Université Jean Moulin Lyon 3
Faculté de Philosophie
Master mention Philosophie
Parcours de M2 : Logique, Histoire & Philosophie des sciences et des technologies

Mémoire de MASTER

préparé sous la direction de M. le Professeur Jean Baptiste JOINET

Membres du jury : Hugues CHABOT et Jean Baptiste JOINET

Titre: L'élimination de coupure en calcul de lambda pour la computation quantique:

Non-determinism de l'élimination de coupure

Année universitaire 2023/2024

Burak ERDOGAN

RÉSUMÉ

Dans ce mémoire, le débat sur le non-déterminisme de la méthode d'élimination des coupes, qui est une théorie de la preuve, et son équivalent dans le contexte de la logique linéaire sera introduit, et la pertinence de ce débat dans le contexte de l'informatique quantique sera questionnée ; pour cela, un modèle de lambda calcul linéaire sera utilisé, qui est construit en considérant les exigences d'un système quantique. De cette manière, les conséquences du non-déterminisme de la méthode d'élimination des coupures sur la réduction, qui est la contrepartie informatique de l'isomorphisme de Curry-Howard, peuvent être analysées dans un modèle quantique.

ABSTRACT

In this master thesis, the debate on the non-determinism of the cut elimination method, which is a proof theory, and its equivalent in the context of linear logic will be introduced, and the relevance of this debate in the context of quantum computing will be questioned; for this purpose, a model of linear lambda calculus will be used, which is constructed by considering the requirements of a quantum system. In this way, the consequences of the non-determinism of the cut elimination method on reduction, which is the computational counterpart of the Curry-Howard isomorphism, can be analysed in a quantum model.

TABLE DES MATİÈRES

INTRODUCTION

La révolution quantique, l'une des plus grandes révolutions du vingtième siècle, a été utilisée dans de nombreux domaines de la vie en peu de temps. De nombreux domaines fonctionnant dans le cadre du paradigme classique ont commencé à se quantifier (devenir quantique). On a essayé d'imiter ce nouveau visage de la nature comme un comportement humain naturel et de le modéliser dans différents contextes. Dans ce domaine, l'un des efforts les plus importants concerne les applications informatiques théoriques, qui tentent d'augmenter notre puissance de calcul en utilisant les phénomènes quantiques.Une autre initiative importante est le contexte de la logique en tant que raisonnement paradigmatique quantique. La fusion de ces deux points distincts, une organisation mentale et un domaine empirique, a été facilitée par l'isomorphisme de Curry-Howard, une relation naturelle entre la théorie de l'évidence, un domaine de la logique et la théorie du calcul.

Une des difficultés de la possibilité de l'interaction de ces trois domaines est que ce nouveau paradigme de la physique exige la transcendance des hypothèses cartésiennes sur lesquelles la physique classique est fondée, mais avec la logique traditionnelle dont nous disposons, ce développement ne trouve pas de correspondance sur le plan logique, d'où la nécessité d'un système plus avancé que la logique traditionnelle. En ce sens, la logique linéaire de Jean Yves Girard apparaît comme un système qui comprend les avantages des deux logiques et qui répond mieux aux conditions du raisonnement dans le monde réel.

Le concept de l’élimination de coupure est l'un des concepts de base de la théorie de la preuve et peut être considéré à première vue comme le processus de remplacement des preuves par des preuves plus simples. L'isomorphisme de Curry-Howard souligne

qu'elle est également fondamentale dans le contexte du calcul ; une application de l'élimination des coupures dans la théorie de la preuve correspond à une opération dans la théorie du calcul. L'un des éléments à considérer à cet égard est de savoir si cette pratique conduit à des résultats malheureusement différents, c'est-à-dire à son non déterminisme. Le thème principal de ce mémoire est l'évaluation de ce concept dans le contexte de la computation quantique et l'étude du comportement de l'élimination de coupure non déterministe dans un modèle de lambda calcul quantique. L'objectif est d'analyser un modèle dans ce contexte pour voir les résultats possibles d'une telle tentative; se demander si le non déterminisme logique peut être une caractéristique utilisable pour une modèle de calcul quantique.

Dans le premier chapitre, quelques notions logiques ont été introduites telle que la correspondance Curry-Howard, le calcul des séquents, l'élimination de coupure et la logique linéaire. Dans le deuxième chapitre, la computation quantique a été mentionnée et des notions techniques simples ont été données. Les motivations de l'utilisation de la logique linéaire dans ce domaine ont ensuite été évoquées. Dans le dernier chapitre, le non déterminisme de l'élimination de coupure est introduit, les motivations d'un système de calcul linéaire sont mentionnées, le système de calcul linéaire lambda de Alejandro Díaz-Caro et Gilles Dowek dans l'article de "Quantum superpositions and projective measurement in the lambda calculus"*[1]. En conclusion, le concept de non déterminisme est discuté sur ce système.

[1] *[25]

CHAPİTRE 1:LOGIQUE

L’isomorphisme Curry-Howard

L’isomorphisme de Curry-Howard est une correspondance naturelle entre les preuves et les computations, les preuves écrites en fonction de la déduction naturelle et les termes du calcul de lambda. La signification est alors que pour chaque série de preuve en déduction naturelle, il existe une terme en calcul de lambda telle que la réduction de telle preuve a la forme cut-free, correspond de l’évolution de telles termes du calcul de lambda. La déduction naturelle peut s'expliquer de la manière suivante: les formules initiales forment une séquence de preuve qui peut être interprétée comme une ensemble d'hypothèses générées par les règles d'inférence. Ces règles d'inférences sont telle que:

Les introduction:

$$\frac{A \quad B}{A \wedge B} \qquad \frac{B}{A => B} \qquad \frac{A}{\forall \varepsilon.\ A}$$

Les éliminations:

$$\frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B} \qquad \frac{A \quad A \rightarrow B}{B} \qquad \frac{\forall \varepsilon.\ A}{A[\alpha/\varepsilon)}$$

Pour les hypothèses en déduction naturelle , il existe toujours une nombre d’étapes pour la réduction qui transforme la séquence en un niveau qui ne possède pas une règle d’introduction qui est suivi par une règle d’élimination; c’est à dire une forme normale. Cette procédure est dite la normalisation. Donc, la normalisation sert à éliminer les détours des règles d'inférence. Elle joue une rôle semblable au théorème

de l'élimination de coupure en sequent calculus. Une application de l'élimination de coupure sera donnée dans les chapitres suivants.

Une application de la normalization d'une raisonnement de l'implication de $(B \to A)$ a partir de $(A \to B)$ donnée dans l'article de Richard Zach*[2]:

$$\dfrac{\dfrac{\dfrac{(A\wedge B)\vdash(A\wedge B)}{(A\wedge B)\vdash B} \qquad \dfrac{(A\wedge B)\vdash(A\wedge B)}{(A\wedge B)\vdash A}}{(A\wedge B)\vdash(B\wedge A)}}{\vdash(A\wedge B)\to(B\wedge A)}$$

La version normalisée est que:

$$\dfrac{\dfrac{\dfrac{[A\wedge B)}{B} \quad \dfrac{[A\wedge B]}{A}}{B\wedge A}}{(A\wedge B)\to(B\wedge A)}$$

L'isomorphisme Curry-Howard correspond aux hypothèses aux termes de lambda calcul. Le lambda calculus, est opérationnellement une langue de programme, travaille avec des fonctions d'ordre supérieur. La notion la plus fondamentale qui représente une fonction est une terme. Une terme est formé par des variables et correspond avec les preuves via l'isomorphisme Curry-Howard. Le calculus de terme est la langue de lambda la plus primitive, qui est aussi dite le untyped lambda calculus. Supposons t est une terme et x est une variable, alors λx.t représente une application de variable x aux variables de terme t; par exemple, (λx.x) est une fonction d'identification . Ce type de calcul de lambda peut se caractériser que si t,m deux termes alors (t m) est aussi une terme et on dit le petit sous-ensemble des séquents finis de lambda termes Λ ; quand une terme t est l'élément de Λ, alors (λx.t) l'est aussi. Les différents trois formes de lambda termes sont le variable x, l'application (t m) et l'abstraction (λx.t). En termes calculus , les fonctions n'ont pas un domaine ou une codomaine déterminée. Pour restreindre les domaines des fonctions, en d'autres termes, il faut préciser le type des termes. Les types sont des structures logiques qui décrivent les species des objets qui associent avec des

[2] *[15]

formules de la déduction naturelle. En calcul de lambda typé , chaque variable existe avec une type qui est écrit par x^T avec une type T. Pour caractériser une type ; si T et M sont deux types, alors T→M et TxM les sont aussi. De ce point de vue, les termes typées sont :

-Les variables x_i^T sont des termes de type T.

-Si x une terme de type X et y de type Y, alors (x y) est une terme de XxY

-Si t une terme de type XxY alors, $\pi_1 t$ est une terme de X et $\pi_2 t$ de Y.

-Si x_i^X est une variable de X et y est une termes de Y, alors (λx.y) est une terme de X→Y.

- Si t est une terme de X→Y et m une terme de X, alors (t m) est une terme de type Y.

A partir de maintenant, il faut écrire les règles inférences en termes de lambda calculus pour un système de l'implication et la conjonction (→,∧) :

Introduction:

$$\frac{x{:}A,\Gamma\vdash t{:}B}{\Gamma\vdash\lambda x.t{:}A\to B} \qquad \frac{\Gamma\vdash t{:}A \quad \Gamma\vdash s{:}B}{\Gamma\vdash <t,s>{:}\, A\wedge B}$$

Elimination:

$$\frac{\Gamma\vdash t{:}A\to B \quad \Gamma'\vdash s{:}A}{\Gamma,\Gamma'\vdash (t\ s){:}B}$$

$$\frac{\Gamma\vdash t{:}A\wedge B}{\Gamma\vdash \pi_1 t{:}A} \qquad \frac{\Gamma\vdash t{:}A\wedge B}{\Gamma\vdash \pi_2 t{:}B}$$

La réécriture en fonction des lambda termes de l'application de l'élimination de coupure ci dessus:

$$\dfrac{\dfrac{x{:}A\wedge B\vdash x{:}A\wedge B}{x{:}A\wedge B\vdash \pi_2 x{:}B}\qquad \dfrac{x{:}A\wedge B\vdash x{:}A\wedge B}{x{:}A\wedge B\vdash \pi_1 x{:}A}}{\dfrac{x{:}A\wedge B\vdash <\pi_2 x,\pi_1 x>{:}B\wedge A}{\vdash \lambda x.<\pi_2 x,\pi_1 x>{:}\,(A\wedge B)\rightarrow(B\wedge A)}}$$

En déduction naturelle, les formes normales, associées avec la correspondance Curry-Howard, a les termes réduites en calcul de lambda. Ces règles de réductions sont suivantes:

$(\lambda x.t) \rightarrow t[a/x]^*$

$\pi_1(t,m) \rightarrow t$

$\pi_2(t,m) \rightarrow m$

L'implication de la correspondance Curry-Howard, c'est de garantir de généraliser le théorème de normalisation qui est dite la théorème forte de normalisation telle qu'une série de réduction va toujours finir à une terme qui correspond à une forme normale et que cette forme normale et toujours existé et unique.

