Un lambda calcul quantique avec mesure : normalisation et confluence, Encadrants: Claudia Faggian et Benoît Valiron

Gaëtan Lopez

Abstract

Subject: A quantum lambda calculus with measurement: confluence and normalization.

The aim of this project is to develop a quantum lambda calculus whose operational behavior is liberal enough to allow for parallel evaluation (in the spirit of [2]) while retaining good operational properties of lambda calculus such as confluence.

The language we have in mind follows the quantum data and classical control paradigm [1]; in order to model quantum computation, a quantum language needs to be equipped with constructs which allow to allocate qbits, to apply unitary gates and to perform measuring. In presence of measurements, the evolution of quantum computation becomes probabilistic; for this reason, it is natural to use probabilitic tools in its analysis. Our working hypothesis is to build a quantum calculus on top of the linear *probabilistic* calculus which is proposed in [3], and then investigate the features of the language and the behavior of the computation. In particular, a properties which we want to achieve is confluence. Confluence is an important property which one may expect in quantum computation; indeed, about ten years ago, two different quantum calculi with measurement and confluent have already been proposed ([4],[5]). It seems a good time to revisit the question, taking advantage of the progresses which have been done in the understanding of probabilistic computation and probabilistic rewriting.

Contents

Chapter 0

Introduction

Le calcul quantique Le calcul quantique utilise les propriétés quantiques de la matière telle que la superposition et l'intrication. Un bit quantique s'appelle un qbit.

Un qbit peut superposer deux valeurs à la fois : 0 ou 1. Tant qu'on ne l'a pas mesuré, celui-ci peut valoir 0 ou 1. Pour opérer sur les bits, on utilise des portes logiques. Pour opérer sur des qbits, on utilisera des portes quantiques, qui correspondent à des opérateurs unitaires. Celles-ci opère sur toutes les valeurs possibles du qbit ou des qbits concernés. Ainsi, une porte quantique traite, en une étape de calcul, la multitude des valeurs possibles d'une mémoire de plusieurs qbits.

Le modèle standard Il y a plusieurs modèle de calcul quantique. Un modèle standard est celui basé sur de la mémoire quantique et un contrôle classique (modèle QRAM). L'intuition est la suivante : le langage devrait pouvoir exprimer n'importe quel calcul classique booléen; il devrait contenir la construction des paires, il devrait contenir des termes constructeurs pour exprimer la création d'un bit quantique (qbit), les unitaires et la mesure. En plus, il faut des contraintes pour interdire la duplication quand la mémoire n'est pas duplicable.

Dans le modèle standard, au delà des constructions usuelles, le programmeur a accès à plusieurs opération sur la mémoire quantique : initialisation de qbits, applications de portes unitaires, et possiblement de la mesure. La deux premières opérations sont *purement quantique*, la dernière, quant à elle, amène un comportement *probabiliste*. Discutons un peu plus de la mémoire quantique.

Une mémoire quantique possède une superposition de plusieurs états. Par exemple, si l'on prend une mémoire composé de 3 qbit, alors cette mémoire peut superposer l'ensemble des $|xyz\rangle$, tel que x, y , z représente la valeur d'un qbit.

L'information quantique ne peut pas être clonée (dû aux propriétés de la physique), ainsi les données utilisées sont linéaires.

La mesure d'un qbit permet de retirer la superposition d'état d'un qbit. On a la valeur mesurée de celui-ci : 0 ou 1. Seulement, il n'est pas possible de "prédire" la valeur avant la mesure. Ainsi l'opération de la mesure d'un qbit introduit un comportement probabiliste. Un tel qbit peut être représenté comme une combinaison linéaire de deux vecteurs unitaires : $|0\rangle$ et $|1\rangle$, à coefficient complexe.

Le lambda-calcul quantique Le lambda calcul est un modèle universel pour le calcul classique. Le lambda calcul quantique est un modèle universel le calcul quantique.

Nous suivons ici Quantum Data et Classical Control paradigm, proposé par Peter Selinger et Benoît Valiron [2].

Les contrôles classiques sont assurés les constructeurs standard du lambda calcul, tandis que pour gérer la mémoire, on utilise constructeurs qui correspondent aux opérations quantiques :

- un terme qui sert à initialiser un qbit dans la mémoire
- un terme pour chaque porte unitaire (qui décrivent les opérations unitaires faites sur les qbits)

À cela on peut rajouter la mesure d'un qbit, qui va amener aux probabilités : soit le qbit est mesuré à 0 soit il est mesuré à 1. Ce qui amène ainsi à une réduction probabiliste.

Les qbits sont représentés dans le termes par des registres. Ceci amène à séparer la notion de qbit (dans la mémoire) de son registre. On ne peut pas cloner les données d'un registre, ainsi un calcul linéaire est adapté à une telle construction.

Nos questions

Le but de ce projet est de développer un lambda calcul quantique, tel que son comportement opérationnel soit assez libre pour qu'il autorise une évaluation parallèle (dans l'esprit de [2]), tout en gardant de bonnes propriétés opérationnel du lambda calcul, comme la confluence.

Le langage, dont nous parlions suit le "quantum data and classical control paradigm" [1]; en premier pour modéliser le calcul quantique, un langage quantique doit être équipé avec des constructeurs, qui alloue des qbits, pour appliquer des portes unitaires et réaliser la mesure. En présence de la mesure, l'évolution d'un calcul quantique devient probabiliste; pour cette raison, il est naturel d'utiliser des outils probabiliste dans son analyse.

Notre hypothèse de travail est de construire un lambda calcul sur le calcul probabiliste et linéaire, qui est proposé en [3], et ensuite de rechercher les caractéristiques du langage, ainsi que le comportement du calcul. En particulier, une propriété qui nous conduira à la confluence.

La confluence est une importante propriété que l'on espère en calcul quantique; en effet, il y a 10 ans, 2 calculs quantiques (avec mesure) différents et confluents ont déjà été proposé ([4],[5]). Cela semble un bon moment pour revisiter la question, en prenant avantage du progrès qui a été fait sur la compréhension du calcul probabiliste et la réécriture probabiliste.

Contenu et Contributions

Dans ce stage, on a développé 3 calculs quantiques qui nous détaillerons ici.

Dans le chapitre 1, nous énoncerons les connaissances nécessaires à la bonne compréhension de ce document : système de réécriture, calcul de Simpson, probabilité, distribution, produit tensoriel et calcul quantique.

Dans le chapitre 2, nous introduisons un lambda calcul quantique pur linéaire, appelé Q, basé sur le calcul de Simpson [8]. Le lambda calcul est linéaire et les opérations quantiques sont purs (c'est à dire, initialisation de qbit et application de porte quantique). Nous définissons les notions de mémoires, de termes et d'états. La notion de réduction est décomposé en réduction quantique et réduction beta-linéaire. Les réductions quantiques exprime l'action d'une porte quantique à une ou deux entrées et l'initialisation d'un qbit avec son registre. Pour finir, nous prouverons que le le système de réécriture $Q := (\mathscr{E}, \rightarrow_Q)$ est confluent.

Dans le chapitre 3, nous définissons le calcul Q^{meas}, en enrichissant le calcul Q avec la mesure d'un qbit. Donc nous ajouterons un nouveau constructeur (meas) à notre précédent lambda calcul. L'ajout d'un nouveau constructeur de mesure nous donnera une nouvelle réduction, une réduction probabiliste. De même que pour le chapitre 2, le système de réécriture $Q^{meas} := (MDST(\mathscr{E}^{meas}), \rightrightarrows_{Q^{meas}})$ est confluent, pour une notion opportune de confluence. On ne considère pas les états, mais plutôt les distributions d'états (plus précisément, des multidistributions, comme on va le voir).

Dans le chapitre 4, finalement, nous définissons le calcul $Q^!$ en rajoutant la récursion et donc la possibilité de dupliquer les termes. Cette extension est délicate, du fait que l'on ne peut pas dupliquer les qbits; donc un registre ne pourra pas être dupliqué. Encore une fois, le calcul est basé sur le calcul de Simpson [8]. Un autre aspect important est que la récursion va permettre de créer un comportement infinitaire et ainsi de diverger. Cela nous amène à étudier la terminaison probabiliste.

Dans le chapitre 5, nous étudierons le passage à la limite de ce calcul, et la terminaison probabiliste, en suivant [6]. Nous rappelons qu'un programme est "Almost Sure Terminating" (Termine presque sûrement) si la probabilité d'atteindre une forme normale est 1. Ce degré de certitude peut ne pas être atteint avec aucun nombre fini d'étape, comme dans l'exemple que l'on construit dans la Section 4.4.1..

Pour conclure, le chapitre 6 résume l'ensemble des trois calculs que nous avons développé dans ce stage : $Q, Q^{meas}, Q^!$.

Chapter 1

Background

1.1 Probabilité et multidistribution

1.1.1 Bases sur les probabilités discrètes

Un espace de probabilité est donné par la paire (Ω, μ), où Ω est un ensemble dénombrable, et μ est une distribution de probilité discrète sur Ω, i.e. est une fonction de Ω dans $[0,1] \subset \mathbb{R}$ tel que $\|\mu\| := \sum_{\omega \in \Omega} \mu(\omega) = 1$.
Dans ce cas, une mesure de probabilité est assignée à n'importe quel sous-ensemble $\mathscr{A} \subset \Omega$ comme ceci $\mu(\mathscr{A}) = \sum_{\omega \in \mathscr{A}} \mu(\omega)$. Dans ce langage de théorie des probabilités, un sous-ensemble de Ω est appelé évènement.
Soit (Ω, μ) comme au dessus. N'importe quel fonction $F : \Omega \to \Delta$, où Δ est un autre ensemble dénombrable, induit une distribution de probabilité μ^F sur Δ par composition : $\mu^F(d \in \Delta) := \mu(F^{-1}(d))$ i.e. $\mu\{\omega \in \Omega \mid F(\omega) = d\}$. Dans ce langage de théorie de probabilité, F est appelé un variable aléatoire discrète sur (Ω, μ).

Exemple. 1) Considérons une lancer de dés équilibré. L'espace des sorties possibles est l'ensemble $\Omega = \{1,2,3,4,5,6\}$.
La mesure de probalité μ de chaque sortie est $\frac{1}{6}$. L'évènement "Le résultat est impair" est le sous-ensemble $\mathscr{O} = \{1,3,5\}$, sa mesure de probabilité est $\mu(\mathscr{O}) = \frac{1}{2}$.
2) Soit Δ un ensemble à deux éléments $\{Pair, Impair\}$, et F la fonction basique de Ω vers Δ. F induit une distribution sur Δ, avec $\mu^F(Pair) = \frac{1}{2}$ et $\mu^F(Impair) = \frac{1}{2}$.

1.1.2 Sous-distribution et $DST(\Omega)$

Étant donné un ensemble dénombrable Ω, une fonction $\mu : \Omega \to [0,1]$ est une sous-distribution de probabilité si $\|\mu\| \leqslant 1$. On écrit $DST(\Omega)$ pour l'ensemble des sous-distributions sur Ω. Avec un petit abus de langage, nous utiliserons le terme distribution aussi pour les sous-distribution.

Ordre : $DST(\Omega)$ est équipée avec la relation d'ordre standard des fonctions : $\mu \leqslant \rho$ si $\mu(\omega) \leqslant \rho(\omega)$ pour tout $\omega \in \Omega$.

