représentation des connaissances (voir, par ex., [7, 11, 15, 16]).

Les représentations en forme normale classiques de fonctions Booléennes, telles que les représentations en forme normale disjonctive (DNF), conjonctive (CNF), ou polynomiale (PNF), peuvent être vues comme des factorisations du clone [1] Ω de toutes les fonctions Booléennes en des compositions de clones minimaux. Ces faits ont été observés dans [3], où la notion de composition de classes a été examinée. La composition de deux clones peut résulter en un clone ou pas, ce qui a motivé l'étude de ce type de compositions et a abouti en une classification complète de toutes les paires de clones en ce sens. Cette classification a montré que chaque clone peut être factorisé en une suite de clones « premiers », ce qui a mené à toutes les factorisations possibles du clone de toutes les fonctions Booléennes en clones minimaux.

Ce résultat a donné lieu à des conséquences intéressantes. Par exemple, il induit un langage qui permet de formaliser la notion intuitive de forme normale (définie comme une factorisation non redondante d'Ω en clones premiers) et qui est capable d'exprimer d'une part les systèmes de formes normales classiques (DNF, CNF, et PNF), mais aussi la forme normale médiane (MNF) qui a un seul connecteur non trivial : la médiane m. De plus, ce cadre fournit un puissant formalisme dans lequel les comparaisons entre les différents systèmes de formes

1. Une classe contenant toutes les projections et fermée par composition.

normales (NFSs) peuvent être menées de façon rigoureuse.

L'étude comparative entre les NFSs classiques et le NFS médian a montré que ce dernier produit des représentations de complexité plus petite que les classiques. La complexité, ici, est mesurée en termes du nombre minimal de connecteurs non-triviaux utilisés pour représenter des fonctions. De plus, les NFSs classiques restent incomparables deux-à-deux. Ceci a ouvert la recherche de procédures algorithmiques pour produire les représentations médianes de fonctions Booléennes les plus efficaces, ce qui constitue un sujet de recherche actuel (voir, par ex., [2, 4]). Récemment, le problème consistant à déterminer si une formule médiane est optimale fut le sujet de [6], dans lequel il est démontré que le problème constant à déterminer si une fonction est en MNF est dans $\Sigma_2^{\mathbf{P}}$.

Dans ce papier, nous dépassons le formalisme proposé dans [3] sur trois points : nous relâchons la notion stricte de NFS de [3] car nous considérons aussi des factorisations en clones qui ne sont pas nécessairement premiers (irréductibles) ; nous considérons des générateurs arbitraires pour les clones (qui jouent le rôle de connecteurs dans les NFSs), par ex., nous considérons des connecteurs médians d'arité arbitraire ; et nous développons une théorie des NFSs qui repose sur des propriétés structurelles des connecteurs et des systèmes, par ex., associativité et linéarité, respectivement.

Plusieurs résultats notables découlent de ces considérations. Par exemple, l'idée assez intuitive selon laquelle des connecteurs non-associatifs encodent plus d'« information » sur les fonctions sera validée de deux manières : ils induisent des NFSs avec un unique connecteur non-trivial, et les NFSs correspondants produisent des représentations qui sont plus efficaces que celles produites en utilisant des connecteurs associatifs. En fait, il peut être démontré que, sous l'hypothèse de non-redondance, les NFSs nécessitent soit plusieurs connecteurs tous associatifs, soit un seul connecteur non-associatif.

Le plan de cet article est le suivant : en Section 2, nous donnons des préliminaires sur la théorie des clones et des NFSs, et rappelons la notion d'efficacité de représentations d'une fonction Booléenne, suivant le cadre de travail de [3]. En Section 3 nous portons notre attention sur les NFSs générés par un unique connecteur. Nous donnons des conditions (Propositions 1, 2, et 3) sur ces connecteurs qui conduisent à des conversions efficaces de formules d'un système à un autre, c'est-à-dire sans que les formules n'explosent de façon exponentielle. En particulier, le système de MNF est polynomialement aussi efficace que n'importe quel autre NFS généré pas un connecteur unique (Théorème 3). Nous considérons aussi des NFSs générés par plus qu'un seul connecteur, comme les formes normales usuelles (disjonctive, conjonctive, polynomiale, et duale polynomiale). En fait, nous établissons une relation entre la non-associativité et le fait d'être quasi-Sheffer : un connecteur génère un NFS (connecteur que nous qualifions de *quasi-Sheffer*) si et seulement si il est non-associatif (Théorème 2). De plus, une méthode a été donnée ([5]) pour convertir des formules qui sont des compositions de connecteurs associatifs en des formules qui sont des compositions d'un unique connecteur non-associatif. Une conséquence que nous tirons de cette étude est que le MNF est polynomialement aussi efficace que n'importe quel autre NFS (Théorème 3), étendant ainsi Théorème 3.

2 Préliminaires et notation

Dans cette section, nous rappelons les notions de bases de la théorie des clones et des systèmes de formes normales dans le contexte des fonctions Booléennes. Pour une présentation plus détaillée, nous nous référons à [8, 10], et [3].

