



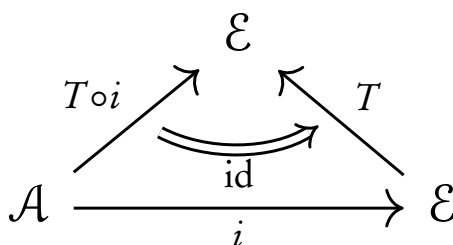
Master Parisien de Recherche en Informatique — 2^e année — Mémoire

Monade d'état quantique et ensembles nominaux

Étudiant : Pierre Cagne

Encadrant : Paul-André Mellès

Mars - Juillet 2015



Résumé

Ce document constitue le rapport d'un stage effectué dans le cadre du MPRI (Master Parisien de Recherche en Informatique) sous la direction de Paul-André Melliès au laboratoire PPS (Preuves, Programmes et Systèmes).

L'objectif du stage était de comprendre les monades et théories de Lawvere à arité, notions dégagées par Mark Weber ([Web07]) et Paul-André Melliès ([Mel10]), afin de reformuler dans ce langage la théorie algébrique des effets de bord en programmation quantique proposée par Sam Staton dans [Sta15].

Ce stage a aussi été l'occasion pour moi de suivre une École de Printemps thématique portant sur le logiciel et assistant de preuve Coq. J'aurais voulu, dans la mesure du possible, implémenter les concepts et preuves présentes dans ce rapport en Coq. Le temps m'a malheureusement manqué mais je garde en projet de formaliser en Coq la théorie des théories de Lawvere à arité.

Ce document est distribuée sous license Creative Commons Attribution - Share Alike 4.0 International (CC BY-SA 4.0). Texte légal complet disponible à l'adresse suivante :

<https://creativecommons.org/licenses/by-sa/4.0/>

Table des matières

Introduction	3
1 Le monde des arités	6
1.1 Nerfs généralisés	6
1.2 Monades et théories de Lawvere à arité	9
1.3 Arité de la forme $\Sigma\mathcal{M}$	11
2 Étude de cas : monade d'état local quantique	15
2.1 Théories algébriques à paramètres linéaires	16
2.2 Monade d'état local quantique	20
2.3 Ensembles nominaux quantiques	22
A Théories algébriques selon Lawvere	29
A.1 Théories de Lawvere	29
A.2 Des théories algébriques aux monades	30
A.3 Des monades aux théories algébriques	34
Bibliographie	36

Fiche synthèse

Pierre Cagne,
encadré par Paul-André Melliès,
Laboratoire PPS, Université Paris Diderot.

Fait le 20 août 2015.

Contexte général

Si la partie pure d'un langage de programmation (simplement typé) s'interprète sans difficulté dans une catégorie cartésienne fermée, l'étude des effets de bords requiert plus de structure. Habituellement, ces structures prennent la forme de monades. L'étude approfondie de ces monades donnent alors accès aux comportements des effets des bords et permet au programmeur d'anticiper les difficultés posées par ces effets. En poussant le processus à l'extrême, il peut être avantageux d'encapsuler directement les effets de bords par des monades dans la syntaxe même du langage (cf. Haskell).

La plupart des monades émergeant dans l'étude des effets de bords ont la propriété d'être *finitaires*, c'est-à-dire qu'elles sont descriptibles par des théories algébriques axiomatiques. L'étude sémantique d'une théorie algébrique est une mine d'informations sur le comportement de la monade associée, et donc sur celui des effets de bord considérés. C'est par exemple le cas de la monade d'état global, intensément étudiée par Moggi ([Mog91]) puis Plotkin et Power ([PP02]).

Malheureusement, quand la monade n'est pas finitaire, cette tentative d'axiomatisation par théorie algébrique échoue. C'est notamment le cas de la monade d'état local. Dans ce contexte, on peut s'interroger sur l'existence d'une axiomatisation algébrique *généralisée* afin de mieux comprendre la monade. C'est ici qu'entre en jeu la notion de *monade à arité*.

Problème étudié et contribution proposée

Dans [Mel10], Melliès introduit les théories de Lawvere à arité comme pendants algébriques des monades à arité de Weber ([Web07]) qu'il utilise ensuite pour décrire algébriquement la monade d'état local dans [Mel14]. On se propose ici de faire de même avec une version quantique de la monade d'état local. Plus précisément, Staton étudie dans [Sta15] les effets de bords induits par l'allocation de qbits, leur désallocation par observation et l'écriture par application d'unitaires complexes.

Dans son article, Staton introduit une notion de théorie algébrique ad hoc, qui se révèle en fait être un cas particulier de théorie de Lawvere à arité. Au-delà de l'effort d'intégration des idées de Staton dans une théorie plus générale déjà étudiée, on

espère par ce procédé capturer plus concrètement la monade associée (non apparente dans l'article), voire même en donner une formule close. Sans aboutir à une formule satisfaisante, on développe néanmoins des outils importants à la compréhension de la monade : les ensembles nominaux quantiques et leurs supports. Enfin, il serait appréciable de trouver une factorisation de la monade d'état local quantique et de la comparer à celle de la monade d'état local classique (cf. [Mel14]).

Arguments en faveur de sa validité

Les monades et théorie de Lawvere à arité sont un formidable outil généralisant tout le travail initié par Lawvere dans sa thèse [Law63]. Malheureusement, on manque cruellement d'exemples concrets (en informatique notamment) permettant de démontrer sa puissance d'expression. Ce travail ajoute ainsi un exemple à un catalogue encore trop restreint, mais qui contient néanmoins des exemples importants, telles que la monade de restriction, ou la monade d'état local ainsi que des variations.

En intégrant l'article de Staton, à première vue très spécifique, dans un cadre plus large et plus abstrait, un nouvel angle de vue est ouvert sur la monade d'état local quantique et permet d'en mieux comprendre le comportement.

Bilan et perspectives

En essayant de factoriser la monade d'état local quantique par les mêmes moyens que la monade d'état local classique, nous nous sommes heurtés à un problème de taille : quelle est la taille minimale de la mémoire quantique nécessaire à l'exécution d'un programme quantique x donné ? Il est alors apparu nécessaire de développer une théorie du support quantique d'un programme, de la même manière qu'il existe une théorie du support dans le cadre classique. Cette notion de support quantique passe par l'élaboration d'une condition de nominalité quantique, remplaçant la condition que satisfont habituellement les ensembles nominaux d'Andrew Pitts.

Deux prolongations de ce travail semblent alors possible. La première consiste à étudier le lien formel entre notre notion de support quantique et les résultats de minimalité présents dans l'article de Staton. Ces derniers sont obtenus grâce à des théorèmes d'algèbre d'opérateurs, n'ayant a priori aucun lien avec la sémantique opérationnelle. Il serait donc intéressant de comprendre le lien exact entre les résultats de Staton et ceux de ce document. Une deuxième possibilité serait de généraliser encore la notion de nominalité. En effet, un processus systématique à partir de l'arité $i: \Sigma \text{Bij} \rightarrow \widehat{\text{Bij}}$ semble être à l'origine de la définition des deux notions nominales (classique et quantique). À quelles conditions sur une théorie de Lawvere d'arité i peut-on répéter ce processus pour définir une notion d'ensemble nominal adaptée aux modèles de cette théorie ?

Introduction

Le λ -calcul simplement typé s'interprète traditionnellement dans une catégorie cartésienne fermée. Cela permet d'étudier le noyau pur (sans effets de bord) des langages de programmation, modélisés par le λ -calcul. Afin de modéliser les *effets de bord*, il est nécessaire d'ajouter une *structure* à la catégorie cartésienne fermée. Cette structure prend généralement la forme d'une monade. Prenons par exemple l'effet de bord suivant : on se donne un langage de programmation où les programmes sont munis d'un *état*, qu'ils mettent à jour au fur et à mesure de leur exécution, cet état pouvant prendre ses valeurs dans un ensemble fixé S . On souhaite interpréter ce langage dans la catégorie $\mathbf{Ens}$. Un programme de type $A \rightarrow B$ ne s'interprète donc plus comme une fonction ensembliste $f : A \rightarrow B$ mais comme une fonction

$$f : S \times A \rightarrow S \times B.$$

Il faut comprendre cette interprétation comme la fonction qui décrit le programme $A \rightarrow B$ qui prend l'état d'entrée et met à jour l'état de sortie tout au long de l'exécution du programme de type $A \rightarrow B$. Alors, comme le foncteur $S \times -$ est adjoint à gauche du foncteur $S \Rightarrow -$, cette fonction f peut tout aussi bien être vue comme sa curryfication

$$\tilde{f} : A \rightarrow S \Longrightarrow (S \times B),$$

c'est-à-dire comme un morphisme de la catégorie de Kleisli de la monade

$$S \Rightarrow (S \times -) : \mathbf{Ens} \rightarrow \mathbf{Ens},$$

appelée monade d'état. Cet exemple motive que l'on n'interprète plus un langage avec effets de bord dans une catégorie $\mathcal{C}$ mais dans la catégorie de Kleisli $\mathcal{C}_T$ associée à une monade T sur $\mathcal{C}$. Bien entendu, le choix de la monade T dépend des effets de bord que l'on veut pouvoir modéliser.

Dans ce document, on s'intéresse à l'étude d'un monade modélisant les effets d'allocation et désallocation d'un langage de programmation *quantique* décrit par Staton dans [Sta15]. La programmation quantique a ceci de particulier que la gestion des qbits est linéaire : la lecture d'une case mémoire au moyen d'une mesure détruit cette dernière et il n'est pas possible de dupliquer une case mémoire. De plus, l'intrication des qbits permet de modifier la mémoire globalement (ou tout du moins régionalement) au moyen d'un opérateur unitaire. C'est donc dans le cadre d'un langage permettant ce genre de manipulations que l'on se place. Plus spécifiquement, on suppose que notre langage de programmation admet la grammaire de types suivante :

$$A, B ::= \text{unit} \mid \text{qbit} \mid \text{bool} \mid A \otimes B$$

et qu'on dispose des primitives suivantes :

$$\text{new: unit} \rightarrow \text{qbit}, \quad \text{measure: qbit} \rightarrow \text{bool}, \quad \text{apply}_U: \text{qbit}^{\otimes n} \rightarrow \text{qbit}^{\otimes n},$$

où la dernière primitive est paramétrée par les matrices unitaires U de tailles 2^n à coefficients dans $\mathbb{C}$, et ce pour tout nombre de qbits $n \in \mathbb{N}$ alloués en mémoire. La primitive `new` a pour effet de renvoyer un pointeur vers un qbit fraîchement alloué à la valeur $|0\rangle$. La primitive `measure` mesure un qbit $q = \alpha|0\rangle + \beta|1\rangle$ et retourne un booléen, à savoir 0 (avec probabilité $|\alpha|^2$) ou 1 (avec probabilité $|\beta|^2$). Enfin, la primitive `applyU` applique la conjugaison unitaire U au programme, qui se comporte donc comme s'il travaillait sur l'espace mémoire après changement de base par U .

Si l'on s'intéresse à la gestion des ressources de tels programmes quantiques, il apparaît nécessaire de comprendre quelles sont (1) les allocations quantiques réellement utiles au programme, (2) celles qui ne sont absolument pas nécessaires, (3) et celles qui auraient pu être remplacées par l'allocation d'un bit classique. En particulier, il nous faut une notion de *support quantique* d'un programme qui décrit les qbits de la sorte (1), et si possible une notion *algébrique* d'un tel support, sur laquelle on puisse calculer facilement. La notion de support d'un programme est étudiée depuis le début des années 1990 du point de vue algébrique, dans le cadre de la théorie des *ensembles nominaux* introduits par Andrew Pitts. La modélisation du support d'un programme par les ensembles nominaux repose historiquement sur le fait qu'une désallocation est une opération unaire : si j'ai un programme x dépendant de n paramètres et que ma mémoire est constituée de $n + 1$ emplacements, je peux désallouer une case mémoire au moyen d'un opérateur collect et continuer selon x . L'idée que nous développons dans ce mémoire est que c'est `measure` qui joue le rôle de la désallocation dans le cadre de la programmation quantique. Une différence déterminante que nous aurons à traiter du point de vue algébrique est que cette opération n'est pas unaire : si je mesure un qbit sur une mémoire constituée de $n + 1$ emplacements, il me faut deux programmes quantiques dépendant de n paramètres pour pouvoir continuer à exécuter ; l'un dans le cas où la mesure renvoie le booléen 0, l'autre dans le cas où elle renvoie le booléen 1.

Il nous faut donc élargir le cadre classique des ensembles nominaux afin de pouvoir prendre en compte des opérations de désallocation non unaires. Cette généralisation nécessite d'introduire des outils conceptuels nouveaux liés aux théories algébriques et à celle des catégories de (pré)faisceaux. En effet, il est bien connu qu'un ensemble nominal peut être défini comme un préfaisceau $\text{Inj} \rightarrow \text{Ens}$ respectant les produits fibrés, où Inj est la catégorie des ordinaux finis et injections entre eux. Autrement dit, l'existence d'un support au sens de Pitts se ramène à une condition de préservation de produits fibrés. On retrouve le cadre fonctoriel dans lequel Gordon Plotkin et John Power ont formulé la monade d'état local

$$L: [\text{Inj}, \text{Ens}] \rightarrow [\text{Inj}, \text{Ens}].$$

Nous partons de la notion de *théorie de Lawvere à arité* qui a permis à Melliès de donner une présentation algébrique de cette monade dans [Mel14]. Cette notion nous amène à introduire une catégorie qInj avec produits finis, qui joue le rôle de Inj dans le cadre quantique qui nous intéresse. En effet, si l'on note $[\text{qInj}, \text{Ens}]_{\times}$ la catégorie des préfaisceaux qui préservent les produits finis, alors les effets quantiques définissent une monade d'état

$$Q: [\text{qInj}, \text{Ens}]_{\times} \rightarrow [\text{qInj}, \text{Ens}]_{\times}$$

que l'on peut analyser de la même manière que la monade d'état local L . En particulier, dans ce cadre « classique », on sait montrer que tout algèbre de la monade L définit un ensemble nominal. Autrement dit, tout élément x d'un type $A \in [\text{Inj}, \text{Ens}]$ muni des opérations d'écriture, de lecture, d'allocation et de désallocation dispose d'un support $\text{supp}(x)$. De la même manière, nous montrerons que tout algèbre de la monade Q détermine un *ensemble qnominale* au sens que nous définirons dans ce mémoire. Cela signifie que tout élément d'un type $A \in [\text{qInj}, \text{Ens}]_\times$ muni des opérations d'allocation, de mesure et de conjugaison quantiques dispose d'un support quantique $\text{supp}(x)$. Cette propriété non triviale permet de raisonner sur la structure des programmes quantiques et l'usage qu'ils font de la mémoire quantique. Rappelons qu'un qbit est élément du support quantique de x lorsqu'il n'est pas mesuré immédiatement par le programme x , et qu'il peut donc potentiellement être intriqué avec d'autres qbits déclarés par le programme (ceci définissant des « régions » dans l'espace mémoire quantique).

Dans l'optique de ce travail, on organise le document de la façon suivante. Le premier chapitre se consacre à la théorie des théories de Lawvere à arité, et à l'étude approfondie d'une forme d'arité spécifique $\Sigma \mathcal{M} \rightarrow \widehat{\mathcal{M}}$, qu'on instanciera par la suite pour étudier les effets de bord quantiques. Cette partie est volontairement théorique, afin de simplifier la manipulation des objets concrets par la suite. Pour justifier les notions introduites et donner une intuition sur ces concepts abstraits, l'auteur a mis en appendice A la théorie classique des théories de Lawvere dont la compréhension a par ailleurs constitué la toute première partie du stage. La lecture de cette appendice peut être omise par le lecteur déjà familier des concepts introduits par Lawvere dans sa thèse [Law63]. Le deuxième chapitre est quant à lui dédié à la compréhension des phénomènes de programmation quantique sous l'angle des théories de Lawvere à arité. On commence par exprimer les *théories algébriques à paramètres linéaires* de Staton comme des théories de Lawvere à arité $\Sigma \text{Bij} \rightarrow \widehat{\text{Bij}}$. On exploite cette présentation de la *monade d'état local quantique* sous la forme de théorie de Lawvere pour en dégager une notion de nominalité et support quantique. Nous établissons de plus que les algèbres de la monade Q induite vérifient cette condition de nominalité. Enfin, on essaye d'éclairer les résultats de minimalité décrits dans [Sta15] à la lumière de ce nouveau support.

Chapitre 1

Le monde des arités

L'appendice A détaille les rapports qu'entretiennent les monades finitaires sur $\mathbf{Ens}$ avec les théories de Lawvere. En particulier, les algèbres d'une monade finitaire sont exactement les modèles d'une théorie algébrique. Quid des monades non finitaires ? Peut-on trouver une notion de « théorie algébrique généralisée » telle que les modèles d'une telle théorie encodent exactement les algèbres d'un certain type de monade ?