Le calcul des séquences

Le calcul des séquences utilise non seulement les formules comme les éléments de preuves mais plutôt une série des formules, telles que $A_1,A_2,\ldots \rightarrow B_1,B_2,\ldots$, ainsi, une série des formules implique disjonctionallement d'une ensemble de conséquences. C'est-à-dire, la gauche du symbole est la conjonction de la série des formules et la droite est la disjonction des formules. Les règles de logique en calcul des séquences, est représentées avec une symétrie de gauche/droite des connectives ; Les règles d'introduction et d'élimination d'une connective en déduction naturelle,

sont écrites en forme de respectivement gauche et droite-règles opérationnelles de telle connective.

En plus des règles d'introductions et d'éliminations en déduction naturelle, il existe un équipement supplémentaire dans le calcul des séquences: Le premier, c'est le règle de contraction qui assume le multi-utilisabilité des formules et le second, c'est le règle d'affaiblissement qui est pertinent pour les assumptions non nécessaire dans le séquence de preuve. Ces deux nouveaux règles peuvent se donner comme suivant:

Contraction: Affaiblissement:

$$\frac{\Gamma,A,A\vdash\Delta}{\Gamma,A\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta,A,A}{\Gamma\vdash\Delta,A} \qquad \frac{\Gamma\vdash\Delta}{\Gamma,A\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta}{\Gamma\vdash\Delta,A}$$

Le calcul des séquences peut être défini à la fois pour la logique classique et pour la logique intuitionniste. Le système du calcul des séquent classique se donne comme suivant:

Règles structurelles:

$$\frac{\Gamma\vdash\Delta}{\Gamma,A\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta}{\Gamma\vdash A,\Delta}$$

$$\frac{\Gamma,A,B,\Gamma'\vdash\Delta}{\Gamma,B,A,\Gamma'\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta,A,B,\Delta'}{\Gamma\vdash\Delta,B,A,\Delta'}$$

$$\frac{\Gamma,A,A\vdash\Delta}{\Gamma,A\vdash\Delta} \qquad \frac{\Gamma\vdash A,A,\Delta}{\Gamma\vdash A,\Delta}$$

Règles de connectives:

$$\frac{\Gamma,A\vdash\Delta}{\Gamma,A\wedge B\vdash\Delta} \qquad \frac{\Gamma,B\vdash\Delta}{\Gamma,A\wedge B\vdash\Delta} \qquad \frac{\Gamma\vdash A,\Delta \quad \Gamma\vdash B,\Delta}{\Gamma\vdash A\wedge B,\Delta}$$

$$\frac{\Gamma,A\vdash\Delta \quad \Gamma,B\vdash\Delta}{\Gamma,A\vee B\vdash\Delta} \qquad \frac{\Gamma\vdash A,\Delta}{\Gamma\vdash A\vee B,\Delta} \qquad \frac{\Gamma\vdash B,\Delta}{\Gamma\vdash A\vee B,\Delta}$$

$$\frac{\Gamma\vdash A,\Delta \quad \Gamma\vdash B,\Delta'}{\Gamma,A\to B\vdash\Delta,\Delta'} \qquad \frac{\Gamma,A\vdash B,\Delta}{\Gamma\vdash A\to B,\Delta}$$

Règle de coupure:

$$\frac{\Gamma\vdash A,\Delta \quad \Gamma,B\vdash\Delta'}{\Gamma\vdash\Delta,\Delta'}$$

Ensuite en système intuitionniste, les règles conclude just a une formule, donc Δ ne consiste pas d'une séquence comme le cas classique. Il est également important de comprendre que le raisonnement en logique intuitionniste, contrairement à la logique classique, est un processus unidirectionnel ; par conséquent, les règles du côté droit du calcul des séquences classiques ne sont pas présentes dans le système intuitionniste. Les règles du système intuitionnistes peuvent s'écrire comme suivant:

Règles structurelles:

$$\frac{\Gamma\vdash}{\Gamma\vdash A} \qquad \frac{\Gamma,A,B,\Gamma'\vdash\Delta}{\Gamma,B,A,\Gamma'\vdash\Delta} \qquad \frac{\Gamma,A,A\vdash\Delta}{\Gamma,A\vdash\Delta}$$

Règles de connectives:

$$\frac{\Gamma,A,B\vdash\Delta}{\Gamma,(A\wedge B)\vdash\Delta} \qquad \frac{\Gamma\vdash A \quad \Gamma\vdash B}{\Gamma\vdash(A\wedge B)}$$

$$\frac{\Gamma,A\vdash\Delta \quad \Gamma,B\vdash\Delta}{\Gamma,(A\vee B)\vdash\Delta} \qquad \frac{\Gamma\vdash A}{\Gamma\vdash(A\vee B)} \qquad \frac{\Gamma\vdash B}{\Gamma\vdash(A\vee B)}$$

$$\frac{\Gamma\vdash A \quad B,\Gamma\vdash\Delta}{\Gamma,(A\to B)\vdash\Delta} \qquad \frac{\Gamma,A\vdash B}{\Gamma\vdash(A\to B)}$$

Règle de négation:

$$\frac{\Gamma \vdash A}{\neg A, \Gamma \vdash} \qquad \frac{A, \Gamma \vdash}{\Gamma \vdash \neg A}$$

Motivation de la logique linéaire

Logique Intuitionniste

Historiquement, la logique intuitionniste est une tentative essentielle en développement de la computation, telle que la correspondance Curry-Howard et le calcul de lambda. Une preuve intuitionniste, porte la connaissance de la déduction d'une conséquence qui peut être construite à partir de l'organisation mentale. Dans ce cadre, l'utilisation des dualismes logiques dans le sens classique n'est pas toujours sûr, parce que la construction ne garantit pas la possibilité d'obtenir la d'une partie d'un dualisme à partir de l'autre. Deux dualité illustrent cette situation: La règle de De Morgan et de négation; selon la logique intuitionniste, il n'est pas certainement possible de raisonner à partir de non-A ou non-B comme la preuve de non-(A et B), de la même manière, la même difficulté pour de la preuve de non-non-A a la preuve de A.

Face à ce défi, la tradition intuitionniste constructiviste a transformé la tradition classique en un système de raisonnement intuitif, utilisant une partie de la logique dans laquelle seule une région restreinte de raisonnement est supposée, dont les preuves ne sont accessibles que par construction mentale. À partir de ce stade, il est remarquable que les sens des dualités se changent en passage de la logique classique à la logique intuitionniste ; par exemple, la bidirectionnalité des dualités devient un processus de raisonnement unidirectionnel dans la logique intuitionniste. Le point bien important sur lequel la logique intuitionniste se distingue de la logique classique

est le principe du tiers exclu telle que (A ou non-A) qui est également une question importante du débat computationnel.

La logique intuitionniste, assume, par l'absence du tiers-exclu, la calculabilité des propositions qui sont prouvés en manière intuitionniste parce que, en présence du tiers-exclu, la valeur de vérité d'une proposition est denotationnellement précise, mais du côté intuitionniste, l'absence de tiers-exclu cause, même le changement de vision épistémologique ; la vision de bivalence des valeurs des propositions est remplacée par la vision que la vérité est définie par l'existence d'une procédure démontrable de la proposition à partir des propositions précédentes et la fausseté par son non-existence. Cette position épistémologique est caractérisée par accepter la dépendance sémantique du statut de méthode de raisonner de la proposition ; la connaissabilité de la proposition à partir des prémisses. Le procédure du calcul dans la logique intuitionniste, peut être interprété par une programme de l'évaluation des démonstrations différentes ; par exemple l'implication peut être considérée comme la transformation de la démonstration de A, à la démonstration de B. En calcul des séquents intuitionnistes, la conclusion de la séquence doit être seule, parce que toutes les démonstrations ne sont pas unique et il faut que la conclusion soit bien connaissable à partir des raisonnements donc, la précision de telle démonstration de chaque proposition en conclusion.

Le changement de vision en dimension des principes logiques, a conduit à des réalisations historiques dans la logique des calculs, en utilisant les non-dualités et un raisonnement sémantiquement antiréaliste. Outre les avantages de la logique intuitionniste, le choix entre la structure symétrique et la richesse contextuelle de la logique classique présente des dimensions et des défis différents sur le plan informatique. Pour donner un exemple d'un enjeu de symétrie; on peut donner la structure symétrique du cas classique contre la syntaxe asymétrique intuitionniste en calcul des séquences; en raison de changement de sens de la négation, les séquences des preuves ne sont plus symétriques. La richesse signifie, en quelque sorte, le privilège d'utiliser des dualités et des règles structurelles, qui apportent la simplicité à la logique classique et sont interdites dans la logique intuitionniste.

La logique linéaire

La logique linéaire proposée par Jean-Yves Girard, dans une optique constructiviste, a permis de reproduire à l'intérieur de ce système logique les pertes subies lors du passage de la logique classique à la logique intuitionniste. Une caractéristique de la logique classique et de la logique intuitionniste est que les règles de raisonnement formel sont indépendantes du contexte des propositions ; la dynamique syntaxique de la connective d'implication ne dépend d'aucun contexte autre que les règles structurelles, telles que la temporalité, la certitude, etc. Un exemple tiré directement de M. Okada*[3] : En logique classique et logique intuitionniste ; Il prend une prémisse C comme « avoir 1 euro » les deux propositions A et B comme respectivement, « peut acheter un chocolat » et « peut acheter une sachet de sucre ». On construit de nouvelles propositions à partir de ces propositions en utilisant les nouvelles propositions qu'on construit par l'implication ; c'est-à-dire de $C \rightarrow A$ et $C \rightarrow B$ comme respectivement « Si avoir 1 euro, alors peut prendre une paquet du chocolat » et « Si avoir 1 euro, alors peut prendre une sachet de sucre » il peut infère $C \rightarrow A \wedge B$ comme « Si avoir 1 euro, alors peut prendre une paquet du chocolat et une sachet de sucre ». Comme on peut le voir ici, le problème est que les connecteurs ne sont pas sensibles à la temporalité des propositions ; ils ne sont pas sensibles au fait que la proposition A soit réalisée en premier ou non. Or, dans la langue naturelle, cette sensibilité est un élément important de la production de sens. En même temps, cette sensibilité est une caractéristique fondamentale de la nature du contexte informatique ; l'ordre causale des opérations, le nouvel état du système après l'opération, sont des facteurs qui peuvent affecter le résultat du calcul.