2.1 Théorie des clones et systèmes de formes normales

Soit $\mathbb{B} = \{0, 1\}$. L'ensemble $\mathbb{B}^n$ est le treillis Booléen (distributif et muni du complément) à 2^n éléments suivant l'ordre composante par

composante $\preceq$. Le *complément* d'un vecteur $\mathbf{a} = (a_1, \ldots, a_n)$ est défini par $\overline{\mathbf{a}} = (1 - a_1, \ldots, 1 - a_n)$. On note $\mathbf{0} = (0, \ldots, 0)$ et $\mathbf{1} = (1, \ldots, 1)$. Pour une fonction $f : \mathbb{B}^n \to \mathbb{B}^m$, le *dual* de f est défini par $f^d(\mathbf{a}) := \overline{f(\overline{\mathbf{a}})}$. Une *fonction Booléenne* est une fonction $f : \mathbb{B}^n \to \mathbb{B}$, pour un certain entier positif n appelé l'*arité* de f, et denotée $\mathrm{ar}(f)$. Une *classe* de fonctions est un sous-ensemble $\mathcal{C} \subseteq \bigcup_{n \geq 1} \mathbb{B}^{\mathbb{B}^n}$. Pour une arité donnée n, les n différentes *projections* $(a_1, \ldots, a_n) \mapsto a_i, 1 \leq i \leq n$, sont appelées *variables* et notées $x_1, \ldots, x_n$, ou simplement x, y, z. À travers ce papier, nous considérerons les fonctions $\wedge$ (conjonction binaire), $\vee$ (disjonction binaire), $\neg$ (négation), $\oplus$ (somme binaire modulo 2), m (médiane, or majorité ternaire, définie par $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$), m_{2n+1} (médiane $2n+1$-aire, aussi appelée majorité ; par exemple, $\mathrm{m}_3 = \mathrm{m}$), $\uparrow$ (barre de Sheffer, définie par $\neg(x \wedge y)$), et son dual $\downarrow$ (défini par $\neg(x \vee y)$), u (défini par $(x \vee y) \wedge z$), et w (défini par $(x \wedge y) \vee z$).

Si f est une fonction n-aire et $g_1, \ldots, g_n$ sont toutes des fonctions m-aires, alors leur *composition* $f(g_1, \ldots, g_n)$ est la fonction m-aire définie par $f(g_1, \ldots, g_n)(a_1, \ldots, a_m) = f(g_1(a_1, \ldots, a_m), \ldots, g_n(a_1, \ldots, a_m))$ pour tout $(a_1, \ldots, a_m) \in \mathbb{B}^m$.

Cette notion s'étend naturellement aux classes de fonctions $\mathcal{I}$ et $\mathcal{J}$. La *composition de $\mathcal{I}$ avec $\mathcal{J}$*, notée $\mathcal{I} \circ \mathcal{J}$, est la classe des fonctions $f(g_1, \ldots, g_n)$ où f est n-aire dans $\mathcal{I}$ et les g_i sont m-aires dans $\mathcal{J}$. Un *clone* est une classe $\mathcal{C}$ de fonctions qui contient toutes les projections et qui satisfait $\mathcal{C} \circ \mathcal{C} \subseteq \mathcal{C}$ (i.e., elle est fermée par composition). L'ensemble des clones des fonctions Booléennes constituent un treillis algébrique, où le meet est l'intersection, le join de deux clones est le plus petit clone qui contient leur union, où le plus grand clone est le clone $\Omega = \bigcup_{n \geq 1} \mathbb{B}^{\mathbb{B}^n}$ de toutes les fonctions Booléennes, et où le plus petit clone est le clone de toutes les projections I_c. Ce treillis fut entièrement décrit par E. Post (voir [14]). Ces clones et le treillis sont souvent appelés les Classes de Post et le Treillis de Post.

Étant donnés k connecteurs $(\alpha_1, \ldots, \alpha_k) \in \Omega^k$, on dénote par $\Phi(\{\alpha_1, \ldots, \alpha_k\})$ ou $\Phi(\alpha_1, \ldots, \alpha_k)$ l'ensemble de toutes les formules obtenues par compositions des connecteurs $\{\alpha_1, \ldots, \alpha_k\}$. Une formule ϕ dans laquelle les variables x_i, $i \in I$, apparaissent *représente* une fonction n-aire f si $I \subseteq \{1, \ldots, n\}$ et pour tout $(a_1, \ldots, a_n) \in \mathbb{B}^n$, on a que $f(a_1, \ldots, a_n) = 1$ si et seulement si $\phi(a_i : i \in I) = 1$ (i.e., l'affectation $(a_i : i \in I)$ pour les variables de ϕ la rend vraie). Deux formules ϕ_1, ϕ_2 sont dites *équivalentes*, ce que l'on dénote par $\phi_1 \equiv \phi_2$, si elles représentent la même fonction. La *portée* d'une instance d'un connecteur α dans une formule ϕ est l'ensemble de toutes les sous-formules qui apparaissent, dans ϕ, comme arguments de α. On dénote par $\Phi(\alpha_1) \circ \cdots \circ \Phi(\alpha_k)$ l'ensemble de toutes les formules dans lesquelles α_i n'apparaît pas dans la portée de α_j si $i < j$.