La réponse à cette question est multiple : on ne va pas construire une unique notion de théorie algébrique généralisée, mais une multitude chacune relative à une *arité*. Intuitivement, l'arité décrit les « formes » qu'on autorise à prendre aux entrées et sorties de nos opérations algébriques. Dans le cadre classique, ces formes sont simplement les puissances exponentielles finies (par exemple la loi $+$: $G^2 \rightarrow G$ d'un groupe abélien) qu'on retrouve dans notre généralisation en étudiant l'arité $\aleph_0 \hookrightarrow \mathbf{Ens}$.

1.1 Nerfs généralisés

La notion d'arité passe par celle de nerf. Le *nerf* d'un foncteur $i : \mathcal{A} \rightarrow \mathcal{E}$ ($\mathcal{A}$ petite) est le foncteur

$$\nu_i : \mathcal{E} \rightarrow \widehat{\mathcal{A}}, \quad e \mapsto \mathcal{E}(i(-), e).$$

Si i est un plongement, alors son nerf est une extension du plongement de Yoneda $\mathfrak{h}^{\mathcal{A}} : \mathcal{A} \rightarrow \widehat{\mathcal{A}}$ à $\mathcal{E}$. En effet, naturellement en $a \in \mathcal{A}$,

$$\nu_i(i(a)) = \mathcal{E}(i(-), i(a)) \simeq \mathcal{A}((-, -), a) = \mathfrak{h}_a^{\mathcal{A}}.$$

Ainsi, le triangle suivant commute :

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\mathfrak{h}^{\mathcal{A}}} & \widehat{\mathcal{A}} \\ i \downarrow & \nearrow \nu_i & \\ \mathcal{E} & & \end{array}$$

Si de plus $\mathcal{E}$ est cocomplète, la théorie des extensions de Kan assure l'existence d'un foncteur ϖ_i , extension de Kan de i à gauche le long du plongement de Yoneda, donné par l'expression

$$\varpi_i : P \mapsto \operatorname{colim} \left(\mathcal{A}_{/P} \rightarrow \mathcal{A} \xrightarrow{i} \mathcal{E} \right)$$

où $\mathcal{A}_{/P}$ est la catégorie des éléments d'un préfaisceau P sur $\mathcal{A}$, et faisant ainsi commuter le diagramme

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\mathfrak{h}^{\mathcal{A}}} & \widehat{\mathcal{A}} \\ i \downarrow & \swarrow \varpi_i & \\ \mathcal{E} & & \end{array}$$

(Le lecteur attentif remarquera qu'habituellement la théorie des extensions de Kan fournit des 2-cellules plutôt que des triangles commutatifs. Ici, comme $\mathfrak{h}^{\mathcal{A}}$ est pleinement fidèle, la 2-cellule est (isomorphe à) l'identité.)

Lemme 1.1.1. *Pour tout plongement i , le foncteur ϖ_i est adjoint à gauche du foncteur ν_i .*

Preuve. Étant donnés $P \in \widehat{\mathcal{A}}$ et $e \in \mathcal{E}$, l'application

$$\alpha \mapsto \left(i(a) \xrightarrow{\alpha_x} e \right)_{x: a \rightarrow P}$$

définit une bijection des transformations naturelles $P \rightarrow \nu_i(e)$ dans les cocônes dans $\mathcal{E}$ de sommet e sur le diagramme $\mathcal{A}_{/P} \rightarrow \mathcal{A} \xrightarrow{i} \mathcal{E}$. On vérifie facilement que cette bijection est naturelle en P et e . Ainsi, naturellement en $P \in \widehat{\mathcal{A}}$ et $e \in \mathcal{E}$,

$$\widehat{\mathcal{A}}(P, \nu_i(e)) \simeq \text{Hom}(\mathcal{A}_{/P} \rightarrow \mathcal{A} \xrightarrow{i} \mathcal{E}, e) \simeq \mathcal{E}(\varpi_i(P), e),$$

où la dernière bijection vient de la définition de colimite. Ceci montre l'adjonction voulue. $\square$

Exemple(s) 1.1.2. (i) Un exemple important de cette construction est le *nerf simplicial*. Notons Δ la catégorie des posets de la forme $[n] = \{0 < \dots < n\}$ et des applications croissantes entre eux. En considérant ces posets comme des catégories (fines), on obtient une inclusion pleine $i: \Delta \rightarrow \text{Cat}$. La construction ν_i explicitée ci-dessus se note alors $N: \text{Cat} \rightarrow \widehat{\Delta}$ et est appelé *foncteur nerf*.

À toute catégorie $\mathcal{A}$, le nerf associe l'ensemble simplicial $N\mathcal{A}_\bullet$ suivant : pour tout $n \in \mathbb{N}$, $N\mathcal{A}_n$ est l'ensemble des suites finies de longueur n de flèches composables de $\mathcal{A}$. Les applications faces sont données par composition locale

$$(a_0 \rightarrow \dots a_{i-1} \xrightarrow{f_i} a_i \xrightarrow{f_{i+1}} a_{i+1} \rightarrow \dots \rightarrow a_n) \mapsto (a_0 \rightarrow \dots a_{i-1} \xrightarrow{f_{i+1}f_i} a_{i+1} \rightarrow \dots \rightarrow a_n)$$

et les applications dégénérescences par l'introduction d'identités

$$(a_0 \rightarrow \dots a_i \xrightarrow{f_{i+1}} a_{i+1} \rightarrow \dots \rightarrow a_n) \mapsto (a_0 \rightarrow \dots a_i \xrightarrow{\text{id}_{a_i}} a_i \xrightarrow{f_{i+1}} a_{i+1} \rightarrow \dots \rightarrow a_n).$$

En particulier, ce foncteur N est pleinement fidèle. C'est-à-dire que l'on peut traiter les (petites) catégories comme des ensembles simpliciaux particulier d'un point de vue catégorique.

(ii) Un autre exemple nous vient de la géométrie algébrique. Après avoir introduit avec Dieudonné les schémas comme recollement (en tant qu'espaces annelés) de schémas affines portant la topologie de Zariski, Grothendieck est revenu sur

cette définition, la jugeant trop *ad hoc*. Il lui préfère par la suite le point de vue du *foncteurs des points* : un schéma est un faisceau pour une bonne topologie (sous-canonique) de Grothendieck sur Cring° , catégorie opposée à celle des anneaux commutatifs unifiés. Dans notre formalisme, cela revient à dire que le nerf de l'inclusion pleine $i : \text{Aff} \rightarrow \text{Sch}$ est un plongement $\nu_i : \text{Sch} \hookrightarrow \widehat{\text{Aff}}$.

On remarque que dans les exemples ci-dessus, le foncteur nerf est pleinement fidèle (ou équivalent, dans le cas où $\mathcal{E}$ est cocomplète, la counité $\varpi_i \nu_i \rightarrow \text{id}_{\mathcal{E}}$ de l'adjonction sus-présentée est un isomorphisme). Cela motive la définition suivante.

Définition 1.1.3 (Arité). Une *arité* est un foncteur pleinement fidèle dont le nerf est pleinement fidèle.

Le lemme suivant nous dit qu'une arité $i : \mathcal{A} \rightarrow \mathcal{E}$ est juste une façon de voir $\mathcal{A}$ comme sous-catégorie pleine de $\mathcal{E}$ et $\mathcal{E}$ comme sous-catégorie pleine de $\widehat{\mathcal{A}}$ de telle manière que le plongement $\mathcal{A} \rightarrow \widehat{\mathcal{A}}$ ainsi obtenu soit le plongement de Yoneda.

Lemme 1.1.4. *Le foncteur $i : \mathcal{A} \rightarrow \mathcal{E}$ est une arité si et seulement s'il existe $F : \mathcal{E} \rightarrow \widehat{\mathcal{A}}$ pleinement fidèle tel que $\mathfrak{h}^{\mathcal{A}} \simeq Fi$.*

Preuve. Si i est une arité, on a vu que $F = \nu_i$ convient.

Réciproquement, supposons qu'il existe F pleinement fidèle tel que Fi soit le plongement de Yoneda. La classe des foncteurs pleinement fidèles a la propriété 2-sur-3 donc, comme F et Fi sont pleinement fidèles, i l'est aussi. De plus, naturellement en $e \in \mathcal{E}$,

$$F(e) \simeq \widehat{\mathcal{A}}(\mathfrak{h}_-^{\mathcal{A}}, F(e)) \simeq \widehat{\mathcal{A}}(Fi(-), F(e)) \simeq \mathcal{E}(i(-), e)$$

la dernière bijection venant du fait que F est pleinement fidèle. Ainsi, le nerf de i s'identifie à F et est en particulier pleinement fidèle. $\square$

Proposition 1.1.5. *Soit $\iota : \mathcal{C} \rightarrow \mathcal{A}$ une arité entre petite catégorie. Alors $\nu_i : \mathcal{A} \rightarrow \widehat{\mathcal{C}}$ est une arité.*

Preuve. Par le lemme précédent, la situation revient à la suivante : $\mathcal{A}$ est une sous-catégorie pleine de $\widehat{\mathcal{C}}$ contenant les représentables. On note $i : \mathcal{A} \rightarrow \widehat{\mathcal{C}}$ cette inclusion. Il faut alors voir que ν_i s'identifie au foncteur extension de Kan à droite $\iota_* \widehat{\mathcal{C}} \rightarrow \widehat{\mathcal{A}}$. En effet, profitant du fait que $\mathfrak{h}_a^{\mathcal{A}} \circ \iota \simeq i(a)$, l'application

$$(F\iota \xrightarrow{\alpha} G) \longmapsto \left\{ \begin{array}{c} F(a) \rightarrow \widehat{\mathcal{C}}(i(a), G) \\ (\mathfrak{h}_a \xrightarrow{x} F) \mapsto (\mathfrak{h}_a \xrightarrow{\iota^* x} F\iota \xrightarrow{\alpha} G) \end{array} \right\}_{a \in \mathcal{A}}$$

définit une bijection (clairement naturelle en F et G) $\widehat{\mathcal{C}}(\iota^* F, G) \simeq \widehat{\mathcal{A}}(F, \nu_i G)$.

Reste alors à remarquer que la counité $\iota^* \nu_i \rightarrow \text{id}_{\widehat{\mathcal{C}}}$ est inversible pour conclure que ν_i est pleinement fidèle. Or comme $i\iota \simeq \mathfrak{h}^{\mathcal{C}}$, la composante sur $G \in \widehat{\mathcal{C}}$ de cette counité est le morphisme de Yoneda

$$\widehat{\mathcal{C}}(\mathfrak{h}^{\mathcal{C}}, G) \rightarrow G$$

qu'on sait inversible par le lemme de Yoneda. $\square$

Exemple(s) 1.1.6. (i) La caractérisation du lemme 1.1.4 montre immédiatement que $\text{id}_{\mathcal{A}}$ est une arité de nerf le plongement de Yoneda. De même $\mathfrak{h}^{\mathcal{A}}$ est une arité de nerf $\text{id}_{\widehat{\mathcal{A}}}$.

- (ii) En considérant $\mathbf{Ens}$ comme la catégorie de préfaisceau $\widehat{\mathcal{E}}$ sur la catégorie finale, la proposition 1.1.5 assure que $\mathfrak{K}_0 \rightarrow \mathbf{Ens}$ est une arité. C'est grâce à celle-ci qu'on retrouvera par la suite les théories de Lawvere classiques comme cas particulier des théories de Lawvere à arité.

1.2 Monades et théories de Lawvere à arité

On va maintenant introduire notre notion de théorie algébrique généralisée grâce à la notion d'arité. Pour toutes les preuves de cette section, on réfère à l'article fondateur [BMW12]. On s'efforcera tant que possible de garder les mêmes notations que cet article.

Définition 1.2.1 (Théorie de Lawvere à arité). Une *théorie de Lawvere d'arité* $i: \mathcal{A} \rightarrow \mathcal{E}$ est la donnée d'une petite catégorie Θ et d'un foncteur $j: \mathcal{A} \rightarrow \Theta$ bijectif sur les objets tel que $j^*j_!$ préserve l'image essentielle de ν_i .

Comme dans le cadre des théories classiques, un morphisme d'une théorie $j_1: \mathcal{A} \rightarrow \Theta_1$ vers une théorie $j_2: \mathcal{A} \rightarrow \Theta_2$ (toutes deux de même arité) est un foncteur $\vartheta: \Theta_1 \rightarrow \Theta_2$ tel que $j_2 = \vartheta j_1$. La catégorie des théories d'arité $i: \mathcal{A} \rightarrow \mathcal{E}$ ainsi formée sera notée $\mathbf{Law}(i)$.

Pour définir la notion de modèle associé à ces théories à arité, il nous faut mettre au point un peu de vocabulaire : un préfaisceau de sur $\mathcal{A}$ est dit *représentable le long d'une arité* $i: \mathcal{A} \rightarrow \mathcal{E}$ s'il est dans l'image essentielle de ν_i . Un préfaisceau sur $\mathcal{A}$ est alors représentable, au sens classique du terme, s'il l'est le long de $\mathrm{id}_{\mathcal{A}}$.

Définition 1.2.2 (Modèle d'une théorie à arité). Soit $j: \mathcal{A} \rightarrow \Theta$ une théorie de Lawvere d'arité $i: \mathcal{A} \rightarrow \mathcal{E}$. Un *modèle* de j est un préfaisceau M sur Θ tel que j^*M est représentable le long de i .

On note $\mathbf{Mod}(j, i)$ la sous-catégorie pleine de $\widehat{\Theta}$ constituée des modèles de j .

Exemple(s) 1.2.3. Ces définitions peuvent sembler absconses de prime abord. Il faut les voir sous le jour de l'exemple canonique qu'est l'arité $\iota: \mathfrak{K}_0 \rightarrow \mathbf{Ens}$ pour comprendre en quoi elles sont pertinentes.

Une théorie $\ell: \mathfrak{K}_0 \rightarrow \mathcal{T}$ d'arité ι est telle que la monade $\ell^*\ell_!$ sur $\widehat{\mathfrak{K}_0}$ se retrace en une monade sur $\mathbf{Ens}$ via le nerf ν_i . Or, l'image essentielle de ν_i contient exactement les préfaisceaux sur $\mathfrak{K}_0$ préservant les produits finis : en effet, les représentables le long de ι préserve clairement les produits finis ; réciproquement si $F \in \widehat{\mathfrak{K}_0}$ préserve les produits finis, alors il est représentable le long de ι par $F(1)$. Ainsi, $\ell^*\ell_!$ envoie les préfaisceaux préservant les produits finis sur des préfaisceaux préservant les produits finis : par le lemme A.2.2, $\ell_!$ a déjà cette propriété, donc ℓ^* se doit aussi de l'avoir. On en déduit immédiatement que ℓ préserve les coproduits finis, i.e. que c'est une théorie de Lawvere au sens classique. Comme on a en fait procédé par équivalence ci-dessus, la réciproque est également vraie : toute théorie de Lawvere classique est une théorie d'arité ι .

Passons aux modèles. Un modèle d'une théorie de Lawvere classique $\ell: \mathfrak{K}_0 \rightarrow \mathcal{T}$ est un préfaisceau sur $\mathcal{T}$ respectant les produits finis. Comme ℓ préserve également les produits finis, c'est équivalent à demander que sa restriction le long de ℓ les préserve : un modèle est donc un préfaisceau $F \in \widehat{\mathcal{T}}$ tel que $F(0)$ soit un singleton et l'image $\ell^*(F)(n) \rightarrow \ell^*(F)(1)$ des différentes inclusions $1 \rightarrow n$ de $\mathfrak{K}_0$ soient toutes des isomorphismes. Alors, naturellement en $n \in \mathfrak{K}_0$, on a

$$\ell^*(F)(n) \simeq (\ell^*(F)(1))^n \simeq \mathbf{Ens}(\iota(n), \ell^*(F)(1)).$$

Ainsi, la restriction d'un modèle est représentable le long de ι , i.e. est un modèle au sens des arités. Réciproquement, tout préfaisceau de la forme $v_i X$ pour $X \in \text{Ens}$ préserve les produits finis donc est un modèle de la théorie de Lawvere au sens classique.

Comme dans le cadre classique, on va associer une monade à une théorie de Lawvere $j: \mathcal{A} \rightarrow \Theta$ d'arité $i: \mathcal{A} \rightarrow \mathcal{E}$. Comme i est une arité, v_i est pleinement fidèle et admet donc un pseudo-inverse ρ_i , qu'on peut choisir adjoint à droite de v_i . Ainsi, on a une adjonction composée

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{v_i} & \hat{\mathcal{A}} \\ \rho_i \swarrow & \perp & \nwarrow j_i \\ & \hat{\mathcal{A}} & \\ j^* \swarrow & \perp & \nwarrow \\ \Theta & \xrightarrow{j_i} & \hat{\Theta} \end{array}$$

induisant une monade $\mathbf{T}(j, i)$. Dans le cadre de l'arité $\aleph_0 \rightarrow \text{Ens}$, on sait que cette monade est finitaire. Pour donner le pendant général de cette propriété, il nous faut introduire une nouvelle notion.