Le statut de connaissance en logique linéaire, est la vision épistémologique révisionnelle que le statut qui représente la « vérité » des formules et celui qui représente la « démonstration » contextuellement statique des assertassions. Le sens de l'objet du raisonnement en logique linéaire plutôt est lié à un choix d'ensemble de contexte d'inférence donc, les preuves d'une « ressource ».

[3] *[12]

La généralisation du statut de connaissance des logiques classiques et intuitionniste s'effectue comme de se faire en définissant l'ensemble des objets de la logique au-delà des règles de contraction et d'affaiblissement, qui sont les règles d'inférence qui s'appliquent à toutes les propositions de la logique classique et intuitionniste. Il s'ensuit que seules certaines formules de la logique linéaire respectent ces règles, de sorte que le sens de la source et le contexte sont cohéremment transmis dans le raisonnement.

Il faut parler d'un point aussi important pour le contexte de ce mémoire qui est le problème en logiques classiques et intuitionniste dans le cadre de l'élimination de coupure et trouvé une solution naturelle en logique linéaire. L'élimination de coupure, à rappeler; pose un théorème qui prévoit l'existence d'une preuve qui n'est pas utilisé la règle de coupure pour chaque preuve avec la coupure. Par exemple, en logique classique, dans le calcul des séquences, la preuve ci-dessous a été faite avec le règle de coupure comme suivant :

$$\frac{\dfrac{\Gamma \to \Delta}{\Gamma \vdash \Delta, A} \qquad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

D'abord le théorème de l'élimination de coupure, il est possible d'avoir la même conclusion en un nombre d'étapes, avec une preuve sans utiliser la règle de coupure. Dans cet exemple, la preuve peut être arrivée avec la règle d'affaiblissement, comme suivant :

$$\frac{\Gamma \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

Le problème de l'élimination de coupure en logique classique est que; l'élimination de coupure est un processus d'étape non-déterministe, c'est-à-dire, il est possible d'arriver des preuves sans coupure différentes à partir d'une preuve avec la règle de coupure ; il n'existe pas un principe qui garantit de trouver la connaissance complète de la conclusion du processus de l'élimination de coupure dans la connaissance d'une preuve classique.

La résolution de ce problème en logique linéaire sera abordée dans les chapitres suivants.

Définition de la Logique Linéaire

Dans ce chapitre, jusqu'à cette petite sous-section, le contexte était la motivation formelle et épistémologique de l'actualisation des logiques traditionnelles sur le chemin de la logique linéaire. Dans cette rubrique, les détails techniques de la logique linéaire seront donnés en utilisant l'ouvrage original de J.Y. Girard*[4] comme référence principale.

La logique linéaire, comme déjà indiqué, un système de logique bien directionnel au calcul grâce à son ressource-sensitivité et son développement sémantique déclenchée par une motivation sémantique contextuelle du monde réel. Le ressource-sensitivité est fourni en logique linéaire, parce que contrairement aux logique classique et intuitionniste les formules ne respectent pas la règle de contraction et la règle d'affaiblissement, dans le cas général, mais de préférence seulement dans certains cas, via certaines connectives. Cette situation peut être décrite comme suit: La règle de contraction, pour rappeler:

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$$

[4] *[4]

Elle provoque qu' une formule d'inférence peut être reproduite et utilisée autant que souhaité, appelée duplication dans le littérature de logique; bien corrélée par exemple avec la sensibilité temporelle. Ensuite, la règle d'affaiblissement, pour rappeler:

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}$$

Elle conduit à ajouter aux prémisses qui impliquent la conclusion un ensemble de propositions qui ne contribuent pas à la nécessité de la conclusion, ou qui peuvent conduire à la proposition d'une conclusion que les ressources d'inférence ne requièrent pas. L'absence de ces deux règles fait que les formules sources de la logique linéaire, contrairement à celles de la logique classique, ne peuvent pas être répétées indéfiniment, ce qui confère au système logique la caractéristique d'un raisonnement causal comme dans le monde réel. Ainsi, la proposition C dans l'exemple de M. Okada permet de représenter une situation dans laquelle, une fois utilisé, 1 euro est épuisé et la proposition "C implique B" ne peut plus être réalisée.

La richesse apportée par l'absence de ces deux règles se traduit par une augmentation de la liberté sémantique des connectives utilisées en logique classique et intuitionniste, ce qui constitue une mise à jour très importante dans la transition vers la logique linéaire : Les connectives de la logique traditionnelle correspondent à deux types de connectives en logique linéaire : Dans la logique linéaire, cette rupture dans les connexions de la logique traditionnelle crée deux groupes de connectives logiques, l'un signifiant concurrence et l'autre choix subjectif; l'addition et la multiplication respectivement. On peut les reconnaître comme suivant:

Les connectives sont séparées en deux types: les multiplicatives et les additives: -"$\wedge$" correspond à la multiplicative "$\otimes$" et additive "&". Le produit tensoriel $\otimes$ décrit une signification que A$\otimes$B veut dire: A et B va se réalisera en même temps ou bien ça donne les ressources de A et de B en une fois et il a l'élément neutre *1*. L'additive "et" & décrit que A&B veut dire: A ou B va se réaliser, mais si l'une ne se réalise pas

alors, l'autre va se réaliser dépendamment du choix des ressources et elle a l'élément neutre $\top$.

-"$\vee$" correspond à la multiplicative "$\parr$ " et additive "$\oplus$" . La disjonction multiplicative $\parr$ décrit que A$\parr$B veut dire: si B ne se réalise pas alors, A se réalisera et vice versa et elle a l'élément neutre $\bot$. La disjonction additive $\oplus$ décrit que A$\oplus$B veut dire: de manière imprévisible, l'une des deux formules sera réalisée et elle a l'élément neutre *0*.

-"$\rightarrow$" correspond à la multiplicative "$\multimap$" qui n'a pas une correspondance additive donc, à propos de choix subjective. Contrairement à la logique traditionnelle, l'implication n'est pas réutilisable en chaque étape en logique linéaire; pour arriver à ce sens traditionnel, il est nécessaire de l'utiliser avec des nouvelles connectives ! et ? , par exemple," C$\rightarrow$A" dans le sens traditionnel correspond à la formule "!C$\multimap$A"; dans l'exemple de M. Okada, la connective "!" redonne le sens de réutilisabilité au ressource C, donc, on a autant de 1 euro qu'on désire qu'on peut utiliser pour acheter le chocolat même le sucre. Un exemple important sur le plan du calcul est qu'une ressource "A", si elle n'a pas d'exponentielle !, devient "$A^{\bot}$ "après l'opération de l'implication, où "$^{\bot}$ " est la négation linéaire qui est involutive telle que "$A^{\bot\bot}$" est équivalent à "A".

- Les exponentielles "!" et "?", sont utilisées pour reproduire les règles structurelles (règles de contraction et d'affaiblissement) de la logique classique et intuitionniste dans la logique linéaire ; elles promettent une utilisation plus dynamique du sens de la modalité et comme les modalités, il existe une dualité entre deux exponentielles telle que " $(!A)^{\bot}$ " est équivalent à "?($A^{\bot}$)".

Après toutes ces explications, on peut dire qu'en appliquant les relations entre la logique traditionnelle et la logique linéaire mentionnées jusqu'à présent au calcul classique et intuitionniste des séries, une version linéaire du calcul des séries peut être obtenue; Cette transition peut se faire en supprimant deux règles; contraction et

affaiblissement et en écrivant des règles d'inférence pour les nouvelles connectives logiques, sinon les règles telles que l'axiome, l'échange, le coupure peuvent être conservées telles quelles. Dans ce cadre, il est possible d'écrire une linéarisation du calcul de séquences classique et intuitionniste; tout d'abord, le calcul des séquences linéaire classique peut être formulé de la manière suivant:

Règles d'axiom et de constantes:

$A \vdash A$

$\Gamma \vdash \Delta, \top \quad \bot \vdash \quad \vdash 1 \quad 0, \Gamma \vdash \Delta$

$$\frac{\Gamma \vdash \Delta}{1, \Gamma \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \bot}$$

Règle d'échange:

$$\frac{\Gamma, A, B, \Gamma' \vdash \Delta}{\Gamma, B, A, \Gamma' \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, A, B, \Delta'}{\Gamma \vdash \Delta, B, A, \Delta'}$$

Règle de coupure:

$$\frac{\Gamma \vdash \Delta, A \quad A, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

Règles de multiplicatives:

$$\frac{\Gamma, A, B \vdash \Delta}{A \otimes B, \Gamma \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, A \quad \Gamma' \vdash \Delta', B}{\Gamma, \Gamma' \vdash \Delta, \Delta', A \otimes B}$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \parr B \vdash \Delta, \Delta'} \qquad \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \parr B}$$

Règles d'additives:

$$\frac{A, \Gamma \vdash \Delta}{A \& B, \Gamma \vdash \Delta} \qquad \frac{B, \Gamma \vdash \Delta}{A \& B, \Gamma \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \& B}$$

$$\frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \oplus B, \Gamma \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \& B} \qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \& B}$$

Règles d'implication:

$$\frac{\Gamma\vdash\Delta,A \quad B,\Gamma'\vdash\Delta'}{(A\multimap B),\Gamma,\Gamma'\vdash\Delta,\Delta'} \qquad \frac{A,\Gamma\vdash\Delta,B}{\Gamma\vdash\Delta,(A\multimap B)}$$

Règles de négation:

$$\frac{\Gamma\vdash\Delta,A}{A^{\perp},\Gamma\vdash\Delta} \qquad \frac{A,\Gamma\vdash\Delta}{\Gamma\vdash\Delta,A^{\perp}}$$