Exemple 1. *$x \wedge (y \vee z) \in \Phi(\wedge) \circ \Phi(\vee)$, et $x \wedge (y \vee z) \notin \Phi(\vee) \circ \Phi(\wedge)$ parce que $\vee$ apparaît dans la portée de $\wedge$ dans la formule $x \wedge (y \vee z)$.*

On dénote par $\mathcal{C}(\{\alpha_1, \ldots, \alpha_k\})$ le plus petit clone qui contient $\{\alpha_1, \ldots, \alpha_k\}$. Le clone $\mathcal{C} = \mathcal{C}(\{\alpha_1, \ldots, \alpha_k\})$ est dit *généré par l'ensemble* $\{\alpha_1, \ldots, \alpha_k\}$ dont les membres sont appelés les *générateurs* de $\mathcal{C}$.

Toute fonction Booléenne peut être représentée sous forme normale disjonctive : $\Omega = \mathcal{C}(\vee) \circ \mathcal{C}(\wedge) \circ \mathcal{C}(\neg)$, Ω désignant le clone de toutes les fonctions Booléennes, et $\mathcal{C}(\neg)$ la classe des tous les littéraux (variables et variables niées). On peut donc exprimer Ω comme une factorisation en clones. Ce fait est la base de la définition suivante.

Définition 1 (Systèmes de formes normales)**.** *Soient $\gamma_1, \ldots, \gamma_{k-1}$ des connecteurs. Si $\Omega = \mathcal{C}(\gamma_1) \circ \cdots \circ \mathcal{C}(\gamma_{k_1}) \circ \Omega(1)$, avec $\Omega(1)$ le clone des littéraux et des fonctions constantes, alors la structure*

$$\mathcal{C}(\gamma_1) \circ \cdots \circ \mathcal{C}(\gamma_{k-1}) \circ \Omega(1) \qquad (1)$$

est appelée un système de formes normales*, ou NFS. Si il existe* $i \in \{1, \ldots, k\}$ *tel que*

$$\mathcal{C}(\gamma_1) \circ \ldots \mathcal{C}(\gamma_{i-1}) \circ \mathcal{C}(\gamma_{i+1}) \circ \cdots \circ \mathcal{C}(\gamma_{k-1}) \circ \Omega(1)$$

est un NFS, alors (1) est dit redondant*, sinon, (1) est dit* non-redondant.

Une fonction α est dite *Sheffer* (resp. *quasi-Sheffer*) si $\Omega = \mathcal{C}(\alpha)$ (resp. $\Omega = \mathcal{C}(\alpha) \circ \Omega(1)$). De façon similaire, un clone $\mathcal{C}$ est dit *complet* (resp. *quasi-complet*) si il est généré par une fonction qui est Sheffer (resp. quasi-Sheffer). Clairement, toute fonction Sheffer est aussi quasi-Sheffer. La barre de Sheffer $\uparrow$ est une fonction Sheffer, et est donc quasi-Sheffer, tandis que la médiane m est quasi-Sheffer ([3]) mais pas Sheffer. En effet, puisque m est monotone non-décroissante, elle ne peut pas générer de fonctions strictement décroissantes. Par la suite, nous allons principalement nous intéresser aux NFSs non-redondants : autoriser l'utilisation d'un autre connecteur pour la MNF, par exemple, peut produire d'autres formules qui représentent la même fonction (considérer, par exemple, la formule $\mathrm{m}(x, y, \wedge(z, t))$, qui peut déjà être exprimée par la formule équivalente en MNF $\mathrm{m}(x, y, \mathrm{m}(z, t, 0))$ – ceci est dû en particulier au fait que m is quasi-Sheffer). Ainsi, dans notre formalisme, nous ne considérerons pas la factorisation $\mathcal{C}(\mathrm{m}) \circ \mathcal{C}(\wedge) \circ \Omega(1)$ comme étant un NFS. Nous introduisons maintenant quelques NFSs qui seront mentionnées dans le présent article. On pourra se référer à [3] pour une description des Classes de Post.

Exemple 2. *Les systèmes de formes normales disjonctif, conjonctif, polynomial, et polynomial dual, dénotés respectivement par* $\mathbf{D}, \mathbf{C}, \mathbf{P}$, *et* $\mathbf{P}^d$*, sont définis respectivement par :*

- $\mathbf{D} = \mathcal{C}(\vee) \circ \mathcal{C}(\wedge) \circ \Omega(1)$,
- $\mathbf{C} = \mathcal{C}(\wedge) \circ \mathcal{C}(\vee) \circ \Omega(1)$,
- $\mathbf{P} = \mathcal{C}(\oplus) \circ \mathcal{C}(\wedge) \circ \Omega(1)$, *et*
- $\mathbf{P}^d = \mathcal{C}(\oplus) \circ \mathcal{C}(\vee) \circ \Omega(1)$.