Étant donné un foncteur $i: \mathcal{A} \rightarrow \mathcal{E}$ et un objet $e \in \mathcal{E}$, il existe un cocône *tautologique* de sommet e sur le diagramme $iU: (i \downarrow e) \rightarrow \mathcal{A} \rightarrow \mathcal{E}$ (avec U le foncteur d'oubli depuis la catégorie comma) : il s'agit du cocône

$$\left(i(a) \xrightarrow{f} e \right)_{f: i(a) \rightarrow e}$$

On appelle *i-cocônes* de tels cocônes. Un corollaire immédiat du lemme 1.1.4 est que i est une arité si et seulement si tout *i-cocône* est colimitant.

Définition 1.2.4 (Monade à arité). Une monade T d'arité $i: \mathcal{A} \rightarrow \mathcal{E}$ est une monade sur $\mathcal{E}$ telle que l'image de tout *i-cocône* par $v_i T$ est colimitant.

Proposition 1.2.5. Soit $j: \mathcal{A} \rightarrow \Theta$ une théorie de Lawvere d'arité $i: \mathcal{A} \rightarrow \mathcal{E}$. La monade $\mathbf{T}(j, i)$ associée est une monade d'arité i .

Preuve. Rappelons que $\mathbf{T}(j, i)$ est définie comme la composition $\rho_i j^* j_i v_i$ où ρ_i est un pseudo-inverse de v_i : donc $v_i \mathbf{T}(j, i) \simeq j^* j_i v_i$. De plus, comme $v_i i = \mathfrak{h}^{\mathcal{A}}$, les *i-cocônes* de $\mathcal{E}$ sont envoyés par v_i sur des $\mathfrak{h}^{\mathcal{A}}$ -cocônes de $\hat{\mathcal{A}}$. Ainsi, il suffit de vérifier que $j^* j_i$ envoie les $\mathfrak{h}^{\mathcal{A}}$ -cocônes sur des cocônes colimitants¹.

□

Proposition 1.2.6. Soit $i: \mathcal{A} \rightarrow \mathcal{E}$ une arité. L'opération

$$\mathbf{T}(-, i): \text{Law}(i) \rightarrow \text{Mnd}(i)$$

peut être prolongée en une équivalence de catégorie.

Preuve. Voir [BMW12, Théorème 3.4].

□

Remarque 1.2.7. Deux « miracles » se produisent dans le cas de l'arité $\aleph_0 \rightarrow \text{Ens}$ et n'ont pas leur équivalent dans le cas général.

Le premier est la possibilité de définir des modèles non ensemblistes : en effet, on a vu que la condition de représentabilité le long de $\aleph_0 \rightarrow \text{Ens}$ est équivalente à la commutation aux produits finis, ce qui permet de généraliser la notion de modèle à toute

1. Comme le plongement de Yoneda est une arité dont le nerf est l'identité, cela revient à dire que $j^* j_i$ est une monade à arité.

catégorie admettant les produits finis. Dans le cadre général en revanche, il n'existe aucune caractérisation de la représentabilité le long d'une arité i qui soit indépendante de Ens . On pourra néanmoins chercher de telles caractérisations pour des arités bien choisies.

Le deuxième est la possibilité de présenter Law comme sous-catégorie pleine coréflexive de Mnd . En effet, dans le cadre classique, on peut définir $\mathbf{L} : \text{Mnd} \rightarrow \text{Law}$ adjoint à droite du foncteur pleinement fidèle $\mathbf{T} : \text{Law} \rightarrow \text{Mnd}$. Il n'en est rien dans le cadre général : pour pouvoir associer une théorie de Lawvere à arité à une monade, il faut que celle-ci ait même arité (cf. [BMW12, Proposition 3.2]).

1.3 Arité de la forme $\Sigma \mathcal{M}$

Dans cette section, on étudie de plus près une certaine forme d'arité. On veut pouvoir définir des théories algébriques dont les opérations sont « multi-colorées » : c'est-à-dire qu'une opération doit pouvoir prendre différents arguments, chacun portant une couleur distinctive, et avoir une sortie de couleur définie. On veut de plus que les couleurs puissent se combiner de façon cohérente. Avant de formaliser cette intuition, il faut bien comprendre qu'elle englobe le cadre des théories de Lawvere classique : c'est le cas où il n'y a qu'une seule couleur à disposition.

Définition 1.3.1. Soit $\mathcal{M}$ une petite catégorie. La *catégorie coproduits finis libres sur $\mathcal{M}$* , notée $\Sigma \mathcal{M}$, est la sous-catégorie pleine de $\widehat{\mathcal{M}}$ constituée des objets de la forme

$$\coprod_{i=1}^k \mathfrak{h}_{m_i}^{\mathcal{M}} \quad (m_i \in \mathcal{M}).$$

On note $\iota_{\mathcal{M}} : \mathcal{M} \rightarrow \Sigma \mathcal{M}$ la corestriction du plongement de Yoneda et $i_{\mathcal{M}} : \Sigma \mathcal{M} \rightarrow \widehat{\mathcal{M}}$ l'inclusion pleine de la définition.

Proposition 1.3.2. Le foncteur $i_{\mathcal{M}}$ associé à une petite catégorie $\mathcal{M}$ est une arité.

Preuve. Par le lemme 1.1.4, $\iota_{\mathcal{M}}$ est une arité de nerf $i_{\mathcal{M}}$. La proposition 1.1.5 assure alors que $i_{\mathcal{M}}$ est une arité. $\square$

Soit $\mathcal{M}$ une petite catégorie. On va détailler un peu $\Sigma \mathcal{M}$. Pour cela, notons encore n la catégorie discrète associée à l'ordinal fini $n \in \mathbb{N}$. Les objets de $\Sigma \mathcal{M}$ sont les foncteurs $n \rightarrow \mathcal{M}$ et les morphismes de $f : n \rightarrow \mathcal{M}$ vers $g : p \rightarrow \mathcal{M}$ sont les couples (h, α) composé d'un foncteur $h : n \rightarrow p$ et d'une 2-cellule

$$\begin{array}{ccc} n & \xrightarrow{h} & p \\ & \searrow f \quad \swarrow g & \\ & \alpha & \\ & \mathcal{M}. & \end{array}$$

Pour faire le lien avec notre intuition de départ, les objets de $\mathcal{M}$ sont les « couleurs » des entrées de notre théorie et un objet $f : n \rightarrow \mathcal{M}$ de $\Sigma \mathcal{M}$ est le choix d'un vecteur de n couleurs.

Il nous reste encore à expliquer comment on va combiner les différentes couleurs. Rappelons que si $\mathcal{M}$ est une petite catégorie monoidale, avec produit $\otimes$ et unité $\mathbb{1}$,

une *action* de $\mathcal{M}$ sur une catégorie $\mathcal{A}$ est un foncteur monoidal fort $\mathcal{M} \rightarrow \text{End}(\mathcal{A})$; équivalemment, c'est un foncteur $a: \mathcal{M} \times \mathcal{A} \rightarrow \mathcal{A}$ tel que naturellement en $m, m' \in \mathcal{M}$,

$$a(m \otimes m', -) \simeq a(m, a(m', -)) \quad \text{et} \quad a(\mathbb{1}, -) \simeq \text{id}_{\mathcal{A}}.$$

La catégorie $\mathcal{M}$ agit alors naturellement sur elle-même par $m \mapsto m \otimes -$ et la catégorie $\Sigma \mathcal{M}$ hérite de cette action : elle est donnée par le foncteur

$$a_{\mathcal{M}}: \mathcal{M} \times \Sigma \mathcal{M} \rightarrow \Sigma \mathcal{M}, \quad (m, f) \mapsto m \otimes f(-).$$

De même, $\mathcal{M}$ agit également sur $\widehat{\mathcal{M}}$, à savoir par

$$d_{\mathcal{M}}: \mathcal{M} \times \widehat{\mathcal{M}}, \quad (m, F) \mapsto F(- \otimes m).$$

Dorénavant, quand il n'y a pas d'ambiguïté, on notera indifféremment toutes les actions par $(m, f) \mapsto m \bullet f$.

On va maintenant pouvoir donner une définition alternative des théories de Lawvere d'arité $i_{\mathcal{M}}$. Pour tout préfaisceau $F \in \widehat{\Sigma \mathcal{M}}$, en précomposant par l'action de $\mathcal{M}$, on obtient un foncteur

$$\mathcal{M}^{\circ} \times (\Sigma \mathcal{M})^{\circ} \xrightarrow{a_{\mathcal{M}}^{\circ}} (\Sigma \mathcal{M})^{\circ} \xrightarrow{F} \text{Ens},$$

dont on note $\widetilde{F}: (\Sigma \mathcal{M})^{\circ} \rightarrow \widehat{\mathcal{M}}$ la curryfication. En particulier, on retrouve F à partir de $\widetilde{F}$ en postcomposant par l'évaluation en $\mathbb{1}$. Le lemme suivant précise cette remarque.

Lemme 1.3.3. *Le foncteur $F \mapsto \widetilde{F}$ établit une équivalence de catégories entre $\widehat{\Sigma \mathcal{M}}$ et la sous-catégorie pleine $\left[(\Sigma \mathcal{M})^{\circ}, \widehat{\mathcal{M}} \right]_{\mathcal{M}}$ de $\left[(\Sigma \mathcal{M})^{\circ}, \widehat{\mathcal{M}} \right]$ des foncteurs commutant à l'action de $\mathcal{M}$.*

Preuve. On commence par montrer que pour tout $F \in \widehat{\Sigma \mathcal{M}}$, le foncteur $\widetilde{F}$ commute à l'action de $\mathcal{M}$. Cela est donné par les isomorphismes naturels suivants : pour tout m et f ,

$$m \bullet \widetilde{F}(f) = F((- \otimes m) \bullet f) \simeq F(- \bullet (m \bullet f)) = \widetilde{F}(m \bullet f).$$

Notons alors $\text{ev}_{\mathbb{1}}$ l'évaluation $\widehat{\mathcal{M}} \rightarrow \text{Ens}$ en $\mathbb{1}$. Ce foncteur en induit un autre

$$\text{ev}_{\mathbb{1}} \circ -: \left[(\Sigma \mathcal{M})^{\circ}, \widehat{\mathcal{M}} \right]_{\mathcal{M}} \rightarrow \widehat{\Sigma \mathcal{M}}$$

qu'on montre maintenant être un pseudo-inverse de $\widetilde{}$. Par construction même de la curryfication, on a $\text{ev}_{\mathbb{1}} \circ \widetilde{} \simeq \text{id}_{\widehat{\Sigma \mathcal{M}}}$. Réciproquement, si $G: (\Sigma \mathcal{M})^{\circ} \rightarrow \widehat{\mathcal{M}}$ préserve l'action de $\mathcal{M}$, alors naturellement en f ,

$$\widetilde{\text{ev}_{\mathbb{1}} \circ G(f)} = G(- \bullet f)(\mathbb{1}) \simeq (- \bullet G(f))(\mathbb{1}) \simeq G(f)(\mathbb{1} \otimes -) \simeq G(f).$$

□

Proposition 1.3.4. *Un préfaisceau $F \in \widehat{\Sigma \mathcal{M}}$ est dans l'image essentielle de $v_{i_{\mathcal{M}}}$ si et seulement si $\widetilde{F}$ préserve les produits finis.*

Preuve. On note i pour $i_{\mathcal{M}}$ dans cette preuve.

Soit $G \in \widehat{\mathcal{M}}$. Montrons que $\widetilde{\nu_i G}$ commute aux produits finis. Le coproduit de $f: n \rightarrow \mathcal{M}$ et $g: p \rightarrow \mathcal{M}$ dans $\Sigma \mathcal{M}$ existe et est donné par le diagramme suivant :

$$\begin{array}{ccccc}
 n & \xrightarrow{\quad} & n + p & \xleftarrow{\quad} & p \\
 & \searrow \text{id} & \downarrow f \sqcup g & \swarrow \text{id} & \\
 & f & \mathcal{M} & g &
 \end{array}$$

Avec cette description, il apparaît immédiatement que l'arité i et l'action de $\mathcal{M}$ sur $\Sigma \mathcal{M}$ commutent aux coproduits. Ainsi,

$$\begin{aligned}
 \widetilde{\nu_i G}(f \sqcup g) &= \widehat{\mathcal{M}}(i(-\bullet(f \sqcup g)), G) \\
 &\simeq \widehat{\mathcal{M}}(i(-\bullet f) \sqcup i(-\bullet g), G) \\
 &\simeq \widehat{\mathcal{M}}(i(-\bullet f), G) \times \widehat{\mathcal{M}}(i(-\bullet g), G) \\
 &= \widetilde{\nu_i G}(f) \times \widetilde{\nu_i G}(g).
 \end{aligned}$$

Réciproquement, supposons $F \in \widehat{\Sigma \mathcal{M}}$ tel que $\widetilde{F}$ commute aux produits finis. On va montrer que F est représentable le long de i par $\widetilde{F}(\mathbf{I})$ où $\mathbf{I}: 1 \rightarrow \mathcal{M}$ est l'objet de $\Sigma \mathcal{M}$ sélectionnant l'unité monoidale $\mathbb{1}$ de $\mathcal{M}$. En effet, tout objet $f: n \rightarrow \mathcal{M}$ de $\Sigma \mathcal{M}$ satisfait à l'équation

$$f \simeq \coprod_{k \in n} (f(k) \bullet \mathbf{I}).$$

Ainsi, comme $\widetilde{F}$ commute à l'action de $\mathcal{M}$ (lemme 1.3.3), naturellement en $f: n \rightarrow \mathcal{M}$,

$$\begin{aligned}
 \widetilde{F}(f) &\simeq \prod_{k \in n} (f(k) \bullet \widetilde{F}(\mathbf{I})) \\
 &\simeq \prod_{k \in n} \widetilde{F}(\mathbf{I})(-\otimes f(k)) \\
 &\simeq \prod_{k \in n} \widehat{\mathcal{M}}(\mathfrak{h}_{-\otimes f(k)}, \widetilde{F}(\mathbf{I})) \\
 &\simeq \widehat{\mathcal{M}}\left(\coprod_{k \in n} \mathfrak{h}_{-\otimes f(k)}, \widetilde{F}(\mathbf{I})\right) \\
 &\simeq \widehat{\mathcal{M}}(i(-\bullet f), \widetilde{F}(\mathbf{I})) \\
 &= \widetilde{\nu_i \widetilde{F}(\mathbf{I})}(f)
 \end{aligned}$$

On a donc $\widetilde{F} \simeq \widetilde{\nu_i \widetilde{F}(\mathbf{I})}$. En composant par l'évaluation $\widehat{\mathcal{M}} \rightarrow \text{Ens}$ en $\mathbb{1}$, on obtient $F \simeq \nu_i \widetilde{F}(\mathbf{I})$. $\square$

Remarque 1.3.5. On fait ici une remarque dont on ne fera usage qu'en chapitre 2. L'action de $\mathcal{M}$ sur $\Sigma \mathcal{M}$ commutant aux coproduits finis, pour tout préfaisceau $F \in \widehat{\Sigma \mathcal{M}}$, F commute aux produits finis si et seulement si $\widetilde{F}$ commute aux produits finis.

Corollaire 1.3.6. *Soit $j : \Sigma\mathcal{M} \rightarrow \Theta$ une théorie de Lawvere d'arité $i_{\mathcal{M}} : \Sigma\mathcal{M} \rightarrow \widehat{\mathcal{M}}$. Un préfaisceau $M \in \widehat{\Theta}$ est un modèle de j si et seulement si $\widetilde{j^*M}$ commute aux produits finis.*

Ainsi, en travaillant modulo l'équivalence du lemme 1.3.3, on pourrait tout aussi bien décrire les modèles de j comme les foncteurs $M : \Theta^\circ \rightarrow \widehat{\mathcal{M}}$ tels que j^*M commute aux produits finis et à l'action de $\mathcal{M}$. Mais alors cette caractérisation ne fait plus appel à la structure de $\widehat{\mathcal{M}}$ mais seulement à ses produits finis et l'action de $\mathcal{M}$ sur celle-ci. Ceci motive la généralisation suivante.

Définition 1.3.7. *Soit $j : \Sigma\mathcal{M} \rightarrow \Theta$ une théorie de Lawvere d'arité $i_{\mathcal{M}} : \Sigma\mathcal{M} \rightarrow \widehat{\mathcal{M}}$ et $\mathcal{C}$ une catégorie admettant les produits finis et une action de $\mathcal{M}$. Un modèle de j dans $\mathcal{C}$ est un foncteur $M : \Theta^\circ \rightarrow \mathcal{C}$ tel que j^*M commute aux produits finis et à l'action de $\mathcal{M}$.*

Remarque 1.3.8. Si Θ admet les coproduits finis et une action de $\mathcal{M}$ et que j les préserve, alors, comme dans le cadre classique, il suffit de requérir que le modèle M lui-même préserve les produits finis et l'action de $\mathcal{M}$ plutôt que sa restriction par j .