Règles de modalité:

$$\frac{A,!\Gamma\vdash?\Delta}{?A,!\Gamma\vdash?\Delta} \qquad \frac{!\Gamma\vdash?\Delta,A}{!\Gamma\vdash?\Delta,!A}$$

$$\frac{A,\Gamma\vdash\Delta}{!A,\Gamma\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta,A}{\Gamma\vdash\Delta,?A}$$

Contraction:

$$\frac{!A,!A,\Gamma\vdash\Delta}{!A,\Gamma\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta,?A,?A}{\Gamma\vdash\Delta,?A}$$

Affaiblissement:

$$\frac{\Gamma\vdash\Delta}{!A,\Gamma\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta}{\Gamma\vdash\Delta,?A}$$

La version intuitionniste du calcul des séquences linéaires diffère de la version classique sur ces points suivants: Les connectives ⅋ et ! ne sont pas inclus dans le système intuitionniste et comme en logiques traditionnelles, seules les règles du côté droit seront prises en compte . En utilisant la même méthode que dans le cas de la logique classique, les règles logiques du calcul intuitionniste des séquences linéaires peuvent être écrites comme suit :

Règles de connectives:

$$\frac{\Gamma\vdash A \quad \Gamma'\vdash B}{\Gamma,\Gamma'\vdash A\otimes B} \qquad \frac{\Gamma\vdash A \quad \Gamma\vdash B}{\Gamma\vdash A\&B}$$

$$\frac{\Gamma\vdash A}{\Gamma\vdash A\oplus B} \qquad \frac{\Gamma\vdash B}{\Gamma\vdash A\oplus B}$$

$$\frac{A,\Gamma\vdash B}{\Gamma\vdash(A\multimap B)} \qquad \frac{A,\Gamma\vdash\Delta}{\Gamma\vdash A^{\perp}}$$

Règle de coupure:

$$\frac{\Gamma\vdash A \quad A,\Gamma'\vdash\Delta}{\Gamma,\Gamma'\vdash\Delta}$$

Règles de modalité:

$$\frac{!\Gamma\vdash\Delta}{!\Gamma\vdash!\Delta} \qquad \frac{\Gamma\vdash\Delta}{!A,\Gamma\vdash\Delta} \qquad \frac{\Gamma\vdash\Delta}{!A,\Gamma\vdash\Delta}$$

$$\frac{!A,!A,\Gamma\vdash\Delta}{!A,\Gamma\vdash\Delta}$$

CHAPİTRE 2: CALCUL QUANTIQUE ET LOGIQUE LINÉAIRE

La computation quantique

La computation quantique est une domaine interdisciplinaire telle que la science théorique de computation et la physique quantique notamment la théorie d'information quantique et secondairement les autres domaines comme la théorie des champs quantique. Considérant l'information comme un concept physique, selon le paradigme physique qui détermine sa dynamique, la croyance sur la nature de l'information, les conditions physiques qui restreignent sa liberté, ou les situations qui prévoient de nouveaux phénomènes, la théorie de l'information fournit un cadre théorique pour la génération et l'étude des processus computationnels. Dans ce cadre, l'information du calcul évolue dans l'incarnation d'une état physique: L'évolution et l'exécution d'une opération calculatoire est faite par l'action des éléments physiques; ce sont des objets classiques ou quantiques.

Le contexte de la théorie de l'information s'intéresse, en général, à la question de savoir quelles informations constituent des « connaissances significatives ». En ce sens, la « signification » de la connaissance classique, par exemple, est qu'elle est conforme aux prédictions de la dynamique newtonienne (ou au formalisme de Lagrange et Hamilton). De plus, suite à l'article de Vasil Penchev*[5], la vision

[5] *[32]

cybernétique de Norbert Wiener a fait du concept d' information un objet commun à de nombreux domaines, en l'occurrence la physique et la logique. Toutefois, il convient de rappeler que l'information est une chose physique réelle et qu'elle ne constitue pas un système idéal comme d'autres objets ; elle est finie et en perte constante pour des raisons thermodynamiques. Cette réalité de l'information, dans le contexte statistique de la physique, nous rappelle la nécessité d'exprimer les états de choses possibles sous forme de distributions de probabilités. À cet égard, la nécessité de l'information classique à la fois comme objet de prédiction de la dynamique complexe de la nature et comme structure que l'observateur peut subjectivement créer parmi les états possibles - par exemple, en préparant un système à se trouver dans un certain état - est à l'origine du fait que la plus petite unité d'information est le « bit », un état de choix entre deux états représentés par "0" et "1". C'est-à- dire, dans la formulation de la théorie d'information, épistémologiquement soit il existe le choix entre au moins deux options, soit il n'existe pas d' information.

Dans le cadre de la computation, Le modèle mathématique de la machine de Turing est l'un des principaux développements théoriques du paradigme classique basé sur la théorie classique de l'information. Comme l'indique l'article de Michael Cuffaro*[6], la principale motivation d'Alan Turing était de l'utiliser pour prouver qu'il n'existe pas de méthode canonique pour prouver le « problème du choix » (Entscheidungsproblem), c'est-à-dire tout énoncé du premier ordre, à partir des axiomes de la logique du premier ordre. La machine de Turing est un système qui consiste à les états, symboles, fonctions de transition et une état initial; Le processus de calcul consiste en la transition d'un ensemble fini d'états d'un état initial à un autre état au moyen d'une fonction de transition, chaque « étape » étant constituée de ces quatre ensembles de concepts ; en ce sens, la machine de Turing est un modèle discontinu dans lequel l'information physique est transportée à travers ces boîtes d'étapes. L'expression spatiale et temporelle du processus de calcul physique en termes de ces « boîtes » et de leurs mémoires a été préservée par de nombreux

[6]* [21]

paradigmes de calcul modernes ; les théories du calcul quantique peuvent être considérées comme préservant cette compréhension.

L'information quantique, comme indiqué précédemment, traite l'information comme une objet quantique, dont la signification dépend de son accord l'équation de Schrödinger (ou l'équation de Dirac dans le cas des champs quantiques). Le changement de définition de l'information que ce changement de paradigme entraîne promet un changement dans la formulation de la théorie de la connaissance; Il est important de noter que la boîte à outils mathématique de la mécanique quantique sera utilisée, que les nouveaux phénomènes physiques comme l'intrication et superposition quantique, la nouvelle nature quantique comme le statut de l'observateur et la contextualité, qui sont les résultats de ce paradigme, doivent être pris en compte, et que deux types de connaissances (classique et quantique) peuvent désormais être utilisés ensemble.

La fonction d'onde, en tant qu'objet fondamental de la mécanique quantique, peut être considérée comme intégrant des informations significatives dans la mécanique quantique, repoussant même la frontière dualiste entre l'information en tant qu'objet mathématique et la réalité physique. La fonction d'onde est une structure qui véhicule des informations sur l'état du système physique. Elles vivent dans l'espace complexe de Hilbert. Cette objet est interprété, dans l'histoire, soit comme une partition des superpositions des état possible, soit comme une statistique des mesures sur le système. Ces deux interprétations de la fonction d'onde ont fait l'objet de controverses entre les différentes interprétations de la mécanique quantique et ont établi des positions métaphysiques différentes sur la relation de la fonction d'onde, un objet mathématique, avec le monde matériel. Selon l'interprétation de Copenhague, qui est l'interprétation la plus favorisée aujourd'hui, la fonction d'onde est un paquet contenant l'information complète de tous les états possibles d'un système, et une mesure sur ces paquets est irréductiblement non déterministe. De plus, la mesure, en

agissant sur l'état du système, provoque la réduction de la fonction d'onde et sa transformation en une information classique du système après la mesure, ce qui signifie la destruction de la structure causale entre la mesure et le produit de la mesure dans le paradigme classique. Par ailleurs, le principe d'incertitude de la mécanique quantique souligne que la mesure de deux observables duales est soumise à une incertitude inhérente et ne relève donc pas d'un problème épistémologique. La conséquence la plus importante de la mécanique quantique pour la théorie de l'information est peut-être la non-localité quantique : dans le paradigme classique, la transmission d'informations sur une distance spatiale est un treillis causal d'étapes locales ; l'effet à une localité ne peut pas se produire causalement avant que la suivante ne le fasse, et en général tous les phénomènes physiques ne peuvent pas agir instantanément dans ce contexte. La mécanique quantique (selon l'interprétation de Copenhague et de nombreuses autres interprétations) viole ce principe de localité : la fonction d'onde est une structure translocale et permet une action instantanée grâce au phénomène d'intrication, ce qui est impossible dans le contexte classique. L'intrication quantique permet à des systèmes binaires d'interagir et de transmettre des informations indépendamment de la localité. Ainsi, alors que de nombreux principes métaphysiques tels que la localité et la séparabilité sont détruits par la physique quantique, la théorie de l'information quantique a acquis de nouvelles ressources quantiques telles que l'intrication et la superposition quantique, qui peuvent être plus efficaces sur le plan informatique.

Les détails techniques et les notions basiques

Le but de ce chapitre est de donner quelques préliminaires sur le formalisme de l'informatique quantique qui seront nécessaires dans les chapitres suivants, de se familiariser avec le langage quantique et d'introduire quelques phénomènes très importants dans ce domaine.

En mécanique quantique, un état quantique doit être écrit à partir d'un système de base vectorielle qui représente les états possibles; il est une point dans l'espace vectoriel complexe séparable de Hilbert avec le norme et l'orthogonalité. Analogue quantique du bit dans l'informatique classique, la plus petite unité d'information dans la théorie quantique est le qubit, un élément de l'espace complexe bidimensionnel $\mathbb{C}^2$. Un qubit est représenté comme $|\psi >= \alpha|0 >+ \beta|1 >$, la superposition de deux états $|0 >$ et $|1 >$ sont des vecteurs de base et α et β sont des coefficients complexe qui représentent la densité de probabilité de l'état telle que $|\alpha|^2 + |\beta|^2 = 1$. Mais, un système est souvent formé par plusieurs qubits. Un système de multi-qubit est dans l'espace de produit tensoriel d'une espace de qubit; pour un n-qubit système, l'espace sera $\mathbb{C}^2 \otimes .... \otimes \mathbb{C}^2$ n fois de produit tensoriel de l'espace d'un qubit. Par exemple, un système de biqubit dans l'espace $\mathbb{C}^2 \otimes \mathbb{C}^2$ est représenté comme ,

$$|\psi >= \alpha|00 >+ \beta|01 >+ \eta|10 >+ \theta|11 >.$$

où $|00 >$ est une écriture pratique de $|0 > \otimes |0 >$. Dans l'espace complexe de Hilbert, $< \psi|$ est le conjugué transposé complexe du vecteur $|\psi >$ qui est l'élément de l'espace dual; c'est à dire, leur produit $< \psi|\psi >$ doit être égale à 1 et le production de deux vecteur $< \varphi|\psi >$ est un nombre complexe.

