Ann. sc. math. Québec, 1988, vol 12, no 1, pp. 55-72

FAMILLE LARGE DE CLONES SUR UN UNIVERS FINI[1]

Lucien Haddad et Ivo G. Rosenberg

Résumé

Soit $B = \{0,1,\ldots,k-1\}$ un univers fini non-vide. Un clone sur B est un ensemble d'opérations finitaires sur B, fermé sous la composition et qui contient toutes les projections. Les clones sur B, ordonnés par l'inclusion, forment un treillis algébrique L. Pour $k = 2$, ce treillis est dénombrable et a été complètement décrit par E. Post (1941), mais on ne connaît pas grand chose sur L pour $k > 2$. Un intervalle I de L est dit large s'il existe un plongement qui préserve l'ordre du treillis $\underset{\sim}{P}$ des sous-ensembles de $\mathbb{N} = \{1,2,\ldots\}$ (ordonné par l'inclusion) dans I. En 1959, Janov et Mučnik ont montré que pour $k > 2$, L possède un intervalle large. Un des exemples est l'intervalle $[E,F]$ engendré par les clones de toutes les opérations que préservent la relation

$$\rho_n = (B^n \backslash \{0,1\}^n) \cup \{(x_1,\ldots,x_n) \in \{0,1\}^n \colon x_1 + \ldots + x_n = 1\}, \qquad (n = 1,2,\ldots).$$

Soit f_n l'opération n-aire sur B définie par $f_n(x_1,\ldots,x_n) = 0$ si $x_1 + \ldots + x_n = 1$, et $f_n(x_1,\ldots,x_n) = k-1$ sinon. Dans cette première partie de notre travail, nous décrivons le clone engendré par l'ensemble $\{f_n,\ n \in \mathbb{N}\}$, puis nous montrons que l'intervalle de clones engendré par $\{f_x,\ x \in X\}$ $(X \subseteq \mathbb{N})$ est large mais non booléen (i.e. n'est pas isomorphe en tant que treillis à $\underset{\sim}{P}$). Finalement, nous mentionnons que pour $k > 1$, le treillis des clones partiels est large.

[1]Recherche subventionnée par le C.R.S.N.G. ainsi que par le F.C.A.R.

Abstract

Let $B = \{0,1,\ldots,k-1\}$ be a finite nonempty universe. A clone on B is a composition closed set of finitary operations on B containing all projections. The clones on B, ordered by inclusion form an algebraic lattice L. For $k = 2$ the lattice is countable and completely known (E. Post 1941) while for $k > 2$ it is largely unknown. An interval I of L is large if there is an order embedding of the lattice $\underset{\sim}{P}$ of subsets of $\mathbb{N} = \{1,2,\ldots\}$ (ordered by inclusion) into I. In 1959 Janov and Mučnik showed that for $k > 2$ the lattice of clones has a large interval. One of the examples is the interval $[E,F]$ generated by the clones of all operations preserving the relation

$$\rho_n = (B^n \backslash \{0,1\}^n) \cup \{(x_1,\ldots,x_n) \in \{0,1\}^n : x_1 + \ldots + x_n = 1\}, \qquad (n = 1,2,\ldots).$$

Let f_n denote the n-ary operation on B which equals 0 if $x_1 + \ldots + x_n = 1$ and $k-1$ otherwise. In this first part of our work, we describe the clone generated by the set $\{f_n,\ n \in \mathbb{N}\}$, then we show that the interval of clones generated by $\{f_x,\ x \in X\}$ $(X \subseteq \mathbb{N})$ is large but not boolean (i.e. is not lattice isomorphic to $\underset{\sim}{P}$). Finally we mention that for $k > 1$, the lattice of partial clones is large.

1. Introduction

Dans ce qui suit, B est un ensemble non vide fixé (appelé univers). Pour tout entier $n \geq 0$, une *opération* n-aire sur B est une application $f: B^n \to B$ (pour $n = 0$, une opération 0-aire est simplement un élément fixé de B). Nous dénotons par $O^{(n)}$ l'ensemble de toutes les opérations n-aires sur B et par $\underset{\sim}{O} := \bigcup_{n=1}^{\infty} O^{(n)}$. Une paire $B := \langle B;X\rangle$ avec $X \subseteq \underset{\sim}{O}$ est une algèbre universelle sur B. De l'ensemble X nous pouvons créer de nouvelles opérations par composition. Ceci signifie

i) nous pouvons remplacer une variable d'une opération de X par une autre opération de X et

ii) nous pouvons obtenir de nouvelles opérations en permutant ou identifiant certaines variables.

Nous suivrons les définitions de [14]. Pour décrire la composition et les clones, nous introduisons un groupoïde $*$ avec trois opérations ζ, τ et Δ et un élément particulier e_1^2 sur $\underset{\sim}{O}$.

Soit $f \in O^{(n)}$, $g \in O^{(m)}$ et $r = m + n - 1$. Nous définissons $f*g \in O^{(r)}$ en posant:

$$(f*g)(x) = f(g(x_1,\ldots,x_m),x_{m+1},\ldots,x_r)$$

pour tout $x = (x_1,\ldots,x_r) \in B^r$, et $e_i^2(x_1,x_2) = x_i$ $(i = 1,2)$ pour tout $(x_1,x_2) \in B^2$.

Il est facile de voir que $<\underset{\sim}{O},*,e_1^1>$ est un monoïde d'élément neutre $e_1^1 = id_B$.

Pour $n > 1$, nous définissons $\zeta f \in O^{(n)}$, $\tau f \in O^{(n)}$ et $\Delta f \in O^{(n-1)}$ en posant:

$$(\zeta f)(x_1,\ldots,x_n) = f(x_2,\ldots,x_n,x_1)$$
$$(\tau f)(x_1,\ldots,x_n) = f(x_2,x_1,\ldots,x_n)$$
$$(\Delta f)(x_1,\ldots,x_n) = f(x_1,x_1,x_2,x_3,\ldots,x_n)$$

pour tous $x_1,\ldots,x_n \in B$.