Support : Le support de μ est $Supp(\mu) = \{\omega \in \Omega \mid \mu(\omega) > 0\}$

Représentation : Nous représentons une distribution en indiquant explicitement le support, et la probabilité assigné à chaque élément par μ. On écrit $\mu = \{a_0^{p_0}, a_1^{p_1}, ..., a_n^{p_n}\}$ si $\mu(a_0) = p_0, ..., \mu(a_n) = p_n$ et $\mu(a_j) = 0$ sinon.

1.1.3 Multidistributions

Pour syntaxiquement, représenté l'évolution globale d'un système probabiliste, nous comptons sur la notion de multidistributions.
Un multiensemble est une liste (finie) d'éléments, modulo réarrangement, i.e. $[a, b, a] = [a, a, b] \doteq [a, b]$. Le multiensemble [a,a,b] a 3 éléments. Soit $\mathscr{X}$ un ensemble dénombrable, et m un multiensemble de paires de la forme pM, avec $p \in]0, 1]$ et $M \in \mathscr{X}$.
Nous appelons $m = [p_i M_i \mid i \in I]$ (l'ensemble(-index) I numérote les éléments de m) une multidistribution sur $\mathscr{X}$ si $\sum_{i \in I} p_i \leqslant 1$, on note $MDST(\mathscr{X})$ l'ensemble des multidistributions sur $\mathscr{X}$.
On note la multidistribution $[1M]$ simplement $[M]$. La somme de multidistribution est exprimé par $+$, c'est l'équivalent de concaténation de liste. Le produit $q.M$ entre un scalaire q et une multidistribution est défini point par point : $q.[p_1 M_1, ..., p_n M_n] = [(qp_1)M_1, ..., (qp_n)M_n]$. Intuitivement, une multidistribution $m \in MDST(\mathscr{X})$ est la représentation syntaxique d'un espace de probabilité discrète où à chaque élément de l'espace est associé une probabilité et un terme de $\mathscr{X}$. À la multidistribution $m = [p_i M_i \mid i \in I]$, on associe une distribution de probabilité $\mu \in DST(\mathscr{X})$ comme suivant :

$$\mu(M) = \begin{cases} p \text{ si } p = \sum_{i \in I} \text{ tel que } M_i = M \\ 0 \text{ sinon} \end{cases}$$

et on appelle μ la distribution de probabilité associée à m.

Exemple. (Distribution vs Multidistribution) Si $m = [\frac{1}{2}a, \frac{1}{2}a]$, alors $\mu = \{a^1\}$. observons la différence entre distribution et multidistribution : si $m' = [1a]$, alors $m \neq m'$, mais $\mu = \mu'$.

1.2 Système de réécriture

Un système de réécriture est une paire $C = (C, \to)$ formé d'un ensemble C et d'une relation binaire $\to$ sur C (appelé réduction), ses paires sont écrites $t \to s$ $(t, s) \in C^2$ et sont appelés étapes; $\to^*$ (respectivement $\to_=$) désigne la clôture transitive (respectivement réflexive) de $\to$.
On écrit $c \not\to$ si il n'existe pas de u tel que $c \to u$; dans ce cas-là, c est en forme normale.

Définition 1.2.1 (Confluence)**.** $\forall (s, r) \in C^2$ avec s $^* \leftarrow m \to^*$ r, il existe t_0 tel que $s \to^* t_0$, $r \to^* t_0$.

Définition 1.2.2 (Propriété du diamant)**.** $\forall(s,r) \in C^2$ avec $s \leftarrow m \rightarrow r$, il existe t_0 tel que $s \rightarrow^* t_0$, $r \rightarrow^* t_0$.

Est bien connu :

Proposition 1.2.3. *La propriété du diamant implique la confluence.*

Définition 1.2.4 (faiblement/fortement normalisant)**.** Un terme est fortement normalisant s'il ne possède pas de séquence de réécriture infinie.
Un temer est faiblement normalisant s'il possède une forme normale.

Une propriété plus fine de confluence a été observé par Newman, celle de la Descente Randomisée :

Définition 1.2.5 (Descente Randomisée)**.** Une réduction a la propriété de la Descente Randomisée si pour n'importe quel terme t qui a une forme normale, alors chaque séquence de réécriture à partir de t mène à cette forme normale, de plus, toutes ces séquences ont la même longueurs.

La propriété mieux connue qui implique la RD, observé par Newman, est la suivante :

Définition 1.2.6 (quasi-diamant)**.** si $s_1 \leftarrow t \rightarrow s_2$ alors :

- soit $s_1 = s_2$
- soit $s_1 \rightarrow u$ et $s_2 \rightarrow u$ pour un certain u

En conséquence

Proposition 1.2.7. *La propriété du quasi-diamant implique:*

- *la confluence;*
- *si un terme est faiblement normalisant alors il est fortement normalisant.*

1.3 Calcul de Simpson

Dans cette section, on introduit un lambda-calcul sans typage. Ses ingrédients principales sont : l'application MN, l'abstraction linéaire $\lambda x.M$, l'abstraction non-linéaire $\lambda^! x.M$, qui requière que son argument soit suspendu par un bang, et les bangs eux-même $!M$.
Formellement, les termes bruts M,N,... sont formés de variables x,y,... selon la grammaire suivante :

$$M, N ::= x \mid MN \mid \lambda x.M \mid \lambda^! x.M \mid !M$$

La variable x est lié dans les deux termes $\lambda x.M$ et $\lambda^! x.M$. On écrit $\equiv$ pour l'égalité syntaxique de terme modulo α-équivalence.
On dit que x est linéaire dans M si x apparaît libre exactement une fois dans M, et, de plus, cette occurrence libre de x n'est pas à l'intérieur d'un bang. Un terme M est dit linéaire si, dans chaque sous-terme de M de forme $\lambda x.M_0$, x est linéaire dans M_0.

1.4 Introduction au calcul quantique

Soit H un espace de Hilbert de dimension 2 : on choisit une base orthonormée : $|0\rangle$ et $|1\rangle$.
Donc en particulier, $\| |x\rangle \| = 1$ et $\langle |0\rangle \mid |1\rangle \rangle = 0$.
Un qbit est un vecteur de norme 1 dans notre espace de Hilbert H :

$$\alpha |0\rangle + \beta |1\rangle$$

Comme il est de norme 1, on a donc $|\alpha|^2 + |\beta|^2 = 1$, c'est à dire qu'on peut regarder α et β comme des probabilités.

Un qbit est localisé dans l'espace: c'est l'état d'un photon, ou d'un spin, ou de n'importe quelle propriété quantique d'une particule localisée quelque part (en A par exemple).
Si je prends une deuxième particule en B: elle aussi a un état dans H.
Si je prends le système composé de A et B, ce système a un état non pas dans le produit cartésien, mais le produit tensoriel $H \otimes H$. On peut le définir comme l'espace engendré par $|x\rangle \otimes |y\rangle$ avec $|x\rangle$ une base de A et $|y\rangle$ une base de B.
On note $|0\rangle \otimes |1\rangle = |01\rangle$.
Cette construction est générique: si E a pour base $\{e_i\}_{i=1..n}$ et F a pour base $\{f_j\}_{j=1..k}$, alors $E \otimes F$ a pour dimension $k \times n$ et on peut représenter sa base avec $\{e_i \otimes f_j\}_{i=1..n,j=1..k}$.
Si j'ai un opérateur $A : E \to E$, je peux fabriquer un opérateur $A \otimes I : E \otimes F \to E \otimes F$.
Son action :

$$(A \otimes I)(e_i \otimes f_j) = \sum_k a_{i,k} e_k \otimes f_j$$

quand $Ae_i = \sum_k a_{i,k} e_k$ et I l'identité sur F.

On a envie d'écrire : $\sum_k a_{i,k} e_k \otimes f_j = \left(\sum_k a_{i,k} e_k \right) \otimes f_j = (Ae_i) \otimes f_j$.
Il suffit de regarder $\otimes$ comme une opération $\otimes : E \times F \to E \otimes F$ bilinéaire.
Donc du coup,

$$(v_1 + v_2) \otimes (w_1 + w_2) = v_1 \otimes w_1 + v_1 \otimes w_2 + v_2 \otimes w_1 + v_2 \otimes w_2$$

et

$$(\alpha v) \otimes (\beta w) = (\alpha\beta)\,(v \otimes w)$$

Ce qui permet de définir littéralement $(A \otimes I)\,(v \otimes w) = (Av) \otimes w$.
Donc reprenons nos qbits.
Si on en a n, l'espace d'état du système est $H \otimes H \otimes ... \otimes H = H^{\otimes n}$.
Un vecteur là-dedans a la forme :

$$Q = \sum_{b=b_1...b_n} \alpha_b |b\rangle$$

On peut le décomposer pour mettre en relief le qbit numéro i si on veut :

$$Q = \sum_{b=b_1...b_{i-1},b'=b_{i+1}...b_n,x=0ou1} \alpha_{bxb'} |b\rangle \otimes |x\rangle \otimes |b'\rangle$$

Du coup, si j'applique $B = I^{i-1} \otimes A \otimes I^{n-i}$ sur Q (A est un opérateur sur 1 seul qbit) :

$$\begin{aligned}
BQ &= \sum_{b=b_1 \ldots b_{i-1}, b'=b_{i+1} \ldots b_n, x=0 ou 1} \alpha_{bxb'} B\left(|b\rangle \otimes |x\rangle \otimes |b'\rangle\right) \\
&= \sum_{b=b_1 \ldots b_{i-1}, b'=b_{i+1} \ldots b_n, x=0 ou 1} \alpha_{bxb'} \left(I^{i-1} \otimes A \otimes I^{n-i}\right)\left(|b\rangle \otimes |x\rangle \otimes |b'\rangle\right) \\
&= \sum_{b=b_1 \ldots b_{i-1}, b'=b_{i+1} \ldots b_n, x=0 ou 1} \alpha_{bxb'} \left(I^{i-1} |b\rangle\right) \otimes \left(A |x\rangle\right) \otimes \left(I^{n-i} |b'\rangle\right) \\
&= \sum_{b=b_1 \ldots b_{i-1}, b'=b_{i+1} \ldots b_n, x=0 ou 1} \alpha_{bxb'} |b\rangle \otimes \left(A |x\rangle\right) \otimes |b'\rangle
\end{aligned}$$

Dans la théorie équationnelle, on a:

$$(v_1 + v_2) \otimes (w_1 + w_2) = v_1 \otimes w_1 + v_1 \otimes w_2 + v_2 \otimes w_1 + v_2 \otimes w_2$$

$$(\alpha v) \otimes (\beta w) = (\alpha\beta)\,(v \otimes w)$$

$$(A \otimes B)\,(v \otimes w) = (Av) \otimes (Bw)$$

Dernière chose: l'ordre des vecteurs de base. Comme on travaille avec des listes de booléens, les vecteurs sont "rangés" dans l'ordre lexicographique. Donc quand on écrit :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

l'ordre des éléments de la base sont $|0\rangle$ puis $|1\rangle$, première colonne = $|0\rangle$ par exemple

$$M = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}$$

	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|00\rangle$	a	b	c	d
$\|01\rangle$	e	f	g	h
$\|10\rangle$	i	j	k	l
$\|11\rangle$	m	n	o	p