La forme normale médiane $\mathbf{M}$ *est définie par* $\mathbf{M} = \mathcal{C}(\mathrm{m}) \circ \Omega(1)$. *Étant donnée une médiane* $2n{+}1$*-aire* m_{2n+1} *nous considérons aussi le système* $\mathbf{M}_{2n+1} = \mathcal{C}(\mathrm{m}_{2n+1}) \circ \Omega(1)$. *Le système de forme normale de Sheffer* $\mathbf{S}$ *est défini par* $\mathbf{S} = \mathcal{C}(\uparrow) \circ \Omega(1)$. *Soit* $a \in \{0, 1\}$. *Une fonction* f *est dite* $a-$séparante *s'il existe* $i, 1 \leq i \leq n$, *tel que pour tout* $(a_1, \ldots, a_n) \in f^{-1}(a)$ *on a* $a_i = a$. U_∞ *et* W_∞ *désignent les classes de toutes les fonctions* $1-$ *et* $0-$*séparantes, respectivement. Finalement,* $\mathbf{U} = M_c U_\infty \circ \Omega(1)$ *et* $\mathbf{W} = M_c W_\infty \circ \Omega(1)$*, les formes normales associées aux fonctions* 1 *et* 0*-séparantes sont définies par* $\mathcal{C}(\mathrm{u}) \circ \Omega(1)$ *et* $\mathcal{C}(\mathrm{w}) \circ \Omega(1)$.

2.2 Efficacité des représentations en NFSs

Soit ϕ une formule et ϵ un connecteur. On dénote par $|\phi|_\epsilon$ le nombre d'occurrences du symbole ϵ dans la formule ϕ. La *taille* d'une formule ϕ vue comme une expression est dénotée par $|\phi|$, et est définie comme le nombre de tous les connecteurs qui apparaissent dans ϕ, sans prendre en compte les fonctions dans $\Omega(1)$ (i.e., ni les constantes ni les littéraux) : $|\phi| = \sum_{\epsilon, \mathrm{ar}(\epsilon) > 1} |\phi|_\epsilon$. Ce n'est pas une restriction car le nombre de littéraux et de constantes dans une formule est linéaire en le nombre de connecteurs dans cette formule. Par exemple, $|x \wedge (y \vee 1)| = |x \wedge (y \vee 1)|_\wedge + |x \wedge (y \vee 1)|_\vee = 1 + 1 = 2$.

Définition 2 ($\mathbf{A}$-complexité)**.** *Soit* $\mathbf{A} = \mathcal{C}(\alpha_1) \circ \cdots \circ \mathcal{C}(\alpha_k) \circ \Omega(1)$ *un NFS. L'ensemble des formules qui correspondent à* $\mathbf{A}$ *est* $\Phi(\alpha_1) \circ \cdots \circ \Phi(\alpha_k) \circ \Omega(1)$. *Étant donnée une fonction* $f \in \Omega$ *on définit la* $\mathbf{A}$-complexité *de* f*, dénotée* $C_\mathbf{A}(f)$*, par* $C_\mathbf{A}(f) = \min\{|\phi| : \phi \in \Phi(\alpha_1) \circ \cdots \circ \Phi(\alpha_k) \circ \Omega(1), \phi \text{ représente } f\}$.

Définition 3 (Efficacité)**.** *Étant donnés deux NFSs* $\mathbf{A}$ *et* $\mathbf{B}$*,* $\mathbf{A}$ *est dit* polynomialement aussi efficace que $\mathbf{B}$*, dénoté* $\mathbf{A} \preceq \mathbf{B}$*, s'il existe un polynôme à coefficients entiers* p *tel que* $C_\mathbf{A}(f) \leq p(C_\mathbf{B}(f))$ *pour tout* $f \in \Omega$. *Remarquons que* $\preceq$ *est un préordre sur n'importe quel ensemble de NFSs, mais qu'il n'est pas total [3]. Si* $\mathbf{A} \not\preceq \mathbf{B}$ *et* $\mathbf{B} \not\preceq \mathbf{A}$*, on dit que* $\mathbf{A}$ *et* $\mathbf{B}$ *sont* incomparables *ou, pour être plus descriptif, que* $\mathbf{A}$ *et* $\mathbf{B}$ produisent des représentations de complexités incomparables*, noté* $\mathbf{A}||\mathbf{B}$. *Dans le cas où*

$\mathbf{A} \preceq \mathbf{B}$ *et* $\mathbf{B} \not\preceq \mathbf{A}$*, on dit que* $\mathbf{A}$ *est* polynomialement plus efficace que $\mathbf{B}$*, ou que* $\mathbf{A}$ produit des représentations de complexité plus petite que $\mathbf{B}$*, noté* $\mathbf{A} \prec \mathbf{B}$*. Dans le cas où* $\mathbf{A} \preceq \mathbf{B}$ *et* $\mathbf{B} \preceq \mathbf{A}$*, on dit que* $\mathbf{A}$ *et* $\mathbf{B}$ *sont* équivalents *ou* produisent des représentations de complexité équivalente*, noté* $\mathbf{A} \sim \mathbf{B}$*. Ainsi définie,* $\sim$ *est une relation d'équivalence.*

Un clone donné peut admettre différents (ensembles de) générateurs. Par exemple, le clone SM des fonctions auto-duales monotones est généré par la médiane ternaire m, ainsi que n'importe quelle médiane $2n+1$-aire. Ceci soulève la question suivante : pour un clone donné, quel(s) générateur(s) produisent les représentations les plus efficaces ? Nous conjecturons que n'importe quel générateur induit des NFSs de complexité équivalente.