L'intrication quantique, c'est la situation où une combination des systèmes quantique ne peut pas être écrit en forme de la décomposition des produits tensoriels des systèmes, par exemple pour une composition de deux systèmes ψ_1 et ψ_2 qui ne peuvent pas être écrit sous la forme de $\psi_1 \otimes \psi_2$. Ces systèmes intriqués sont connectés, c'est-à-dire qu' il n'y a pas encore de libre choix pour chaque système et cette connexion ne respecte pas le principe de localité comme déjà dite. Le phénomène où un changement de la situation d'un état, cause en manière non-locale

et non-séquentielle une changement de la situation de l'état corrélé, peut être confirmé par l'experiment de mesurer l'inégalité de Bell auxquelles obéissent les systèmes locaux comme indiqué à l'article de Pouria Abbasalinejad et Hamid Tebyanian*[7]:

$$S = |E(a,b) - E(a,b')| + |E(a',b) + E(a',b')| \leq 2$$

Dans cette formule, les petites lettres représentent les états corrélés telle que $|\psi >= |a> |b> + |a'> |b'>$ et $E(a,b)$ représente la valeur attendue dans le cas de préparation a et b .Les résultats expérimentaux montrent que cette inégalité n'est pas respectée ($S \geq 2$). Il s'agit d'une démonstration expérimentale de l'existence d'effets non locaux, c'est-à-dire de l'intrication quantique.

L'état du système porte la connaissance complète, donc toutes les réponses possibles (la distribution de probabilité des réponses possibles) des questions physiques sur le système. En mécanique quantique la façon de poser ces questions, c'est de multiplier les fonction d'onde par les opérateurs unitaire qui sont les représentation des observables telle que la multiplication avec son adjoint donne l'opérateur d'identité, $UU^t = Id$, donc, ce sont des fonctions linéaires inversibles ; dans le contexte computationnel, ces opérateurs apparaissent comme des "portes quantiques". Les portes quantiques sont des structures qui agissent sur les états quantiques pour réaliser les opérations calculatoires.

Certaines portes quantiques peuvent être citées en référant du livre de Phillip Kaye et al.*[8] et de l'article de Díaz-Caro et al**[9]. comme suivant:

[7] *[16]

[8] *[30]

[9] **[25]

- La porte Not: C'est l'opérateur qui transforme de l' état à son état orthogonale comme suivant,

  $Not|0>=|1>$

  $Not|1>=|0>$

- La porte Cnot: C'est un opérateur pour la superposition de deux systèmes qubits qui sert à appliquer la porte Not au deuxième qubit conditionnellement au premier qubit.

  $Cnot|0\psi>=|0\psi>$

  $Cnot|1\psi>=|1>\otimes Not|\psi>$

- La porte $R_i\theta$: C'est un opérateur qui change la phase du système d'un quantité θ dans la direction de i.

  $R_x\frac{\pi}{4}|0>=|0>$

  $R_x\frac{\pi}{4}|1>=e^{i\frac{\pi x}{4}}|1>$

- la porte de Hadamard Had: C'est l'opérateur qui fait une rotation de 45 degré à l'état appliqué:

  $Had|0>=\frac{1}{\sqrt{2}}|0>+\frac{1}{\sqrt{2}}|1>$

$$Had|1>=\frac{1}{\sqrt{2}}|0>-\frac{1}{\sqrt{2}}|1>$$

Le chapitre se termine par la présentation du théorème de non-clonage, un théorème limite très important de la théorie de l'information quantique, qui stipule que les informations quantiques qui n'existent pas dans le cas classique ne peuvent pas être dupliquées.

La théorème de non-clonage est un résultat de la nature quantique, qui dit qu'il est impossible de trouver une façon de dupliquer pour tous les états dans le formalisme de la mécanique quantique. Dans un langage plus formel, il n'y a pas d'une opérateur unitaire telle que pour un état $|\varphi>$, $U|\varphi\psi>=|\psi\psi>$.

Les limites de la logique traditionnelle

La réflexion sur les motivations des modèles logiques de calcul quantique est un point d'ancrage important de ce travail. L'inspiration principale de ce chapitre est l'article de J.Y.Girard*[10] . L'informatique quantique n'est pas seulement alimentée par la logique en tant qu'application physique ou informatique de la logique, mais elle est aussi un cadre expérimental dans les débats internes de la logique ; elle peut servir à la fois de test de la validation de la logique par le monde physique et matériel, mais aussi de moteur expérimental de la puissance du paradigme quantique pour tester les

[10] *[27]

fondements métaphysiques du paradigme classique (inégalités de Bell**[11], débats sur la causalité quantique***[12], etc.)), il acquiert le pouvoir de démontrer ce pouvoir sur la métaphysique des fondements métaphysiques de la logique à travers le domaine de la computation. L'une des difficultés des discussions en logique quantique, comme le souligne Girard, est que les propriétés quantiques vont « à l'encontre du sens commun ». Dans le monde phénoménal de l'expérience humaine, dans lequel les hypothèses métaphysiques du développement historique des règles traditionnelles de la logique ont mûri, il n'y a pas de chose quantique. Il s'agit d'une situation difficile, non seulement pour donner un sens aux choses quantiques, mais aussi pour les discussions métaphysiques : Dans le monde quantique, il y a des choses qui sont inimaginables dans le monde classique ; d'autre part, la reproduction d'entités classiques dans le paradigme quantique change radicalement la nature de l'être et la met hors de portée du sens commun ; en même temps, la relation entre l'observateur et le monde extérieur, le rôle ontologiquement actif de la mesure (contextualité quantique), la vision discrète de la nature doit être ancrée dans le monde physique des phénomènes expérimentaux de la science physique, plus sensible au contexte quantique qu'aux sources phénoménales de la logique.

Les difficultés rencontrées par les tentatives d'écriture d'un système de logique quantique en termes de logique classique pour ces raisons peuvent être mentionnées comme suit : Premièrement, la sémantique Tarskienne de la logique classique, est remise en cause par la nature superpositionnelle des états de la mécanique quantique; Une événement classique possède une valeur de vérité inclusive, indépendant de l'observateur et la mesurement; par exemple, l'existence d'une particule a une coordinate donnée prend une valeur de vraie ou fausse, qui découle de la cause inhérente à la réalité physique. Mais une question sur un événement quantique a deux natures différentes, tout d'abord la réponse avant la mesure (avant que la réponse finale ne soit donnée) et la réponse après la mesure, la réponse avant la mesure étant

[11] **[17]

[12] ***[18]

un ensemble de tous les états possibles de la particule, ou plus précisément, ayant à la fois des valeurs vraies et fausses, et étant inévitablement indéterminée d'un point de vue métaphysique ; la réponse après la mesure, semblable à la réponse classique, n'en ayant qu'une seule. En d'autres termes, le fait même que l'observateur pose la question conduit sémantiquement à deux états différents ; la réalité immanente est anti-réaliste et non-déterministe, à l'opposé de ce que suppose la logique classique. Il est donc difficile de trouver une place pour le principe de tiers exclu dans la logique quantique.

Ensuite, bien que la logique quantique ne pose pas de problèmes avec les règles de De Morgan, elle n'est pas conforme à la logique classique en ce qui concerne la distributivité des connectives logiques les unes par rapport aux autres; l'algèbre des observables quantiques a une structure non-commutative en raison du principe d'incertitude, simplement, le mesure d'un observable A et B et le mesure B et A ne donnent pas toujours le même résultat.

Dans la logique quantique, l'interprétation des connectives logiques est différente de celle de la logique classique; il n'est pas aussi évident de dire « et » pour une connexion ∨, « ou » pour une connexion ∧ ; les tables de valeurs de ces connectives logiques peuvent être différentes en logique quantique qu'en logique classique ; pour donner un exemple tiré du livre de Klaas Landsmann** suivant$A \vee B$ peut être vrai même si A et B ne sont pas vrais ou bien $A \wedge B$ peut être faux même si A et B ne sont pas faux . En bref, une approche logique holistique de la logique classique est nécessaire dans le contexte du monde quantique, qui ne parvient pas à englober le comportement quantique parce que la logique classique et la logique intuitionniste ne sont pas resource-sensibles, comme je l'ai mentionné dans le premier chapitre.

Bien que l'inexistence naturelle du principe d'exclusion des tiers soit une bonne chose pour la logique quantique, le manque d'inclusivité par rapport aux phénomènes quantiques découlant de cette indépendance du contexte persiste dans la logique intuitionniste de la même manière que dans la logique classique ; l'exemple d'Okada du premier chapitre peut être adapté ici au cas de la pré-mesure quantique et de la réduction de la fonction d'onde.

Motivation de la logique linéaire pour la computation quantique

Avant d'annoncer un système de logique linéaire pour l'informatique quantique, il est nécessaire de revenir à l'article de Girard dans la section précédente et de mentionner brièvement que la logique linéaire est un système qui peut englober le paradigme quantique à la fois sémantiquement et syntaxiquement, conformément à la façon dont la logique linéaire dans la première partie de ce document transforme la logique traditionnelle en un système plus à l'écoute du monde expérimental.

La logique linéaire prend les preuves comme l'action des prémisses; le dynamisme des connectives logiques que la logique linéaire impose à la logique traditionnelle, est une bonne propriété pour être candidate de modéliser la nature dynamique des actions quantique telle que le problème de mesurement; la séparation en multiplicatives et additives; d'un côté de cette distinction, les effets non locaux des phénomènes quantiques, que nous connaissons à partir du monde physique du monde quantique, qui est étranger à l'expérience, ont les propriétés syntaxiques nécessaires pour modéliser les états antérieurs à la mesure ; l'autre côté continue d'exprimer le raisonnement du monde phénoménal sur les objets, qui est nécessaire pour penser les

résultats de la mesure à l'écran du comportement classique du système perturbé par la mesure. Les connectives de modalité qui permettront la transition entre les deux angles de cette distinction fournissent un système de raisonnement dépendant du contexte pour modéliser les systèmes quantiques. Le succès de cette tentative peut être testé par le fait que les théories de l'information quantique, telles que le non-clonage dans le contexte de la computation, et les sources quantiques, telles que la téléportation quantique, peuvent être exprimées en termes de ce système de raisonnement. Dans la section suivante, je présenterai la tentative de Gilles Dowek et A. Diaz-Caro d'exprimer l'informatique quantique comme un système de lambda calcul linéaire.