Pour $n = 1$, $\zeta f = \tau f = \Delta f = f$.

L'algèbre $M_B = <\underset{\sim}{O},*,\zeta,\tau,\Delta,e_1^2>$ est appelée l'*algèbre post-itérative de Mal'cev* sur B. Un sous-univers de M_B est dit un *clone* (sur B). Ainsi un clone C est un sous-monoïde de $<\underset{\sim}{O},*>$ qui contient e_1^2 et satisfait $\zeta(C) \subseteq C$, $\tau(C) \subseteq C$ et $\Delta(C) \subseteq C$, ou c'est encore une extension analogue d'un monoïde d'auto-applications de B (ou d'un groupe de permutations sur B) à plusieurs variables. L'ensemble $J = \{e_i^n\colon 1 \le i \le n\}$ des projections remplace l'identité id_B (ou e_1^1) et nous avons ζ, τ, et Δ afin de manipuler les variables (qui sont évidemment absentes dans le cas des applications de B dans lui-même). Il existe d'autres types de compositions mais celles-ci reflètent bien les constructions standard en logique (calcul propositionnel), en algèbre (groupes, anneaux, treillis, etc.), en algèbre universelle et en théories des modèles.

Nous dénotons par L l'ensemble des clones sur B et soit $L_B = (L,\subseteq)$. Il est bien connu que L_B est un treillis algébrique. En commençant par le plus petit univers non-trivial, disons $B = \underline{2} = \{0,1\}$, l'ensemble $\underset{\sim}{O}_2$ est alors l'ensemble des fonctions booléennes 0-1 (dites aussi fonctions de l'algèbre de la logique). L'étude de $\underset{\sim}{O}_2$ a débuté en 1848 (G. Boole). En 1941, E. Post [16] détermina complètement le treillis L_2 des clones sur $\underline{2}$, (une partie des résultats furent trouvés indépendamment par C. Benzaken [2,3]). Cependant en tirant une citation de [12, p. 7.4.24]:

> *"Forty five years after its publications, Post's paper of 1941 still occupies a unique and isolated niche in the annuals of clone theory."*

Effectivement peu de choses sont connues sur L_B pour $|B| > 2$. Pour un bout de temps, on croyait que pour un entier $k > 2$, les clones sur $\underline{k} = \{0,\ldots,k-1\}$ étaient essentiellement (mais en plus compliqué) de même nature, en particulier si B est fini avec $|B| > 2$, le treillis L_B est aussi dénombrable (par exemple pour la question concernant les bases finies des clones (voir [10, p. 78])). Ainsi ce fut une surprise quand Janov et Mučnik dans "Existence of k-valued closed classes without a finite basis" [11]; montrèrent que pour $|B| > 2$, il y a $2^{\aleph_0}$ clones sur B (un résultat similaire a été mentionné par Ehrenfeucht, mais sa construction est perdue). Janov et Mučnik donnèrent une construction basée sur les opérations f_i (introduites à la Section 2). En utilisant des relations, ceci a été reformulé en [19, p. 166.7] et en [5,9]. Naturellement la question "quels sont les clones sur B qui contiennent $2^{\aleph_0}$ sous-clones?" se posait. L'exemple de Janov et Mučnik était facilement modifié (essentiellement en allant plus bas dans le treillis des clones) pour répondre par l'affirmative pour la plupart des clones maximaux (voir [8]) (qui sont des coatomes ou atomes duaux de L, i.e. les clones couverts par $\underset{\sim}{O}$ [10,17,19]). L'unique exception est le clone maximal des opérations affines (ou quasi-linéaires [17]) qui contient seulement un nombre dénombrable de sous-clones (mais qui n'existe que pour $|B|$ = la puissance d'un nombre premier). La classe suivante de clones maximaux nécessite un traitement spécial.

Soit s une permutation de B et on dénote par Pol s l'ensemble de toutes les opérations $f \in O^{(n)}$ qui satisfont $f(s(x_1),\ldots,s(x_n)) = s(f(x_1,\ldots,x_n))$, pour tous $x_1,\ldots,x_n \in B$, (i.e. s est un automorphisme de $\langle B,f\rangle$). Si s est une permutation sans point fixe et dont tous les cycles ont la même longueur p (un nombre premier), alors Pol s est un clone maximal. Dans une série d'articles [5-9,14,15], il a été montré que pour $|B| > 2$ et s une permutation de B, le clone Pol s a aussi $2^{\aleph_0}$ sous-clones. Le cas $3 \le |B| \le 4$ et s une permutation cyclique de B nécessite une analyse bien plus détaillée [14]. Demetrovics a modifié l'exemple de Janov et Mučnik de 3 façons (une d'entre elles était pour répondre par l'affirmative à la question suivante posée par R. McKenzie: Existe-t-il $2^{\aleph_0}$ clones sur B qui contiennent chacun toutes les constantes?). Dans cet article qui est la première partie de notre travail (la seconde contient des résultats plus importants que celle-ci paraîtra dans ce même journal), nous introduisons les notions requises d'Algèbre Universelle, nous décrivons le clone engendré par l'ensemble $\{f_n,\ n \in \mathbb{N}\}$, puis nous montrons que l'intervalle I de L engendré par $\{f_x,\ x \in X\}$ $(X \subseteq \mathbb{N})$ est large mais non booléen (i.e. il existe un plongement qui préserve l'ordre du treillis $\underset{\sim}{P}$ des sous-ensembles de $\mathbb{N} = \{1,2,\ldots\}$ ordonné par l'inclusion dans I, mais ce plongement n'est pas un isomorphisme de treillis).