L'action de M su $|00\rangle$ rend le vecteur colonne correspondant, donc :

$$a\,|00\rangle + e\,|01\rangle + i\,|10\rangle + m\,|11\rangle$$

La matrice correspondant à $I \otimes A$ (ou I et A sont sur 1 qbit), la matrice est : $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ en représentation par bloc.
Et $A \otimes I$ (quand $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$)

$(A \otimes I)\,|00\rangle = (A \otimes I)\,(|0\rangle \otimes |0\rangle) = (A\,|0\rangle) \otimes |0\rangle = (a\,|0\rangle + c\,|1\rangle) \otimes |0\rangle = a\,|00\rangle + c\,|10\rangle$
$(A \otimes I)\,|01\rangle = (A \otimes I)\,(|0\rangle \otimes |1\rangle) = (A\,|0\rangle) \otimes |1\rangle = (a\,|0\rangle + c\,|1\rangle) \otimes |1\rangle = a\,|01\rangle + c\,|11\rangle$

	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|00\rangle$	a	0	b	0
$\|01\rangle$	0	a	0	b
$\|10\rangle$	c	0	d	0
$\|11\rangle$	0	c	0	d

$$\begin{pmatrix} aI & bI \\ cI & dI \end{pmatrix}$$

Un exemple d'opérateur sur deux qbits qui n'est pas un tenseur de bidules :
Control-Not (CNOT) : $\begin{cases} |0x\rangle \mapsto |0x\rangle \\ |1x\rangle \mapsto |1\bar{x}\rangle \end{cases}$

	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|00\rangle$	1	0	0	0
$\|01\rangle$	0	1	0	0
$\|10\rangle$	0	0	0	1
$\|11\rangle$	0	0	1	0

par bloc :

$$\begin{pmatrix} I & 0 \\ 0 & bitflip \end{pmatrix}$$

Nota : un vecteur de $H \otimes H$ n'est pas nécessairement sous la forme $v \otimes w$!
Exemple : $|00\rangle + |11\rangle$.

Une porte quantique est une opération sur un ou plusierus qbits. Elle est réversible et préserve la mesure. Dans ce document, nous ne verrons que des portes quantiques opérant sur 1 ou 2 qbits.
Ainsi elle peut être représentée par une matrice unitaire ($A \times \bar{A}^t = I$) à coefficients complexes.

Exemple. Porte d'Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Porte Control-Not

$$CNOT = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Chapter 2

Calcul quantique pur linéaire

Nous définissons ici un langage quantique pur linéaire que l'on dénote Q. Nous allons donc reprendre

2.1 Langage

Un programme quantique est donné par une paire de terme et mémoire quantique, nous appellerons une telle paire, un état. La relation de réduction réécrira donc un état en un état.

Nous définissons les termes de notre langage :

Définition 2.1.1 (termes $\mathscr{T}$)**.**

$$M, N ::= x \mid \lambda x.M \mid MN \mid U_A \mid r_i \mid q_{init}$$

On note $\mathscr{T}$, l'ensemble des termes.

Les termes x , $\lambda x.M$ et MN ont l'intérêt usuel du lambda calcul (les variables, l'abstraction linéaire ici).
r_i désigne le registre lié à un qbit ($i \in \mathbb{N}$), c'est le registre i.
q_{init} nous sert à rajouter de la mémoire quantique, et U_A à opérer sur la mémoire quantique en fonction de A.

Pour définir la mémoire quantique, nous avons besoin de la notion de registre.

Définition 2.1.2 (Registre d'un terme)**.** Les registres d'un terme est l'ensemble de ses numéros de registres.

Exemple. (1) si $M_1 = r_1\ y\ r_4$ alors $RE(M_1) = \{1; 4\}$.
(2) si $M_2 = \lambda z.r_3 z$ alors $RE(M_2) = \{3\}$.

Nous pouvons donc maintenant définir la mémoire quantique.

Définition 2.1.3 (mémoire)**.** Soit $n \in \mathbb{N}^*$, une mémoire Q_n de taille n est défini par :

$$Q_n = \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b\rangle \; avec \begin{cases} b \in \{0,1\}^n \\ \sum_b |\alpha_b|^2 = 1 \end{cases}$$

On note $\mathscr{Q}$, l'ensemble des mémoires.

Exemple. (1) Si $Q_1 = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

(2) si $Q_2 = \frac{1}{2}|00\rangle + \frac{1}{2}i|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}i|11\rangle$.

(3) si $Q_3 = 0,8|101\rangle + 0,6|001\rangle$.

2.1.1 Bonne formation de termes

Nos termes actuels ne sont pas linéaire, de plus, un même registre peut apparaître plusieurs fois dans un même terme. Il nous faut donc introduire des règles pour que nos termes soit correctes par rapport à nos attentes.

Définition 2.1.4 (Bonne formation des termes de $\mathscr{T}$)**.** Soit $M \in \mathscr{T}$, on définit $\vdash M$ (M est un terme bien formé / un terme valide) si :

- tout sous-terme de M de la forme $\lambda x.M_0$, on a x qui est linéaire dans M_0
- pour chaque registre i de M, le registre i n'apparaît qu'une seule fois

Exemple. (1)$\vdash r_0 r_1 q_{init}$
(2) $\nvdash r_0 r_0$
(3)$\vdash xxy$
(4) $\nvdash \lambda x.xxy$
(5)$\vdash (U_H r_4)$

2.1.2 Paires

Dans notre langage, nous avons besoin des paires, pour par exemple, utiliser les portes agissant sur plusieurs qbits. Au lieu d'ajouter un nouveau constructeur, formulons une synthaxe "paire" avec nos termes existants.

Définition 2.1.5 (constructeur de paire)**.** On définit $\langle \cdot, \cdot \rangle$ comme étant :

$$\langle a, b \rangle := \lambda f.fab$$

avec la condition que f n'apparaisse pas libre dans a ni dans b.

Exemple. (1) $\langle r_0, r_1 \rangle = \lambda f.f\ r_0\ r_1$

De même que le constructeur, formulons un destructeur de paire avec nos termes. On définit le terme suivant, qui permet de récupérer les coordonnées x et y d'une paire M, puis de créer un nouveau terme N avec ces coordonnées, on écrit :

Définition 2.1.6 (destructeur de paire)**.**

$$let\langle x, y \rangle = M\ in\ N$$

comme sucre syntaxique pour :

$$M(\lambda x.\lambda y.N)$$

2.2 Sémantique opérationnelle

Dans cette section, nous allons définir le système de réécriture $Q = (\mathscr{E}, \rightarrow_Q)$, composé de l'ensemble des états et d'une réduction $\rightarrow_Q$.

2.2.1 Etat

Maintenant, nous avons la notion de terme et de mémoire, définissons les états. Pour cela, on a besoin d'avoir :

- certaine propriété sur nos termes (linéarité du λ, pas de duplication de registre), ce qui est assuré par une bonne formation du terme
- une correspondance entre mémoire et terme

Définition 2.2.1 (état)**.** Un état est un couple $[Q_n, M]$ avec $Q_n \in \mathscr{Q}$ (de taille $n \in \mathbb{N}$) et $M \in \mathscr{T}$, tel que :

- $\vdash M$, c'est à dire que M est bien formé, comme défini en (2.1.6).
- $RE\,(M) = \{k \in \mathbb{N} \mid 0 \leqslant k \leqslant n-1\}$

Exemple. (1) $[0,5\,|00\rangle + 0,5\,|01\rangle + 0,4\,|10\rangle + 0,6\,|11\rangle\,, r_0\ \ (U_H\ r_1)]$
(2) $[|00\rangle\,, \lambda x.r_1\ x\ r_0]$
(3) $[0,8\,|00\rangle + 0,6\,|10\rangle\,, q_{init}\ r_0\ r_1]$

Comme pour les termes qui sont α-équivalents, on a besoin de définir une équivalence pour les états.
En effet, prenons l'état $[, \langle H\ q_{init}, q_{init}\rangle]$ (H étant la porte d'Hadamard), on peut alors initialiser de deux façon différentes en réduisant le terme de la 1ère coordonnée de la paire puis celui de la deuxième ou inversement.
Ce qui nous donnera deux états possibles :

- soit $[|0\rangle \otimes |0\rangle\,, \langle H\ r_0, r_1\rangle]$
- soit $[|0\rangle \otimes |0\rangle\,, \langle H\ r_1, r_0\rangle]$

Les termes de chaque état sont les mêmes, à permutation des registres près.
Cependant, si l'on permute les registres, il ne faut pas oublier de permuter aussi la mémoire (les qbit correspondants).
En effet, si l'on applique la porte quantique dans ces deux états cela nous donne :

- soit $\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle\,, \langle r_0, r_1\rangle\right]$
- soit $\left[|0\rangle \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \langle r_1, r_0\rangle\right]$

Faire une équivalence de terme (pour les numéros de registres) ne suffit pas, il nous faut faire de même pour la mémoire. Nous allons donc définir la permutation de registres :

- dans un terme
- dans une mémoire

Définition 2.2.2 (substitution de registre dans un terme)**.** Soit $\sigma \in S_n$, soit $M \in \mathscr{T}$, on définie M^σ, par :
$\Rightarrow$ si $M = r_i$, $M^\sigma = r_{\sigma(i)}$
$\Rightarrow$ si $M = x$ ou q_{init} ou U, $M^\sigma = M$
$\Rightarrow$ si $M = \lambda x.M_0$, $M^\sigma = \lambda x.{M_0}^\sigma$
$\Rightarrow$ si $M = OP$, $M^\sigma = O^\sigma P^\sigma$

Exemple. (1) Soit $\sigma = (0\ 1)$ et $M = \langle H\ r_0, r_1\rangle$, on a $M^\sigma = \langle H\ r_1, r_0\rangle$

Définition 2.2.3 (substitution de qbit dans une mémoire)**.** Soit $\sigma \in S_n$, soit Q_n ($= \sum_{b=(b_0,\dots,b_{n-1})} \alpha_b |b\rangle$ avec $b \in \{0,1\}^n$) une mémoire, on définie ${Q_n}^\sigma$ par :

$$ {Q_n}^\sigma = \sum_{b'=(b_{\sigma(0)},\dots,b_{\sigma(n-1)})} \alpha_b |b'\rangle $$

Exemple. (1) Soit $\sigma = (0\ 1)$ et $Q = \frac{|00\rangle}{\sqrt{2}} + \frac{|10\rangle}{\sqrt{2}}$, on a $Q^\sigma = \frac{|00\rangle}{\sqrt{2}} + \frac{|01\rangle}{\sqrt{2}}$

Maintenant que l'on a défini ces deux notions, on peut alors définir notre équivalence d'état.
Cette équivalence lie des états qui auraient un même terme et mémoire en permutant les registres.

Définition 2.2.4 (σ-équivalence pour état)**.** Soit $e = [Q, M]$ et $e_0 = [Q', M']$, on appelle σ-équivalence la relation binaire définie par $e \equiv_\sigma e_0$ ssi il existe une permutation σ_0 tel $Q^{\sigma_0} = Q'$ et $M^{\sigma_0} = M'$.

Exemple. $\left[\frac{8}{10}|01\rangle + \frac{6}{10}|10\rangle, r_0\ r_1\right]$ et $\left[\frac{6}{10}|01\rangle + \frac{8}{10}|10\rangle, r_1\ r_0\right]$ sont équivalents.

