Notes sur l'article de Lafont : Towards an algebraic theory of boolean circuits

Florence Clerc

Définition 1. On note $\mathcal{M}$ la catégorie dont les objets sont les entiers vus comme des ensembles

$$[n] = O, ..., n-1$$

et dont les morphismes sont les fonctions croissantes. La composition est la composition au sens usuel. Les identités, notées id_n, sont les fonctions identités $[n] \to [n]$ usuelles, pour $[n]$ un objet de $\mathcal{M}$.

Lemme 2. On munit la catégorie $\mathcal{M}$ du produit tensoriel défini de la façon suivante.

Pour deux objets $[m]$ et $[n]$ de $\mathcal{M}$,

$$[m] \otimes [n] = [m+n].$$

Pour deux morphismes $f_1 : [m_1] \to [n_1]$ et $f_2 : [m_2] \to [n_2]$,

$$\begin{array}{rlll} f_1 \otimes f_2 : & [m_1 + m_2] & \to [n_1 + n_2] & \\ & m & \mapsto f_1(m) \text{ si } m < m_1 & \\ & m & \mapsto n_1 + f_2(m) \text{ sinon } & (m_1 \leq m < m_1 + m_2) \end{array}$$

La catégorie $(\mathcal{M}, \otimes, [0])$ est monoidale.

Lemme 3. Il existe un unique morphisme $[2] \to [1]$ de $\mathcal{M}$, noté μ.

Il existe un unique morphisme $[0] \to [1]$ de $\mathcal{M}$, noté η.

Démonstration. L'objet $[1]$ est terminal dans la catégorie $\mathcal{M}$. □

Définition 4. On appelle PRO une catégorie monoïdale stricte dont les objets sont les entiers naturels vus comme des ensembles et dont le produit tenosriel est donné par l'addition.

Définition 5. On note $\underline{PRO}$ la catégorie dont les objets sont les PROs et dont les morphismes sont les foncteurs monoïdaux. La composition et les identités sont entendus au sens usuel.

Définition 6. On appelle signature la donnée de deux ensembles E_1 et E_2 et de deux applications $s, t : E_2 \to E_1^*$ où E_1^* est le monoïde libre engendré par E_1. On note une telle signature (E_1, s, t, E_2).

Définition 7. On note $\underline{Sig}$ la catégorie dont les objets sont les signatures et dont les morphismes $f : (E_1, s, t, E_2) \to (E_1', s', t', E_2')$ sont la donnée de deux morphismes $f_1 : E_1 \to E_1'$ et $f_2 : E_2 \to E_2'$ tels que les deux diagrammes suivant commutent :

$$\begin{array}{ccc} E_2 & \xrightarrow{s} & E_1^* \\ {\scriptstyle f_2}\downarrow & & \downarrow{\scriptstyle f_1^*} \\ E_2' & \xrightarrow[s']{} & (E_1')^* \end{array} \quad \text{et} \quad \begin{array}{ccc} E_2 & \xrightarrow{t} & E_1^* \\ {\scriptstyle f_2}\downarrow & & \downarrow{\scriptstyle f_1^*} \\ E_2' & \xrightarrow[t']{} & (E_1')^* \end{array}$$

où f_1^* est le morphisme de monoïdes $E_1^* \to (E_1')^*$ induit par f_1. On peut noter $f = (f_1, f_2)$.

On définit la composition de $(f_1, f_2) : (E_1, s, t, E_2) \to (E_1', s', t', E_2')$ et de $(g_1, g_2) : (E_1', s', t', E_2') \to (E_1'', s'', t'', E_2'')$ comme

$$(g_1 \circ f_1, g_2 \circ f_2) : (E_1, s, t, E_2) \to (E_1'', s'', t'', E_2'').$$

L'identité sur une signature (E_1, s, t, E_2) est donnée par (id_{E_1}, id_{E_2}).

Définition 8. On définit le foncteur d'oubli

$$U : \underline{PRO} \to \underline{Sig}$$

Pour tout PRO $\mathcal{C}$, on pose

$$U(\mathcal{C}) = ([1], s, t, E_2)$$

avec $E_2 = Hom\mathcal{C}$ et pour tout morphisme $f : A \to B$ de $\mathcal{C}$, $s(f) = A$ et $t(f) = B$.