Les opérations f_i peuvent être interprétées comme étant des extensions en un point d'opérations partielles, ainsi les résultats ci-haut montrent qu'il existe $2^{\aleph_0}$ clones partiels sur tout univers fini avec plus qu'un élément.

2. Opérations f_n et relations ρ_m, $n \ge 1$ et $m \ge 1$

Nous supposerons que $B = \{0,\ldots,k-1\}$, où $k > 2$. Il sera avantageux de dénoter $k-1$ par ∞. Une *relation* m-aire sur B est un sous-ensemble de B^m $(m \ge 1)$. Soit ρ une relation m-aire et f une opération n-aire sur B $(m \ge 1,\ n \ge 1)$. Nous dirons que l'opération f préserve ρ si pour toute matrice $X := (x_{ij})$ de type $m \times n$ dont toutes les colonnes $X_{*j} = (x_{1j},x_{2j},\ldots,x_{mj})^T$, $j = 1,2,\ldots,n$, sont dans ρ, alors le m-tuple $(f(X_{1*}),f(X_{2*}),\ldots,f(X_{m*})) \in \rho$ où le vecteur $X_{k*} = (x_{k1},x_{k2},\ldots,x_{kn})$ est la k-ième ligne de la matrice $X = (x_{ij})$.

Pour une relation m-aire ρ sur B, on note

$$\text{Pol } \rho = \{f \in \underset{\sim}{O}: \ f \ \text{préserve} \ \rho\}.$$

Il est facile de vérifier que Pol ρ est un clone pour toute relation m-aire ρ, $m \geq 1$.

Soit $R^{(m)}$ l'ensemble de toutes les relations m-aires sur B et $\underset{\sim}{R} = \bigcup_{m=1}^{\infty} R^{(m)}$. Il est connu que tout clone sur B est l'intersection d'une chaîne descendante au plus dénombrable de clones Pol $\rho_1 \supseteq$ Pol $\rho_2 \supseteq \ldots$, pour certaines relations $\rho_i \in \underset{\sim}{R}$ $(i = 1,2,\ldots)$. En vue de ceci, il est important de savoir quand est-ce que Pol $\rho \subseteq$ Pol σ pour $\rho,\sigma \in \underset{\sim}{R}$. La formulation est plus simple pour les relations σ qui suivent. Nous disons qu'une relation h-aire σ est *sans répétition* si pour tout $1 \leq i < j \leq h$ il existe $(a_1,\ldots,a_h) \in \sigma$ avec $a_i \neq a_j$. Il est facile de voir que pour toute relation ρ il existe une relation sans répétition σ tel que Pol ρ = Pol σ. Des résultats de [2], on peut déduire le résultat fondamental suivant:

Soit $I \neq \emptyset$ un ensemble d'indices et pour tout $i \in I$ soit ρ_i une relation h_i-aire sur B. Soit σ une relation sans répétition h-aire sur B. Alors $\bigcap_{i \in I}$ Pol $\rho_i \subseteq$ Pol σ si et seulement s'il existe un sous-ensemble fini J de I, un entier $n \geq h$ et des applications $\varphi_j\colon \{1,\ldots,h_j\} \to \{1,\ldots,n\}$ $(j \in J)$ tel que σ consiste des $(x_1,\ldots,x_h)$ pour lesquels il existe $(x_{h+1},\ldots,x_n) \in B$ qui satisfont $(x_{\varphi_j(1)},\ldots,x_{\varphi_j(h_j)}) \in \rho_j$ pour tout $j \in J$. Le produit $\rho_1 \cdot \rho_2$ des relations binaires ρ_1 et ρ_2 est un exemple usuel, ici

$$\rho_1 \cdot \rho_2 = \{(x_1,x_2)\colon \ (x_1,x_3) \in \rho_1, \ (x_3,x_2) \in \rho_2, \ \text{pour un} \ x_3 \in B\}.$$

Nous choisissons $h = 2$, $n = 3$, $\varphi_1(1) = 1$, $\varphi_1(2) = 3$, $\varphi_2(1) = 3$, $\varphi_2(2) = 2$. Ici

$$\text{Pol } \rho_1 \cap \text{Pol } \rho_2 \subseteq \text{Pol } \rho_1 \cdot \rho_2$$

ce qui peut être vérifié directement.

Pour k un entier positif, posons $\underline{k} = \{0,1,\ldots,k-1\}$. On peut supposer que $B = \underline{k}$.

On pose, pour $m \geq 1$

$$\rho_m = (B^m \backslash \underline{2}^m) \cup \{(x_1,\ldots,x_m) \in \underline{2}^m: \sum_{i=1}^{m} x_i = 1\},$$

où la somme est l'addition ordinaire des entiers.

Exemples:

$$\rho_1 = (B\backslash \underline{2}) \cup \{1\} = B\backslash\{0\}$$

$$\rho_2 = (B^2\backslash \underline{2}^2) \cup \{(0,1),(1,0)\}.$$

On définit sur B les opérations n-aires suivantes:

$$f_n(x_1,\ldots,x_n) = \begin{cases} 0 & \text{si } \sum_{i=1}^{n} x_i = 1 \\ \infty & \text{sinon.} \end{cases}$$

Exemples:

$$f_1(1) = 0, \quad f_1(x) = \infty \quad \text{pour} \quad x \neq 1$$

$$f_2(0,1) = f_2(1,0) = 0, \quad f_2(x,y) = \infty \quad \text{pour} \quad (x,y) \notin \{(1,0),(0,1)\}.$$

L'idée générale revient à l'origine à Janov et Mučnik et sa forme actuelle se trouve dans Demetrovics et Hannák [9].