Proposition 2.2.5. *L'σ-équivalence est une relation d'équivalence.*

Proof. (1) Soit $e = [Q_n, M]$.
Soit id, l'identité sur S_n, on a :

$$\begin{aligned} {Q_n}^{id} &= \sum_{b'=(b_{id(0)},\dots,b_{id(n-1)})} \alpha_b |b'\rangle \\ &= \sum_{b'=(b_0,\dots,b_{n-1})} \alpha_b |b'\rangle \\ &= \sum_{b=(b_0,\dots,b_{n-1})} \alpha_b |b\rangle \\ &= Q_n \end{aligned}$$

De plus, par induction, $M^{id} = M$.
On a donc $e \equiv_\sigma e$.

(2) Soit e et e' tel que $(e, e') \in \mathscr{E}$ et que $e \equiv_\sigma e'$. Posons $e = [Q_n, M]$ et $e' = [Q'_n, M']$.
On a $e \equiv_\sigma e'$ donc il existe σ_0 tel que :
- ${Q_n}^{\sigma_0} = Q'_n$
- $M^{\sigma_0} = M'$

Par ces deux inégalités et induction sur les termes et les mémoires, on obtient que $e' \equiv_\sigma e$ par la permutation σ_0^{-1} en appliquant σ_0^{-1} de part et d'autre de chacune des égalités.

(3) Soit $(e_0, e_1, e2) \in \mathscr{E}$, tel que $e_0 \equiv_\sigma e_1$ et que $e_1 \equiv_\sigma e_2$.
On a donc :
- $e_0 \equiv_\sigma e_1$ pour une certaine σ_0
- $e_1 \equiv_\sigma e_2$ pour une certaine σ_1

La bonne permutation est pour que $e_0 \equiv_\sigma e_2$ est $\sigma_1 \circ \sigma_0$. □

Ceci est une notation pour alléger l'écriture des réductions.

Notation. Soit $n \in \mathbb{N}^*$, on définit $\sigma_{i,j} \in S_n$ comme étant la permutation définie par :

$$\begin{gathered} 0 \longmapsto i \\ 1 \longmapsto j \\ i \longmapsto 0 \\ j \longmapsto 1 \\ k \longmapsto k \text{ sinon} \end{gathered}$$

2.2.2 Réduction

La relation $\to_Q$ est composé de plusieurs réductions. Nous avons d'une part la beta-réduction linéaire, qui substitue une variable linéaire par un terme, et d'autre part les réductions quantiques.
Les réductions quantiques sont composés de :

- $\to_q$, permettant d'introduire un nouveau registre
- $\to_{U_A^{(1)}}$, traduisant l'effet de d'une porte quantique à 1 entrée sur la mémoire
- $\to_{U_A^{(2)}}$, traduisant l'effet de d'une porte quantique à 2 entrée sur la mémoire

2.2.3 Relation $\to_Q$

Pour définir, la beta-réduction, donnons d'abord la définition d'une substitution de variable par un terme.

Définition 2.2.6 (substitution de variable par un terme)**.** Pour toute variable x et tous $(M, N) \in \mathscr{T}^2$, la substitution simple M[x := N] de N à x dans M se laisse définir par induction structurelle sur M à l'aide des clauses suivantes :

$\Rightarrow$Si $M = x$, alors $M\,[x := N] = N$.
$\Rightarrow$Si M est une variable $\neq$ x, alors $M\,[x := N] = M$.
$\Rightarrow$Si $M = \lambda x.M_0$, alors $M\,[x := N] = M$.
$\Rightarrow$Si $M = \lambda y.M_0$ avec $y \neq x$, alors $M\,[x := N] = \lambda y.M_0\,[x := N]$.
$\Rightarrow$Si $M = M_1 M_2$, alors $M\,[x := N] = M_1\,[x := N]\,M_2\,[x := N]$.

Le contexte de surface nous permets d'écrire les réductions avec la clôture contextuelle. On l'appelle contexte de surface et non contexte car plus tard, on s'interdira de réduire nos termes lorsqu'ils sont formés d'une certaine façon.

Définition 2.2.7 (Contexte de Surface)**.** On définit le contexte de surface par induction :

$$\mathbf{S} ::= \square \mid \lambda x.S \mid SN \mid MS$$

Soit M un terme, et un contexte de Surface $\mathbf{S}$ (contenant uniquement un seul $\square$), on note $\mathbf{S}\,(M)$ le terme $\mathbf{S}\,[\square := M]$.

Définition 2.2.8 (réduction $\rightarrow$)**.** On note $\rightarrow_Q$ la plus petite relation binaire sur l'ensemble des classes d'σ-équivalence des états, (c'est-à-dire l'intersection des relations binaires sur l'ensemble des classes d'σ-équivalence des états), telle que pour toute variable x et tous M, N termes :
- $[Q_n, \mathbf{S}\,((\lambda x.M)\,N)] \rightarrow_\beta [Q_n, \mathbf{S}\,(M\,[x := N])]$ (réduction β)
- $[Q_n, \mathbf{S}\,(q_{init})] \rightarrow_q [Q_n \otimes |0\rangle\,, \mathbf{S}\,(r_n)]$ (réduction de q_{init})
- $[Q_n, \mathbf{S}\,(U_A\ r_i)] \rightarrow_{U_A^{(1)}} [I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n, \mathbf{S}\,(r_i)]$ (réduction de U : $qbit \rightarrow qbit$)
- $[Q_n, \mathbf{S}\,(U_A\ \langle r_i, r_j\rangle)] \rightarrow_{U_A^{(2)}} \left[(A \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}\,, \mathbf{S}\,(\langle r_i, r_j\rangle)\right]$ (réduction de U : $qbit \times qbit \rightarrow qbit \times qbit$)

On a donc $\rightarrow_Q = \rightarrow_\beta \cup \rightarrow_q \cup \rightarrow_{U_A^{(1)}} \cup \rightarrow_{U_A^{(2)}}$.

Notation. On notera par la suite $\rightarrow_Q$ avec $\rightarrow$ pour plus de lisibilité.

Définition 2.2.9. On note $\rightarrow_*$ la clôture réflexive, transitive de la relation $\rightarrow$.

Le théorème suivant nous permet de dire que $\rightarrow \subset \mathscr{E} \times \mathscr{E}$.

Proposition 2.2.10 (Soundness)**.** *Soit $e \in \mathscr{E}$, $Q \in \mathscr{Q}$, $M \in \mathscr{T}$ tel que $e \rightarrow [Q, M]$ alors $[Q, M] \in \mathscr{E}$.*

2.3 Propriétés de la réduction

Dans cette section, on va prouver que la réduction $\rightarrow$ est confluente en prouvant une propriété plus forte, le quasi-diamand (voir Def. 1.2.6 et Prop. 1.2.7) que l'on utilisera au chapitre 5.

Proposition 2.3.1 (Propriété du quasi-diamant)**.** *Soit $(e, e_0, e_1) \in \mathscr{E}^3$, tels que $e \rightarrow e_0$ et $e \rightarrow e_1$, alors :*
$\Rightarrow$ *soit $e_0 = e_1$*
$\Rightarrow$ *soit il existe $e' \in \mathscr{E}$ tel que $e_0 \rightarrow e'$ et $e_1 \rightarrow e'$.*

Démonstration. Faisons une induction sur les termes :

(1) si $e = [Q, q_{init}]$, alors il y a une seule réduction possible : $\rightarrow_q$.
Et donc $[Q', N'] = [Q'', N'']$.

(2) si $e = [Q, x]$ alors il n'y a pas de réduction possible, l'hypothèse ne tient pas.

(3) si $e = [Q, r_i]$ alors il n'y a pas de réduction possible, l'hypothèse ne tient pas.

(4) si $e = [Q, \lambda x.T]$, la réduction se fait à l'intérieur de T, donc par hypothèse de récurrence, on conclut.

(5) si $M = OP$ alors par hypothèse on a :
(*) $[Q, OP] \rightarrow_{c_1} [Q', N']$
(**) $[Q, OP] \rightarrow_{c_2} [Q'', N'']$

Décomposons en 3 sous-cas :
(1') Seul le terme O (ou P) est impliqué dans les 2 réductions des hypothèses.
(2') Le terme O est impliqué par une réduction et le terme P par l'autre.
(3') Le terme OP est directement impliqué dans l'une des réduction.

(1') si les réductions se font à l'intérieur de O uniquement ou à l'intérieur de P uniquement, alors par hypothèse de récurrence et clôture de surface, on conclut.

(2') si la réduction c_1 se fait dans O et c_2 dans P :
$\Rightarrow$ Si c_1 et c_2 sont des réductions agissant sur la mémoire.

$\rightarrow$ si $c_1 = q$ et $c_2 = q$, alors les hypothèses de récurrences deviennent :
(*) $[Q_n, \mathbf{S}_1(q_{init})\ P] \rightarrow_q [Q_n \otimes |0\rangle, \mathbf{S}_1(r_n)\ P]$ (on a juste remplacé le q_{init} par r_n dans le terme O)
(**) $[Q_n, O\ \mathbf{S}_2(q_{init})] \rightarrow_q [Q_n \otimes |0\rangle, O\ \mathbf{S}_2(r_n)]$(on a juste remplacé le q_{init} par r_n dans le terme P)

On a $O = \mathbf{S}_1(q_{init})$ et $P = \mathbf{S}_2(q_{init})$.

Si on re-applique $\rightarrow_q$, à chacun des états obtenus, on obtient :
(o) $[Q_n \otimes |0\rangle, \mathbf{S}_1(r_n)\ \mathbf{S}_2(q_{init})] \rightarrow_q [(Q_n \otimes |0\rangle) \otimes |0\rangle, \mathbf{S}_1(r_n)\ \mathbf{S}_2(r_{n+1})]$ (on a remplacé q_{init} dans le terme P par r_{n+1})
(oo) $[Q_n \otimes |0\rangle, \mathbf{S}_1(q_{init})\ \mathbf{S}_2(r_n)] \rightarrow_q [(Q_n \otimes |0\rangle) \otimes |0\rangle, \mathbf{S}_1(r_{n+1})\ \mathbf{S}_2(r_n)]$ (on a remplacé q_{init} dans le terme O par r_{n+1})

On a donc trouvé deux termes : $\mathbf{S}_1(r_{n+1})\ \mathbf{S}_2(r_n)$ et $\mathbf{S}_1(r_n)\ \mathbf{S}_2(r_{n+1})$. Ces deux termes diffèrent au numéro de registre près.
Ce sont donc les mêmes, car on raisonne sur les classes de σ-équivalence.
De plus, les mémoires sont les mêmes.

On a donc retrouvé le même état.

$\rightarrow$ si $c_1 = q$ et $c_2 = U_A^{(2)}$, alors les hypothèses de récurrences deviennent :
(*) $[Q_n, \mathbf{S}_1\,(q_{init})\ P] \rightarrow_q [Q_n \otimes |0\rangle\,, \mathbf{S}_1\,(r_n)\ P]$ (on remplace q_{init} par r_n dans O)
(**) $[Q_n, O\ \mathbf{S}_2\,(U_A\ r_i)] \rightarrow_{U_A^{(1)}} [I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n, O\ \mathbf{S}_2\,(r_i)]$ (on remplace $UU_A\ r_i$ par r_i dans P)

On a $O = \mathbf{S}_1\,(q_{init})$ et $P = \mathbf{S}_2\,(U_A\ r_i)$.