Conjecture 1. *Considérons le clone* $\mathcal{C}(\alpha) \circ \Omega(1)$*. Soit* α' *un autre générateur de ce clone. Alors,* $\mathcal{C}(\alpha) \circ \Omega(1) \sim \mathcal{C}(\alpha') \circ \Omega(1)$*. En d'autres termes, le choix de générateur n'a pas d'effet sur l'efficacité des représentations produites.*

Cette conjecture est vraie pour l'ensemble de générateurs de $\mathbf{M}$ constitué de toutes les médianes $2n+1$-aires ($n \geq 1$) ; voir Corollaire 2. Toutefois, cette conjecture reste ouverte en général. Au vu de la Conjecture 1, nous allons principalement porter notre attention sur les NFSs générés par les connecteurs d'arités minimales. Par exemple, dans le cas du clone SM et du NFS $\mathbf{M}$, nous choisissons le connecteur m. Dans le cas du clone $M_c U_\infty$ et du NFS $\mathbf{U}$, nous choisissons u. Nous rappelons le résultat suivant portant sur la comparaison de NFSs bien connus avec le NFS médian $\mathbf{M}$, obtenu dans [3].

Théorème 1 (Théorème 5, [3])**.** *Pour tout* $\mathbf{A}, \mathbf{B} \in \{\mathbf{D}, \mathbf{C}, \mathbf{P}, \mathbf{P}^d\}$*, on a* $\mathbf{A} || \mathbf{B}$ *si* $\mathbf{A} \neq \mathbf{B}$*. De plus, pour chaque* $\mathbf{B}$ *dans* $\{\mathbf{D}, \mathbf{C}, \mathbf{P}, \mathbf{P}^d\}$*, on a* $\mathbf{M} \prec \mathbf{B}$*.*

Nous rappelons aussi le système de décomposition médian ([12]), qui caractérise la classe des fonctions Booléennes monotones f :

$$f(\mathbf{x}) \equiv \mathrm{m}(f(\mathbf{x}_k^0), x_k, f(\mathbf{x}_k^1)) \qquad (2)$$

pour tout $\mathbf{x} = (x_1, \ldots, x_n)$, $k \in \{1, \ldots, n\}$, où $\mathbf{x}_k^c := (x_1, \ldots, x_{k-1}, c, x_{k+1}, \ldots, x_n)$, $c \in \mathbb{B}$.

3 NFSs générés par un unique connecteur

3.1 Relation entre non-associativité et quasi-Sheffer

Rappelons la notion d'associativité d'un connecteur (voir, par ex., [1, 9, 13]). Soit un ensemble non vide X tel que $|X| > 1$ et soit $n \geq 2$ un entier. Un connecteur n-aire $\phi : X^n \to X$ est dit *associatif* s'il vérifie :

$$\phi(\phi(x_1, \ldots, x_n), x_{n+1}, \ldots, x_{2n-1}) \equiv \cdots \equiv$$
$$\phi(x_1, \ldots, x_i, \phi(x_{i+1}, \ldots, x_{i+n}), x_{i+n+1}, \ldots, x_{2n-1})$$
$$\equiv \cdots \equiv \phi(x_1, \ldots, x_{n-1}, \phi(x_n, \ldots, x_{2n-1})).$$

La médiane m n'est pas associative [2], alors que $\wedge, \vee$, et $\oplus$ le sont. Comme nous allons le voir en Section 3.4, d'autres NFSs, générés par des connecteurs non-associatifs tels que la barre de Sheffer $\uparrow$, produisent des représentations de complexité équivalente à celles de $\mathbf{M}$.

Théorème 2. *Un connecteur est quasi-Sheffer si et seulement si il est non-associatif.*

Lemme 1. *Soit* $n > 1$ *et soit* $\mathbf{B} = \mathcal{C}(\beta_1) \circ \cdots \circ \mathcal{C}(\beta_n) \circ \Omega(1)$ *un NFS non-redondant. Alors, tous les* β_i *sont associatifs.*

Exemple 3. *Les NFSs non-redondants* $\mathbf{D}, \mathbf{C}, \mathbf{P}, \mathbf{P}^d$ *sont générés respectivement par* $\vee$ *et* $\wedge$*,* $\wedge$ *et* $\vee$*,* $\oplus$ *et* $\wedge$*, et* $\oplus$ *et* $\vee$*. Tous ces connecteurs sont associatifs.*

3.2 Quels sont les connecteurs qui sont quasi-Sheffer ?

Dans cette section, nous étudions les factorisations du type $\mathcal{C}(\alpha) \circ \Omega(1) = \Omega$, $\mathcal{C}(\alpha)$ étant

2. $\mathrm{m}(1, 0, \mathrm{m}(0, 0, 1)) \neq \mathrm{m}(1, \mathrm{m}(0, 0, 0), 1)$.