Pour $X \subseteq \mathbb{N} = \{1,2,\ldots\}$, on pose

$$\chi(X) := \bigcap_{i \in \mathbb{N}\backslash X} \mathrm{Pol}\, \rho_i,$$

la correspondance χ est une application monotone de $(P(\mathbb{N}),\subseteq)$ dans le treillis des clones L_B sur B. Ceci est implicite dans Janov et Mučnik [11] et explicite dans Rosenberg [19]. Donc L_B (en tant qu'ensemble ordonné) contient une copie de $P(\mathbb{N})$, en particulier $|L_B| \geq 2^{\aleph_0}$. Par ailleurs les clones sont des sous-ensembles de l'ensemble dénombrable $\underset{\sim}{O}_B$, donc $|L_B| \leq 2^{\aleph_0}$.

Nous avons:

LEMME 1 [19, p. 172]. *Soit* $C_m := \mathrm{Pol}\, \rho_m$, $m \geq 1$. *Alors*

$$f_n \in C_m \iff n \nmid m.$$

DÉMONSTRATION. ($\Rightarrow$) Il suffit de démontrer, par un contre-exemple, que $f_n \notin \mathrm{Pol}\, \rho_n$.

On considère la matrice identité $n \times n$.

On note $\underline{a}_j$ le n-tuple $(0,0,\dots,1,\dots,0)$ où la j-ième coordonnée est égale à 1, il est clair que $\underline{a}_j^T \in \rho_n$ et $f_n(\underline{a}_j) = 0$ $\forall j = 1,\dots,n$, donc toutes les colonnes de la matrice appartiennent à ρ_n tandis que $(f_n(\underline{a}_1),\dots,f_n(\underline{a}_n)) = (0,\dots,0) \notin \rho_n$ donc $f_n \notin \mathrm{Pol}\, \rho_n$.

($\Leftarrow$) On suppose que $n \nmid m$. Soit

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

et on suppose que

$$(f_n(a_{11},\dots,a_{1n}), f_n(a_{21},\dots,a_{2n}),\dots,f_n(a_{m1},\dots,a_{mn})) \notin \rho_m.$$

Puisque f_n prend les valeurs 0 ou ∞, il en découle que $f_n(a_{i1},\dots,a_{in}) = 0$ $\forall i = 1,\dots,m$, donc

$$\sum_{k=1}^{n} a_{ik} = 1 \qquad \forall i = 1,\dots,m,$$

et par conséquent dans chaque ligne de la matrice A, un et un seul élément est 1, tandis que tous les autres éléments sont nuls.

<u>1^{er} cas</u>: Si $n < m$, alors au moins une colonne de la matrice A contient deux éléments (ou plus) égaux à 1, donc cette colonne n'appartient pas à ρ_m.

<u>2^e cas</u>: Si $m < n$, au moins une colonne de la matrice A est nulle, et n'appartient donc pas à ρ_m. □

3. <u>Clones engendrés par les</u> f_n $(n = 1,2,\ldots)$

Soit A une matrice 0-1 de type $m \times n$. Notons par $s(A) = \{\underline{x} \in \underline{2}^n : A\underline{x}^T = \underline{1}_m^T\}$, où $\underline{1}_m$ est le m-vecteur $(1,1,\ldots,1)$. Posons $\underline{S} = \{s(A) : A$ est une matrice 0-1$\}$. Pour $s \in \underline{S}$, $s \subseteq \underline{2}^n$ soit $g_s \in 0^{(n)}$ définie par $g_s(\underline{x}) = 0$ si $\underline{x} \in s$ et $g_s(\underline{x}) = \infty$ sinon. Par exemple, $f_n = g_{s(\underline{1}_n)}$.

Soit F le clone engendré par les opérations f_n, $n = 1,2,\ldots$.

PROPOSITION 2. $G = \{g_s,\ s \in \underline{S}\}$ *est le clone* F *engendré par* $\{f_n,\ n = 1,2,\ldots\}$.

DÉMONSTRATION. Nous montrons d'abord que G est un clone.

1) Soient A et A' des matrices 0-1 de type $m \times n$ et $m' \times n'$, $r = n' + n-1$ et $I = g_{s(A)} * g_{s(A')}$ (l'opération $*$ a été définie à la Section 1).

(a) Supposons $n > 1$. Soit A'' la matrice de type $m \times (n-1)$ obtenue en supprimant la première colonne de A. Posons

$$M = \left[\begin{array}{c|c} A' & 0 \\ \hline 0 & A'' \end{array}\right].$$

Nous montrons que $I = g_{s(A)} * g_{s(A')} = g_{s(M)}$. Il est clair que I ne prend que des valeurs 0 et ∞. Soit $\underline{x} = (x_1,\ldots,x_r) \in \underline{2}^r$, $\underline{y} = (x_1,\ldots,x_{n'})$, $\underline{z} = (x_{n'+1},\ldots,x_r)$ et $\alpha = g_{s(A')}(x_1,\ldots,x_{n'})$.

Soit $I(\underline{x}) = 0$. Par la définition de g_s, on a $\alpha = 0$. Donc $A(0,\underline{z})^T = \underline{1}_n$, i.e. $A''\underline{z}^T = \underline{1}_{n-1}$. De plus, pour une raison identique $A'\underline{y}^T = \underline{1}_{m'}$, et donc ensemble $M\underline{x}^T = \underline{1}_r$, i.e. $g_{s(M)}(\underline{x}) = 0$.

Cet argument peut être inversé pour montrer que $g_{s(M)}(\underline{x}) = 0 \Rightarrow I(\underline{x}) = 0$.