Si l'on applique chacune des réductions à l'état obtenu par l'autre, on obtient :
(o) $[Q_n \otimes |0\rangle\,, \mathbf{S}_1\,(r_n)\ \mathbf{S}_2\,(U_A\ r_i)] \rightarrow_{U_A^{(1)}} [I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i}(Q_n \otimes |0\rangle), \mathbf{S}_1\,(r_n)\ \mathbf{S}_2\,(r_i)]$
(on remplace $U_A\ r_i$ par r_i dans P si c'est le registre i qui est impliqué dans cette réduction)
(oo) $[I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n, \mathbf{S}_1\,(q_{init})\ \mathbf{S}_2\,(r_i)] \rightarrow_q [(I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n) \otimes |0\rangle\,, \mathbf{S}_1\,(r_n)\ \mathbf{S}_2\,(r_i)]$
(on remplace q_{init} par r_n dans O)

On a retrouvé le même terme, il reste donc à vérifier si les mémoires sont correctes.
Par le lemme adéquate, on a donc retrouvé aussi la même mémoire, donc on a retrouvé le même état.

$\rightarrow$ si $c_1 = q$ et $c_2 = U_A^{(2)}$, alors les hypothèses de récurrences deviennent :
(*) $[Q_n, \mathbf{S}_1\,(q_{init})\ P] \rightarrow_q [Q_n \otimes |0\rangle\,, \mathbf{S}_1\,(r_n)\ P]$
(on remplace q_{init} par r_n dans O)
(**) $[Q_n, O\ \mathbf{S}_2\,(U_A\ \langle r_i, r_j\rangle)] \rightarrow_{U_A^{(2)}} \left[(A \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}\,, O\ \mathbf{S}_2\,(\langle r_i, r_j\rangle)\right]$
(on remplace $U_A\ \langle r_i, r_j\rangle$ par $\langle r_i, r_j\rangle$ dans P)

Ici, les deux qbit influencés par l'action de U_A doivent être des qbit présent dans la mémoire Q_n, car on peut réduire avec $\rightarrow_{U_A^{(2)}}$ avant $\rightarrow_q$.
Si l'on applique chacune des réductions à l'état obtenu par l'autre, on obtient :
(o) $[Q_n \otimes |0\rangle\,, \mathbf{S}_1\,(r_n)\ \mathbf{S}_2\,(U_A\ \langle r_i, r_j\rangle)] \rightarrow_{U_A^{(2)}} \left[(A \otimes I^{\otimes n-2}(Q_n \otimes |0\rangle)^{\sigma_{i,j}})^{\sigma_{i,j}}\,, \mathbf{S}_1\,(r_n)\ \mathbf{S}_2\,(\langle r_i, r_j\rangle)\right]$
(on remplace $U_A\ \langle r_i, r_j\rangle$ par $\langle r_i, r_j\rangle$ dans P si ce sont les registres i et j qui sont impliqués dans cette réduction)
(oo) $\left[(A \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}\,, \mathbf{S}_1\,(q_{init})\ \mathbf{S}_2\,(\langle r_i, r_j\rangle)\right] \rightarrow_q \left[\left((A \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}\right) \otimes |0\rangle\,, \mathbf{S}_1\,(r_n)\ \mathbf{S}_2\,(\langle r_i, r_j\rangle)\right.$
(on remplace q_{init} par r_n dans O)

On a retrouvé le même terme, il reste donc à retrouvé la même mémoire.

Par le lemme adéquate, on a donc retrouvé aussi la même mémoire, donc on a le même état.

$\rightarrow$ si $c_1 = U_{A_1}^{(1)}$ et $c_2 = U_{A_2}^{(1)}$, alors les hypothèses de récurrences deviennent :
(*) $[Q_n, \mathbf{S}_1\,(U_{A_1}\ r_{i_1})\ P] \rightarrow_{U_A^{(1)}} [I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1} Q_n, \mathbf{S}_1\,(r_{i_1})\ P]$
(on remplace $U_{A_1}\ r_{i_1}$ par r_{i_1} dans O)
(**) $[Q_n, O\ \mathbf{S}_2\,(U_{A_2}\ r_{i_2})] \rightarrow_{U_A^{(1)}} [I^{\otimes i_2-1} \otimes A_2 \otimes I^{\otimes n-i_2} Q_n, O\ \mathbf{S}_2\,(r_{i_2})]$
(on remplace $U_{A_2}\ r_{i_2}$ par r_{i_2} dans P)

On a que $i_1 \neq i_2$, car on ne peut pas avoir un même registre dans un même terme (par validité des termes).
Sans perte de généralité, admettons que $i_1 < i_2$.

Si l'on applique chacune des réductions à l'état obtenu par l'autre, on obtient :
(o) $[I^{\otimes i_1 - 1} \otimes A_1 \otimes I^{\otimes n - i_1} Q_n, \mathbf{S}_1\,(r_{i_1})\ \mathbf{S}_2\,(U_{A_2}\ r_{i_2})]$
$\rightarrow_{U_A^{(1)}}$ $[I^{\otimes i_2 - 1} \otimes A_2 \otimes I^{\otimes n - i_2} (I^{\otimes i_1 - 1} \otimes A_1 \otimes I^{\otimes n - i_1} Q_n), \mathbf{S}_1\,(r_{i_1})\ \mathbf{S}_2\,(r_{i_2})]$
(on remplace $U_{A_2}\ r_{i_2}$ par r_{i_2} dans P)
(oo) $[I^{\otimes i_2 - 1} \otimes A_2 \otimes I^{\otimes n - i_2} Q_n, \mathbf{S}_1\,(U_{A_1}\ r_{i_1})\ \mathbf{S}_2\,(r_{i_2})]$
$\rightarrow_{U_A^{(1)}}$ $[I^{\otimes i_1 - 1} \otimes A_1 \otimes I^{\otimes n - i_1} (I^{\otimes i_2 - 1} \otimes A_2 \otimes I^{\otimes n - i_2} Q_n), \mathbf{S}_1\,(r_{i_1})\ \mathbf{S}_2\,(r_{i_2})]$
(on remplace $U_{A_1}\ r_{i_1}$ par r_{i_1} dans O)

On a donc le même terme, il reste à vérifier la mémoire.
Par le lemme adéquate, on a donc retrouvé aussi la même mémoire, et donc le même état.

$\rightarrow$ si $c_1 = U_{A_1}^{(1)}$ et $c_2 = U_{A_2}^{(2)}$, alors les hypothèses de récurrences deviennent :
(*) $[Q_n, \mathbf{S}_1\,(U_{A_1}\ r_{i_1})\ P] \rightarrow_{U_A^{(1)}} [I^{\otimes i_1 - 1} \otimes A_1 \otimes I^{\otimes n - i_1} Q_n, \mathbf{S}_1\,(r_{i_1})\ P]$
(on remplace $U_{A_1}\ r_{i_1}$ par r_{i_1} dans O)
(**) $[Q_n, O\ \mathbf{S}_2\,(U_{A_2}\ \langle r_i, r_j \rangle)] \rightarrow_{U_A^{(2)}} \left[(A_2 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}, O\ \mathbf{S}_2\,(\langle r_i, r_j \rangle)\right]$
(on remplace $U_{A_2}\ \langle r_i, r_j \rangle$ par $\langle r_i, r_j \rangle$ dans P)

On a $i \neq i_1$ et $j \neq i_1$ (par validité des termes).

Si l'on applique chacune des réductions à l'état obtenu par l'autre, on obtient :
(o)$[I^{\otimes i_1 - 1} \otimes A_1 \otimes I^{\otimes n - i_1} Q_n, \mathbf{S}_1\,(r_{i_1})\ \mathbf{S}_2\,(U_{A_2}\ \langle r_i, r_j \rangle)]$
$\rightarrow_{U_A^{(2)}}$ $\left[\left(A_2 \otimes I^{\otimes n-2} (I^{\otimes i_1 - 1} \otimes A_1 \otimes I^{\otimes n - i_1} Q_n)^{\sigma_{i,j}}\right)^{\sigma_{i,j}}, \mathbf{S}_1\,(r_{i_1})\ \mathbf{S}_2\,(\langle r_i, r_j \rangle)\right]$
(on remplace $U_{A_2}\ \langle r_i, r_j \rangle$ par $\langle r_i, r_j \rangle$ dans P)

(oo)$\left[(A_2 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}, \mathbf{S}_1\,(U_{A_1}\ r_{i_1})\ \mathbf{S}_2\,(\langle r_i, r_j \rangle)\right]$
$\rightarrow_{U_A^{(1)}}$ $\left[I^{\otimes i_1 - 1} \otimes A_1 \otimes I^{\otimes n - i_1} \left((A_2 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}\right), \mathbf{S}_1\,(r_{i_1})\ \mathbf{S}_2\,(\langle r_i, r_j \rangle)\right]$
(on remplace $U_{A_1}\ r_{i_1}$ par r_{i_1} dans O)

On a retrouvé le même terme O'P', il reste à vérifier les 2 mémoires.

Par le lemme adéquate, on a donc retrouvé la même mémoire et donc le même terme.

$\rightarrow$ si $c_1 = U_{A_1}^{(2)}$ et $c_2 = U_{A_2}^{(2)}$, alors les hypothèses de récurrences deviennent :

(*) $[Q_n, \mathbf{S}_1\,(U_{A_1}\ \langle r_{i_1}, r_{j_1} \rangle)\ P] \rightarrow_{U_A^{(2)}} \left[(A_1 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}, \mathbf{S}_1\,(\langle r_{i_1}, r_{j_1} \rangle)\ P\right]$
(**) $[Q_n, O\ \mathbf{S}_2\,(U_{A_2}\ \langle r_{i_2}, r_{j_2} \rangle)] \rightarrow_{U_A^{(2)}} \left[(A_2 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}, O\ \mathbf{S}_2\,(\langle r_{i_2}, r_{j_2} \rangle)\right]$

Si l'on applique chacune des réductions à l'état obtenu par l'autre, on obtient :

(o) $\left[(A_1 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}, \mathbf{S}_1\left(\langle r_{i_1}, r_{j_1}\rangle\right)\ \mathbf{S}_2\left(U_{A_2}\ \langle r_{i_2}, r_{j_2}\rangle\right)\right]$
$\rightarrow_{U_A^{(2)}} \left[\left(A_2 \otimes I^{\otimes n-2}\left((A_1 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}\right)^{\sigma_{i_2,j_2}}\right)^{\sigma_{i_2,j_2}}, \mathbf{S}_1\left(\langle r_{i_1}, r_{j_1}\rangle\right)\ \mathbf{S}_2\left(\langle r_{i_2}, r_{j_2}\rangle\right)\right]$
(oo) $\left[(A_2 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}, \mathbf{S}_1\left(U_{A_1}\ \langle r_{i_1}, r_{j_1}\rangle\right)\ \mathbf{S}_2\left(\langle r_{i_2}, r_{j_2}\rangle\right)\right]$
$\rightarrow_{U_A^{(2)}} \left[\left(A_1 \otimes I^{\otimes n-2}\left((A_2 \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}\right)^{\sigma_{i_1,j_1}}\right)^{\sigma_{i_1,j_1}}, \mathbf{S}_1\left(\langle r_{i_1}, r_{j_1}\rangle\right)\ \mathbf{S}_2\left(\langle r_{i_2}, r_{j_2}\rangle\right)\right]$

Vu que les registres ne peuvent pas être présent plus d'une fois dans chaque terme, on a donc que i_1, j_1, i_2, j_2 sont deux à deux distincts.