Le calcul de lambda linéaire pour la computation quantique

Comme nous l'avons vu dans la section précédente, les principales motivations pour un calcul quantique linéaire sont l'utilisation de connexions multiplicatives et additives comme généralisation de la logique traditionnelle pour un système logique approprié au comportement des phénomènes quantiques, ainsi que la prise en compte des limites de la théorie de l'information quantique sur le comportement de l'information ; l'utilisation de la propriété de linéarité de la logique linéaire, qui garantit qu'une proposition quantique ne peut pas être copiée, conformément au principe de non-clonage quantique. Dans leurs travaux, A. Diaz-Caro et Gilles

Dowek*[13]'**[14] proposent, dans ce contexte, un lambda calcul typé linéaire pour la computation quantique.

Le système de calcul de ce travail repose sur deux concepts, tous deux appelés linéarité. L'un linéarité, c'est de linéarité algébrique qui est la distributivité des fonctions sur l'addition; dans ce contexte, il sert à définir la superposition par l'addition des vecteurs de base en évitant la réduction de l'application d'une fonction sur la superposition. Le deuxième linéarité, c'est la linéarité dans le sens de l'utilisation en " Logique Linéaire ", avec la motivation de la ressource-sensitivité; d'assumer le caractère à usage unique des arguments quantique telle que le non-clonage.

Dans ce formalisme, la superposition quantique est représentée par la conjonction additive ($u\&v$ dans l'écriture populaire de logique linéaire) $u + v$ des vecteurs de base, et $< u, v >$ en termes de calcul lambda qui est commutative et associative - la superposition de u avec v c'est physiquement la même chose que la superposition de v avec u et la superposition de la superposition u et v avec z,c'est la même chose que la superposition de la superposition v et z avec u - et ensuite, la réduction de la superposition c'est à dire le mesurement, est formalisé par la projection de type de l'état, de la superposition $\pi_A < u, v >$; l'interprétation que le choix dépendent de la conjonction additive telle que de dire qu'on peut choisir l'un des états possibles, assumer la distinction des états dans la superposition et la projection sans spécialiser le type de chaque état assume la nature probabiliste du mesure quantique. Il faut remarquer que si un état est de type A, alors il est une vecteur de base, c'est à dire un état atomique comme le vecteur $|0 >$; afin qu' un état soit une superposition comme

[13] *[25]

[14] **[24]

le vecteur $\alpha|0>+\ \beta|1>$, il doit être de type $A \wedge A$ (ou de type $A \wedge \ldots . \wedge A$ comme indiqué sur l'article*[15]).

Dans la langage de ce système de calcul, pour séparer les objets duplicables et non-duplicables, ils ont introduit deux types; le type de base A_0 qui est le types des termes duplicables comme le séparation par le connective modal ! A en logique linéaire qui consiste le type de système qubit $\mathbb{Q}$, le type d'implication $A \to A$ et le produit tensoriel des types de base $A_0 \otimes A_0$; le type de superposition $S(A)$ qui est le type des termes non-duplicables.

Pour la modélisation des systèmes corrélés des qubits qui sont générés par le produit tensoriel des espaces de Hilbert, il faut introduire le produit tensoriel $\otimes$, comme une conjonction qui est non-commutative au contraire de la conjonction additive $+$.

İls ont introduit trois catégories de term telle que, le termes de base $\mathfrak{B}$ qui consiste en variables x , abstractions $\lambda x.\ At$ et constantes de qubit $|0>$ et $|1>$ et le produit tensoriel des termes de base $b \otimes b$; les termes de valeur qui consiste en termes de base b, paires $v + v$, valeurs négatives $-\ v$ où "-" est une opérateur qui change le type de terms de A au type $S(A)$, le vecteur nul 0 et le produit tensoriel des termes de valeurs $v \otimes v$; enfin les termes de ces catégories de termes telle que, v, tt, l'addition des termes (t+t), la projection $\pi_A t$,la connective ?. qui prend sens de la réduction au soit au premier soit au deuxième terme dépendamment au choix de base, le terme négative $-\ t$, le produit tensoriel des termes $t \otimes t$, la projection sur le produit tensoriel au premier terme $fst\ t$ et le deuxième terme $snd\ t$. Sur la base de ce qui

[15] *[25]

précède, pour donner le système de règles de ce système lambda linéaire de Diaz-Caro et Dowek*[16], en conservant la notation de l'article:

Règles pour les termes de base:

$$\frac{}{x{:}A \vdash x{:}A} \qquad \frac{}{\vdash 0{:}S(A)} \qquad \frac{}{\vdash |0\rangle{:}\mathbb{Q}} \qquad \frac{}{\vdash |1\rangle{:}\mathbb{Q}}$$

Règles pour la superposition:

$$\frac{\Gamma \vdash t{:}A}{\Gamma \vdash t{:}S(A)} \qquad \frac{\Gamma \vdash t{:}S(S(A))}{\Gamma \vdash t{:}S(A)}$$

$$\frac{\Gamma \vdash t{:}A}{\Gamma \vdash -t{:}S(A)}$$

Règles d'implication:

$$\frac{\Gamma \vdash t{:}A \to B \quad \Delta \vdash u{:}A}{\Gamma,\Delta \vdash tu{:}B} \qquad \frac{\Gamma \vdash t{:}S(A \to B) \quad \Delta \vdash u{:}S(A)}{\Gamma,\Delta \vdash tu{:}S(B)}$$

$$\frac{}{\vdash ?.{:}\mathbb{Q} \to \mathbb{Q} \to \mathbb{Q} \to \mathbb{Q}} \qquad \frac{\Gamma, x{:}A \vdash t{:}B}{\Gamma \vdash \lambda x{:}A\ t{:}A \to B}$$

Règles de conjonction:

[16] *[25]

$$\frac{\Gamma\vdash t{:}S(A)\quad \Delta\vdash u{:}S(A)}{\Gamma,\Delta\vdash (t+u){:}S(A)} \qquad \frac{\Gamma\vdash t{:}S(A)}{\Gamma\vdash \pi_A t{:}A}$$

$$\frac{\Gamma\vdash t{:}B}{\Gamma,x{:}A_0\vdash t{:}B} \qquad \frac{\Gamma,x{:}A_0,y{:}A_0\vdash t{:}B}{\Gamma,x{:}A_0\vdash (x/y)t{:}B}$$

Règles pour le produit tensoriel:

$$\frac{\Gamma\vdash t{:}A\quad \Delta\vdash r{:}B}{\Gamma,\Delta\vdash t\otimes r{:}\ A\otimes B} \qquad \frac{\Gamma\vdash t{:}A\otimes B}{\Gamma\vdash fst\ t{:}A}$$

$$\frac{\Gamma\vdash t{:}\ S(A)\otimes B}{\Gamma\vdash t{:}S(A\otimes B)} \quad \frac{\Gamma\vdash t{:}\ A\otimes S(B)}{\Gamma\vdash t{:}\ S(A\otimes B)}$$

$$\frac{\Gamma\vdash t{:}S(A\otimes S(B))}{\Gamma\vdash t{:}\ S(A\otimes B)} \qquad \frac{\Gamma\vdash t{:}S(S(A)\otimes B)}{\Gamma\vdash t{:}\ S(A\otimes B)}$$

CHAPİTRE 3: NONDETERMİNİSM DE L'ÉLİMİNATİON DE COUPURE

L’élimination de coupure, pour rappeler, est une procédure pour enlever les application de la règle de coupure en décomposant les séquents raisonnés par cette règle et ensuite de les reconstruire avec les autres règles logiques; le théorème de l’élimination de coupure (Hauptsatz) indique qu’il est possible de trouver toujours au moins un façon d’éliminer le coupure et d’arriver sans règle de coupure (la forme normale) au même conclusion que celle avec la règle de coupure.Dans le calcul des séquences, la règle de coupure est le seul moyen de rendre une séquence de preuves moins complexe. L'élimination de cette règle signifie que chaque étape suivante des preuves qui peuvent être écrites sans cette règle conduira le raisonnement à une preuve plus irréductiblement complexe . Cependant, dans les systèmes logiques en général, certains résultats difficiles peuvent être obtenus en utilisant cette méthode ; par exemple, dans le raisonnement sans l'utilisation d'une règle de coupure, plus d'une conclusion possible peut être atteinte ; un autre problème possible est que l'application d'une règle de coupure peut avoir plus d'une voie d'élimination ; ces situations nécessitent un choix parmi les résultats possibles, et il n'y a généralement pas de méthode canonique pour faire ce choix ; cela indique le non-déterminisme de la méthode d'élimination de la coupure. Les systèmes logiques doivent avoir des défauts qui causent ce non-déterminisme ; comme nous le verrons dans la première section, la logique linéaire est un système plus moderne que la logique traditionnelle dans le sens où elle est un raffinement de ces logiques afin de profiter des avantages de la logique classique et intuitionniste, en particulier en révisant les aspects de la logique classique qui mènent au non-déterminisme de la méthode d'élimination des coupes.

Dans le cadre de la logique classique, une preuve n'a pas un contenu informatif suffisamment détaillé en raison de la structure des règles classiques qui la constituent,

de sorte que la preuve d'un processus de l'élimination des coupures peut conduire à une forme normale unique. Un nombre inutilement élevé de choix pour une sélection de forme normale résulte du fait qu'un raisonnement met en œuvre plus de conclusions qu'il ne le devrait ; c'est-à-dire qu'en logique classique, il n'y a pas de mécanisme de contrôle sélectif sur les règles structurelles, par exemple la règle de contraction droite, qui met en œuvre plus de conclusions que nécessaire.