(b) Soit $n = 1$. On peut vérifier que $I(x_1,\dots,x_r) = \infty$ pour tous $x_1,\dots,x_r \in B$ (car même si $f = g_{s(1)}$ on a $g_{s(1)}(0) = \infty$), donc $I = g_{s(\underline{0}r)}$, et par la suite $I \in G$.

2) Soit A une matrice 0-1 de type $m \times n$. Soit A_1 la matrice obtenue de A en échangeant les deux premières colonnes si $n > 1$ et $A = A_1$ si $n = 1$. Alors $\tau g_{s(A)} = g_{s(A)} \in G$ l'opération τ a été définie à la Section 1). Par un argument similaire $\zeta g_{s(A)} \in G$.

(a) Supposons que $n \geq 2$. Pour montrer que G est fermé sous l'opération Δ, nous construisons A^Δ de type $k \times (n-1)$, avec $k \geq m$ de la façon suivante:

(α) Chaque ligne A_{i*} de A avec $A_{i1} + A_{i2} = 2$ est remplacée par les deux lignes $(1,A_{i3},\dots,A_{in})$ et $(0,A_{i3},\dots,A_{in})$.

(β) Chaque ligne A_{i*} avec $\varepsilon = A_{i1} + A_{i2} < 2$ est remplacée par une ligne $(\varepsilon,A_{i3},\dots,A_{in})$, e.g. on a

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad A^\Delta = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

(b) Si $n = 1$, on pose $A^\Delta = A$.

Il est facile de vérifier que $\Delta g_{s(A)} = g_{s(A^\Delta)}$, e.g. pour A plus haut on a

$$g_{s(A)}(\underline{x}) = 0 \iff x_1 + x_2 + x_3 = 1, \quad x_2 + x_4 = 1, \quad x_5 = 1$$

$$\Delta g_{s(A)}(\underline{y}) = 0 \iff 2y_1 + y_2 = 1, \quad y_1 + y_3 = 1, \quad y_4 = 1 \iff \underline{y} = (0,1,1,1)$$

et

$$g_{s(A^\Delta)}(\underline{y}) = 0 \iff \underline{y} = (0,1,1,1).$$

On vient donc de démontrer que G est un clone. On a remarqué plus haut que $f_n = g_{s(\underline{1}_n)} \in G$. Ceci prouve que $F \subseteq G$.

Nous montrons que $G \subseteq F$. Soit A une matrice 0-1 de type $m \times n$ qui n'a pas de ligne $\underline{0}_n$. Pour $i = 1,\dots,m$ posons

$$t_i = \{j: A_{ij} = 1\}, \qquad e(i) = |t_i|.$$

Ecrivons $t_i = \{t_{i1},\dots,t_{ie(i)}\}$ où $t_{i1} < \dots < t_{ie(i)}$, et posons $u = m-1+e(1)$. Soit g l'opération u-aire sur B définie en posant

$$g(x_1,\dots,x_u) = f_u(x_{t_{11}},\dots,x_{t_{1e(1)}}, f_{e(2)}(x_{t_{21}},\dots,x_{t_{2e(2)}}),\dots,$$
$$\dots,f_{e(m)}(x_{t_{m1}},\dots,x_{t_{me(m)}})),$$

pour tous $x_1,\dots,x_u \in B$. Il est évident que $g \in F$. On vérifie facilement que $g = g_{s(A)}$. Supposons que A a une ligne $\underline{0}_n$. Alors $s(A) = \emptyset$. Si $n = 1$ alors $g_\emptyset(x_1) = (\Delta f_2)(x_1)$ pour tout $x_1 \in B$ donc $g_\emptyset \in F$. Si $n > 1$ alors $g_\emptyset(x_1,\dots,x_n) = f_1(f_n(x_1,\dots,x_n))$ pour tous $x_1,\dots,x_n$, donc $g_\emptyset \in F$. Donc $G \subseteq F$ et $G = F$. □

REMARQUE 3. Il est clair que la correspondance $A \to s(A)$ n'est pas injective (en effet il suffit de considérer A' obtenue en permutant les lignes de A, alors $s(A) = s(A')$).

On considère la correspondance

$$\varphi: \underset{\sim}{P} \to L_B$$
$$X \to \varphi(x) = \langle f_i,\ i \in X\rangle.$$

où $\langle f_i,\ i \in X\rangle$ est le clone engendré par les f_i.

PROPOSITION 4. i) φ *est une application croissante injective de* $\underset{\sim}{P}$ *dans le treillis des sous-clones de* F,

ii) $\operatorname{Im}\varphi$ *n'est pas un sous-treillis de* L_B.

DÉMONSTRATION. i) Nous savons (Lemme 1) que pour tout $i \in X$, $f_i \in \chi(X) = \bigcap_{j \in \mathbb{N}\setminus X} \operatorname{Pol}\rho_j$, donc le clone $\varphi(X)$ engendré par $\{f_i,\ i \in X\}$ satisfait $\varphi(X) \subseteq \chi(X)$. D'autre part pour tout $j \in \mathbb{N}\setminus X$, on a $f_j \notin \operatorname{Pol}\rho_j$, donc $f_j \notin \chi(X)$

et par conséquent $f_j \notin \varphi(X)$. On a

$$f_i \in \varphi(X) \iff i \in X$$

ce qui montre que φ est injective. Evidemment φ est croissante.

ii) Pour montrer que $\mathrm{Im}\,\varphi$ n'est pas un sous-treillis de L_B, on considère