Pour tout foncteur monoidal $f : \mathcal{C} \to \mathcal{D}$, on pose

$$(f_1, f_2) = U(f) : ([1], s, t, Hom\mathcal{C}) \to ([1], s', t', Hom\mathcal{D})$$

avec f_1 la fonction identité sur $[1]$ et pour tout morphisme α de la catégorie $\mathcal{C}$, $f_2(\alpha) = f(\alpha)$.

Lemme 9. Le foncteur U admet un adjoint à gauche $F : \underline{Sig} \to \underline{PRO}$.

Définition 10. On appelle $\mathbb{M}_0$ le PRO libre défini par $\mathbb{M}_0 = F(\Sigma)$ où Σ est la signature

$$\Sigma = ([1], \{\mu : [2] \to [1], \eta : [0] \to [1]\})$$

(où $[2]$ et $[0]$ s'expriment comme produits tensoriels de $[1]$).

Définition 11. $\mathcal{E}(E_1, s_1, t_1, E_2)$

Définition 12. On appelle théorie la donnée de trois ensembles E_1, E_2 et E_3 et de quatre applications $s_1, t_1 : E_2 \to E_1^*$ et $s_2, t_2 : E_3 \to E_2^*$ où (E_1, s_1, t_1, E_2) est une signature, où E_2^* est l'ensemble des morphismes de la catégorie $\mathcal{E}(E_1, s_1, t_1, E_2)$ et où

$$s_1^* \circ s_2 = s_1^* \circ t_2 \quad \text{et} \quad t_1^* \circ s_2 = t_1^* \circ t_2$$

On la note $(E_1, s_1, t_1, E_2, s_2, t_2, E_3)$

Définition 13. On note $\underline{Th}$ la catégorie dont les objets sont les théories et dont les morphismes sont

$$(f_1, f_2, f_3) : (E_1, s_1, t_1, E_2, s_2, t_2, E_3) \to (E_1', s_1', t_1', E_2', s_2', t_2', E_3')$$

où $f_i : E_i \to E_i'$ pour $i = 1, 2, 3$, tels que (f_1, f_2) soit un morphisme de $\underline{Sig}$ et tels que les diagrammes suivant commutent :

$$\begin{array}{ccc} E_3 & \xrightarrow{f_3} & E_3' \\ {\scriptstyle s_2}\downarrow & & \downarrow{\scriptstyle s_2'} \\ E_2^* & & (E_2')^* \\ {\scriptstyle s_1^*}\downarrow & & \downarrow{\scriptstyle (s_1')^*} \\ E_1^* & \xrightarrow[f_1^*]{} & (E_1')^* \end{array} \qquad \begin{array}{ccc} E_3 & \xrightarrow{f_3} & E_3' \\ {\scriptstyle s_2}\downarrow & & \downarrow{\scriptstyle s_2'} \\ E_2^* & & (E_2')^* \\ {\scriptstyle t_1^*}\downarrow & & \downarrow{\scriptstyle (t_1')^*} \\ E_1^* & \xrightarrow[f_1^*]{} & (E_1')^* \end{array}$$

Définition 14. On définit le foncteur d'oubli $V : \underline{PRO} \to \underline{Th}$ tel que pour tout PRO $\mathcal{C}$,

$$V(\mathcal{C}) = ([1], s_1, t_1, E_2, s_2, t_2, E_3)$$

avec pour tout $f : [m] \to [n]$, α_f dans E_2 avec $s_1(\alpha_f) = [m]$ et $t_1(\alpha_f) = [n]$ et pour tous morphismes f, g de $\mathcal{C}$ tels que $f = g$, $\beta_{f,g}$ dans E_3 avec $s_2(\beta_{f,g}) = f$ et $t_2(\beta_{f,g}) = g$.

Lemme 15. Le foncteur V admet un adjoint à gauche $T : \underline{Th} \to \underline{PRO}$.

Définition 16. On note $\mathbb{M}$ le PRO libre

$$V([1], s_1, t_1, \{\mu, \eta\}, s_2, t_2, \{ass, \eta_g, \eta_d\})$$

où

$$\begin{array}{rrr} s_1(\mu) = [2] & s_1(\eta) = [0] & t_1(\mu) = t_1(\eta) = [1] \\ s_2(ass) = \mu \circ (\mu \otimes id_1) & t_2(ass) = \mu \circ (id_1 \otimes \mu) & \\ s_2(\eta_g) = \mu \circ (\eta \otimes id_1) & s_2(\eta_d) = \mu \circ (id_1 \otimes \eta) & t_2(\eta_g) = t_2(\eta_d) = id_1 \end{array}$$