un clone engendré par α, pour localiser dans le Treillis de Post les connecteurs quasi-Sheffer. Les possibilités pour $\mathcal{C}(\alpha)$ peuvent être lues directement dans la description complète de la composition de deux clones (voir [3]). Elles sont Ω, T_0, T_1, T_c, M, M_0, M_1, M_c, S, S_c, SM, et U_m, MU_m, T_cU_m, M_cU_m, W_m, MW_m, T_cW_m, M_cW_m où $m = 2, \ldots, \infty$. Comme on peut le lire sur le Treillis de Post, générer les fonctions monotones autoduales grâce au générateur de SM, m, génère aussi toutes les fonctions monotones, M. Un générateur de SM est donc aussi un générateur pour M. Puisque l'on a choisi comme générateurs ceux d'arité minimale, lorsque l'on a $\mathcal{C}_2 \subseteq \mathcal{C}_1$ dans le Treillis de Post on a aussi $\mathcal{C}_2 \circ \Omega(1) \sim \mathcal{C}_1 \circ \Omega(1)$, car ils ont même générateur. En fait, dans ce cas, toute fonction monotone peut être écrite grâce à la médiane m : voir, par ex., (2). Ainsi, nous n'avons besoin de considérer que quelques classes et leurs générateurs dans le Treillis, i.e., $SM, M_cU_\infty, M_cW_\infty$, et Ω, pour considérer tous les générateurs possibles qui sont quasi-Sheffer et d'arité minimale. Le générateur de SM est la médiane m, dont certaines propriétés ont été données ci-haut. Les générateurs de M_cU_∞ et M_cW_∞ sont les connecteurs ternaires u et son dual w, respectivement. Les générateurs d'arité minimale pour Ω sont $x \uparrow y = \neg(x \wedge y)$ ou son dual $x \downarrow y = \neg(x \vee y)$.

3.3 Comparer des NFSs générés par un unique connecteur

Dans cette section, nous comparons les complexités des représentations produites par deux NFSs suivant certaines conditions sur les connecteurs qui génèrent ces NFs. En particulier, nous examinons des identités qui permettent de convertir des formules d'un système à un autre (par ex., l'identité $\mathrm{u}(x, y, z) \equiv \mathrm{m}(\mathrm{m}(x, 1, y), 0, z)$ pour convertir des formules de $\mathbf{U}$ en des formules médianes de $\mathbf{M}$). Plus précisément, nous donnons des conditions sur le nombre d'occurrences d'une même variable du côté droit de ces identités. Définissons formellement ces « identités de conversion » .

Définition 4 (Relations linéaires et quasi-linéaires entre NFSs)**.** *Soient* $\mathbf{A} = \mathcal{C}(\alpha) \circ \Omega(1)$ *et* $\mathbf{B} = \mathcal{C}(\beta) \circ \Omega(1)$. *Supposons que* β *a pour arité* n. *On dit qu'il existe une* relation linéaire entre NFSs*, notée* $\textsc{lin}(\mathbf{B}, \mathbf{A})$*, si* $\exists \phi \in \Phi(\alpha, x_1, \ldots, x_n)$,

$$\beta(x_1, \ldots, x_n) \equiv \phi \quad \textit{et} \quad \forall j,\ |\phi|_{x_j} = 1;$$

une relation quasi-linéaire universelle entre NFSs*, notée* $\forall\textsc{qlin}(\mathbf{B}, \mathbf{A})$*, si* $\forall j \in \{1, \ldots, n\}, \exists \phi_j \in \Phi(\alpha, x_1, \ldots, x_n)$,

$$\beta(x_1, \ldots, x_n) \equiv \phi_j \quad \textit{et} \quad |\phi_j|_{x_j} = 1;$$

une relation quasi-linéaire existentielle entre NFSs*, notée* $\exists\textsc{qlin}(\mathbf{B}, \mathbf{A})$*, si* $\exists \phi \in \Phi(\alpha, x_1, \ldots, x_n)$,

$$\beta(x_1, \ldots, x_n) \equiv \phi \quad \textit{et} \quad \exists j,\ |\phi|_{x_j} = 1.$$

Fait 1. *Pour toute paire de NFSs* $\mathbf{A}, \mathbf{B}$*, on a*

$$\textsc{lin}(\mathbf{B}, \mathbf{A}) \Rightarrow \forall\textsc{qlin}(\mathbf{B}, \mathbf{A}) \Rightarrow \exists\textsc{qlin}(\mathbf{B}, \mathbf{A}).$$

Exemple 4. *Le fait qu'on ait* $\textsc{lin}(\mathbf{U}, \mathbf{M})$ *provient de l'identité linéaire* $\mathrm{u}(x, y, z) \equiv \mathrm{m}(\mathrm{m}(x, 1, y), 0, z)$. *Toutefois, on n'a pas* $\textsc{lin}(\mathbf{M}, \mathbf{U})$ *(cela peut se voir par une recherche exhaustive). Par contre, nous pouvons induire la propriété, plus faible, que* $\exists\textsc{qlin}(\mathbf{M}, \mathbf{U})$*, grâce à l'identité* $\mathrm{m}(x, y, z) \equiv \mathrm{u}(\mathrm{u}(x, 0, y), \mathrm{u}(x, y, z), 1)$*, et ce parce que* $|\,\mathrm{u}(\mathrm{u}(x, 0, y), \mathrm{u}(x, y, z), 1)|_z = 1$. *Le fait que* $\forall\textsc{qlin}(\mathcal{C}(\alpha) \circ \Omega(1), \mathbf{M})$ *(Théorème 3) provient du fait que* m *vérifie le système de décomposition médiane (2).*

Proposition 1. *Soient* $\mathbf{A} = \mathcal{C}(\alpha) \circ \Omega(1)$ *et* $\mathbf{B} = \mathcal{C}(\beta) \circ \Omega(1)$. *Si* $\textsc{lin}(\mathbf{B}, \mathbf{A})$*, alors* $\mathbf{A} \preceq \mathbf{B}$.