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Ici $s(A) = \{(1,0,1),(0,1,0)\}$. Soit $g = g_{s(A)}$. Par la construction dans la démonstration de la Proposition 2, on a

$$g(x_1,x_2,x_3) = f_3(x_1,x_2,f_2(x_2,x_3))$$

pour tous $x_1,x_2,x_3 \in B$ donc $g \in \langle f_2,f_3\rangle$ et par conséquent $\langle g\rangle \subseteq \langle f_2,f_3\rangle$. Pour montrer que l'inclusion est stricte, il suffit de considérer la relation ρ_3. Nous montrons que $g \in \mathrm{Pol}\,\rho_3$, donc $\langle g\rangle \subseteq \mathrm{Pol}\,\rho_3$ où $f_3 \notin \mathrm{Pol}\,\rho_3$, donc $\langle f_2,f_3\rangle \nsubseteq \mathrm{Pol}\,\rho_3$. En effet soit M une matrice 3×3 telle que

$$(g(M_{1*}),g(M_{2*}),g(M_{3*})) \notin \rho_3.$$

Comme les valeurs de g sont 0 ou ∞ on a

$$g(M_{1*}) = g(M_{2*}) = g(M_{3*}) = 0$$

$M_{i*} \in s(A)$ $(i = 1,2,3)$. Comme $|s(A)| = 2$ on a $M_{i*} = M_{j*}$ pour certains $1 \leq i < j \leq 3$. Il est facile de voir qu'il y a une colonne M_{*t} dont la somme est au moins 2, donc $M_{*t} \notin \rho_3$. Ainsi $\langle g\rangle \subset \langle f_2,f_3\rangle$. Or $f_2(x,y) = g(x,y,x)$, pour tous $x,y \in B$, donc $f_2 \in \langle g\rangle$, d'où $\langle f_2\rangle \subseteq \langle g\rangle$. Nous montrons à présent que $g \notin \langle f_2\rangle$, donc que l'inclusion $\langle f_2\rangle \subset \langle g\rangle$ est stricte. Pour cela, on considère:

$$\begin{aligned}\rho = \ &\{(0,0,x,y):\ x,y \in \{0,1,\infty\}\}\setminus\{(0,0,\infty,\infty)\}\\ &\cup \{(0,1,0,1),(1,0,1,1),(0,1,1,0)\}\\ &\cup [\{\infty\} \times \{0,\infty\}^3] \cup [\{0,\infty\} \times \{\infty\} \times \{0,\infty\}^2].\end{aligned}$$

En prenant la matrice

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

dont toutes les colonnes A_{*i} $(i = 1,2,3)$ appartiennent à ρ avec $(g(A_{1*}),g(A_{2*}),g(A_{3*}),g(A_{4*})) = (0,0,\infty,\infty) \notin \rho$, on voit que $g \notin \mathrm{Pol}\,\rho$. Or $f_2 \in \mathrm{Pol}\,\rho$, en effet soit A une matrice 0-1-∞ de type 4×2, et supposons que

$$(a_1,a_2,a_3,a_4) = (f_2(A_{1*}),f_2(A_{2*}),f_2(A_{3*}),f_2(A_{4*})) \notin \rho,$$

puisque $\mathrm{Im}\, f_2 \subseteq \{0,\infty\}$ on a

$$(a_1,a_2,a_3,a_4) = (0,0,\infty,\infty),$$

il en résulte, de la définition de f_2, que A_{1*} et $A_{2*} \in \{(0,1),(1,0)\}$. Si $A_{1*} = A_{2*}$, l'une des colonnes A_{*1} ou A_{*2} débute par 1, 1 et par conséquent n'appartient pas à ρ. On suppose donc $A_{1*} = (0,1)$ et $A_{2*} = (1,0)$, or $f(A_{3*}) = f(A_{4*}) = \infty$, il en découle que A_{3*} et $A_{4*} \in \{(0,0),(1,1),(0,\infty),(\infty,0),(1,\infty),(\infty,1),(\infty,\infty)\}$, or si $A_{32} \neq 1$, la colonne $A_{*2} \notin \rho$, et de même si $A_{31} = \infty$, la colonne $A_{*1} \notin \rho$, on suppose donc $A_{3*} = \{(1,1)\}$. De plus, pour que $A_{*2} \in \rho$, il faut que $A_{42} = 1$, donc que $A_{4*} \in \{(1,1),(\infty,1)\}$, et dans l'un ou l'autre des cas, $A_{*1} \notin \rho$, donc $f_2 \in \mathrm{Pol}\,\rho$.

On a ainsi $\langle f_2\rangle \subset \langle g\rangle \subset \langle f_2,f_3\rangle$, vu que φ est croissante, ceci montre que $\mathrm{Im}\,\varphi$ n'est pas un sous-treillis de L_B. □

Pour conclure, nous donnons la remarque suivante:

REMARQUE 5. Soit A un ensemble tel que $1 < |A| < \aleph_0$, n un entier positif. Une *opération* n-aire *partielle* sur A est une application f d'un sous-ensemble D_f de A^n dans A, (D_f est dit le *domaine* de f). On note $P^{(n)}$ l'ensemble des opérations n-aires partielles sur A et $P = \bigcup_{n\geq 1} P^{(n)}$. Pour

$X \subseteq P$, la paire $\langle A,X \rangle$ est dite une *algèbre partielle.*

Un moyen pour manipuler une algèbre partielle consiste à la plonger dans une algèbre totale, ce qui se fait en ajoutant un nouvel élément ∞ à A.