Définition 17. On note $\pi : \mathbb{M}_0 \to \mathbb{M}$ le foncteur monoïdal donné par

$$\pi([1]) = [1] \quad , \quad \pi(\mu) = \mu \quad \text{et} \quad \pi(\eta) = \eta.$$

Définition 18. On note $\iota : \mathbb{M}_0 \to \mathcal{M}$ le foncteur monoïdal donné par

$$\iota([1]) = [1] \quad , \quad \iota(\mu) = \mu \quad \text{et} \quad \iota(\eta) = \eta.$$

Lemme 19. Les égalités suivantes sont vraies dans $\mathcal{M}$:

$$\mu \circ (\mu \otimes id_1) = \mu \circ (id_1 \otimes \mu) \quad \text{et} \quad \mu \circ (\eta \otimes id_1) = id_1 = \mu \circ (id_1 \otimes \eta) = id_1$$

Démonstration. L'objet [1] est terminal, par conséquent, il existe un unique morphisme $[3] \to [1]$, ce qui donne la première égalité.

De même, il existe un unique morphisme $[1] \to [1]$, ce qui donne la seconde égalité. □

Lemme 20. Il existe un unique foncteur monoïdal $F : \mathbb{M} \to \mathcal{M}$ tel que

$$F([1]) = [1] \quad , \quad F(\mu) = \mu \quad \text{et} \quad F(\eta) = \eta.$$

Notre objectif est de montrer que F est une bijection. Le résultat est immédiat sur les objets.

Définition 21. On dit qu'un diagramme ϕ de $\mathbb{M}_0$ est une forme canonique si ϕ est l'identité sur l'ensemble vide ou

$$\phi = (\mu \otimes id_{q-1}) \circ (id_1 \otimes \psi) \quad \text{ou } \phi = \eta \otimes \psi$$

où ψ est en forme canonique.

Lemme 22. Notons $cf(\mathbb{M}_0)$ l'ensemble des diagrammes en forme canonique de $\mathbb{M}_0$. Le morphisme ι induit une bijection entre $cf(\mathbb{M}_0)$ et les morphismes de $\mathcal{M}$

Démonstration. Soit $f : [p] \to [q]$ un morphisme de $\mathcal{M}$. On montre par induction sur $p + q$ qu'il existe un diagramme $g : [p] \to [q]$ de $\mathbb{M}_0$ en forme canonique tel que $\iota(g) = f$.

Si $p + q = 0$, alors le morphisme f est l'identité sur l'ensemble vide, représenté par le diagramme vide, qui est bien en forme canonique.

Sinon, si en plus $f(1) \neq 1$, On pose $h : [p] \to [q - 1]$ défini par :

$$h(n) = f(n) - 1.$$

Par induction, le morphisme h est représenté par un diagramme h' de $cf(\mathbb{M}_0)$ et la fonction f est représentée par le diagramme $\eta \otimes h'$ qui est bien en forme canonique.

Sinon, on a alors $p + q \neq 0$ et $f(1) = 1$. On pose $h : [p - 1] \to [q]$ définie par

$$h(n) = f(n + 1)$$

Par induction, le morphisme h est représenté par un diagramme h' de $cf(\mathbb{M}_0)$ et la fonction f est représentée par le diagramme $(\mu \otimes id_{q-1}) \circ h'$.

L'unicité du diagramme g est une conséquence de la distinction de cas faite. □

Lemme 23. Le foncteur F est surjectif.

Démonstration. Soit $\phi : [p] \to [q]$ un morphisme de $\mathcal{M}$. Par le lemme 22, on sait qu'il existe un diagramme en forme canonique $\hat{f} : [p] \to [q]$ dans $\mathbb{M}_0$ tel que $\pi(\hat{f}) = \phi$. Au diagramme $\hat{f}$ correspond une classe de diagrammes f dans $\mathbb{M}$.