Exemple(s) 1.3.9. Nous verrons dans le chapitre suivant un exemple non trivial de cette construction d'arité et de théorie de Lawvere. Pour le moment, examinons le cas où $\mathcal{M}$ est la catégorie finale. Alors, $\Sigma\mathcal{M}$ est isomorphe à $\aleph_0$ et l'arité $i_{\mathcal{M}}$ n'est autre que l'inclusion $\aleph_0 \rightarrow \text{Ens}$. On retrouve donc le cadre des théories de Lawvere classiques. L'action de $\mathcal{M}$ étant ici toujours triviale, la définition 1.3.7 de modèle généralisé est alors exactement la définition classique d'un modèle d'une théorie de Lawvere dans une catégorie admettant les produits finis.

Chapitre 2

Étude de cas : monade d'état local quantique

Staton établit dans [Sta15] une théorie algébrique des effets de bords d'un langage de programmation quantique. Un tel langage contient trois opérations interagissant avec la mémoire dont on donne ici la « sémantique intuitive » :

- une allocation de qbit : pour tout programme quantique x dépendant d'un qbit a , $\text{new}(a.x)$ dénote le programme qui alloue un nouveau qbit a , lui donne la valeur $|0\rangle$ puis exécute le programme x ,
- un branchement conditionnel : pour tous programmes quantiques x, y et qbit a , $\text{measure}(a, x, y)$ dénote le programme qui, après mesure physique du qbit a , branche sur x si le résultat est le bit classique 0 et sur y si c'est 1,
- et une opération de rotation sur l'espace mémoire (que l'on peut interpréter comme une forme d'écriture quantique) : pour tout programme quantique x dépendant de n qbits $\vec{b} = (b_1, \dots, b_n)$, tout vecteur $\vec{a} = (a_1, \dots, a_n)$ de n qbits et toute matrice unitaire $U \in \mathcal{M}_{2^n}(\mathbb{C})$, $\text{apply}_U(\vec{a}, \vec{b}.x)$ dénote le programme x conjugué par changement de base U , qui travaille donc sur un espace mémoire sur lequel la rotation unitaire U a été appliquée.

L'auteur donne un formalisme dans lequel il peut exprimer la théorie équationnelle de ces trois opérations : il l'appelle *théorie algébrique à paramètres linéaires*. On va montrer dans un premier temps que ces théories sont exactement les théories de Lawvere d'une certaine arité. Les conséquences de ce résultat sont avant tout conceptuelles : la notion de théorie à paramètres linéaires décrite par Staton n'est pas donc pas totalement *ad hoc* et gagne une certaine légitimité.

Staton poursuit son article avec une étude détaillée d'un modèle particulier de sa théorie algébrique quantique, qui a l'avantage d'être « fully complete » (dans la terminologie de l'article) en termes de théorie de Lawvere, c'est dire que ce modèle est pleinement fidèle. Ainsi, des égalités entre programmes quantiques peuvent être directement déduites de résultats d'algèbre linéaire. Pour tenter de mieux comprendre les conséquences de ces résultats sur le comportement de la mémoire quantique lors de l'exécution d'un programme, on développe une notion d'ensemble nominal quantique et du support qui lui est associée. On obtient ainsi une description du nombre minimal de qbit réellement utile à un programme quantique, qu'on espère rapprocher des résultats de [Sta15] obtenus par application du théorème de Stinespring.

2.1 Théories algébriques à paramètres linéaires

On commence par retranscrire ici la définition de théorie algébrique à paramètres linéaires que donne Staton dans [Sta15].

Définition 2.1.1 (Signature à paramètres linéaires). Une *signature à paramètres linéaires* est la donnée d'un ensemble $\mathcal{O}_{(p, \vec{m})}$ pour chaque couple $(p, \vec{m})$ constitué d'un entier $p \in \mathbb{N}$ et d'un vecteur $\vec{m} = (m_1, \dots, m_k) \in \mathbb{N}^k$ ($k \geq 0$).

Dans une signature σ , les éléments de $\mathcal{O}_{(p, \vec{m})}$ sont appelés *opérations d'arité* $(p, \vec{m})$. Intuitivement, si $\vec{m} = (m_1, \dots, m_k)$, il faut les penser comme des opérations ayant p paramètres linéaires et k entrées, la i^e dépendant de m_i paramètres linéaires. On fera l'abus de noter encore Σ l'ensemble de toutes ses opérations d'arité quelconque.

On suppose également disposer

- d'un ensemble infini Par de *variables de paramètres linéaires*,
- pour tout $m \in \mathbb{N}$, d'un ensemble infini Var_m de *variable d'entrées à m paramètres*.

On pose $\text{Var} = \coprod_{m \in \mathbb{N}} \text{Var}_m$. Pour un élément $x \in \text{Var}$, on écrira $x : m$ pour signifier son appartenance à Var_m . On prendra pour convention d'utiliser les lettres $a, b, c, \dots$ pour les éléments de Par et les lettres $\dots, x, y, z$ pour les éléments de Var .

Un *contexte linéaire* est alors défini comme un couple $(\vec{a}; \vec{x})$ avec $\vec{a} \in \text{Par}^p$ et $\vec{x} \in \text{Var}^k$ ($p, k \geq 0$). On notera facilement $(\vec{\alpha}, \vec{\beta})$ pour le vecteur concaténé $(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l)$.

Définition 2.1.2 (Terme à paramètres linéaires). Les *termes contextualisés* d'une signature σ sont définis inductivement comme suit :

- (i) $x(a_1, \dots, a_p)$ est un terme dans le contexte $(a_1, \dots, a_p; x : p)$,
- (ii) si t est un terme dans le contexte $(a_1, \dots, a_p; x_1, \dots, x_k)$, il l'est également dans le contexte $(a_{\rho(1)}, \dots, a_{\rho(p)}; x_{\tau(1)}, \dots, x_{\tau(k)})$ pour toutes permutations ρ et τ ,
- (iii) si t est un terme dans le contexte $(\vec{a}; \vec{x})$, il l'est aussi dans le contexte $(\vec{a}; x, \vec{x})$ pour tout $x \in \text{Var}$,
- (iv) si t est un terme dans le contexte $(\vec{a}; x, x, \vec{x})$, il l'est aussi dans le contexte $(\vec{a}; x, \vec{x})$,
- (v) si, pour tout $i \in \{1, \dots, k\}$, t_i est un terme dans le contexte $(\vec{c}, \vec{b}_i; \vec{x})$ avec $|\vec{b}_i| = m_i$ et si f est une opération d'arité $(p, (m_1, \dots, m_k))$, alors

$$f(\vec{a}, \vec{b}_1.t_1, \dots, \vec{b}_k.t_k)$$

est un terme dans le contexte $(\vec{c}, \vec{a}; \vec{x})$ pour tout $\vec{a} \in \text{Par}^p$.

Remarque 2.1.3. La règle (iii) est appelée règle d'affaiblissement, et la règle (iv) règle de contraction. Il est très important de noter que ces règles opèrent sur la deuxième composante du contexte (i.e. la partie non linéaire) : il est crucial de ne pas soumettre la partie linéaire du contexte à ces mêmes règles !

Un *axiome* sur la signature σ est un mot de la forme $t = u$ où t et u sont des termes de σ **dans le même contexte**.

Définition 2.1.4 (Théorie à paramètres linéaires). Une *théorie algébrique à paramètres linéaires* sur une signature σ est un ensemble d'axiomes sur σ .

Le reste de cette section est dédié à montrer que la donnée d'une théorie algébrique à paramètres linéaires est équivalente à celle d'une théorie de Lawvere d'une certaine arité.

On définit Bij comme la sous-catégorie de $\mathfrak{N}_0$ contenant tous les entiers et les bijections entre eux. Cette catégorie admet une structure monoidale symétrique **stricte** avec produit $m \otimes n = m + n$ et unité $\mathbb{1} = 0$. On peut alors appliquer la théorie générale décrite en section 1.3 : le foncteur

$$i: \Sigma \text{Bij} \rightarrow \widehat{\text{Bij}}$$

est une arité. De plus, le produit monoidal de Bij induit une action $m \bullet (f: n \rightarrow \text{Bij}) = m + f(-)$ sur ΣBij , et une action $m \bullet F = F(- + m)$ sur $\widehat{\text{Bij}}$. Enfin, pour toute théorie de Lawvere $j: \Sigma \text{Bij} \rightarrow \Theta$ d'arité i , un préfaisceau $M \in \widehat{\Theta}$ est un modèle si et seulement si le foncteur

$$(\Sigma \text{Bij})^\circ \rightarrow \widehat{\text{Bij}}, \quad f \mapsto M(- \bullet f)$$

commute aux produits finis et à l'action de Bij .

Étant donné une signature à paramètres linéaires σ , on construit la *catégorie syntaxique* Θ_σ de la signature σ comme suit :

- on part de ΣBij dont on prend le graphe sous-jacent $\mathbf{G}$;
- pour toutes opérations $(f_i)_{i=0,\dots,k}$ de σ d'arité $(p_i, \vec{m})$ et tout $n \in \mathbb{N}$, on ajoute une arête étiquetée $n \bullet \vec{f}$ de $n \bullet \vec{p}$ vers $n \bullet \vec{m}$ (où $\vec{m}$ et les p_i sont vu comme des objets de ΣBij) ;
- on obtient ainsi un graphe $\mathbf{G}_\sigma$;
- on peut alors poser sur la catégorie libre $\mathcal{G}_\sigma$ engendrée par $\mathbf{G}_\sigma$ la relation d'équivalence $\sim$ identifiant
 - (i) deux morphismes f et g s'ils existent déjà dans ΣBij et y sont égaux,
 - (ii) $0 \bullet f$ avec f et $(n + m) \bullet f$ avec $n \bullet (m \bullet f)$ pour tout $m, n \in \mathbb{N}$,
 - (iii) $n \bullet f_i$ avec $n \bullet \vec{f} \circ (p_i \rightarrow \vec{p})$ où $p_i \rightarrow \vec{p}$ est l'injection canonique de ΣBij , pour tout $n \in \mathbb{N}$, tout vecteur $\vec{f} = (f_j)_{j=0,\dots,k}$ d'opérations d'arités respectives $(p_j, \vec{m})$ et tout $i \in \{0, \dots, k\}$;
- Θ_σ est alors obtenue en quotientant $\mathcal{G}_\sigma$ par $\sim$.

En bref, la catégorie Θ_σ est la catégorie obtenue à partir de ΣBij en ajoutant « librement » un morphisme $n \bullet f: n \bullet p \rightarrow n \bullet \vec{m}$ pour toute opération $f \in \mathcal{O}_{(p, \vec{m})}$ et les coproduits finis relatifs à ces morphismes. En particulier, l'inclusion $\Sigma \text{Bij} \rightarrow \Theta_\sigma$ crée évidemment les coproduits finis.

Définition 2.1.5 (Interprétation d'un terme). Soit σ une signature à paramètres linéaires. L'interprétation $\llbracket t \rrbracket_{(\vec{a}; \vec{x})}$ dans Θ_σ d'un terme t dans le contexte $(a_1, \dots, a_p; x_1 : m_1, \dots, x_k : m_k)$ est un morphisme $p \rightarrow \vec{m}$ défini inductivement par :

- (i) $\llbracket x(a_1, \dots, a_p) \rrbracket_{(\vec{a}; x; p)} = \text{id}_p$,
- (ii) si t est un terme dans le contexte $(\vec{a}; \vec{x} : \vec{m})$, si $\rho \in \mathfrak{S}_p$ et $\tau \in \mathfrak{S}_k$ avec $p = |\vec{a}|$ et $k = |\vec{x}|$, alors

$$\llbracket t \rrbracket_{(\rho(\vec{a}); \tau(\vec{x}))} = \tau(\vec{m}) \circ \llbracket t \rrbracket_{(\vec{a}; \vec{x})} \circ (\rho \bullet p)$$

où $\rho \bullet p$ et $\tau(\vec{m})$ sont les flèches respectives de ΣBij suivantes :

$$\begin{array}{ccc} 1 & \xrightarrow{\text{id}} & 1 \\ \swarrow \rho & & \searrow \rho \\ p & & p \end{array} \quad \text{et} \quad \begin{array}{ccc} k & \xrightarrow{\tau^{-1}} & k \\ \swarrow \vec{m} & & \searrow (m_{\tau(i)})_i \\ & \xrightarrow{\text{id}} & \end{array} \quad \text{Bij}$$

(iii) si t est un terme dans le contexte $(\vec{a}; \vec{x} : \vec{m})$, et $(x : m) \in \text{Var}$, alors

$$\llbracket t \rrbracket_{(\vec{a}; x, \vec{x})} = w_{m, \vec{m}} \circ \llbracket t \rrbracket_{(\vec{a}; \vec{x})}$$

où $w_{m, \vec{m}}$ est la flèche de ΣBij suivante ($k = |\vec{x}|$) :

$$\begin{array}{ccc} k & \xrightarrow{i \mapsto i+1} & k+1 \\ \swarrow \vec{m} & \xrightarrow{\alpha} & \searrow (m, \vec{m}) \\ & \text{Bij} & \end{array} \quad \text{où } \alpha_i = \text{id}_{m_i} : m_i \rightarrow m_i$$

(iv) si t est un terme dans le contexte $(\vec{a}; x : m, x : m, \vec{x} : \vec{m})$, alors

$$\llbracket t \rrbracket_{(\vec{a}; x, \vec{x})} = c_{m, \vec{m}} \circ \llbracket t \rrbracket_{(\vec{a}; x, x, \vec{x})}$$

où $c_{m, \vec{m}}$ est la flèche de ΣBij suivante ($k = |\vec{x}|$) :

$$\begin{array}{ccc} k+2 & \xrightarrow[\substack{0 \mapsto 0 \\ i \mapsto i-1}]{} & k+1 \\ \swarrow (m, m\vec{m}) & \xrightarrow{\alpha} & \searrow (m, \vec{m}) \\ & \text{Bij} & \end{array} \quad \text{où } \begin{array}{l} \alpha_0 = \alpha_1 = \text{id}_m \\ \alpha_i = \text{id}_{m_i} : m_i \rightarrow m_i \end{array}$$

(v) si f est une opération d'arité $(p, \vec{m})$ et pour tout $i \in \{1, \dots, k\}$ t_i est un terme dans le contexte $(\vec{c}, \vec{b}_i; \vec{x} : \vec{m})$ avec $m_i = |b_i|$, alors pour tout $\vec{a} \in \text{Par}^p$ et en notant $q = |\vec{c}|$

$$\llbracket f(\vec{a}, \vec{b}_1.t_1, \dots, \vec{b}_k.t_k) \rrbracket_{(\vec{c}, \vec{a}; \vec{x})} = \left\langle \llbracket t_i \rrbracket_{(\vec{c}, \vec{b}_i; \vec{x})} \right\rangle_{i=1, \dots, k} \circ (q \bullet f)$$

où $\langle \cdot \rangle_{i=1, \dots, k}$ est l'application « morphisme induit » de la propriété universelle du coproduit.

L'interprétation des termes dans Θ_σ permet d'interpréter les axiomes sur σ comme des règles d'identification de morphismes. Plus précisément, si T est une théorie sur la signature σ , on pose $\sim_T$ la relation d'équivalence sur les morphismes de Θ_σ engendrée par

$$\llbracket t \rrbracket_{(\vec{a}; \vec{x})} \sim_T \llbracket u \rrbracket_{(\vec{a}; \vec{x})}$$

pour tout axiome $t = u$ de T dans le contexte $(\vec{a}; \vec{x})$.

Définition 2.1.6 (Catégorie syntaxique). La catégorie syntaxique d'une théorie algébrique à paramètres linéaires T sur une signature σ , notée Θ_T , est la catégorie quotient $\Theta_\sigma / \sim_T$.

Pour une théorie T , on a toujours une inclusion $j_T: \Sigma \text{Bij} \rightarrow \Theta_T$ bijective sur les objets. On va maintenant montrer la propriété suivante.

Proposition 2.1.7. *Soit T une théorie algébrique à paramètres linéaires. Le foncteur j_T est une théorie de Lawvere d'arité $i: \Sigma \text{Bij} \rightarrow \widehat{\text{Bij}}$.*

Preuve. Il s'agit de voir que la monade $j_T^* j_T!$ sur $\widehat{\Sigma \text{Bij}}$ respecte l'image essentielle de $v_i: \widehat{\text{Bij}} \rightarrow \widehat{\Sigma \text{Bij}}$. Or, par la proposition 1.3.4 et la remarque qui suit, l'image essentielle de v_i est exactement constituée des préfaisceaux sur ΣBij commutant aux produits finis.