On pose $B = A \cup \{\infty\}$ et on peut ainsi étendre chaque $f \in P^{(n)}$ à une opération $\hat{f} \in O^{(n)}$ $(n = 1,2,\ldots)$ (voir l'introduction) en posant

$$\hat{f}(a_1,\ldots,a_n) = \begin{cases} f(a_1,\ldots,a_n) & \text{si } (a_1,\ldots,a_n) \in D_f \\ \infty & \text{sinon.} \end{cases}$$

Soit $f \in O^{(n)}$. On dit que f *dépend* de sa i-ième variable (ou que la i-ième variable de f est *essentielle*) s'il existe $\underline{x} = (x_1,\ldots,x_n)$ et $\underline{y} = (y_1,\ldots,y_n) \in B^n$ tel que $x_i \neq y_i$, $x_j = y_j$ pour tout $j \neq i$, $j = 1,\ldots,n$ avec $f\underline{x} \neq f\underline{y}$. On considère $\hat{P} = \{\hat{f}\colon f \in P\}$. On dénote par R le clone sur B engendré par $\hat{P}$ et il est connu que [20]: Une *opération* g *sur* B *appartient à* R *si et seulement si*

i) $g(x_1,x_2,\ldots,x_n) = \infty$ *si, pour un certain* $i = 1,\ldots,n$, g *dépend de sa* i-*ième variable et* $x_i = \infty$,

ii) $g(\infty,\infty,\ldots,\infty) = \infty$.

On considère de plus que le clone Q des opérations sur B qui vérifient i) uniquement. Il est facile de montrer que Q s'obtient de R en ajoutant toutes les opérations n-aires constantes à valeurs dans A $(n = 1,2,\ldots)$.

Ainsi pour k un entier positif, $k \geq 2$, on pose $A = \underline{k-1} = \{0,\ldots,k-2\}$, $B = A \cup \{\infty\} = \underline{k}$ où ∞ dénote l'élément $k-1$. Les opérations f_i définies à la Section 2 peuvent être considérées comme des extensions à B d'opérations partielles sur A, et il est évident que $f_n \in R$, $\forall n \geq 1$. Nous avons ainsi

COROLLAIRE 6. *On note* $C\ell(R)$ *(respectivement* $C\ell(Q)$*) le treillis des sous-clones de* R *(respectivement de* Q*). Alors* $|C\ell(R)| = |C\ell(Q)| = 2^{\aleph_0}$.

DÉMONSTRATION. On considère l'application χ_R

$$\chi_R\colon \underset{\sim}{P} \to C\ell(R)$$
$$X \to \chi_R(X) = R \cap \Big(\bigcap_{j \in \mathbb{N} \setminus X} \operatorname{Pol} \rho_j \Big) .$$

Il est clair que χ_R est croissante. Soient $X, X' \subseteq N$ et $n \in X \backslash X'$. Par le Lemme 1, $f_n \in R \cap (\bigcap_{x \in \mathbb{N}\backslash X} \text{Pol } \rho_x)$ tandis que $f_n \notin R \cap (\bigcap_{x \in \mathbb{N}\backslash X'} \text{Pol } \rho_x)$, donc $f_n \in \chi_R(X) \backslash \chi_R(X')$, ce qui prouve que χ_R est injective. Il en résulte que $|C\ell(R)| \geq 2^{\aleph_0}$.

L'ensemble A étant fini, on déduit que le sous-ensemble $C\ell(R)$ de $P(\underset{\sim}{Q})$ satisfait $|C\ell(R)| \leq 2^{\aleph_0}$, d'où l'égalité pour $C\ell(R)$. D'autre part $R \subset Q$, donc $|C\ell(Q)| \leq 2^{\aleph_0}$, et alors $|C\ell(Q)| = 2^{\aleph_0}$. □

REMARQUE 7. χ_R n'est pas une application surjective de $\underset{\sim}{P}$ sur $C\ell(R)$.

DÉMONSTRATION. On pose $\sigma_2 = \{(x,y) : (x,x,y) \in \rho_3\}$. De la théorie générale, on voit que $\text{Pol } \rho_3 \subseteq \text{Pol } \rho_2$. Donc

(1) $$\text{Pol } \rho_3 \cap \text{Pol } \rho_2 \subseteq \text{Pol } \rho_2 \cap \text{Pol } \rho_2 \subseteq \text{Pol } \rho_2.$$

Nous allons montrer que les deux inclusions sont strictes.

Soit f une opération ternaire, définie par $f(0,0,0) = 1$, $f(1,1,1) = 0$, $f(x_1,x_2,x_3) = \infty$ ailleurs. On montre que $f \notin \text{Pol } \sigma_2$, pour cela, on considère la matrice

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

dont toutes les colonnes sont dans σ_2 tandis que

$$(f(0,0,0), f(1,1,1)) = (1,0) \notin \sigma_2.$$

On montre que $f \in \text{Pol } \rho_2$.

Soit $A = [a_{ij}]$ une matrice 2×3 telle que $b_i = f(A_{i*})$ $(i = 1,2)$ satisfont $(b_1,b_2) \notin \rho_2$. Alors $b_1, b_2 \in \{0,1\}$ et $b_1 = b_2$. Par la définition de f, on a $a_{ij} = 1-b_1$, pour tous i,j. En particulier $(a_{11},a_{21}) = (1-b_1, 1-b_1) \notin \rho_2$. Ce qui prouve que $f \in \text{Pol } \rho_2$, il s'ensuit que la dernière inclusion en (1) est stricte.

On montre à présent que $\mathrm{Pol}\ \rho_3 \subset \mathrm{Pol}\ \sigma_2$. Pour cela, il suffit de montrer que f_3 (définie à la Section 2) appartient à $\mathrm{Pol}\ \sigma_2$. Soit $A = [a_{ij}]$ une matrice 2×3 telle que $a_i = f_3(A_{i*})$ $(i = 1,2)$ satisfont $(a_1,a_2) \notin \sigma_2$. Alors $a_1,a_2 \in \{0,1\}$ et par la définition de f_3, $a_1 = a_2 = 0$. Alors

$$a_{11} + a_{12} + a_{13} = a_{21} + a_{22} + a_{23} = 1,$$

donc on a $a_{1t} = 1$ pour un $1 \leq t \leq 3$ et $(a_{1t},a_{2t}) \notin \sigma_2$. Donc $f_3 \in \mathrm{Pol}\ \sigma_2$. On sait (Lemme 1) que $f_3 \in \mathrm{Pol}\ \rho_2 \backslash \mathrm{Pol}\ \rho_3$, d'où la première inclusion de (1) est aussi stricte.