La Proposition 1 peut être renforcée et énoncée en termes de quasi-linéarité universelle.

Proposition 2. *Soient* $\mathbf{A} = \mathcal{C}(\alpha) \circ \Omega(1)$ *et* $\mathbf{B} = \mathcal{C}(\beta) \circ \Omega(1)$. *Si* $\forall\textsc{qlin}(\mathbf{B}, \mathbf{A})$ *alors* $\mathbf{A} \preceq \mathbf{B}$.

Si α est symétrique, les Propositions 1 et 2 peuvent être affinées. Une fonction Booléenne f d'arité n est dite *symétrique* si pour toute permutation $\pi \in \mathfrak{S}_n$, on a $f(x_1, \ldots, x_n) \equiv f(x_{\pi(1)}, \ldots, x_{\pi(n)})$.

Proposition 3. *Soient* $\mathbf{A} = \mathcal{C}(\alpha) \circ \Omega(1)$ *et* $\mathbf{B} = \mathcal{C}(\beta) \circ \Omega(1)$. *Si* $\exists \text{QLIN}(\mathbf{B}, \mathbf{A})$ *et* α *est symétrique, alors* $\mathbf{A} \preceq \mathbf{B}$.

3.4 Applications : Efficacité de la MNF

Dans cette section, nous illustrons l'utilité des notions de relations entre NFSs et les Théorèmes qu'elles induisent en les appliquant à la comparaison de NFSs générés par un unique connecteur. En particulier, nous obtenons que $\mathcal{C}(\mathrm{m}) \circ \Omega(1)$ est polynomialement aussi efficace que n'importe quel autre $\mathcal{C}(\alpha) \circ \Omega(1)$. Cela est dû au système de décomposition médian (2) qui nous permet d'appliquer le résultat de la Proposition 2 en montrant que $\forall \text{QLIN}(\mathcal{C}(\alpha) \circ \Omega(1), \mathbf{M})$ est vérifié. Nous donnons d'abord un corollaire.

Corollaire 1. $\mathbf{U} \sim \mathbf{M}$, $\mathbf{W} \sim \mathbf{M}$, *et* $\mathbf{S} \sim \mathbf{M}$.

Grâce au système (2), on peut exhiber, pour toute fonction Booléenne monotone α, une relation linéaire entre α et m, et appliquer la Proposition 3. En effet, la variable x_k n'apparaît qu'une seule fois dans le membre droit de l'expression (2). Le cas où α n'est pas monotone est réglé par la construction d'une fonction intermédiaire d'arité double, monotone, et qui coïncide avec α sur un sous-ensemble de son domaine (voir [4]).

Théorème 3. $\mathbf{M} \preceq \mathbf{B} = \mathcal{C}(\beta) \circ \Omega(1)$.

Le corollaire suivant va dans le sens de la Conjecture 1 : elle est vraie pour l'ensemble de générateurs de SM constitué par les médianes $2n+1$-aires.

Corollaire 2. *Pour tout* $n \geq 1$, $\mathbf{M} \sim \mathbf{M}_{2n+1}$.

3.5 NFSs générés par plusieurs connecteurs

Nous pouvons à présent établir une relation entre le nombre de connecteurs qui génèrent un NFS et l'efficacité des représentations qu'il produit. Curieusement, utiliser plus de connecteurs ne permet pas d'obtenir de représentations plus efficaces.

Proposition 4. $\mathcal{C}(\alpha) \circ \Omega(1) \preceq \mathcal{C}(\beta) \circ \mathcal{C}(\gamma) \circ \Omega(1)$.

Théorème 4. $\mathcal{C}(\alpha) \circ \Omega(1) \preceq \mathcal{C}(\beta_1) \circ \cdots \circ \mathcal{C}(\beta_n) \circ \Omega(1)$ *pour* $n > 1$.

Les Théorèmes 3 et 4 permettent de conclure sur $\mathbf{M}$: il est polynomialement aussi efficace que tout autre NFS.

Corollaire 3. *Soit* $\mathbf{B}$ *un NFS. Alors,* $\mathbf{M} \preceq \mathbf{B}$.

4 Conclusion

Dans cet article, nous avons considéré des NFSs selon certaines propriétés vérifiées par leurs générateurs, telles que l'associativité, la symétrie, ou, simplement, leur nombre, et nous avons comparé l'efficacité des représentations produites par ces NFSs pour représenter des fonctions Booléennes. Nous avons donné des conditions suffisantes pour qu'un NFS soit polynomialement aussi efficace qu'un autre. Par exemple, si nous exhibons une dépendance linéaire entre α et β, une dépendance quasi-linéaire sous l'hypothèse que α est symétrique, ou des dépendances quasi-linéaires pour toutes les variables, nous pouvons en conclure que $\mathcal{C}(\alpha) \circ \Omega(1) \preceq \mathcal{C}(\beta) \circ \Omega(1)$. Un autre résultat notable lié à l'associativité est le fait que des systèmes générés par un connecteur unique sont toujours polynomialement aussi efficaces que tout autre système généré par plusieurs connecteurs : l'utilisation de plusieurs connecteurs n'implique pas des représentations plus efficaces. De plus, nous avons montré que $\mathbf{M}$ est polynomialement aussi efficace que tout autre NFS, ce qui motive d'autant plus son étude. Ces résultats, associés avec ceux de [3], sont résumés dans la figure 1.