Il s'agit donc de vérifier que $j_T^* j_T!$ envoie les foncteurs préservant les produits finis sur des foncteurs préservant les produits finis. Or par le lemme A.2.2, on sait que $j_T!$ admet déjà cette propriété. Il suffit donc de montrer que j_T^* également, ce qui sera le cas si j_T préserve les coproduits finis.

Or j_T est la composée $\Sigma \text{Bij} \rightarrow \Theta_\sigma \rightarrow \Theta_T$. On sait déjà que l'inclusion $\Sigma \text{Bij} \rightarrow \Theta_\sigma$ préserve les coproduits finis. Il reste donc à montrer que la projection canonique $\Theta_\sigma \rightarrow \Theta_\sigma / \sim_T$ elle-même préserve les coproduits finis. C'est un fait général bien connu. $\square$

Remarque 2.1.8. On a une sorte de pseudo-inverse à l'application $T \mapsto j_T$.

En effet, si l'on suppose avoir une théorie de Lawvere $j: \Sigma \text{Bij} \rightarrow \Theta$ d'arité i , alors la monade $j^* j!$ sur $\widehat{\Sigma \text{Bij}}$ envoie les préfaisceaux respectant les produits finis sur des préfaisceaux respectant les produits finis. Toujours par le lemme A.2.2, $j!$ a cette propriété et donc j^* se doit de l'avoir également. En appliquant cette propriété à $\Theta(-, \vartheta)$, $\vartheta \in \Theta$, on a exactement que j commute aux coproduits finis.

On note alors σ' la signature à paramètres linéaires dont les opérations d'arité $(p, \vec{m})$ sont les éléments de $\Theta(p, \vec{m})$. Tous les termes sur σ' s'interprètent tautologiquement dans Θ et on peut alors former la théorie T' sur σ' constituée des axiomes $t = u$ dès que les interprétations de t et u dans Θ sont en effet le même morphisme.

Alors, j préservant les coproduits finis, il se factorise en $\Sigma \text{Bij} \rightarrow \Theta_{\sigma'} \rightarrow \Theta$ où le second foncteur s'identifie à la projection canonique $\Theta_{\sigma'} \rightarrow \Theta_{T'}$. C'est-à-dire que j et $j_{T'}$ sont des théories de Lawvere isomorphes.

Mais l'association de T' à j décrite ci-dessus n'est pas pour autant un inverse de $T \mapsto j_T$. En effet, partant d'une théorie T sur une signature σ , et en appliquant la construction ci-dessus à j_T , on obtient une signature σ' a priori bien plus grosse que σ : pour toute opération f de σ d'arité $(p, \vec{m})$, on a des opérations $\underline{n \bullet f}$ d'arité $(n + p, n \bullet \vec{m})$ pour tout $n \in \mathbb{N}$. En revanche, T' sera tout de même « équivalente » à T car elle contiendra tous les axiomes de la forme $\underline{n \bullet f} = n \bullet (0 \bullet f)$. On peut donc penser à j_T comme à une version « saturée » de la théorie T .

Étant donnée une théorie algébrique à paramètres linéaires T , la théorie de Lawvere associée j_T est dans les hypothèses de la définition 1.3.7 et de la remarque qui suit. Ainsi, un modèle de j_T dans une catégorie $\mathcal{C}$ admettant une action de Bij et les produits finis est tout simplement un foncteur $\Theta_T^\circ \rightarrow \mathcal{C}$ respectant l'action et les produits finis. On retrouve ainsi la définition donnée par Staton dans [Sta15] à ceci près qu'il requiert que l'action de Bij commute aux produits finis dans $\mathcal{C}$. Notre cadre de travail permet de ce passer de cette hypothèse : l'action de Bij commute en effet aux coproduits finis dans Θ_T et donc pour un modèle $M: \Theta_T^\circ \rightarrow \mathcal{C}$ on aura bien (et c'est

tout ce qui nous importe)

$$n \bullet \left(\prod_{i=1}^k M(m_i) \right) \simeq n \bullet M(\vec{m}) \simeq M(n \bullet \vec{m}) \simeq \prod_{i=1}^k M(n + m_i) \simeq \prod_{i=1}^k n \bullet M(m_i).$$

2.2 Monade d'état local quantique

On attaque maintenant notre problème concret : raisonner algébriquement sur la manipulation dynamique de la mémoire dans un langage de programmation quantique. On pose χ la signature à paramètres linéaires composées des opérations (munies de leur arité) suivantes :

$$\text{measure} : (1, (0, 0)), \quad \text{new} : (0, (1)), \quad \text{apply}_U : (n, (n)) \quad \forall U \in \mathbb{U}_{2^n}(\mathbb{C})$$

où $\mathbb{U}_p(k)$ est le groupe des matrices unitaires de taille p à coefficients dans le corp k .

Avant de présenter les axiomes de la théorie quantique que l'on va considérer, on pose quelques notations. On particularise une matrice unitaire de taille 2×2 :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On note aussi swap la matrice

$$\text{swap} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{U}_4(\mathbb{C}).$$

Pour tout $U, V \in \mathbb{U}_p(\mathbb{C})$, on note $D(U, V)$ la matrice diagonale par blocs Si $U \in \mathbb{U}_p(\mathbb{C})$ et $V \in \mathbb{U}_q(\mathbb{C})$, on note $U \otimes V \in \mathbb{U}_{pq}(\mathbb{C})$ le produit de Kronecker des matrices U et V . Enfin, on définit par récurrence un opérateur $\text{discard}_n(\vec{a}; t)$ qui mesure les qbits de $\vec{a}$ les un après les autres en renvoyant à chaque fois le terme t sans tenir compte de la mesure : le cas initial est

$$\text{discard}_0((); t) = t$$

puis pour tout $n \in \mathbb{N}$, et tout terme t et tout vecteur $(a, \vec{b})$ de longueur $n+1$, on pose

$$\text{discard}_{n+1}(a, \vec{b}; t) = \text{measure}(a, \text{discard}_n(\vec{b}; t), \text{discard}_n(a, \vec{b}; t)).$$

On considère la théorie Q sur la signature χ axiomatisée par :

$$\text{apply}_X(a, b.\text{measure}(b, x, y)) = \text{measure}(a, y, x) \quad (\text{A})$$

$$\begin{aligned} \text{measure}(a, \text{apply}_U(\vec{b}, \vec{c}.x(\vec{c})), \text{apply}_V(\vec{b}, \vec{c}.x(\vec{c}))) \\ = \text{apply}_{D(U,V)}((a, \vec{b}), (d, \vec{c}).\text{measure}(d, x(\vec{c}), y(\vec{c}))) \end{aligned} \quad (\text{B})$$

$$\text{apply}_U(\vec{a}, \vec{b}.\text{discard}_n(\vec{b}; x)) = \text{discard}_n(\vec{a}; x) \quad (\text{C})$$

$$\text{new}(a.\text{measure}(a, x, y)) = x \quad (\text{D})$$

$$\text{new}(a.\text{apply}_{D(U,V)}((a, \vec{b}), d, \vec{c}.x(d, \vec{c}))) = \text{apply}_U(\vec{b}, \vec{c}.\text{new}(a.x(a, \vec{c}))) \quad (\text{E})$$

$$\text{apply}_{\text{swap}}((a, b), (c, d).x(c, d)) = x(b, a) \quad (\text{F})$$

$$\text{apply}_{I_n}(\vec{a}, \vec{b}.x(\vec{b})) = x(\vec{a}) \quad (\text{G})$$

$$\text{apply}_{UV}(\vec{a}, \vec{b}.x(\vec{b})) = \text{apply}_U(\vec{a}, \vec{b}.\text{apply}_V(\vec{b}, \vec{c}.x(\vec{c}))) \quad (\text{H})$$

$$\text{apply}_{U \otimes V}((\vec{a}, \vec{b}), (\vec{c}, \vec{d}).x(\vec{c}, \vec{d})) = \text{apply}_U(\vec{a}, \vec{c}.\text{apply}_V(\vec{b}, \vec{d}.x(\vec{c}, \vec{d}))) \quad (\text{I})$$

$$\begin{aligned} \text{measure}(a, \text{measure}(b, u, v), \text{measure}(b, x, y)) \\ = \text{measure}(b, \text{measure}(a, u, x), \text{measure}(a, v, y)) \end{aligned} \quad (\text{J})$$

$$\text{new}(a.\text{new}(b.x(a, b))) = \text{new}(b.\text{new}(a.x(a, b))) \quad (\text{K})$$

$$\text{new}(a.\text{measure}(b, x(a), y(a))) = \text{measure}(b, \text{new}(a.x(a)), \text{new}(a.y(a))) \quad (\text{L})$$

Les axiomes (A) à (C) gèrent les interactions entre apply et measure . Les axiomes (F) à (I) assurent que les matrices de permutations (qui sont unitaires) agissent comme les permutations sur les qbits, et que deux unitaires se composent comme il se doit. Dans la suite, on met l'emphasis sur les axiomes (D) et (J) à (L) qui expliquent l'interaction des opérations new et measure : on va voir que la compréhension de cette interaction est cruciale dans la recherche de termes canoniques.

La notion de catégorie syntaxique et la propriété 2.1.7 nous permet alors de considérer la théorie de Lawvere $j_Q: \Sigma \text{Bij} \rightarrow \Theta_Q$ d'arité $i: \Sigma \text{Bij} \rightarrow \widehat{\text{Bij}}$. On rappelle alors (définition 1.3.7 et remarque en-dessous) qu'un modèle dans une catégorie $\mathcal{C}$ admettant produits finis et action de Bij est un foncteur $M: \Theta_Q^\circ \rightarrow \mathcal{C}$ préservant ceux-ci. De plus, $j_Q: \Sigma \text{Bij} \rightarrow \Theta_Q$ préserve les coproduits finis et l'action de Bij , donc les objets de Θ_Q sont tous, comme dans ΣBij , des coproduits finis d'objets de la forme $n \bullet 0$. Il suffit donc, pour décrire un modèle $M: \Theta_Q^\circ \rightarrow \mathcal{C}$ de donner l'objet $M(0)$ et les morphismes

$$M(\text{measure}), \quad M(\text{new}), \quad M(\text{apply}_U) \quad \forall U \in \mathbb{U}_{2^n}(\mathbb{C}), \forall n \in \mathbb{N}.$$

C'est ce que l'on va faire dans la catégorie $\mathcal{C}_{\text{CPU}}^*$. Ses objets sont les algèbres stellaires et ses morphismes sont les applications complètement positives unifères entre algèbres stellaires, c'est-à-dire les applications linéaires $f: X \rightarrow Y$ telles que pour tout $n \in \mathbb{N}$, l'application induite

$$\mathcal{M}_n(f): \mathcal{M}_n(X) \rightarrow \mathcal{M}_n(Y)$$

préserve les éléments positifs (i.e. de la forme A^*A). Notamment, les morphismes d'algèbres stellaires sont des morphismes de $\mathcal{C}_{\text{CPU}}^*$. La catégorie $\mathcal{C}_{\text{CPU}}^*$ admet tous les produits finis : ce sont les sommes directes d'espaces vectoriels avec les opérations d'algèbres stellaires membre à membre. Elle admet aussi une action de Bij que l'on décrit

maintenant. Pour tout objet $n \in \text{Bij}$, son action sur l'algèbre stellaire X est donnée par $n \bullet X = \mathcal{M}_{2^n}(X)$. L'action d'une permutation $\tau: n \rightarrow n$ sur l'algèbre X est un peu plus subtile : τ induit une permutation de l'ensemble des fonctions $n \rightarrow \{0, 1\}$ par précomposition ; en notant $P_\tau \in \mathcal{M}_{2^n}(X)$ la matrice de permutation associée, on définit

$$\tau \bullet X : A \mapsto P^* A P.$$

Cela définit en effet une action de la catégorie monoidale Bij sur $\mathcal{C}_{\text{CPU}}^*$ car il existe un isomorphisme naturel

$$\mathcal{M}_p(\mathcal{M}_q(X)) \simeq \mathcal{M}_{pq}(X)$$

pour tout $p, q \in \mathbb{N}$ qui consiste à regarder les matrices de tailles p à coefficients dans les matrices de taille q comme des matrices de tailles pq présentées par blocs.

On pose alors $\mathbf{C}$ le foncteur $\Theta_Q^\circ \rightarrow \mathcal{C}_{\text{CPU}}^*$ commutant à l'action de Bij et aux produits finis donné par l'algèbre stellaire canonique $\mathbf{C}(0) = \mathbb{C}$ et par les morphismes suivants

$$\begin{aligned} \mathbf{C}(\text{measure}) : \mathbb{C} \times \mathbb{C} &\rightarrow \mathcal{M}_2(\mathbb{C}), & (\alpha, \beta) &\mapsto \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \\ \mathbf{C}(\text{apply}_U) : \mathcal{M}_{2^n}(\mathbb{C}) &\rightarrow \mathcal{M}_{2^n}(\mathbb{C}), & A &\mapsto U^* A U \\ \mathbf{C}(\text{new}) : \mathcal{M}_2(\mathbb{C}) &\rightarrow \mathbb{C}, & \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} &\mapsto \alpha \end{aligned}$$

Le foncteur $\mathbf{C}$ définit en fait un modèle $\Theta_Q^\circ \rightarrow \mathcal{C}_{\text{CPU}}^*$ de Q . En effet, on peut vérifier par un calcul direct que tous les axiomes de la théorie sont bien vérifiés. Le résultat principal de l'article [Sta15] peut alors se traduire comme suit.

Théorème 2.2.1 (Staton). *Le modèle $\mathbf{C} : \Theta_Q^\circ \rightarrow \mathcal{C}_{\text{CPU}}^*$ de Q est pleinement fidèle.*

Le caractère plein de $\mathbf{C}$ est déjà contenu dans les travaux de Selinger. L'apport de Staton tient donc dans la fidélité du modèle.

2.3 Ensembles nominaux quantiques

On va maintenant introduire une version quantique des ensembles nominaux. Les ensembles nominaux sont traditionnellement utilisés pour caractériser algébriquement les variables libres et liées d'une construction syntaxique (par exemple un λ -terme clos ou un énoncé logique du premier ordre). On peut typiquement penser au langage engendré par une grammaire sur un alphabet contenant un ensemble A de *variables*. Devant un terme de cette grammaire, il n'est pas toujours facile de savoir si un variable est liée ou non : la grammaire peut être ambiguë et il est alors difficile d'utiliser une induction pour repérer les variables liées ; ou bien on peut avoir un terme sans avoir accès à son écriture sur l'alphabet. L'idée des techniques nominales est alors la suivante : changer le point de vue syntaxique pour traiter les termes de manière algébrique. Plus précisément, la permutation des variables de A induit une action de $\mathfrak{S}_A$ sur l'ensemble des termes : si un ensemble $S \subseteq A$ est telle que toute permutation fixant chacun des éléments de S fixe aussi le terme t , alors les variables apparaissant dans t sont nécessairement parmi les éléments de S .

On rappelle dans un premier temps la notion d'ensemble nominal et celle de support. Puis on donne l'interprétation faisceautique de ces notions qui nous servira dans

un second temps à généraliser les techniques nominales au cadre quantique. Enfin, on utilisera ces dernières pour mieux comprendre les algèbres de la monade d'état local quantique.

2.3.1 Ensembles nominaux. Soit A un ensemble dénombrable, dont on nomme *variables* les éléments. On note $\mathfrak{S}_A$ le groupe des permutations de A .

Définition 2.3.1. Soient X un $\mathfrak{S}_A$ -ensemble. On dit que $S \subseteq A$ *supporte* $x \in X$ si toute permutation de $\mathfrak{S}_A$ fixant S point à point est dans le stabilisateur de x .

Un élément de X est dit de *support fini* s'il est supporté par au moins un ensemble fini.

On remarque tout de suite que l'ensemble des supports d'un élément $x \in X$ contient toujours A lui-même et est fermé par sur-ensemble dans $\mathcal{P}(A)$.

Définition 2.3.2 (Ensemble nominal). Un $\mathfrak{S}_A$ -ensemble X est *nominal* si tous ses éléments sont finiment supportés.

Les ensembles nominaux et les morphismes de $\mathfrak{S}_A$ -ensembles forment une sous-catégorie pleine Nom de $[\mathfrak{S}_A, \text{Ens}]$

Lemme 2.3.3. Soit X un $\mathfrak{S}_A$ -ensemble. Si $S, S' \subseteq A$ sont finis et supportent $x \in X$, alors $S \cap S'$ aussi.