Par le lemme adéquate, on a donc retrouvé la même mémoire en plus des mêmes termes.
On a bien retrouvé le même état.

$\Rightarrow$ Si c_1 et c_2 sont deux β-réduction, alors elle commutent, car chaque registre et variable n'apparaissent qu'une seule fois dans chaque terme.

$\Rightarrow$ Si c_1 et c_2 sont une réduction sur la mémoire et une β-réduction, alors elles commutent, car chaque registre et variable n'apparaissent qu'une seule fois dans chaque terme.

(3') Traitons maintenant le cas où le terme OP est directement impliqué dans la réduction :

$\Rightarrow$ si $e = [Q, U_A\ r_i]$, alors une seule réduction possible : $\rightarrow_{U_A^{(1)}}$.
Et donc $e_0 = e_1$.

$\Rightarrow$ si $e = [Q, U_A\ \langle r_i, r_j\rangle]$, alors une seule réduction possible : $\rightarrow_{U_A^{(2)}}$.
Et donc $e_0 = e_1$.

$\Rightarrow$ si $e = [Q, (\lambda x.T)P]$ et que $c_1 = \beta$.
Alors les hypothèses deviennent :
(*) $[Q, (\lambda x.T)P] \rightarrow_\beta [Q, T\,[x := P]]$
(**) $[Q, (\lambda x.T)P] \rightarrow_{c_2} [Q'', N'']$
$\rightarrow_{c_2}$ peut se faire :
- soit dans P
- soit dans T

- si $\rightarrow_{c_2}$ se fait dans P, on a donc :
(*) $[Q, (\lambda x.T)P] \rightarrow_\beta [Q, T\,[x := P]]$
(**) $[Q, (\lambda x.T)P] \rightarrow_{c_2} [Q'', (\lambda x.T)P'']$
On a que :
(1) $[Q'', (\lambda x.T)P''] \rightarrow_\beta [Q'', T\,[x := P'']]$
De plus, notons que P est toujours présent dans $T\,[x := P]$ et en un seul exemplaire car nos termes sont linéaires (x apparaît exactement une fois dans un terme avec abstraction de la variable x).
Donc la réduction $\rightarrow_{c_2}$ peut toujours se faire.

On a donc :
(2) $[Q, T\,[x := P]] \rightarrow_{c_2} [Q'', T\,[x := P'']]$

On a donc retrouvé le même état.

- si $\rightarrow_{c_2}$ se fait dans T, on a donc :
(*) $[Q, (\lambda x.T)P] \rightarrow_\beta [Q, T\,[x := P]]$
(**) $[Q, (\lambda x.T)P] \rightarrow_{c_2} [Q'', (\lambda x.T'')P]$
On a que :
(1) $[Q'', (\lambda x.T'')P] \rightarrow_\beta [Q'', T''\,[x := P]]$
- si c_2= q, alors cela ne pose pas de problème et les deux réductions commutent car le "x" n'est pas impacté par cette réduction.
- si $c_2 = U_A^{(1)}$, alors cela ne pose pas de problème et les deux réductions commutent car le "x" n'est pas impacté par cette réduction.
- si $c_2 = \beta$, vu que le x n'apparaît qu'une seule fois, qu'un seul "changement" à chaque fois. Donc les deux réductions commutent.
- si $c_2 = U_A^{(2)}$, alors cela ne pose pas de problème et les deux réductions commutent car le "x" n'est pas impacté par cette réduction.

□

Corollaire 2.3.2. *Soit $(e, e_0, e_1) \in \mathscr{E}^3$ tel que, $e \rightarrow e_0$, $e \rightarrow e_1$.*
Alors :
$\Rightarrow$ *soit e_0 et e_1 n'est pas en forme normale*
$\Rightarrow$ *soit $e_0 = e_1$*

Démonstration. Soit $(e, e_0, e_1) \in \mathscr{E}^3$ tel que $e \rightarrow e_0$, $e \rightarrow e_1$.

D'après la propriété précédente, on a soit :
$\Rightarrow$ soit $\mathscr{T}(e_0) = \mathscr{T}(e_1)$
$\Rightarrow$ soit il existe e' tel que $e_0 \rightarrow e'$ et $e_1 \rightarrow e'$.
Donc cela veut dire que e' n'est pas en forme normale. □

2.3.1 Confluence

De la propriété 2.3.1, découle la propriété de confluence de notre système de réécriture.

Théorème 2.3.3 (Confluence)**.** *Le système $(\mathscr{E}, \rightarrow)$ est confluent.*

2.4 Expressivité du langage

Reprenons maintenant nos paires.
On a :

$$let\langle q_1, q_2\rangle = CNOT\langle q_{init}, H\,q_{init}\rangle\; in\; \langle U\,q_1, q_2\rangle = (CNOT\langle q_{init}, H\,q_{init}\rangle)(\lambda q_1.\lambda q_2.\langle U\,q_1, q_2\rangle)$$

De plus, soit $Q \in \mathscr{M}$, on a :

$$\begin{aligned}
[Q, (CNOT\langle q_{init}, H\, q_{init}\rangle)(\lambda q_1.\lambda q_2.\langle U\, q_1, q_2\rangle)] &\to [Q^{(1)}, (CNOT\langle r_n, H\, q_{init}\rangle)(\lambda q_1.\lambda q_2.\langle U\, q_1, q_2\rangle)] \\
&\to [Q^{(2)}, (CNOT\langle r_n, H\, r_{n+1}\rangle)(\lambda q_1.\lambda q_2.\langle U\, q_1, q_2\rangle)] \\
&\to [Q^{(3)}, (CNOT\langle r_n, r_{n+1}\rangle)(\lambda q_1.\lambda q_2.\langle U\, q_1, q_2\rangle)] \\
&\to [Q^{(4)}, (\langle r_n, r_{n+1}\rangle)(\lambda q_1.\lambda q_2.\langle U\, q_1, q_2\rangle)] \\
&(= [Q^{(4)}, (\lambda f.f\ r_n\ r_{n+1})(\lambda q_1.\lambda q_2.\langle U\, q_1, q_2\rangle)] \\
&\to [Q^{(4)}, (\lambda q_1.\lambda q_2.\langle U\, q_1, q_2\rangle)\ r_n\ r_{n+1}] \\
&\to [Q^{(4)}, (\lambda q_2.\langle U\, r_n, q_2\rangle)\ r_{n+1}] \\
&\to [Q^{(4)}, \langle U\, r_n, r_{n+1}\rangle]
\end{aligned}$$

Ce destructeur est plus général que les destructeurs usuels fst et snd (il permet de les former) (si l'on avait des abstractions affine et non linéaire).

De plus, il ne duplique pas le fait d'utiliser la paire M plusieurs fois, contrairement aux 2 destructeurs usuels (fst et snd).

En effet, les 2 destructeurs usuels (fst et snd) ne conviennent pas pour reconstruire une paire.

Par exemple, si je voudrais faire une nouvelle paire p' identique à une paire p, alors le seul moyen de la construire serait :

$$p := \langle fst\ p, snd\ p\rangle$$

Ce qui a dupliqué p et ainsi créer un terme qui n'est pas valide.

Chapter 3

Calcul quantique linéaire avec mesure

Nous définissons ici un langage quantique (linéaire) que l'on dénote Q^{meas}, où on ajoute au langage Q une opération de mesure.

3.1 Langage

Nous rajoutons aux langage de termes un nouveau constructeur qui va correspondre à la mesure d'un qbit : $\texttt{meas}(R, M, N)$.
Intuitivement, nos termes R, M et N vont correspondre à :

- pour R, notre registre à mesurer
- pour M, le terme à choisir si notre qbit mesuré est 0
- pour N, le terme à choisir si notre qbit mesuré est 1

M et N correspondent à deux branches de possibilités.

Définition 3.1.1 (Termes $\mathscr{T}^{meas}$)**.** Le langage est définie par la grammaire :

$$M, N, R ::= x \mid \lambda x.M \mid MN \mid (U_A)_{A \in Matrice} \mid r_i \mid q_{init} \mid \texttt{meas}(R, M, N)$$

On note $\mathscr{T}^{meas}$ l'ensemble de nos termes.

3.1.1 Bonne formation des termes

Maintenant que nous avons ajouté un nouveau constructeur, il nous faut définir sa bonne formation avant de pouvoir l'utiliser pour former nos états.
Avant cela, l'idée derrière un registre mesuré, est de ne plus le retrouver ensuite.
Ainsi un registre mesuré ne doit plus apparaître. L'ensemble des registres de $\texttt{meas}(R, M, N)$ est alors défini comme suivant :

Définition 3.1.2. On définit $RE\left(\texttt{meas}(R, M, N)\right)$ par :

$$RE\left(\texttt{meas}(R, M, N)\right) := RE\left(R\right) \cup RE\left(M\right) \cup RE\left(N\right)$$

Si l'on veut abstraire une variable avec l'abstraction linéaire λ, il faut qu'elle soit :

- uniquement linéaire dans la condition R OU
- uniquement linéaire dans les 2 branches M et N

En effet, car un terme comme $\lambda x.\texttt{meas}(r_0, x, y)$, donnerai des complications. Après mesure du registre 0, on pourrait avoir un terme comme $\lambda x.y$, si le qbit est mesuré à 1, ce qui créerait des termes non valide après mesure.

On a donc :

Définition 3.1.3 (Bonne formation de λ 2.0)**.** On a $\vdash \lambda x.M$ si $\vdash M$. De plus, on doit respecter une des deux conditions suivantes :

- x est linéaire dans M (si M ne possède aucun sous terme de la forme $\texttt{meas}(R, M, N)$)
- il existe un unique sous terme de la forme $\texttt{meas}(R, M, N)$, tel que :
  - x est linéaire dans R mais n'est libre ni dans M ni dans N
  - x est linéaire dans M et dans N mais n'est pas libre dans R

Il faut maintenant créer une règle de bonne formation pour $\texttt{meas}(R, M, N)$. Déjà, les termes R, M et N devrait être bien formé. De plus, un registre présent dans la condition R ne peut plus être présent dans les 2 branches M et N, car celui est mesuré dans la condition.
Si l'on mesurait tous les qbit d'une machine, on aimerait avoir une mémoire fixe. Pour cela il faut que chaque registre présent dans la branche M soit aussi présent dans la branche N.