Toutefois, cette figure reste incomplète, ce qui nous amène à formuler trois conjectures à relever : la relation stricte entre le niveau du dessus et celui du bas, ce dernier correspondant

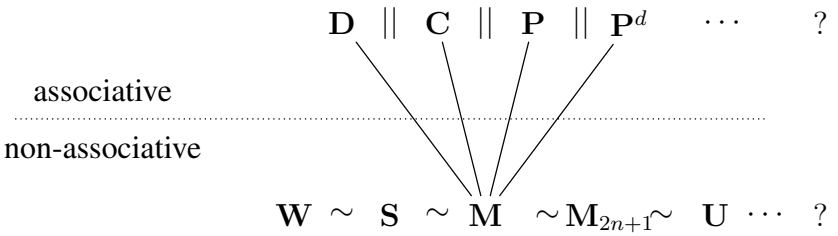

Figure 1 – Demi-treillis de quelques NFSs, ordonné par $\preceq$, avec une séparation entre les NFSs générés par des connecteurs associatifs et ceux, asymptotiquement plus efficaces, générés par des connecteurs non-associatifs.

aux NFSs basés sur un unique connecteur associatif, et le niveau du dessus correspondant aux NFSs basés sur des connecteurs associatifs ; puis, la relation d'incomparabilité entre deux NFSs quelconques au niveau du dessus ; enfin, la relation d'équivalence entre deux NFSs quelconques du niveau du bas. Une réponse positive à la conjecture 1 serait un outil précieux pour résoudre ce dernier point.

Remerciements :

Les auteurs souhaitent remercier Emmanuel Hainry et Erkko Lehtonen, pour les discussions utiles et fructueuses ainsi que leurs commentaires pertinents.

Références

[1] János Aczél, Gary J. Erickson, and Yuxiang Zhai. The associativity equation re-revisited. In *Proc. of the AIP Conference*, volume 707, pages 195–203. AIP, 2004.

[2] Luca Amarú, Pierre-Emmanuel Gaillardon, and Giovanni De Micheli. Majority-inverter graph : A novel data-structure and algorithms for efficient logic optimization. In *Proc. of the 51st Annual Design Automation Conference*, pages 1–6. ACM, 2014.

[3] Miguel Couceiro, Stephan Foldes, and Erkko Lehtonen. Composition of post classes and normal forms of Boolean functions. *Discrete Mathematics*, 306(24) :3223–3243, 2006.

[4] Miguel Couceiro, Erkko Lehtonen, Jean-Luc Marichal, and Tamás Waldhauser. An algorithm for producing median formulas for Boolean functions. In *Proc. of the Reed Muller 2011 Workshop*, pages 49–54, 2011.

[5] Miguel Couceiro, Pierre Mercuriali, and Romain Péchoux. Comparing the efficiency of normal form systems to represent Boolean functions. https ://hal.archives-ouvertes.fr/hal-01551761v1.

[6] Miguel Couceiro, Pierre Mercuriali, Romain Péchoux, and Abdallah Saffidine. Median based calculus for lattice polynomials and monotone Boolean functions. To appear in *Proc. of the 47th IEEE International Symposium on Multiple-Valued Logic (ISMVL)*, may 2017.

[7] Yves Crama and Peter L. Hammer. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, volume 2. Cambridge University Press, 2010.

[8] Klaus Denecke and Shelly L. Wismath. *Universal Algebra and Coalgebra*. World Scientific, 2009.

[9] Wilhelm Dörnte. Untersuchungen über einen verallgemeinerten gruppenbegriff. *Mathematische Zeitschrift*, 29 :1–19, 1929.

[10] Dietlinde Lau. *Function Algebras on Finite Sets : Basic Course on Many-Valued Logic and Clone Theory*. Springer Science & Business Media, 2006.

[11] Heikki Mannila and Hannu Toivonen. Multiple uses of frequent sets and condensed representations : Extended abstract. In *Proc. of the 2nd International Conference on Knowledge Discovery and Data Mining (KDD'96)*, pages 189–194, 1996.

[12] Jean-Luc Marichal. Weighted lattice polynomials. *Discrete Mathematics*, 309(4) :814–820, 2009.

[13] Emil L. Post. Polyadic groups. *Transactions of the American Mathematical Society*, 48(2) :208–350, 1940.

[14] Emil L. Post. *The Two-Valued Iterative Systems of Mathematical Logic*, volume 5, pages 1–122. Princeton, 1941.

[15] Jilles Vreeken and Nikolaj Tatti. *Interesting Patterns*, pages 105–134. Springer International Publishing, Cham, 2014.

[16] Ingo Wegener. *Complexity Theory : Exploring the Limits of Efficient Algorithms*. Springer Science & Business Media, 2005.