Preuve. Toute permutation τ peut se décomposer en produit de transpositions dont le support évite les point fixe de τ . Il suffit donc de vérifier que pour tout $a, a' \in A \setminus (S \cap S')$, la transposition $(a \ a')$ fixe x . On écrit alors $(a \ a')$ comme le produit $(a'' \ a)(a'' \ a')(a \ a'')$ avec $a'' \notin (S \cup S')$ (c'est possible car S et S' sont finis et A infini). Chacun des termes du produit fixe x car fixe S ou S' point par point. $\square$

Définition 2.3.4. Soit X un $\mathfrak{S}_A$ -ensemble. Le *support* de $x \in X$ est le plus petit ensemble fini supportant x . Il existe par le lemme précédent et s'écrit :

$$\text{supp}(x) = \bigcap_{\substack{S \text{ fini} \\ S \text{ supporte } x}} S.$$

Sous cette forme, la présentation des ensembles nominaux est difficilement généralisable au cadre quantique. Heureusement, il existe une présentation des ensembles nominaux bien plus agréable de notre point de vue : Nom s'identifie à une sous-catégorie pleine de la catégorie de préfaisceaux $[\text{Inj}, \text{Ens}]$, où Inj est la sous-catégorie de $\aleph_0$ constituée de tous les objets mais seulement des injections entre eux.

On construit un foncteur $N : \text{Nom} \rightarrow [\text{Inj}, \text{Ens}]$ comme suit. On note Inj_A la catégorie des parties finies de A et des injections entre elles. Comme Inj_A est équivalente à Inj , il suffit de construire un foncteur $N_A : \text{Nom} \rightarrow [\text{Inj}_A, \text{Ens}]$ pour définir N . Pour tout ensemble nominal X , et toute partie finie S de A , on pose $N_A X(S)$ l'ensemble des éléments de X supporté par S ; de plus, toute injection $f : S \rightarrow S'$ donne lieu à une permutation τ_f de A , et on pose $N_A X(f) : N_A X(S) \rightarrow N_A X(S')$ la fonction $x \mapsto \tau_f \cdot x$ où $\cdot$ dénote l'action de $\mathfrak{S}_A$ sur X , faisant ainsi de $N_A X$ un objet de $[\text{Inj}_A, \text{Ens}]$. On a ainsi défini N_A sur les objets et on l'étend aisément en un foncteur. Ce foncteur admet un adjoint à gauche Π : c'est le foncteur qui associe à $F \in [\text{Inj}_A, \text{Ens}]$ le $\mathfrak{S}_A$ -ensemble $\text{colim}_{\text{Inj}_A}(F)$ sur lequel l'action d'une permutation τ est induite par l'image par F des injections obtenues en restreignant τ aux parties finies de A . On vérifie facilement

que la counité de cette adjonction est un isomorphisme : ainsi, N_A est pleinement fidèle. En composant par l'équivalence observée plus haut, on obtient un plongement $N: \text{Nom} \rightarrow [\text{Inj}, \text{Ens}]$.

L'avantage de ce plongement $\text{Nom} \hookrightarrow [\text{Inj}, \text{Ens}]$ est qu'on peut directement caractériser les ensembles nominaux grâce à des propriétés faisceautiques. À partir de maintenant, on appellera *nominal* un élément de $[\text{Inj}, \text{Ens}]$ s'il est dans l'image de N .

Lemme 2.3.5. *Un foncteur $F: \text{Inj} \rightarrow \text{Ens}$ est nominal si et seulement s'il préserve les produits fibrés.*

Preuve. Si F est nominal, alors c'est la transposition exacte du lemme 2.3.3 à travers N que de dire que F préserve les produits fibrés.

Réciproquement, si F préserve les produits fibrés, alors tous éléments $x \in F(n)$ et $y \in F(m)$ identifiés par la prise de colimite sont également identifiés avec un $z \in F(k)$ pour $k \leq m, n$. Ainsi le processus $N \Pi$ ne « crée » pas de nouveau point. Autrement dit, la composante $F \rightarrow N \Pi F$ de l'unité, habituellement un monomorphisme seulement, est ici un isomorphisme. $\square$

Cette caractérisation permet en fait de voir les ensembles nominaux comme des faisceaux sur Inj° muni d'une bonne topologie de Grothendieck. Cette topologie, dite topologie de Schanuel, est celle où les cribles couvrants d'un objet n sont engendré par les singletons $\{f\}$ où f a codomaine n . Cela montre en particulier que Nom est un topos, lieu agréable pour toutes sortes de manipulation.

Muni de cette caractérisation, on peut montrer que les algèbres de la monade d'état local classique sont des ensembles nominaux. Intuitivement, cela dit que tout élément d'une algèbre de la monade d'état local dispose d'un support, qui contient les variables que l'élément utilise effectivement lors de son exécution. Et c'est tout le point de cette introduction aux ensembles nominaux : ils servent à tracer les cases mémoires réellement utiles à un programme. On pourra alors tenter de faire de même avec les programmes quantiques en introduisant une légère généralisation des ensembles nominaux.

Considérons σ_{coll} la signature à paramètres linéaires comportant l'unique opération coll d'arité $(1, (0))$ (coll pour « collect »), et T_{coll} la théorie sur σ_{coll} constituée de l'axiome :

$$\text{coll}(a, \text{coll}(b, x)) = \text{coll}(b, \text{coll}(a, x)).$$

Cette théorie induit une théorie de Lawvere $j_{T_{\text{coll}}}: \Sigma \text{Bij} \rightarrow \Theta_{T_{\text{coll}}}$ d'arité $i: \Sigma \text{Bij} \rightarrow \widehat{\text{Bij}}$. Par construction même de la catégorie syntaxique associée à T_{coll} , la catégorie $\Theta_{T_{\text{coll}}}$ est isomorphe à $\Sigma(\text{Inj}^\circ)$ et la théorie $j_{T_{\text{coll}}}$ est alors l'inclusion canonique $\Sigma \text{Bij} \rightarrow \Sigma(\text{Inj}^\circ)$. Or on a vu que les modèles d'une telle théorie $j_{T_{\text{coll}}}$ sont les préfaisceaux sur son codomaine respectant les produits finis, donc la catégorie des modèles de $j_{T_{\text{coll}}}$ s'identifie à $[\text{Inj}, \text{Ens}]$.

Ainsi, toute théorie T sur une signature σ telles que $\sigma_{\text{coll}} \subseteq \sigma$ et $T_{\text{coll}} \subseteq T$ induit un morphisme $k: \Theta_{T_{\text{coll}}} \rightarrow \Theta_T$ de théories de Lawvere à arité. La monade associée $j_T^* j_{T!}$ se factorise donc par une monade $k^* k_!$ sur $[\text{Inj}, \text{Ens}]$ dont les algèbres sont équivalents aux modèles de j_T . C'est notamment le cas de la théorie T présentant la monade d'état local (cf. [Mel14]). On peut alors montrer que les (restriction à Inj° des) modèles de cette théorie sont nominaux. On ne s'étend pas ici sur la preuve de ce fait car elle est similaire au cas quantique que l'on traite ci-dessous.

2.3.2 Ensembles qnominaux. Afin de généraliser la notion d'ensemble nominal au cadre quantique, il convient de remplacer l'opération coll de désallocation. En effet, la désallocation d'un qbit se fait par l'observation de celui-ci : il passe d'une superposition d'états à un état de bit classique, 0 ou 1. L'opération de désallocation quantique est donc un branchement conditionnel.

Formellement, on pose σ_{meas} la signature dont l'unique opération est meas d'arité $(1, (0, 0))$. Intuitivement, le terme $\text{meas}(a, x, y)$ doit être compris comme : on mesure le qbit a , et selon que le résultat est 0 ou 1, on branche sur le programme x ou y . On pose alors T_{meas} la théorie à paramètres linéaires sur σ_{meas} contenant l'unique axiome

$$\text{meas}(a, \text{meas}(b, u, v), \text{meas}(b, x, y)) = \text{meas}(b, \text{meas}(a, u, x), \text{meas}(a, v, y)). \quad (13)$$

Afin de bien faire apparaître le parallèle avec la monade d'état local classique, on note qlnj la catégorie syntaxique $(\Theta_{T_{\text{meas}}})^\circ$.¹

Pour plus de simplicité, dans la catégorie qlnj , pour tout $j \in n + 1$ on note meas_j^n le morphisme

$$(n, n) \xrightarrow{n \bullet \text{meas}} n + 1 \xrightarrow{\tau_j^n} n + 1$$

où τ_j^n est la transposition $(j \ n)$ sur l'ensemble $n + 1$. Intuitivement, meas_j^n est l'opération de « mesure sur le j^{e} qbit d'un contexte de $n + 1$ qbits ». En particulier, meas_n^n est égal à $n \bullet \text{meas}$. L'axiome (13) de la théorie T_{meas} se traduit alors dans qlnj comme suit : pour tout $n \geq 0$, pour tout $i < j \in n + 2$, le diagramme suivant commute

$$\begin{array}{ccc} (n, n, n, n) & \xrightarrow{\text{meas}_{j-1}^n \times \text{meas}_{i-1}^n} & (n + 1, n + 1) \\ \downarrow & & \downarrow \text{meas}_i^{n+1} \\ (n, n, n, n) & & \\ \text{meas}_i^n \times \text{meas}_j^n \downarrow & & \downarrow \\ (n + 1, n + 1) & \xrightarrow{\text{meas}_j^{n+1}} & n + 2 \end{array} \quad (14)$$

où la flèche verticale $(n, n, n, n) \rightarrow (n, n, n, n)$ est l'isomorphisme induit par

$$\begin{array}{ccc} n & \xrightarrow{\text{id}_n} & n \\ n & \searrow \text{id}_n & \nearrow \text{id}_n \\ n & \xrightarrow{\text{id}_n} & n \\ n & \xrightarrow{\text{id}_n} & n \end{array}$$

On est maintenant prêt à donner la définition d'un ensemble qnominal, pendant quantique des ensembles nominaux. La terminologie choisie prend modèle sur l'élaboration du terme « qbit » à partir du mot *bit*.

Définition 2.3.6 (Ensemble qnominal). Un *ensemble qnominal* est un foncteur $\text{qlnj} \rightarrow \text{Ens}$ préservant les produits finis et envoyant le diagramme (14) sur un carré cartésien.

1. Attention, qlnj joue le rôle de $\Sigma(\text{lnj}^\circ)^\circ$ et non de lnj directement.

Remarque 2.3.7. On requiert qu'un ensemble qnominal préserve les produits finis afin qu'il soit modèle de la théorie T_{meas} , de même façon que les ensembles nominaux classiques sont modèles la théorie T_{coll} .

Définition 2.3.8 (Support quantique). Soient F un ensemble qnominal et $n \in \mathbb{N}$. Le *support quantique* d'un élément $x \in F(n+1)$, noté $\text{supp}(x)$, est le ensemble des $j \in n+1$ tels que $x \notin \text{im}(\text{meas}_j^n)$.

2.3.3 Monade d'état local quantique et qnominalité. La signature σ_{meas} s'injecte naturellement dans χ de telle façon que $T_{\text{meas}} \subseteq Q$. Du point de vue des théories de Lawvere associée, cela se traduit par l'existence d'un morphisme $k: \Theta_{T_{\text{meas}}} \rightarrow \Theta_Q$ de théorie de Lawvere entre $j_{T_{\text{meas}}}$ et j_Q . En particulier, la monade $j_Q^* j_{Q!}$ se factorise en

$$\widehat{\Sigma \text{Bij}} \xrightarrow{(j_{T_{\text{meas}}})_!} [\text{qInj}, \text{Ens}] \xrightarrow{(j_{T_{\text{meas}}})^*} \widehat{\Sigma \text{Bij}}.$$

$\begin{array}{c} k^* k_! \\ \curvearrowright \end{array}$

Dans la catégorie Θ_Q , on note respectivement $\text{new}_{j,|0\rangle}^n$ et $\text{new}_{j,|1\rangle}^n$ les morphismes

$$\begin{aligned} n &\xrightarrow{n \bullet \text{new}} n+1 \xrightarrow{\tau_j^n} n+1 \quad \text{et} \\ n &\xrightarrow{n \bullet \text{new}} n+1 \xrightarrow{n \bullet \text{apply}_x} n+1 \xrightarrow{\tau_j^n} n+1 \end{aligned}$$

où τ_j^n est toujours la transposition $(j \ n)$ de l'ensemble $n+1$. Intuitivement, $\text{new}_{j,|0\rangle}^n$ et $\text{new}_{j,|1\rangle}^n$ allouent chacun un qbit en j^e position à la valeur $|0\rangle$ et $|1\rangle$. On peut maintenant prouver le résultat principal de cette section.

Proposition 2.3.9. Soit $M \in \widehat{\Theta_Q}$ un modèle de j_Q . Alors $k^* M$ est qnominal.

Preuve. Comme M et k^* respectent les produits finis, $k^* M$ aussi. Il suffit donc de vérifier que pour tout $n \in \mathbb{N}$, $k^* M$ envoie le diagramme (14) sur un produit fibré.

Soit $x \in M(n+2)$ et supposons qu'il existe $t, u, v, w \in M(n+1)$ tels que

$$\text{meas}_i^{n+1}(t, u) = x = \text{meas}_j^{n+1}(v, w).$$

Alors les axiomes (A) et (D) nous assure les quatres égalités suivantes :

$$\begin{cases} \text{new}_{i,|0\rangle}^{n+1}(x) = t \\ \text{new}_{i,|1\rangle}^{n+1}(x) = u \\ \text{new}_{j,|0\rangle}^{n+1}(x) = v \\ \text{new}_{j,|1\rangle}^{n+1}(x) = w \end{cases}$$

Concentrons-nous sur la première égalité, les autres se traitent de manière analogue : on rappelle que dans notre hypothèse $i < j$, puis on utilise l'axiome (L) pour obtenir

$$\begin{aligned} t &= \text{new}_{i,|0\rangle}^{n+1}(\text{meas}_j^{n+1}(v, w)) \\ &= \text{meas}_{j-1}^n(\text{new}_{i,|0\rangle}^n(v), \text{new}_{i,|0\rangle}^n(w)) \\ &= \text{meas}_{j-1}^n(\text{new}_{i,|0\rangle}^n(\text{new}_{j,|0\rangle}^{n+1}(x)), \text{new}_{i,|0\rangle}^n(\text{new}_{j,|1\rangle}^{n+1}(x))). \end{aligned}$$

En procédant de même sur u , v et w , on obtient :

$$\begin{cases} t = \text{meas}_{j-1}^n \left(\text{new}_{i,|0\rangle}^n (\text{new}_{j,|0\rangle}^{n+1}(x)), \text{new}_{i,|0\rangle}^n (\text{new}_{j,|1\rangle}^{n+1}(x)) \right) \\ u = \text{meas}_{j-1}^n \left(\text{new}_{i,|1\rangle}^n (\text{new}_{j,|0\rangle}^{n+1}(x)), \text{new}_{i,|1\rangle}^n (\text{new}_{j,|1\rangle}^{n+1}(x)) \right) \\ v = \text{meas}_i^n \left(\text{new}_{j-1,|0\rangle}^n (\text{new}_{i,|0\rangle}^{n+1}(x)), \text{new}_{j-1,|0\rangle}^n (\text{new}_{i,|1\rangle}^{n+1}(x)) \right) \\ w = \text{meas}_i^n \left(\text{new}_{j-1,|1\rangle}^n (\text{new}_{i,|0\rangle}^{n+1}(x)), \text{new}_{j-1,|1\rangle}^n (\text{new}_{i,|1\rangle}^{n+1}(x)) \right) \end{cases}$$

Or l'axiome (K) nous dit exactement que pour tout $n \in \mathbb{N}$, pour tout $r < s \in n+2$ et pour tout $q, q' \in \{|0\rangle, |1\rangle\}$,

$$\text{new}_{r,q}^n \circ \text{new}_{s,q'}^{n+1} = \text{new}_{s-1,q'}^n \circ \text{new}_{r,q}^{n+1}.$$

Donc en notant

$$\begin{aligned} a &= \text{new}_{i,|0\rangle}^n (\text{new}_{j,|0\rangle}^{n+1}(x)), & b &= \text{new}_{i,|0\rangle}^n (\text{new}_{j,|1\rangle}^{n+1}(x)), \\ c &= \text{new}_{i,|1\rangle}^n (\text{new}_{j,|0\rangle}^{n+1}(x)), & d &= \text{new}_{i,|1\rangle}^n (\text{new}_{j,|1\rangle}^{n+1}(x)), \end{aligned}$$

on a ce que l'on cherchait à montrer :

$$\begin{cases} t = \text{meas}_{j-1}^n (a, b) \\ u = \text{meas}_{j-1}^n (c, d) \\ v = \text{meas}_i^n (a, c) \\ w = \text{meas}_i^n (b, d) \end{cases} \quad \square$$

2.3.4 Interprétation stellaire de la qnominalité. Comme déjà signalé dans la preuve de la proposition 2.3.9, si $x \in M(n+1)$, pour un modèle M de j_Q s'écrit $x = \text{meas}_j^n(t, u)$ pour certains $t, u \in M(n)$, alors

$$x = \text{meas}_j^n (\text{new}_{j,|0\rangle}^n(x), \text{new}_{j,|1\rangle}^n(x)).$$

On en déduit directement le résultat suivant.