Pour toute classe de diagrammes g dans $\mathbb{M}$, Fg est la fonction croissante représentée par g. Cela signifie que, par construction, f est un antécédent de ϕ par F. □

Nous avons besoin de la notion de hauteur d'un diagramme de $\mathbb{M}$. Pour cela, on commence par introduire la catégorie $\mathcal{N}$ ayant un unique objet $*$ et donc les morphismes sont $\mathbb{N}$. La composition de deux morphismes est la somme :

$$m \circ n = m + n$$

et l'identité est le morphisme 0. On peut munir la catégorie $\mathcal{N}$ d'une structure de catégorie monoïdale avec :

$$* \otimes * = * \quad , \quad n \otimes m = n + m \quad \text{et } I = *.$$

La hauteur est définie comme le foncteur monoïdal $h : \mathbb{M}_0 \to \mathcal{N}$ tel que :

$$h([1]) = * \quad , \quad h(\mu) = 1 \quad \text{et} \quad h(\eta) = 1$$

Lemme 24. Tout diagramme f de $\mathbb{M}$ s'écrit comme id_p pour p un entier ou comme $\psi_1 \circ \psi_2$ où ψ_2 est un diagramme et où ψ_1 est un diagramme de hauteur 1.

Démonstration. Si la hauteur de f est supérieure ou égale à 1, cela signifie par définition de la hauteur que f s'écrit comme $\phi_1 \otimes \phi_2$ ou comme $\phi_1 \circ \phi_2$ avec ϕ_1 et ϕ_2 deux diagrammes de $\mathbb{M}$.

On le montre par induction sur la hauteur de f.

Dans le premier cas, f peut s'écrire comme $(\phi_1 \otimes id_m) \circ (id_n \otimes \phi_2)$. Par induction, ϕ_1 et ϕ_2 admettent une telle décomposition.

De plus, dans le deuxième cas, on peut choisir ϕ_1 tel que $\phi_1 = \alpha \otimes \beta$ (par associativité de $\circ$). Par la règle de commutation, on peut écrire $\phi_1 = (\alpha \otimes id_a) \circ (id_b \otimes \beta)$ pour a et b deux entiers. On obtient alors

$$f = ((\alpha \otimes id_a) \circ (id_b \otimes \beta) \circ \phi_2,$$

ce qui donne le résultat par induction. □

Cela signifie en particulier que tout diagramme ϕ peut s'écrire comme la composition de diagrammes élémentaires où on appelle diagramme élémentaire un diagramme de la forme

$$id_a \otimes \mu \otimes id_b \quad \text{ou} \quad id_a \otimes \eta \otimes id_b$$

avec a et b deux entiers.

Lemme 25. Pour tout diagramme $\phi : [p] \to [q]$ de $\mathbb{M}_0$, il existe un diagramme ϕ' en forme canonique tel que $\pi(\phi) = \pi(\phi')$.

Démonstration. On introduit les règles de réécriture :

$$\begin{aligned} id_1 &\to \mu \circ (id_1 \otimes \eta) \\ \mu \circ (\eta \otimes id_1) &\to id_1 \\ \mu \circ (\mu \otimes id_1) &\to \mu \circ (id_1 \otimes \mu) \end{aligned}$$

Nous allons montrer le lemme par induction sur la structure de ϕ (cf lemme 24 puis par induction sur $p + q$.

On vérifie à chaque étape que le diagramme ψ obtenu par application des règles de réduction vérifie $\pi(\psi) = \pi(\phi)$.

Si $f = id_{[p]}$. On montre le résultat par induction sur p. Si $p = 0$, le diagramme est le diagramme vide qui est bien en forme canonique. Sinon, $id_{[p]} = id_1 \otimes id_{[p-1]} \to (\mu \circ (id_1 \otimes \eta)) \otimes id_{[p-1]}$. Par induction $id_{[p-1]}$ se réécrit en forme normale. Par conséquent, $id_{[p]}$ se réécrit en forme canonique.

Si f s'écrit comme $\xi \circ \psi$ avec ξ cellule élémentaire, alors ψ se réécrit en forme normale $\hat{\psi}$. Par conséquent, le diagramme f se réécrit en $\xi \circ \hat{\psi}$.

Le diagramme ξ est de la forme

$$id_a \otimes \mu \otimes id_b \quad \text{ou} \quad id_a \otimes \eta \otimes id_b.$$

Le diagramme $\hat{\psi}$ est de la forme

$$(\mu \otimes id_a) \circ (id_1 \otimes nf) \quad \text{ou} \quad \eta \otimes nf$$

où nf est une forme canonique. Par conséquent, $\xi \circ \hat{\psi}$ peut être de 8 formes différentes.

Si $\xi \circ \hat{\psi}$ est de la forme $(\mu \otimes id_{q-1}) \circ (\mu \otimes id_q) \circ (id_1 \otimes nf)$, par la dernière règle de réécriture, $\xi \circ \psi$ se réécrit en $(\mu \otimes id_{q-1}) \circ (id_1 \otimes \gamma)$ avec $\gamma = (\mu \otimes id_b) \circ nf$. On peut appliquer l'hypothèse de récurrence sur $\gamma : [p-1] \to [q]$. On obtient bien une forme canonique.