En logique intuitionniste, ce problème est mieux évité que dans la logique classique par la restriction de la conséquence en qu'une formule et en écrivant les règles structurelles juste à gauche, donc en raisonnant de manière unidirectionnelle; cette situation suppose une contrôle sur l'élimination de coupure. Pour illustrer notre propos, reprenons l'exemple de l'élimination par la règle d'affaiblissement pour la logique classique du premier chapitre, mais cette fois-ci avec des antécédentes et des conséquences identiques telle que $\Gamma = \Gamma'$ et $\Delta = \Delta'$ avec Π et Σ sont deux preuves qui concluent la formule $\Gamma \vdash \Delta$:

$$\dfrac{\begin{array}{cc}\Pi & \Sigma \\ \vdots & \vdots \\ \dfrac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} & \dfrac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\end{array}}{\Gamma, \Gamma \vdash \Delta, \Delta}$$ est , après le procédure de l'élimination de coupure,

transformé :

soit à: soit à :

$$\dfrac{\begin{array}{c}\Pi \\ \vdots \\ \Gamma \vdash \Delta\end{array}}{\Gamma, \Gamma \vdash \Delta, \Delta} \qquad \dfrac{\begin{array}{c}\Sigma \\ \vdots \\ \Gamma \vdash \Delta\end{array}}{\Gamma, \Gamma \vdash \Delta, \Delta}$$

İci, le problème, c’est que quand les deux preuves qui concluent Γ⊢Δ sont différentes, les différentes stratégies de l’élimination de coupure ne donnent pas le même résultat.

La logique linéaire a une capacité de contrôle plus stratifiée que cette logique traditionnelle, puisque l'exclusion radicale des règles structurelles et le fonctionnement de ces règles par des connexions logiques qui peuvent être utilisées pour écrire des séquences de preuves permettent une spécialisation plus poussée du raisonnement en question. il est utile de réexaminer cet exemple en logique linéaire ; pour ce faire, nous utiliserons les connectives de modalité et nous rappellerons que chaque formule sans modalité ne peut être utilisée qu'une seule fois dans une séquence:

$$\dfrac{\dfrac{\begin{matrix}\Pi\\ :\\ \Gamma\vdash\end{matrix}}{\Gamma\vdash ?A}\quad\dfrac{\begin{matrix}\Sigma\\ :\\ \vdash ?\Delta,A^{\perp}\end{matrix}}{\vdash ?\Delta,!A^{\perp}}}{\Gamma\vdash ?\Delta}$$ est transformé avec le procédure de l’élimination de coupure par l’affaiblissement de connective ? :

$$\dfrac{\begin{matrix}\Pi\\ :\\ \Gamma\vdash\end{matrix}}{\Gamma\vdash ?\Delta}$$

Dans ce cas, la logique linéaire a construit ce raisonnement en n'utilisant les antécédents qu'une seule fois. En conséquence, le besoin de choisir entre les preuves A et B est éliminé, et la conclusion sans coupure est réduite à une seule possibilité, devenant ainsi déterministe. La logique linéaire est capable de contrôler les ressources sans causer de distorsion de symétrie, contrairement au cas de la logique intuitionniste, comme mentionné dans la première section.

Le contexte computationnel

Comme indiqué dans la première section, l'isomorphisme de Curry-Howard souligne que les structures du contenu logique correspondent aux structures du contenu computationnel et que cette correspondance préserve les liens entre ces structures ; les formules logiques correspondent à des types, les preuves à des programmes. En ce sens, la logique intuitionniste a une correspondance avec le lambda-calcul typé ; cette connexion préserve la relation inter-structurelle ; le processus de réduction des preuves à la forme normale ou l'élimination de coupure correspond à la réduction des lambda-termes ; dans le contexte informatique, il correspond à la réalisation du calcul.

Dans le contexte de la logique linéaire, la forte capacité de contrôle de la source de cette logique est également importante dans un contexte d’effectivité computationnel comme pouvoir déclarer la copiabilité et effaçabilité des variables par la séparation de ses connectives logiques. L'avantage est que la diversité de la procédure de calcul peut être modélisée. Afin de spécifier comment les étapes de calcul se déroulent, la sémantique opérationnelle, basée sur le contexte de l'exécution d'un programme, est un ensemble de stratégies pour la réduction des termes linéaires à des formes canoniques qui sont déterminées par un certain contexte.

Dans la sémantique opérationnelle le, les stratégies de l'évaluation sont les liens pour traduire les preuves sans coupure en programme exécuté. Deux types d'évaluation doivent être mentionnés en deux formes: l'évaluation paresseuse (lazy evaluation) et l'évaluation stricte (eager evaluation). L'évaluation paresseuse entraîne une évolution du système qui, au lieu d'exécuter le programme de manière brutale, retarde l'achèvement du calcul et atteint des programmes accompagnés d'une règle d'introduction. L'évaluation stricte permet au programme d'être exécuté de cette manière immédiate, les formes canoniques de ce développement sont toutes des abstractions. La forme canonique en évaluation paresseuse est une étape de réduction qui n'est pas terminée, donc n'est pas une preuve sans coupure et son étape suivant est contrôlable; avec soit les connectives de l'évaluation paresseuse soit de l'évaluation stricte.

En tant que stratégie d'évaluation, l'implication linéaire $\multimap$ est appelée appel-par -valeur (call by name), ce qui permet l'évaluation d'une fonction qui ne peut être utilisée qu'une seule fois ; la conséquence de l'implication entre dans le processus de mise en œuvre déjà exécuté ; en ce sens, elle est catégorisée comme une évaluation stricte. Parmi les connectives logiques, le produit tensoriel $\otimes$ et la disjonction additive $\oplus$ sont également considérés comme des évaluations strictes, tandis que les types multiplicatifs & et les types exponentiels ! sont considérés comme des évaluations paresseuses.

A partir de l'article de Samson Abramsky*[17], en calcul de lambda typé linéaire, le déterminisme des preuves est fourni par le théorème convergence indique qu'une preuve quelconque peut être réduite par l'élimination de coupure à une forme normale; c'est-à-dire, chaque évaluation va être terminée à une forme canonique. Ensuite, la constructivité des preuves suppose que les programmes ne possèdent pas des exécutions non terminées comme les boucles de computation sur soi-même.

[17] *[14]

Néanmoins, comme le mentionne l'article de S. Abramsky, le processus déterministe d'évaluation paresseuse aboutissant à une forme canonique peut devenir non déterministe avec des ajouts externes - complexité -, c'est-à-dire en rendant possibles différentes possibilités de réduction avant d'atteindre la forme canonique. La caractéristique déterministe ci-dessus est donc valable dans le cas où le système n'est pas une complexité additionnelle; bien que le théorème de convergence soit préservé puisqu'il dépend du modèle sémantique lui-même, la normalisation forte (strong normalization) n'est pas garantie. Dans la section suivante, nous discutons de la relation du lambda calcul linéaire de A. Diaz-Caro et G. Dowek pour la computation quantique avec l'élimination des coupures et les conséquences de la discussion sur le non déterminisme dans ce contexte.

Les conclusion pour le contexte quantique

D'abord la section précédente, la correspondance de preuve- computation implique que l'élimination de coupure d'une formule, correspond dans le contexte computationnel, une exécution de programme; donc, la réalisation et la finalisation du calcul; le mesurement sur un système doit être modéliser par une réduction a une forme sans coupure. Par ailleurs, un système de calcul de lambda linéaire avec la sémantique opérationnelle, en l'absence des complexités additionnelles, a une attitude de réduction bien déterministe; même la convergence est valable malgré l'existence de ces complexités; comme à l'article de S.Abramsky*, elle est incarnée dans la correction sémantique (semantical soundness). A partir de ce stade, les stratégies de réduction en sémantique opérationnelle peuvent être arrivées à une forme normale.

Le nondeterminism est une caractéristique à éviter, parce que, un système de raisonnement doit se terminer dans chaque essaie de même séquence de raisonnement, par un résultat fixe pour chaque étape de la raisonnement; l'élimination de coupure doit suivre une voie précise pour arriver à une conclusion déterminée. Mais, pour les calculs probabilistes, une séquence d'étape de la calculation peut se terminer l'une des conclusions possibles donc, une terme peut être réduit à l'une des plusieurs formes possibles; par exemple, une terme est réduite à une forme avec une probabilité de p_1 est une autre avec une probabilité de p_2. Toutefois, un tel système peut encore être modélisé par un système de réduction déterministe; une sortie d'un système classiquement probabiliste, est encore dépend aux conditions initiales, en parlant opérationnellement, la situation de l'entrée; donc ce système est encore classiquement déterministe; la question de le représenter est une question purement logique dans le sens où les hypothèses métaphysique ne sont pas définies, donc en accord de la logique traditionnelle.

Un système quantique, d'autre part, comme indiqué au deuxième chapitre, intrinsèquement non déterministe ; système dans lequel, contrairement aux probabilités classiques, les interférences sont prises en compte, ce qui conduit à des résultats non-classiques. Par conséquent, un système de calcul quantique doit prendre en compte les attitudes quantiques qui ne sont pas présentes dans les systèmes classiques. En ce sens, la capacité d'un système de calcul à inclure des caractéristiques non déterministes devient une stratégie privilégiée pour un modèle quantique. En outre, le fait qu'un système quantique soit un paradigme qui englobe également l'informatique classique exige que ce modèle ait également une attitude de réduction déterministe. Ainsi, dans le prolongement du sous-titre précédent, un système de lambda calcul linéaire enrichi de complexités additionnelles semble être un candidat solide pour répondre à ces exigences.

Le système de calcul de A.Diaz-Caro et G.Dowek s'agit, dans cette optique, d'un enrichissement du lambda calcul typé afin de couvrir les propriétés de calcul quantique. Cet enrichissement a été fait en ajoutant des règles de projection qui représente le mesurement quantique et d'addition pour la superposition quantique à la sémantique opérationnelle. La nature non-deterministe du mesurement quantique est exprimée par la non-déterminisme réductive de la projection des deux termes de même type sur ce type. Le non-déterminisme est dû au fait que les deux termes entrant dans la projection sont du même type du fait que les paires sont commutatives sous l'addition; l'imprévisibilité de la forme sous laquelle cette réduction sera finalisée. Par conséquent, la caractéristique non déterministe de la projection n'apparaît que lorsqu'on agit sur ces paires commutatives: une paire $(t + u)$ est de type $(A \wedge A)$ et la projection de ce terme ($proj_n$ avec la notation de l'article* en sémantique opérationnelle) réduit ce terme à l'une de ces termes disons, t de type A. Par contre, la règle de projection $proj_1$ est une réduction déterministe qui est la projection des termes non superposition; cela est relié à la nature probabiliste de la réduction de la fonction d'onde par le mesurement, à l'une des vecteurs de base composées, mais ce non déterminisme n'existe pas dans le cas d'une mesure d'un vecteur de base; le résultat, c'est d'ailleurs la soi-meme du vecteur.