Corollaire 2.3.10. *Soit M un modèle j_Q . Le support d'un élément $x \in M(n+1)$ est exactement l'ensemble des $j \in n+1$ tels que*

$$x \neq \text{meas}_j^n (\text{new}_{j,|0\rangle}^n(x), \text{new}_{j,|1\rangle}^n(x)).$$

Intuitivement, ce corollaire nous dit que le support de x est l'ensemble des qbits qui servent au programme x en tant que vrais qbits, et pas en tant qu'émulation de bits classiques. La taille du support de x est donc en quelque sorte le nombre minimal de qbits nécessaire au programme x .

L'article [Sta15] fait aussi apparaître une notion de minimalité dans la mémoire quantique d'un programme. En effet, la preuve du théorème 2.2.1 passe par l'application du théorème de Stinespring, aussi dit théorème de dilatation minimale. C'est un théorème général sur les algèbres de Banach, qui prend la forme suivante dans le cadre des algèbres matricielles sur $\mathbb{C}$. On note $\uparrow_p^n : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_p(\mathbb{C})$ le morphisme (de $\mathbb{C}_{\text{CPU}}^*$) qui restreint une matrice de taille $n \geq p$ à ses p premières lignes et colonnes.

Théorème 2.3.11 (Dilatation minimale). *Soient A une algèbre stellaire, $p \in \mathbb{N}$ et $f : A \rightarrow \mathcal{M}_p(\mathbb{C})$ un morphisme de $\mathbf{C}_{\text{CPU}}^*$. Il existe $q \geq p$ et un morphisme stellaire $g : A \rightarrow \mathcal{M}_q(\mathbb{C})$ tels que commute le diagramme*

$$\begin{array}{ccc} A & & \\ g \downarrow & \searrow f & \\ \mathcal{M}_q(\mathbb{C}) & \xrightarrow{\downarrow_p^q} & \mathcal{M}_p(\mathbb{C}) \end{array}$$

Ils sont universels au sens suivant : pour tout $r \geq p$ et morphisme stellaire $h : A \rightarrow \mathcal{M}_r(\mathbb{C})$ satisfaisant à l'équation $f = h(\cdot) \downarrow_p^r$, on a $r \geq q$ et il existe $U \in \mathbb{U}_r(\mathbb{C})$ tels que le diagramme suivant commute

$$\begin{array}{ccccc} & & h & & A \\ & & \swarrow & & \downarrow g \\ \mathcal{M}_r(\mathbb{C}) & \xrightarrow{U^* \cdot U} & \mathcal{M}_r(\mathbb{C}) & \xrightarrow{\downarrow_q^r} & \mathcal{M}_q(\mathbb{C}) \end{array}$$

On rappelle que le modèle $\mathbf{C}$ de Q est pleinement fidèle (théorème 2.2.1). Comme d'autre part, Staton prouve que la restriction de $\mathbf{C}$ à la sous-théorie maximale de Q sur la signature ne contenant que `new` et les `applyU` est un modèle pleinement fidèle dans la catégorie $\mathbf{C}^*$ (des algèbres stellaires et morphismes stellaires entre elles), le théorème de dilatation minimal tend à dire la chose suivante : tout terme sur χ est équivalent sous la théorie Q à un terme où tous les `new` sont en tête ; de plus, le nombre de `new` peut être optimisé.

Il se pose cependant un problème : dans l'énoncé du théorème, même si A est de la forme $\prod_{i=1}^k \mathcal{M}_{2^{m_i}}(\mathbb{C})$ et p de la forme $2^{\hat{p}}$, rien n'assure que le q de la dilatation minimale soit une puissance de 2. On peut néanmoins y remédier. Considérons i un indice réalisant le minimum des m_i et notons $\pi : A \rightarrow \mathcal{M}_{2^{m_i}}(\mathbb{C})$ la projection canonique. Notons ℓ le plus petit entier tel que $2^\ell \leq q < 2^{\ell+1}$. Alors, le diagramme suivant commute

$$\begin{array}{ccc} A & \xrightarrow{\langle g^{2^{m_i}}, \pi_i^{2^\ell - q} \rangle} (\mathcal{M}_q(\mathbb{C}))^{2^{m_i}} \times (\mathcal{M}_{2^{m_i}}(\mathbb{C}))^{2^\ell - q} & \xrightarrow{\text{blocs}} \mathcal{M}_{2^{m_i} + \ell}(\mathbb{C}) \\ & \searrow g & \downarrow \downarrow_q^{2^{m_i} + \ell} \\ & & \mathcal{M}_q(\mathbb{C}) \end{array}$$

Conjecture 2.3.12. *Soient $M \in \widehat{\Theta_Q}$ un modèle de Q , t un terme sur χ dans le contexte $(a_1, \dots, a_p; \vec{y} : \vec{m})$ et $x \in M(p)$. Si x est dans l'image de $M(\llbracket t \rrbracket_{(\vec{a}; \vec{y})})$, alors le cardinal de $\text{supp}(x)$ est égal au nombre $m_i + \ell$ calculé précédemment sur l'application complètement positive $\mathbf{C}(\llbracket t \rrbracket_{(\vec{a}; \vec{y})})$.*

Appendice A

Théories algébriques selon Lawvere

Dans sa thèse [Law63], Lawvere propose de revisiter l'algèbre universelle d'un point de vue fonctoriel. Le cadre catégorique lui permet de bouleverser le schéma de pensée classique : l'algèbre universelle considère une théorie algébrique comme un ensemble d'identités syntaxiques contextualisées dont la sémantique est donnée par ses modèles, i.e. des ensembles interprétant les fonctions du langage choisi et satisfaisant les axiomes. Dans l'approche de Lawvere, syntaxe comme sémantique sont des morphismes de certaines catégories. Les symboles de fonctions n -aires sont les morphismes $n \rightarrow 1$ d'une catégorie $\mathcal{T}$ dont les objets sont les entiers, et les modèles de la théorie sont certains foncteurs de $\mathcal{T}$ vers une catégorie $\mathcal{C}$. Cette approche permet de manipuler facilement les théories algébriques et les liens qu'il peut y avoir entre elles. On y gagne aussi la possibilité de considérer des modèles non ensemblistes : là où le cadre classique multiplie les définitions de groupes, groupes topologiques, groupes de Lie, etc., les modèles de la théorie de Lawvere $\mathcal{T}_{\text{Grp}}$ sont simplement des foncteurs $\mathcal{T}_{\text{Grp}} \rightarrow \mathcal{C}$, où $\mathcal{C}$ peut être tout aussi bien la catégorie des ensembles Ens , celles des espaces topologique Top , celles des variétés différentielles lisses $\mathcal{C}^\infty \text{Mfd}$, etc.

Dans ce chapitre, on rappelle rapidement les différentes notions introduites par Lawvere : théorie de Lawvere, modèles, foncteur d'oubli, etc. Puis on donnera un rapide aperçu du traitement monadique des théories de Lawvere : toute théorie de Lawvere donne lieu à un monade sur Ens , qu'on sait caractériser précisément.

A.1 Théories de Lawvere

On dénote $\aleph_0$ la sous-catégorie pleine de Ens dont les objets sont les ensembles de la forme $n = \{0, 1, \dots, n-1\}$. Elle admet en particulier toutes les sommes finies (y compris la somme vide, 0 étant initial dans $\aleph_0$).

Définition A.1.1 (Théorie de Lawvere¹). Une *théorie de Lawvere* est la donnée d'une catégorie $\mathcal{T}$ avec coproduits finis et d'un foncteur $\ell : \aleph_0 \rightarrow \mathcal{T}$ bijectif sur les objets et préservant les coproduits finis.

Le foncteur $\ell : \aleph_0 \rightarrow \mathcal{T}$ d'une théorie de Lawvere étant bijectif sur les objets, on fera souvent l'abus de noter $0, 1, 2, \dots$ pour les objets de $\mathcal{T}$ plutôt que $\ell(0), \ell(1), \ell(2), \dots$. Dans la catégorie $\mathcal{T}$ l'équation $n \simeq \coprod_{i=1}^n 1$ est satisfaite pour tout n , donc $\mathcal{T}$ est entièrement déterminé par les ensembles $\mathcal{T}(1, n)$.

1. Le lecteur averti pourra être surpris de la donnée du foncteur $\aleph_0 \rightarrow \mathcal{T}$ quand il attend plutôt $\aleph_0^\circ \rightarrow \mathcal{T}$. Il en verra le bénéfice dans le chapitre 1 quand on présentera les théories de Lawvere à arité.

Définition A.1.2 (Modèle). Soit $\mathcal{C}$ une catégorie admettant les produits finis. Un *modèle* dans $\mathcal{C}$ (ou plus simplement $\mathcal{C}$ -*modèle*) d'une théorie de Lawvere $\ell : \mathbb{N}_0 \rightarrow \mathcal{T}$ est un foncteur $M : \mathcal{T}^\circ \rightarrow \mathcal{C}$ commutants aux produits finis.

Un modèle d'une théorie $\ell : \mathbb{N}_0 \rightarrow \mathcal{T}$ est entièrement déterminé par l'image de 1 et des morphismes $1 \rightarrow n$ de $\mathcal{T}$. Ainsi, un modèle dans $\mathcal{C}$ est la donnée d'un objet x et d'un morphisme $x^n \rightarrow x$ pour chaque élément de $\mathcal{T}(1, n)$. Avec $\mathcal{C} = \text{Ens}$ et en pensant $\mathcal{T}(1, n)$ comme l'ensemble des opérations n -aires d'une théorie algébrique, on retrouve la notion classique de modèle de l'algèbre universelle.

On note $\text{Mod}_\ell^{\mathcal{C}}$ la sous-catégorie pleine de $[\mathcal{T}^\circ, \mathcal{C}]$ dont les objets sont les modèles de la théorie de Lawvere ℓ .

La proposition de Lawvere ne s'arrête pas à formaliser les théories algébriques dans un langage élégant. Le cadre catégorique nous autorise maintenant à mettre l'accent sur les morphismes, c'est-à-dire les relations entre théories algébriques.

Définition A.1.3 (Morphisme entre théories de Lawvere). Un morphisme d'une théorie de Lawvere $\ell_1 : \mathbb{N}_0 \rightarrow \mathcal{T}_1$ vers $\ell_2 : \mathbb{N}_0 \rightarrow \mathcal{T}_2$ est un foncteur $f : \mathcal{T}_1 \rightarrow \mathcal{T}_2$ faisant commuter

$$\begin{array}{ccc} & \mathbb{N}_0 & \\ \ell_1 \swarrow & & \searrow \ell_2 \\ \mathcal{T}_1 & \xrightarrow{f} & \mathcal{T}_2. \end{array}$$

Remarque A.1.4. Un morphisme de théorie de Lawvere respecte nécessairement les coproduits finis. En particulier, si $\mathcal{C}$ est une catégorie admettant les produits finis, alors (avec les notations de la définition) pour tout morphisme $f : \ell_1 \rightarrow \ell_2$ et tout modèle $M_2 : \mathcal{T}_2^\circ \rightarrow \mathcal{C}$ de ℓ_2 , le foncteur $M_2 f$ est un modèle de ℓ_1 . Ainsi, le foncteur de restriction $f^* : [\mathcal{T}_2^\circ, \mathcal{C}] \rightarrow [\mathcal{T}_1^\circ, \mathcal{C}]$ induit par f se restreint en un foncteur, dit « d'oubli »,

$$f^* : \text{Mod}_{\ell_2}^{\mathcal{C}} \rightarrow \text{Mod}_{\ell_1}^{\mathcal{C}}.$$

On note Law la catégorie des théories de Lawvere et des morphismes entre elles. Il découle de la remarque précédente que pour toute catégorie $\mathcal{C}$ admettant les produits finis, on a un foncteur

$$\text{Mod}^{\mathcal{C}} : \text{Law} \rightarrow \text{Cat}$$

à valeurs dans la catégorie Cat des petites catégories (on fait ici l'hypothèse que l'on dispose d'un univers contenant l'ensemble $\text{Ob}(\mathcal{C})$ des objets de $\mathcal{C}$). La catégorie Law admet un élément initial : pour toute théorie de Lawvere $\ell : \mathbb{N}_0 \rightarrow \mathcal{T}$, le foncteur ℓ lui-même est un morphisme de la théorie $\text{id}_{\mathbb{N}_0}$ vers ℓ (et est évidemment le seul). Ainsi, pour toute théorie ℓ , on dispose d'un foncteur d'oubli particulier :

$$\text{U}_\ell^{\mathcal{C}} = \ell^* : \text{Mod}_\ell^{\mathcal{C}} \rightarrow \text{Mod}_{\mathbb{N}_0}^{\mathcal{C}} \simeq \mathcal{C}.$$

Ce dernier n'est autre que le foncteur $M \mapsto M(1)$.

A.2 Des théories algébriques aux monades

Les modèles ensemblistes jouent un rôle central dans la compréhension des théories de Lawvere. Non seulement on y retrouve la notion de modèle donnée par l'algèbre universelle, mais ils produisent aussi une monade correspondant à la théorie de

Lawvere. Plus précisément, on va montrer que le foncteur d'oubli U_ℓ^{Ens} d'une théorie de Lawvere ℓ est monadique : il admet un adjoint à gauche et la catégorie des algèbres de la monade induite est précisément $\text{Mod}_\ell^{\text{Ens}}$.

Pour plus de concision, on supprimera désormais les indices relatifs à Ens dans les notations.

Proposition A.2.1. *Soit $\ell : \aleph_0 \rightarrow \mathcal{T}$ une théorie de Lawvere. Le foncteur U_ℓ admet un adjoint à gauche.*

Preuve. Rappelons que le foncteur de restriction $\ell^* : \widehat{\mathcal{T}} \rightarrow \widehat{\aleph_0}$ admet un adjoint à gauche, appelé foncteur extension de Kan à gauche,

$$\ell_! : \widehat{\aleph_0} \rightarrow \widehat{\mathcal{T}}.$$

Il reste alors à montrer que $\ell_!$ restreint à $\text{Mod}_{\text{id}_{\aleph_0}}$ est à valeurs dans Mod_ℓ . C'est une conséquence immédiate du lemme suivant. $\square$

Lemme A.2.2. *Soient $j : \mathcal{A} \rightarrow \mathcal{B}$ un foncteur entre petites catégories admettant les co-produits finis. Si $F : \mathcal{A}^\circ \rightarrow \text{Ens}$ préserve les produits finis, alors son extension de Kan $j_! F$ aussi.*

Preuve. Commençons par remarquer que c'est vrai pour les représentables. Plus précisément, pour tout $a \in \mathcal{A}$,

$$j_! \mathcal{A}(-, a) \simeq \mathcal{B}(-, j(a)).$$

En effet, la transformation naturelle $\chi : \mathcal{A}(-, a) \rightarrow \mathcal{B}(j(-), j(a))$ définie par $f \mapsto j(f)$ satisfait la propriété universelle des extensions de Kan à gauche : pour tout foncteur $G : \mathcal{B}^\circ \rightarrow \text{Ens}$ et toute transformation naturelle $\mu : \mathcal{A}(-, a) \rightarrow G \circ j$, on peut définir $\lambda : \mathcal{B}(-, j(a)) \rightarrow G$ par

$$\lambda_b : \left(b \xrightarrow{k} j(a) \right) \mapsto G(k)(\mu_a(\text{id}_a)),$$

factorisant ainsi μ comme $\lambda j \circ \chi$.