En effet, on a besoin que $RE(M) = RE(N)$, car sinon un état comme celui-ci serait autorisé :

$$\left[\frac{1}{2}\left(|000\rangle + |001\rangle\right) + \frac{1}{2}\left(|100\rangle + |101\rangle\right), \texttt{meas}(\texttt{meas}(r_0, r_1, r_2), x, y)\right]$$

Et si l'on réduit cet état, on aurait :

$$\left\{\frac{1}{2}\left[\frac{1}{\sqrt{2}}\left(|000\rangle + |001\rangle\right), \texttt{meas}(r_1, x, y)\right], \frac{1}{2}\left[\frac{1}{\sqrt{2}}\left(|100\rangle + |101\rangle\right), \texttt{meas}(r_2, x, y)\right]\right\}$$

Et ainsi :

$$\left\{\frac{1}{2}\left[\frac{1}{\sqrt{2}}\left(|000\rangle + |001\rangle\right), x\right], \frac{1}{4}\left[|100\rangle, x\right], \frac{1}{4}\left[|101\rangle, y\right]\right\}$$

Ici le premier élément de cette multidistribution possède une mémoire quantique superposée : $\frac{1}{\sqrt{2}}\left(|000\rangle + |001\rangle\right)$, ce que l'on ne veut pas dans notre calcul.

On ajoute ainsi une règle de bonne formation de $\texttt{meas}(\cdot, \cdot, \cdot)$.

Définition 3.1.4. Soit $(R, M, N) \in \mathscr{T}^{meas}$, $\texttt{meas}(R, M, N)$ est bien formé si on a toutes les conditions suivantes :

- R, M, N est bien formé

- pas de registre en commun entre R et M (ou N)
- même registre entre M et N

Remarque. On pourrait donc croire qu'avec cette règle de formation de $\texttt{meas}(.,.,.)$ on ne peut pas faire de choix sur un registre (par exemple faire $\texttt{meas}(r_0, r_1, r_2)$, et ainsi choisir r_1 ou r_2 en fonction de la mesure de r_0).
Cependant pour simuler un tel choix il nous suffit de créer un terme comme celui-ci :

$$\texttt{meas}(r_0, \texttt{meas}(r_1, r_2, r_2), \texttt{meas}(r_2, r_1, r_1))$$

3.2 Sémantique opérationnelle

3.2.1 État

Définissons les états avec des termes possédant de la mesure.

Définition 3.2.1 (état)**.** Un état est un couple $[Q_n, M]$ avec $Q_n \in \mathscr{Q}$ (de taille $n \in \mathbb{N}$) et $M \in \mathscr{T}^{meas}$, tel que :

- $\vdash M$, c'est à dire que M est bien formé, comme défini en (2.1.6) et (3.1.4).
- $RE(M) = \{k \in \mathbb{N} \mid 0 \leqslant k \leqslant n-1\}$

Exemple. (1) $[0,5\,|00\rangle + 0,5\,|01\rangle + 0,4\,|10\rangle + 0,6\,|11\rangle\,, \texttt{meas}(U_H\ r_1, r_0, r_0)]$
(2) $\left[\frac{1}{\sqrt{2}}\,|000\rangle + \frac{1}{\sqrt{2}}\,|100\rangle\,, U_H\texttt{meas}(r_0, \texttt{meas}(r_1, r_2, r_2), \texttt{meas}(r_2, r_1, r_1))\right]$
(3) $[|10\rangle\,, \texttt{meas}(q_{init}, x, y)]$

3.2.2 Réduction

Nous allons définir deux relations de réduction:

- une relation $\rightarrow_{Q^{meas}} \subset \mathscr{E}^{meas} \times MDST(\mathscr{E}^{meas})$.
- une relation $\rightrightarrows_{Q^{meas}} \subset MDST(\mathscr{E}^{meas}) \times MDST(\mathscr{E}^{meas})$

3.2.3 Relation $\rightarrow_{Q^{meas}}$.

Avant d'introduire la relation $\rightarrow_{Q^{meas}}$, nous devons revoir la définition de contexte de surface .
C'est ici que le contexte de surface se distingue du contexte, on va s'interdire de réduire nos termes lorsqu'ils sont dans les branches.
C'est à dire que l'on va geler nos branches pour éviter de créer des termes non bien formé.
Si l'on se l'autorisait, on pourrait avoir un terme comme celui-ci :

$$\texttt{meas}(r_0, q_{init}, q_{init})$$

Qui au bout de deux réductions viendrait contredire que ce terme est bien formé :

$$\texttt{meas}(r_0, r_1, r_2)$$

On a donc :

Définition 3.2.2 (Contexte de Surface 2.0)**.** On définit le contexte de surface par induction :

$$\mathbf{S} ::= \square \mid \lambda x.\mathbf{S} \mid \mathbf{S}N \mid M\mathbf{S} \mid \texttt{meas}(\mathbf{S}, M, N)$$

Le but de la relation $\rightarrow_{meas}$ est d'exprimer un terme en choisissant avec une certaine probabilité l'un de ses sous-termes. C'est à dire qu'en fonction de la valeur du qbit mesuré (0 ou 1), on choisit un sous-terme plutôt qu'un autre.
Bien sûr, après mesure, il faut que la mémoire de l'état corresponde au terme, tout en restant un état bien défini.
Ainsi pour que $\rightarrow_{meas}$ soit bien défini, il nous faut énoncer cette propriété de séparation :

Proposition 3.2.3. *Soit $n \neq 0$, pour tout $Q_n \in \mathscr{M}$, pour tout $i \leqslant n$ on peut décomposer Q_n de la façon suivante :*

$$Q_n = \alpha \underbrace{\sum_{b'=(b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{n-1})} \gamma_{b'} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{n-1}\right\rangle}_{L_n} + \beta \underbrace{\sum_{b''=(b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{n-1})} \gamma_{b''} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{n-1}\right\rangle}_{R_n}$$

avec :

$$\alpha = \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{n-1}} \left|\alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{n-1}}\right|^2}$$

$$\beta = \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{n-1}} \left|\alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{n-1}}\right|^2}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$(L_n, R_n) \in \mathscr{Q}$$

Maintenant que l'on sait que l'on peut "séparer" n'importe quel mémoire comme il faut, on définit la relation $\rightarrow_{meas}$.
Elle va réécrire un état en une multidistribution d'état. Chaque élément de cette multidistribution exprimera le choix du sous-terme.
Pour bien définir cette relation, il nous faut introduire, le garbage collector. La réduction meas supprime un registre du terme. Donc après réduction, un qbit de la mémoire n'aura plus son registre dans le terme. Il faut alors bien redéfinir ce qu'est un état.
On aimerait bien pouvoir calculer avec une mémoire plus grande que nécessaire.
Cependant, gardons à l'esprit que plus tard, on ne voudrait pas avoir des états ayant un terme sans registre et une mémoire superposée.

Garbage Collector Soit $(e, e') \in (\mathscr{E}^{meas})^2$, définissons la relation $\mathscr{G}$. On a $\mathscr{G}(e, e')$ si et seulement si :
(1) $\mathscr{T}(e) = \mathscr{T}(e)$
(2) si $\mathscr{Q}(e) = \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b\rangle$ alors $\mathscr{Q}(e') = \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b\ i\rangle$
avec $i \in \{0, 1\}$

Remarque. Notons maintenant $\mathscr{G}^*$ la clôture réflexive,symétrique et transitive de la relation $\mathscr{G}$.

Exemple. Regardons un peu ce que veut dire un peu notre relation $\mathscr{G}^*$, sur quoi nous travaillons.
(1) Soit $e = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), r_0\right]$.
Nous avons maintenant par exemple $e_1 = \left[\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle), r_0\right]$ qui est en relation avec e.
Cependant $e_2 = \left[\frac{1}{\sqrt{2}}(|01\rangle + |00\rangle), r_0\right]$ n'est pas en relation avec e.
Cette relation rajoute des registres dans la mémoire qui sont inutilisés dans le terme, sans que cela ne contredise le fait que si l'on "regarde" dans la mémoire l'ensemble des qbits alors celle-ci est fixé.

Etat modulo Nous travaillerons à partir de maintenant avec les classes d'équivalence de cette relation.
Nous utiliserons le mot "état" pour désigner un représentant d'une classe.

Représentant canonique Nous pouvons toujours travailler sur une mémoire qui correspond au terme strictement. Si un registre est présent dans le terme alors le qbit associé est représenté dans la mémoire et vice-versa.

La relation $\rightarrow_{meas}$ défini comme suit :

Définition 3.2.4 (Réduction de $\texttt{meas}(.,.,.)$)**.** On définit la réduction $\rightarrow_{meas}$ ($\subset \mathscr{E} \times MDST(\mathscr{E})$) par :

$$[Q_n, \mathbf{S}(\texttt{meas}(r_i, M, N))] \rightarrow_{meas} \left\{|\alpha|^2 [L_n, \mathbf{S}(M)], |\beta|^2 [R_n, \mathbf{S}(N)]\right\} \text{ où } (i, n) \in \mathbb{N}^2$$

(pour Q_n étant comme dans la Proposition 5.6)

$\rightarrow_{meas}$ est un sous ensemble de $\mathscr{E} \times MDST(\mathscr{E})$ alors que $\rightarrow_Q$ est un sous ensemble de $\mathscr{E} \times \mathscr{E}$.
On peut voir $\rightarrow_Q$ comme des réductions probabiliste avec probabilité 1.
Ainsi on redéfinit la relation $\rightarrow_Q$ comme suivant :

Définition 3.2.5.
- $[Q_n, \mathbf{S}((\lambda x.M)\, N)] \rightarrow_\beta \{[Q_n, \mathbf{S}(M[x := N])]\}$ (réduction β)
- $[Q_n, \mathbf{S}(q_{init})] \rightarrow_q \{[Q_n \otimes |0\rangle, \mathbf{S}(r_n)]\}$ (réduction de q_{init})

- $[Q_n, \mathbf{S}(U_A\ r_i)] \rightarrow_{U_A^{(1)}} \{[I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n, \mathbf{S}(r_i)]\}$ (réduction de U : $qbit \rightarrow qbit$)
- $[Q_n, \mathbf{S}(U_A\ \langle r_i, r_j\rangle)] \rightarrow_{U_A^{(2)}} \left\{\left[(A \otimes I^{\otimes n-2} {Q_n}^{\sigma_{i,j}})^{\sigma_{i,j}}, \mathbf{S}(\langle r_i, r_j\rangle)\right]\right\}$ (réduction de U : $qbit \times qbit \rightarrow qbit \times qbit$)

Ainsi on peut faire l'union de $\rightarrow_{meas}$ et $\rightarrow_Q$.

Définition 3.2.6. On définit la relation $\rightarrow_{Q^{meas}}$ comme étant :

$$\rightarrow_{Q^{meas}} := \rightarrow_Q \cup \rightarrow_{meas}$$

Notation. Par simplification de notation, on utilisera $\rightarrow$ pour utiliser la réduction $\rightarrow_{Q^{meas}}$.

3.2.4 Relation $\rightrightarrows_{Q^{meas}}$.

La réduction $\rightarrow_{Q^{meas}}$ est un sous-ensemble de $\mathscr{E}^{meas} \times MDST(\mathscr{E}^{meas})$. On va lifter cette relation de la façon la plus naturelle possible sur $MDST(\mathscr{E}^{meas}) \times MDST(\mathscr{E}^{meas})$.
Cette réduction va pouvoir nous permettre de réduire chaque élément de la multidistribution en une seule étape de réécriture, de plus celle-ci va nous servir à exprimer correctement la propriété de confluence sur les multidistribution d'état.

Par abus de notation, dans la suite du chapitre, on notera $\rightarrow$ la flèche $\rightarrow_{Q^{meas}}$ et $\rightrightarrows$ la flèche $\rightrightarrows_{Q^{meas}}$.