Vu que $f \in R$, on déduit que

$$\chi_R(N \backslash \{2,3\}) \subset R \cap \mathrm{Pol}\ \sigma_2 \cap \mathrm{Pol}\ \rho_2 \subset \chi_R(N \backslash \{2\}).$$

Puisque χ_R est croissante, $R \cap \mathrm{Pol}\ \sigma_2 \cap \mathrm{Pol}\ \rho_2$ n'est pas dans l'image de χ_R, et par conséquent χ_R n'est pas surjective. □

Références

[1] AGOSTON, I., DEMETROVICS, J., HANNÁK, L., On the cardinality of clones containing all constants, *Coll. Math. Soc. J. Bolyai* 43(1985), North Holland.

[2] BENZAKEN, C., *Contribution des structures algébriques ordonnées à la théorie des réseaux*, Thèse d'Etat, Grenoble (France), 1968.

[3] BENZAKEN, C., Post's closed systems and the weak chromatic number of hypergraphs, *Discrete Mathematics* 23(1978), 77-84.

[4] BODNARCUK, V.G., KALUZNIN, L.A., KOTOV, V.N., ROMOV, B.A., Galois theory for Post algebras I-II (Russian), *Kibernetika* 5(1969), 1-10 et 5(1969), 1-9; Version anglaise: *Cybernetics* 5(1969), 243-252 et 531-539.

[5] DEMETROVICS, J., HANNÁK, L., MARCENKOV, S.S., Some remarks on the structure of P_3, *C.R. Math. Rep. Acad. Sci.* 2(1980), 251-219, Canada.

[6] DEMETROVICS, J., HANNÁK, L., MARCENKOV, S.S., On closed classes of self-dual functions in P_3, *Colloq. Math. Soc. J. Bolyai* 28(1981), 183-189, North-Holland.

[7] DEMETROVICS, J., HANNÁK, L., RONYAI, L., Prime element algebras with transitive automorphism groups, *C.R. Comp. Rend. Math. Acad. Sci.* 3(1981), 1, 19-22, Canada.

[8] DEMETROVICS, J., HANNÁK, L., The number of reducts of a preprimal algebras, *Alg. Univ.* 16(1983), 178-185.

[9] DEMETROVICS, J., HANNÁK, L., On construction of large set of clones, *Zeitschr. f. math. Logik und Grundlagen d. Math. Bd.* 33(1987), S.127-133.

[10] JABLONSKII, S.V., Functional constructions in a k-valued logic (Russian), *Trudy Mat. Inst. Steklov* 51(1958), 5-142; MR21 # 3331.

[11] JANOV. JU. I, MUCNIK, A.A., Existence of k-valued closed classes without a finite basis (Russian), *Dokl. Akad. Nauk. SSR* 127(1959), 44-46; MR 21 # 7174.

[12] McKENZIE, R., McNULTY, G., TAYLOR, W., *Algebras, Lattices, Varieties*, Vol. I., Wadswisth & Brooks/Cole, 1987.

[13] MAL'CEV, A.I., Iterative algebras and Post's varieties (Russian), *Algebra i Logika* 5(1966), 5-24, Version anglaise: *The Metamathematics of Algebraic Systems*, Collected Papers 1936-1967; Studies in Logics and Foundations of Mathematics, Vol. 66, North-Holland, 1971.

[14] MARCENKOV, S.S., On closed classes of self-dual functions in k-valued logics (Russian), *Problemy Kibernet.* 36(1979).

[15] PÖSCHEL, R., KALUŽNIN, L.A., *Funktionen und Relationenalgebren. Ein Kapitel der diskreten Mathematik*, Deutscher Verlag der Math. Wiss. Berlin 1979 and Birkhauser, Basel and Stuttgart, 1979.

[16] POST, E.L., *The Two-valued Iterative Systems of Mathematical Logic*, Ann. Math. Studies 5, Princeton Univ. Press, 1941.

[17] ROSENBERG, I.G., La structure des fonctions de plusieurs variables sur un ensemble fini, *C.R. Acad. Sci. Paris*, Ser. A-B, 260(1965), 3817-3819; MR 31 # 1185.

[18] ROSENBERG, I.G., Uber die funktionale Vollständigkeit in der mehrwertigen Logiken, *Rozpravy Československé Akad. Věd.*, Řada Mat. Přir, Věd. 80, 4(1970), 1-93; MR 45 # 1732.

[19] ROSENBERG, I.G., Composition of functions on finite sets, completeness and relations, a short survey, *Multiple-Valued Logic and Computer Science* (D. Rine, ed.), North-Holland (1977), 144-187. Second Edition ibid. (1984), 150-192.

[20] ROSENBERG, I.G., Partial clones (in preparation).

[21] HADDAD, L., *Le treillis des clones partiels sur un univers fini et ses coatomes*, Thèse de Philosophiae Doctor, Université de Montréal, Septembre 1986.

[22] HADDAD, L., ROSENBERG, I.G., Familles larges de clones sur un univers fini, Preprint CRM-1352, Université de Montréal, Mars 1986.

Lucien Haddad
Pure Mathematics Department
University of Waterloo
Waterloo, Ontario N2L 3G1

Ivo G. Rosenberg
Département de mathématiques
et de statistique
Université de Montréal
C.P. 6128, Succ. "A"
Montréal, Québec H3C 3J7

Manuscrit reçu le 29 août 1986.
Revision le 25 juin 1987.