Soit alors $F \in \widehat{\mathcal{A}}$ quelconque. Le lemme de Yoneda nous assure que

$$F \simeq \text{colim} \left(\mathcal{A}_{/F} \rightarrow \mathcal{A} \xrightarrow{\eta^{\mathcal{A}}} \widehat{\mathcal{A}} \right).$$

Or $j_! : \widehat{\mathcal{A}} \rightarrow \widehat{\mathcal{B}}$ est un adjoint à gauche donc commute aux colimites. En utilisant de plus l'expression de $j_!$ sur les représentables précédemment trouvée, on a

$$j_! F \simeq \text{colim} \left(\mathcal{A}_{/F} \rightarrow \mathcal{A} \xrightarrow{j} \mathcal{B} \xrightarrow{\eta^{\mathcal{B}}} \widehat{\mathcal{B}} \right).$$

Les colimites de $\widehat{\mathcal{B}}$ sont évaluées point par point dans Ens , donc on a, naturellement en $b \in \mathcal{B}$,

$$j_! F(b) \simeq \text{colim}_{a \rightarrow F \in \mathcal{A}_{/F}} (\mathcal{B}(b, j(a))).$$

Notamment si $b, b' \in \mathcal{B}$, on a

$$j_! F(b \sqcup b') \simeq \text{colim}_{a \rightarrow F \in \mathcal{A}_{/F}} (\mathcal{B}(b, j(a)) \times \mathcal{B}(b', j(a))).$$

Les colimites tamisantes commutant aux produits finis, il suffit maintenant de montrer que la catégorie $\mathcal{A}_{/F}$ est tamisante. On va même faire mieux en montrant qu'elle admet les coproduits finis :

- Elle admet un objet initial. Le préfaisceau F respecte les produits donc envoie l'élément initial $0_{\mathcal{A}}$ de $\mathcal{A}$ sur un singleton $\{*\}$. Ainsi, il y a une unique flèche $0_{\mathcal{A}} \rightarrow F$, initiale dans $\mathcal{A}_{/F}$ car pour tout élément $x: a \rightarrow F$, le diagramme suivant commute nécessairement :

$$\begin{array}{ccc} 0_{\mathcal{A}} & \xrightarrow{!} & a \\ & \searrow ! & \downarrow x \\ & & F \end{array}$$

- Elle admet les coproduits binaires. F préservant les produits binaires, tout couple $x: a \rightarrow F, y: a' \rightarrow F$ induit un élément $z: a \sqcup a' \rightarrow F$. C'est un coproduit de x et y : étant donné un diagramme commutatif,

$$\begin{array}{ccccc} a & \xrightarrow{f} & a'' & \xleftarrow{g} & a' \\ & \searrow x & \downarrow t & \swarrow y & \\ & & F, & & \end{array}$$

la propriété universelle du coproduit dans $\mathcal{A}$ induit une unique flèche $h: a \sqcup a' \rightarrow a''$ s'incrivant dans le diagramme commutatif suivant

$$\begin{array}{ccccc} a & \xrightarrow{i_1} & a \sqcup a' & \xleftarrow{i_2} & a' \\ & \searrow f & \downarrow h & \swarrow g & \\ & & a'' & & \\ & \searrow x & \downarrow t & \swarrow y & \\ & & F, & & \end{array}$$

Il reste à montrer que $th = z$ pour conclure que z est bien le coproduit de x et y . Par définition même de z , cela revient à vérifier que $thi_1 = x$ et $thi_2 = y$, ce qui est donné par le diagramme ci-dessus.

□

Ainsi, pour toute théorie de Lawvere ℓ , le foncteur d'oubli U_{ℓ} admet un adjoint à gauche F_{ℓ} . On sait que F_{ℓ} est point par point une extension de Kan à gauche le long de ℓ^* , ce qui nous donne une expression informelle assez simple du foncteur F_{ℓ} : il transporte un ensemble X sur le modèle $F_{\ell}(X): \mathcal{T}^{\circ} \rightarrow \text{Ens}$ où $F_{\ell}(X)(1)$ est l'ensemble, modulo les axiomes de la théorie, de toutes les expressions formelles « $f(x_1, \dots, x_n)$ » avec $f \in \mathcal{T}(1, n)$ une opération n -aires et $x_i \in X$.

L'adjonction $F_{\ell} \dashv U_{\ell}$ munie de son unité η et de sa counité ε induit, comme toute adjonction, une monade

$$\mathbf{T}_{\ell} = (U_{\ell} F_{\ell}, \eta, U_{\ell} \varepsilon F_{\ell}).$$

L'application $\mathbf{T}: \ell \mapsto \mathbf{T}_\ell$ peut être étendue en un foncteur : par le lemme A.2.2 un morphisme de théorie de Lawvere

$$\begin{array}{ccc} \mathcal{T}_1 & \xrightarrow{f} & \mathcal{T}_2 \\ \ell_1 \swarrow & & \nearrow \ell_2 \\ & \mathbb{K}_0 & \end{array}$$

induit une adjonction $f_!: \text{Mod}_{\ell_1} \rightarrow \text{Mod}_{\ell_2} : f^*$ d'unité $\eta_f: \text{id}_{\text{Mod}_{\ell_1}} \rightarrow f^*f_!$; en précomposant par ℓ_1 et postcomposant par ℓ_1^* , on obtient une transformation naturelle

$$\ell_1^* \eta_f \ell_1: \mathbf{T}_{\ell_1} \rightarrow \mathbf{T}_{\ell_2}.$$

L'application $f \mapsto \ell_1^* \eta_f \ell_1$ étend $\mathbf{T}$ en un foncteur de la catégorie Law dans celle Mnd des monades sur Ens .

On finit cette section par deux propriétés de la monade associée à une théorie de Lawvere. La première donne le pendant monadique du caractère *algébrique* des théories de Lawvere. La deuxième assure que $\mathbf{T}_\ell$ est caractéristique de ℓ .

Lemme A.2.3. *Le foncteur d'inclusion $\text{Mod}_\ell \rightarrow \widehat{\mathcal{T}}$ associé à une théorie de Lawvere ℓ crée les colimites tamisantes.*

Preuve. Soient $\ell: \mathbb{K}_0 \rightarrow \mathcal{T}$ une théorie de Lawvere, $\mathcal{J}$ une catégorie tamisante et $D: \mathcal{J} \rightarrow \text{Mod}_\ell$ un diagramme. Posons M sa colimite dans $\widehat{\mathcal{T}}$. Alors M est encore un modèle de ℓ : naturellement en $n_1, \dots, n_k \in \mathcal{T}$

$$M\left(\prod_{i=1}^k n_i\right) \simeq \text{colim}_{j \in \mathcal{J}} \left(D(j) \left(\prod_{i=1}^k n_i \right) \right) \quad (1)$$

$$\simeq \text{colim}_{j \in \mathcal{J}} \left(\prod_{i=1}^k D(j)(n_i) \right) \quad (2)$$

$$\simeq \prod_{i=1}^k \text{colim}_{j \in \mathcal{J}} (D(j)(n_i)) \quad (3)$$

$$\simeq \prod_{i=1}^k M(n_i) \quad (4)$$

où (1) vient de ce que les colimites de préfaisceaux sont calculées point à point, (2) du fait que les $D(j)$ sont des modèles, (3) du caractère tamisant de $\mathcal{J}$ et enfin (4) admet la même justification que (1).

L'inclusion $\text{Mod}_\ell \rightarrow \widehat{\mathcal{T}}$ étant pleine, il suit que les colimites tamisantes de Mod_ℓ se calculent dans $\widehat{\mathcal{T}}$, c'est-à-dire que l'inclusion crée ces colimites. $\square$

Corollaire A.2.4. *La monade sur Ens associée à une théorie de Lawvere est finitaire.*

Preuve. Soit ℓ une théorie de Lawvere. On vient de voir que les colimites tamisantes sont calculer point par point dans Mod_ℓ . En particulier, U_ℓ (qui n'est autre que l'évaluation au point $1 \in \mathcal{T}$) préserve les colimites filtrantes. Comme F_ℓ est adjoint à gauche, il commute à toutes les colimites, en particulier aux filtrantes. Ainsi, la monade $\mathbf{T}_\ell = U_\ell F_\ell$ commute aux colimites filtrantes, i.e. est finitaire. $\square$

Proposition A.2.5. *Soit ℓ une théorie de Lawvere. L'adjonction $F_\ell : \text{Ens} \rightleftarrows \text{Mod}_\ell : U_\ell$ est monadique.*

Preuve. D'après le théorème de monadicité de Beck, il suffit de montrer que U_ℓ réfléchit les isomorphismes et préserve les coégaliseurs de paires réflexives².

Soit $\varphi : M \rightarrow N$ est un morphisme entre deux modèles de ℓ tel que $U_\ell \varphi$ est une bijection. Comme U_ℓ est l'évaluation au point 1, on a que $\varphi_1 : M(1) \rightarrow N(1)$ est une bijection. De plus, M et N préservent les produits finis : la naturalité de φ relativement aux projections $M(k) \rightarrow M(1)$ assure que $\varphi_k = \varphi_1 \times \cdots \times \varphi_1$ pour tout $k > 0$. Enfin, φ_0 est un morphisme de $M(0) \simeq 1$ vers $N(0) \simeq 1$ donc nécessairement une bijection. Ainsi, φ est un isomorphisme de Mod_ℓ .

Les coégaliseurs de paires réflexives sont des colimites sur la catégorie index

$$0 \begin{array}{c} \xrightarrow{r} \\ \xleftarrow{i} \\ \xrightarrow{s} \end{array} 1, \quad ri = si = \text{id}_1.$$

Cette catégorie est tamisante et on a déjà vu que U_ℓ commute aux colimites tamisantes. $\square$

Ainsi, pour une théorie de Lawvere ℓ , le morphisme de comparaison

$$\text{Mod}_\ell \rightarrow \text{Alg}(\mathbf{T}_\ell), M \mapsto (U_\ell F_\ell U_\ell M \xrightarrow{\varepsilon} U_\ell M)$$

est une équivalence de catégorie, sous laquelle les foncteurs d'oubli et libre deviennent respectivement

$$(\mathbf{T}_\ell A \rightarrow A) \mapsto A, \quad A \mapsto (\mathbf{T}_\ell \mathbf{T}_\ell A \xrightarrow{\mu_\ell} \mathbf{T}_\ell A)$$

Cela nous permet de retrouver la théorie de Lawvere ℓ à partir de la monade $\mathbf{T}_\ell$. En effet, étant donné une théorie de Lawvere $\ell : \aleph_0 \rightarrow \mathcal{T}$, les représentables $\mathcal{T}(-, n)$ sont des modèles de ℓ isomorphes à $F_\ell(n)$. Ainsi, en notant $\mathcal{T}'$ la sous-catégorie pleine de $\text{Alg}(\mathbf{T}_\ell)$ constituée des $\mathbf{T}_\ell$ -algèbres libres sur les ensembles finis, la restriction $\aleph_0 \rightarrow \mathcal{T}'$ du foncteur libre est une théorie de Lawvere isomorphe à ℓ .

A.3 Des monades aux théories algébriques

Dans la section précédente, on a construit un foncteur $\mathbf{T} : \text{Law} \rightarrow \text{Mnd}$ dont le codomain peut se restreindre à la catégorie FinMnd des monades finitaires. Le but de cette section est de montrer que cette corestriction est en fait une équivalence de catégorie.

On commence par construire un foncteur $\mathbf{L} : \text{Mnd} \rightarrow \text{Law}$ comme suit. Étant donnée une monade (T, η, μ) sur Ens , on note $\text{Kl}_{\text{fin}}(T)$ l'image du foncteur $\mathcal{F}_T \iota$ où $\mathcal{F}_T : \text{Ens} \rightarrow \text{Alg}(T)$ est le foncteur algèbre libre et $\iota : \aleph_0 \rightarrow \text{Ens}$ est l'inclusion classique. Comme $\mathcal{F}_T$ est adjoint à gauche (du foncteur d'oubli $\mathcal{U}_T$), il commute aux colimites, donc notamment aux coproduits finis. Ainsi, $\mathcal{F}_T \iota : \aleph_0 \rightarrow \text{Kl}_{\text{fin}}(T)$ est une théorie de Lawvere. Cela définit une application

$$\mathbf{L} : \text{Ob}(\text{Mnd}) \rightarrow \text{Ob}(\text{Law}), \quad T \mapsto \mathcal{F}_T \iota$$

² Le théorème de Beck énonce habituellement une condition nécessaire et suffisante : l'adjoint à droite U réfléchit les isomorphismes et préserve les coégaliseurs des paires U -scindées. On profite ici de ce que U_ℓ satisfait une condition plus forte.

qu'on peut facilement étendre en un foncteur : profitant de l'adjonction $\mathcal{F}_T \dashv \mathcal{U}_T$, on a

$$\mathrm{Kl}_{\mathrm{fin}}(T)(\mathcal{F}_T(m), \mathcal{F}_T(n)) \simeq \mathrm{Ens}(m, T(n)) \quad (m, n \in \aleph_0)$$

pour toute monade T sur Ens , une transformation naturelle $\alpha: T \rightarrow T'$ induit un morphisme $\mathbf{L}(\alpha)$ de théorie de Lawvere défini sur les objets et les flèches respectivement par

$$\mathcal{F}_T(n) \mapsto \mathcal{F}_{T'}(n), \quad \left(m \xrightarrow{f} T(n)\right) \mapsto \left(m \xrightarrow{f} T(n) \xrightarrow{\alpha_n} T'(m)\right).$$

Proposition A.3.1. *Le foncteur $\mathbf{T}: \mathrm{Law} \rightarrow \mathrm{Mnd}$ est adjoint à gauche du foncteur $\mathbf{L}: \mathrm{Mnd} \rightarrow \mathrm{Law}$.*

Preuve. On a vu précédemment qu'une théorie de Lawvere ℓ est isomorphe à la théorie $\aleph_0 \rightarrow \mathrm{Kl}_{\mathrm{fin}}(\mathbf{T}_\ell)$ induite par la restriction du foncteur algèbre libre de $\mathbf{T}_\ell$. Donc, pour $\ell: \aleph_0 \rightarrow \mathcal{T}$ une théorie de Lawvere et $T \in \mathrm{Mnd}$, $\alpha \mapsto \mathbf{L}(\alpha)$ donne une application

$$\mathrm{Mnd}(\mathbf{T}_\ell, T) \rightarrow \mathrm{Law}(\ell, \mathbf{L}_T).$$

Cette opération est inversible. En effet, si $f: \mathcal{T} \rightarrow \mathrm{Kl}_{\mathrm{fin}}(T)$ est un morphisme de la théorie ℓ vers la théorie $\mathbf{L}_T$, on peut contruire une transformation naturelle $\alpha: \mathbf{T}_\ell \rightarrow T$ comme suit : comme

$$\mathbf{T}_\ell(n) \simeq \mathcal{T}(1, n) \quad \text{et} \quad T(n) \simeq \mathrm{Ens}(1, T(n)) \simeq \mathrm{Alg}(T)(\mathcal{F}_T(1), \mathcal{F}_T(n)),$$

le foncteur f induit une famille naturelle $(\alpha_n: \mathbf{T}_\ell(n) \rightarrow T(n))_{n \in \aleph_0}$; comme tout ensemble X est colimite filtrante de ses sous-ensembles finis, donc le caractère finitaire de $\mathbf{T}_\ell$ donne une unique façon de prolonger cette famille en une transformation naturelle $\mathbf{T}_\ell \rightarrow T$, à savoir celle dont la composante $\mathbf{T}_\ell(X) \rightarrow T(X)$ est induite par les fonctions

$$\mathbf{T}_\ell(I) \xrightarrow{\simeq} \mathbf{T}_\ell(n) \xrightarrow{\alpha_n} T(n) \xrightarrow{\simeq} T(I) \xrightarrow{T(I \subseteq X)} T(X)$$

où n est le cardinal de la partie finie I de X . □

La preuve ci-dessus montre en fait que l'unité $\mathrm{id}_{\mathrm{Law}} \rightarrow \mathbf{L}\mathbf{T}$ de l'adjonction est inversible, i.e. que $\mathbf{T}$ est pleinement fidèle. Autrement dit, $\mathbf{T}$ présente Law comme une sous-catégorie pleine coréflexive de Mnd . On peut de plus caractériser cette sous-catégorie pleine de Mnd . En effet, on a vu que toute monade issue d'une théorie de Lawvere est finitaire. Réciproquement, si T est une monade finitaire sur Ens , alors la composante $\mathbf{T}_{\mathbf{L}_T} \rightarrow T$ en T de la counité est inversible : pour tout ensemble X , la composante $\mathbf{T}_{\mathbf{L}_T}(X) \rightarrow T(X)$ est la flèche canonique

$$\mathrm{colim}_{I \in 2^X} (T(I)) \rightarrow T(X)$$

inversible par hypothèse sur T .

Corollaire A.3.2. *L'adjonction $\mathbf{T} \dashv \mathbf{L}$ se restreint en une équivalence de catégories*

$$\mathrm{Law} \xrightarrow{\simeq} \mathrm{FinMnd}.$$

Bibliographie

- [BMW12] C. Berger, P.-A. Melliès & M. Weber – « Monads with arities and their associated theories », *Journal of Pure and Applied Algebra* **216** (2012), no. 8, p. 2029–2048.
- [Law63] F. W. Lawvere – « Functorial semantics of algebraic theories », Thèse, Columbia University, 1963.
- [Mel10] P.-A. Melliès – « Segal condition meets computational effects », in *Logic in Computer Science (LICS), 2010 25th Annual IEEE Symposium on*, IEEE, 2010, p. 150–159.
- [Mel14] — , « Local states in string diagrams », in *Rewriting and Typed Lambda Calculi*, Springer, 2014, p. 334–348.
- [Mog91] E. Moggi – « Notions of computation and monads », *Information and computation* **93** (1991), no. 1, p. 55–92.
- [PP02] G. Plotkin & J. Power – « Notions of computation determine monads », in *Foundations of Software Science and Computation Structures*, Springer, 2002, p. 342–356.
- [Sta15] S. Staton – « Algebraic effects, linearity, and quantum programming languages », in *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, ACM, 2015, p. 395–406.
- [Web07] M. Weber – « Familial 2-functors and parametric right adjoints », *Theory and Applications of Categories* **18** (2007), no. 22, p. 665–732.