Les superpositions sont créés par les règles de linéarité lin_r et lin_l respectivement définies comme $t(u + v) \rightarrow (tu + tv)$ et $(t + u)v \rightarrow (tv + uv)$ et leurs analogies de produit tensoriel pour des systèmes composés $linten_r$ et $linten_l$, respectivement $t((r + s) \otimes u) \rightarrow (t(r \otimes u) + t(s \otimes u))$ et $t(u \otimes (r + s)) \rightarrow (t(u \otimes r) + t(u \otimes s))$; qui ne réduisent pas totalement, donc la forme canonique est encore une superposition. C'est-à-dire, une opération qui ne cause pas la réduction de la fonction d'onde, ne crée pas aussi une non-déterminisme de réduction; comme souhaité lors de la représentation de l'évaluation lors de la pré-mesure. Les règles de produit tensoriels ne contribuent pas aussi au non-déterminisme parallèlement pour la même raison. On peut également remarquer que le type du terme est préservé dans toutes les réductions, même dans le processus

$proj_n$ comme le garantit le théorème de réduction du sujet (Subject reduction) énoncé par les auteurs de l'article*[18].

Nous pouvons dire ici que les objets présentant un comportement quantique sont de type superposition et ne peuvent pas être dupliqués, tandis que les objets présentant un comportement classique, qui ont déjà été mesurés, sont de type vecteur de base et peuvent être dupliqués. De ce point de vue, ce système de lambda calcul linéaire représentait à la fois les évaluations qui ne changent pas la nature quantique de l'objet, comme la propriété de non-clonage, la représentation des états intriqués et leurs applications de réduction faible (weak reduction), et l'évaluation de l'état classique après la mesure, représentée par un système de réduction déterministe. Seule la représentation de la mesure nécessite une réduction non déterministe, où le caractère non déterministe de la réduction de la fonction d'onde est considéré comme l'exigence d'une transition probabiliste irréversible de $S(A)$ à A, qui ne peut être définie comme telle, parmi les deux types utilisés.

Le non-déterminisme utilisé ici est l'imprévisibilité du terme, pour répéter, du terme auquel il doit être réduit. Ce système n'est pas non-déterministe au sens d'autres sources de non-déterminisme, comme la circularité, comme l'autoréflexivité du processus de réduction ; il fournit, par exemple, le principe d'acyclicité.

Nous voyons que le paradigme quantique provoque un changement dans les hypothèses métaphysiques traditionnelles, dans la logique traditionnelle produite par le monde de l'expérience de la vie quotidienne, et dans les attentes de la théorie du calcul dérivée d'une compréhension parallèle de la nature (dans ce cas, une élimination de coupure déterministe). La différenciation des significations des

[18] [25] p.7

éléments d'un système logique et les changements syntaxiques effectués dans le but de représenter les phénomènes quantiques sont, comme le souligne Girard*[19], à l'instar de Xerxès fouettant la mer, l'un des indicateurs de la nécessité de faire passer le fonctionnement de la nature avant la réalité logique. Comme on le voit dans le travail illustré par ce mémoire, il semble avoir renoncé à fouetter la mer en rendant non-déterminisme le déterminisme d'un système linéaire de lambda calcul en définissant les superpositions comme des paires commutatives et la réduction de la projection sur les mêmes types. Le fait que la méthode de l'élimination de coupure acquiert la propriété d'imprévisibilité comme une nécessité de modélisation de la nature quantique, et qu'elle soit utilisée sous cette forme dans des applications telles que l'algorithme de téléportation, semble être en un sens un pont très important entre la théorie de l'information quantique et la logique, où la métaphysique peut être discutée expérimentalement dans la correspondance de Curry-Howard.

[19] *[27] p.2

Bibliographie

Chapitre 1:

1. Benthem, Johan (2008). The information in intuitionistic logic. *Synthese* 167 (2):251-270.
2. Christian Retoré. Logique linéaire et syntaxe des langues. Mathématiques [math]. Université de Nantes, 2002. □tel-00354041
3. Dong-Tsan Lee, C.P. Tsang, Finding relevant knowledge in a knowledge base of linear logic, Knowledge-Based Systems, Volume 10, Issue 6, 1998, Pages 359-361, ISSN 0950-7051, https://doi.org/10.1016/S0950-7051(97)00048-8.
4. Girard, Jean-Yves, Linear logic, Theoretical Computer Science, Volume 50, Issue ,1987,Pages 1-101, ISSN 0304-3975, https://doi.org/10.1016/0304-3975(87)90045-4.
5. Girard, Jean-Yves, Yves Lafont, and Paul Taylor. 1989. Proofs and Types. Cambridge Tracts in Theoretical Computer Science 7. Cambridge University Press.
6. Joseph Vidal-Rosset. Philosophie de la connaissance et logique intuitionniste. Philosophie. Université de Lorraine, 2012. □tel-01231395□
7. Laird, J.. (2002). A Deconstruction of Non-deterministic Classical Cut Elimination.
8. Marion, Mathieu & Sadrzadeh, Mehrnouche. (2004). Reasoning About Knowledge In Linear Logic: Modalities and Complexity. 10.1007/978-1-4020-2808-3_17.
9. Mihályi, Daniel & Novitzká, Valerie. (2013). What about Linear Logic in Computer Science?. Acta Polytechnica Hungarica. 10. 2013-147.
10. Nerode, A. (1990). Some lectures on intuitionistic logic. In: Odifreddi, P. (eds) Logic and Computer Science. Lecture Notes in Mathematics, vol 1429. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0093923
11. OKADA, Mitsuhiro. An introduction to linear logic: Expressiveness and phase semantics. In: *Theories of Types and Proofs*. Mathematical Society of Japan, 1998. p. 255-296.

12. OKADA Mitsuhiro, « Linear Logic and Intuitionistic Logic », *Revue internationale de philosophie*, 2004/4 (n° 230), p. 449-481. DOI : 10.3917/rip.230.0449. URL : https://www.cairn.info/revue-internationale-de-philosophie-2004-4-page-449.htm
13. Roussel, Tristan, Introduction à la Logique Linéaire, 2012
14. Samson Abramsky, Computational interpretations of linear logic, Theoretical Computer Science, Volume 111, Issues 1–2, 1993, Pages 3-57, ISSN 0304-3975, https://doi.org/10.1016/0304-3975(93)90181-R.
15. Zach, Richard. "The Significance of the Curry-Howard Isomorphism". *Philosophy of Logic and Mathematics: Proceedings of the 41st International Ludwig Wittgenstein Symposium*, edited by Gabriele M. Mras, Paul Weingartner and Bernhard Ritter, Berlin, Boston: De Gruyter, 2020, pp. 313-326. https://doi.org/10.1515/9783110657883-018

Chapitre 2 et 3:

.

16. Abbasalinejad, P., & Tebyanian, H. (2024). Quantum Entanglement Through the Lens of Paraconsistent Logic. *arXiv preprint arXiv:2405.08775*.
17. Bell JS, Aspect A. On the Einstein–Podolsky–Rosen paradox. In: *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*. Cambridge University Press; 2004:14-21.
18. Brukner, Č. Quantum causality. *Nature Phys* 10, 259–263 (2014). https://doi.org/10.1038/nphys2930
19. Bub, J. (2006). Quantum computation from a quantum logical perspective. *arXiv preprint quant-ph/0605243*.
20. Bub, Jeffrey, "Quantum Entanglement and Information", *The Stanford Encyclopedia of Philosophy* (Summer 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.), URL = <https://plato.stanford.edu/archives/sum2023/entries/qt-entangle/>.

21. Cuffaro, M. E. (2022). The philosophy of quantum computing. In *Quantum Computing in the Arts and Humanities: An Introduction to Core Concepts, Theory and Applications* (pp. 107-152). Cham: Springer International Publishing.
22. Cuffaro, Michael and Amit Hagar, "Quantum Computing", *The Stanford Encyclopedia of Philosophy* (Spring 2024 Edition), Edward N. Zalta & Uri Nodelman (eds.), URL = <https://plato.stanford.edu/archives/spr2024/entries/qt-quantcomp/>.
23. Díaz-Caro, A., & Dowek, G. (2017, November). Typing quantum superpositions and measurement. In *International Conference on Theory and Practice of Natural Computing* (pp. 281-293). Cham: Springer International Publishing.
24. Díaz-Caro, A., Dowek, G., & Rinaldi, J. P. (2019). Two linearities for quantum computing in the lambda calculus. *BioSystems*, *186*, 104012.
25. Díaz-Caro, A., Dowek, G.(2016), Quantum superpositions and projective measurement in the lambda calculus, arXiv:1601.04294v3.
26. Díaz-Caro, A., Dowek, G. Linear Lambda-Calculus is Linear. In 7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022). Leibniz International Proceedings in Informatics (LIPIcs), Volume 228, pp. 21:1-21:17, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2022) https://doi.org/10.4230/LIPIcs.FSCD.2022.21.
27. Girard J-Y. Between Logic and Quantic: a Tract. In: Ehrhard T, Girard J-Y, Ruet P, Scott P, eds. *Linear Logic in Computer Science*. London Mathematical Society Lecture Note Series. Cambridge University Press; 2004:346-381.
28. Gomatam, Ravi. (2007). Physics and Commonsense - Reassessing the connection in the light of quantum theory.
29. Hagar, Amit. (2007). Quantum Algorithms: Philosophical Lessons. Minds and Machines. 17. 233-247. 10.1007/s11023-007-9057-3.
30. Kaye, Phillip ; Laflamme, Raymond & Mosca, Michele (2006). *An Introduction to Quantum Computing*. Oxford, England: Oxford University Press UK.
31. Landsman, Klaas. (2017). Foundations of Quantum Theory. 10.1007/978-3-319-51777-3
32. Penchev, Vasil, Both Classical & Quantum Information; Both Bit & Qubit: Transcendental Time. Both Physical & Transcendental Time (April 10, 2021).

Available at SSRN: https://ssrn.com/abstract=3823665 or http://dx.doi.org/10.2139/ssrn.3823665

33. Penchev, Vasil, Gentzen's 'Cut Rule' and Quantum Measurement in Terms of Hilbert Arithmetic. Metaphor and Understanding Modeled Formally (July 28, 2022). Available at SSRN: https://ssrn.com/abstract=4174692 or http://dx.doi.org/10.2139/ssrn.4174692
34. Penchev, Vasil, Quantum Computer: Quantum Model and Reality (June 5, 2020). Available at SSRN: https://ssrn.com/abstract=3619711 or http://dx.doi.org/10.2139/ssrn.3619711