Si $\xi \circ \hat{\psi}$ est de la forme $(id_a \otimes \mu \otimes id_b) \circ (\mu \otimes id_{q-1}) \circ (id_1 \otimes nf)$ (avec $a \geq 1$), par la règle de commutation, $\xi \circ \psi$ se réécrit en $(\mu \otimes id_{q-1}) \circ (id_a \otimes \mu \otimes id_b) \circ (id_1 \otimes nf)$. On note $\gamma = (id_{a-1} \otimes \mu \otimes id_b) \circ nf$. On peut appliquer l'hypothèse de récurrence sur $\gamma : [p-1] \to [q]$. On obtient bien une forme canonique.

Si $\xi \circ \hat{\psi}$ est de la forme $(\eta \otimes id_{q-1}) \circ (\mu \otimes id_q) \circ (id_1 \otimes nf)$, par la règle de commutation, $\xi \circ \psi$ se réécrit en $\eta \otimes ((\mu \otimes id_{q-2}) \circ (id_1 \otimes nf))$ qui est bien en forme canonique.

Si $\xi \circ \hat{\psi}$ est de la forme $(id_a \otimes \eta \otimes id_b) \circ (\mu \otimes id_{q-1}) \circ (id_1 \otimes nf)$ (avec $a \geq 1$), par la règle de commutation, $\xi \circ \psi$ se réécrit en $(\mu \otimes id_{q-1}) \circ (id_1 \otimes \gamma)$ avec $\gamma = (id_{a-1} \otimes \eta \otimes id_b) \circ nf$. On peut appliquer l'hypothèse de récurrence sur $\gamma : [p] \to [q-1]$. On obtient bien une forme canonique.

Si $\xi \circ \hat{\psi}$ est de la forme $\mu \otimes id_{q-1} \circ (\eta \otimes nf)$, alors $\xi \circ \hat{psi}$ se réécrit par la deuxième règle de réécriture en nf. Par conséquent, $\xi \circ \psi$ se réécrit bien en une forme canonique.

Si $\xi \circ \hat{\psi}$ est de la forme $(id_a \otimes \mu \otimes id_b) \circ (\eta \otimes nf)$ (avec $a \geq 1$), par la règle de commutation, $\xi \circ \psi$ se réécrit en $\eta \otimes \gamma$ avec $\gamma = (id_{a-1} \otimes \mu \otimes id_b) \circ nf$. On peut appliquer l'hypothèse de récurrence sur $\gamma : [p] \to [q-1]$. On obtient bien une forme canonique.

Si $\xi \circ \hat{\psi}$ est de la forme $(\eta \otimes id_{q-1}) \circ (\eta \otimes nf)$, par la règle de commutation, $\xi \circ \hat{\psi}$ est bien en forme canonique.

Si $\xi \circ \hat{\psi}$ est de la forme $(id_a \otimes \eta \otimes id_b) \circ (\eta \otimes nf)$ (avec $a \geq 1$), alors par la règle de commutation, $\xi \circ \psi$ se réécrit en $\eta \otimes \gamma$ avec $\gamma = (id_{a-1} \otimes \eta \otimes id_b) \circ nf$. Comme $\gamma : [p] \to [q-1]$, on peut lui appliquer l'hypothèse de récurrence pour obtenir une forme canonique. □

Une conséquence immédiate du lemme précédent est que pour tout diagramme ϕ dans $\mathbb{M}$, il existe ψ diagramme de $\mathbb{M}_0$ en forme normale tel que $\pi(\psi) = \phi$.

Lemme 26. Le morphisme F est injectif.

Démonstration. On considère ϕ et ψ fonctions de $\mathbb{M}$ telles que $F\phi = F\psi$. Par le lemme 22, il existe un unique diagramme en forme canonique $\hat{f}$ dans $\mathbb{M}_0$ tel que $\iota(\hat{f}) = F\phi = F\psi$.

Par le lemme précédent, il existe $\hat{\phi}$ (respectivement $\hat{\psi}$) antécédent en forme canonique de ϕ (respectivement ψ) par π. L'unicité de $\hat{f}$ donne donc

$$\hat{\psi} = \hat{f} = \hat{\phi}$$

Par conséquent, $\phi = \psi$, ce qui prouve l'injectivité de F. □