Définition 3.2.7 (Liftage de $\rightrightarrows$)**.** On définit la relation $\rightrightarrows$ ($\subset MDST(\mathscr{E}) \times MDST(\mathscr{E})$) à partir de la réduction $\rightarrow$ ($\subset \mathscr{E} \times MDST(\mathscr{E})$) par :
(1) si $e \not\rightarrow$ alors $\{e\} \rightrightarrows \{e\}$
(2) si $e \rightarrow m$ alors $\{e\} \rightrightarrows m$
(3) si $(\{e_i\} \rightrightarrows m_i)_{i \in I}$ alors $\{p_i e_i | i \in I\} \rightrightarrows \sum_{i \in I} p_i m_i$

3.3 Propriété de la réduction

Dans cette section, on va prouver que la réduction $\rightrightarrows_{Q^{meas}}$ est confluente en prouvant une propriété plus forte, le quasi-diamand (voir Def. 1.2.6 et Prop. 1.2.7), que l'on utilisera au chapitre 5.

Proposition 3.3.1 (Propriété du quasi-diamant 2)**.** *Soient $e \in \mathscr{E}$ et $(m_0, m_1) \in MDST(\mathscr{E})^2$, tels que $e \rightarrow_{Q^{meas}} m_0$ et $e \rightarrow_{Q^{meas}} m_1$, alors il existe $m' \in MDST(\mathscr{E})$ tel que $m_0 \rightrightarrows m'$ et $m_1 \rightrightarrows m'$.*

Démonstration. Par la propriété du quasi-diamant 1 (Proposition 4.2), on en déduit que les réductions tel que la β-réduction, réduction q_{init} ou bien la réduction U_A "commutent" entre elles.

Il reste donc à voir si celles-ci "commutent" avec la réduction $\rightarrow_{meas}$, et si elle commute avec elle-même. On a donc ces 5 cas à traiter :
(1') β
(2') q_{init}
(3') $U_A^{(1)}$
(4') $U_A^{(2)}$
(5') $meas$

Posons $e = [Q, M]$.

Traitons le cas (1').
Au niveau des mémoires, il n'y a pas de problème : il n'y a que meas qui opère dessus. Soit i le registre impliqué dans la réduction meas. Le fait de faire la réduction meas peut dupliquer le fait de faire une β-réduction(si l'on veut retrouver le même terme.
Mais cela n'est pas grave car on peut compléter le schéma avec plusieurs β-réduction en seul étape grâce à troisième règle de formation de $\rightrightarrows$.

Traitons le cas (2').
Alors on a :
(1) $[Q_n, \mathscr{C}(q_{init}, \texttt{meas}(r_i, M, N))] \rightarrow_{q_{init}} \{[Q_n \otimes |0\rangle, \mathscr{C}(r_n, \texttt{meas}(r_i, M, N))]\}$
(2) $[Q_n, \mathscr{C}(q_{init}, \texttt{meas}(r_i, M, N))] \rightarrow_{meas} \left\{|\alpha|^2 [L_n, \mathscr{C}(q_{init}, M)], |\beta|^2 [R_n, \mathscr{C}(q_{init}, N)]\right\}$

La réduction de q_{init} crée à chaque fois un nouveau qbit, on a donc $i \neq n$.
Donc le qbit mesuré à 0 ou 1 (séparant ainsi la mémoire e) ne peut être le n-ième qbit.

Tout se passe bien grâce au lemme adéquate.
Pour la multidistribution $\left\{|\alpha|^2 [L_n, \mathscr{C}(q_{init}, M)], |\beta|^2 [R_n, \mathscr{C}(q_{init}, N)]\right\}$, on a pour le premier élément :

$$\{[L_n, \mathscr{C}(q_{init}, M)]\} \rightrightarrows \{[L_n \otimes |0\rangle, \mathscr{C}(r_n, M)]\}$$

De même pour le second élément :

$$\{[R_n, \mathscr{C}(q_{init}, N)]\} \rightrightarrows \{[R_n \otimes |0\rangle, \mathscr{C}(r_n, N)]\}$$

On a (par la troisième règle de formation de $\rightrightarrows$) :

$$\left\{|\alpha|^2 [L_n, \mathscr{C}(q_{init}, M)], |\beta|^2 [R_n, \mathscr{C}(q_{init}, N)]\right\} \rightrightarrows \left\{|\alpha|^2 [L_n \otimes |0\rangle, \mathscr{C}(r_n, M)], |\beta|^2 [R_n \otimes |0\rangle, \mathscr{C}(r_n, N)]\right\}$$

Traitons le cas (3').
On ne peut pas avoir $i = j$ sinon le terme ne serait pas bien formé (multiplication des registres). Donc $i \neq j$.
Alors on a :
(1) $[Q_n, \mathscr{C}(U_A^1\ r_j, \texttt{meas}(r_i, M, N))] \rightarrow_{U_A^{(1)}} \{[I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} Q_n, \mathscr{C}(r_j, \texttt{meas}(r_i, M, N))]\}$

(2) $[Q_n, \mathscr{C}(U_A^1\ r_j, \texttt{meas}(r_i, M, N))] \rightarrow_{meas} \left\{|\alpha|^2\ [L_n, \mathscr{C}(U_A^1\ r_j, M)]\ , |\beta|^2\ [R_n, \mathscr{C}(U_A^1\ r_j, N)]\right\}$

Sur la multidistribution $\left\{|\alpha|^2\ [L_n, \mathscr{C}(U_A^1\ r_j, M)]\ , |\beta|^2\ [R_n, \mathscr{C}(U_A^1\ r_j, N)]\right\}$, on peut réduire chaque état de celle-ci avec une réduction $U_A^{(1)}$.
En effet, on a premièrement :

$$\left\{\left[L_n, \mathscr{C}(U_A^1\ r_j, M)\right]\right\} \rightrightarrows \left\{\left[I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} L_n, \mathscr{C}(r_j, M)\right]\right\}$$

et deuxièmement :

$$\left\{\left[R_n, \mathscr{C}(U_A^1\ r_j, N)\right]\right\} \rightrightarrows \left\{\left[I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} R_n, \mathscr{C}(r_j, N)\right]\right\}$$

On a donc :

$$\left\{|\alpha|^2\ [L_n, \mathscr{C}(U_A^1\ r_j, M)]\ , |\beta|^2\ [R_n, \mathscr{C}(U_A^1\ r_j, N)]\right\} \rightrightarrows \left\{|\alpha|^2\ [I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} L_n, \mathscr{C}(r_j, M)]\ , |\beta|^2\ [I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} R_n, \mathscr{C}(r_j, N)]\right\}$$

Maintenant, si l'on réduit le meas de $\{[I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} Q_n, \mathscr{C}(r_j, \texttt{meas}(r_i, M, N))]\}$,
on obtient :

$$\left\{\left[I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} Q_n, \mathscr{C}(r_j, \texttt{meas}(r_i, M, N))\right]\right\} \rightrightarrows \left\{|\alpha'|^2\ [L'_n, \mathscr{C}(r_j, M)]\ , |\beta'|^2\ [R'_n, \mathscr{C}(r_j, N)]\right\}$$

Il faut donc vérifier que les probabilités α' et β' issus de cette réduction sont les mêmes
que dans la multidistribution $\left\{|\alpha|^2\ [I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} L_n, \mathscr{C}(r_j, M)]\ , |\beta|^2\ [I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} R_n, \mathscr{C}(r_j, N\right.$
c'est à dire que $\alpha = \alpha'$ et que $\beta = \beta'$.

Ensuite, il nous suffira de voir que :

$$L'_n = I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} L_n$$

et

$$R'_n = I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} R_n$$

Deux cas possible, $i < j$ ou $j < i$.
Sans perte de généralité, admettons que $i < j$.

Tout se passe bien grâce au lemme adéquate.

Traitons le cas (4').
Alors on a :
(1) $[Q_n, \mathscr{C}(U_A^2\ \langle r_{j_1}, r_{j_2}\rangle, \texttt{meas}(r_i, M, N))] \rightarrow_{U_A^{(2)}} \left\{\left[(A \otimes I^{\otimes n-2} Q_n^{\sigma_{j_1,j_2}})^{\sigma_{j_1,j_2}}, \mathscr{C}(\langle r_{j_1}, r_{j_2}\rangle, \texttt{meas}(r_i, M, N))\right]\right\}$
(2) $[Q_n, \mathscr{C}(U_A^2\ \langle r_{j_1}, r_{j_2}\rangle, \texttt{meas}(r_i, M, N))] \rightarrow_{meas} \left\{|\alpha|^2\ [L_n, \mathscr{C}(U_A^2\ \langle r_{j_1}, r_{j_2}\rangle, M)]\ , |\beta|^2\ [R_n, \mathscr{C}(U_A^2\ \langle r_{j_1}, r_{j_2}\rangle, N)]\right\}$

Tout se passe bien grâce au lemme adéquate.

Traitons le cas (5').
Sans perte de généralité, supposons que $i < j$. Alors on a :
(1) $[Q_n, \mathscr{C}(\texttt{meas}(r_i, M, N), \texttt{meas}(r_j, M', N'))]$
$\rightarrow_{meas} \left\{|\alpha|^2\ [L_n, \mathscr{C}(M, (\texttt{meas}(rj, M', N'))]\ , |\beta|^2\ [R_n, \mathscr{C}(N, \texttt{meas}(r_j, M', N'))]\right\}$

(2) $[Q_n, \mathscr{C}(\texttt{meas}(r_i, M, N), \texttt{meas}(r_j, M', N'))]$
$\rightarrow_{meas} \left\{|\alpha'|^2 [L'_n, \mathscr{C}(\texttt{meas}(r_i, M, N), M')], |\beta'|^2 [R'_n, \mathscr{C}(\texttt{meas}(r_i, M, N), N')]\right\}$

Posons $Q_n = \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b\rangle$.

D'après la propriété 5.6, on a :

$$\alpha = \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{n-1}}\right|^2}$$

$$L_n = \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{n-1}} \frac{\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{n-1}}}{\alpha} |b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{n-1}\rangle$$

$$\beta = \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{n-1}}\right|^2}$$

$$R_n = \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{n-1}} \frac{\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{n-1}}}{\beta} |b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{n-1}\rangle$$

Appliquons une nouvelle fois une réduction meas sur la multidistribution

$$\left\{|\alpha|^2 [L_n, \mathscr{C}(M, (\texttt{meas}(r_j, M', N'))], |\beta|^2 [R_n, \mathscr{C}(N, \texttt{meas}(r_j, M', N'))]\right\}$$

On a donc :
$\left\{|\alpha|^2 [L_n, \mathscr{C}(M, (\texttt{meas}(r_j, M', N'))], |\beta|^2 [R_n, \mathscr{C}(N, \texttt{meas}(r_j, M', N'))]\right\}$
$\rightrightarrows \left\{|\alpha|^2 |\gamma|^2 [LL_n, \mathscr{C}(M, M')], |\alpha|^2 |\xi|^2 [LR_n, \mathscr{C}(M, N')], |\beta|^2 |\gamma'|^2 [RL_n, \mathscr{C}(N, M')], |\beta|^2 |\xi'|^2 [RR_n, \mathscr{C}(N, N')]\right\}$

Tout se passe bien grâce au lemme adéquate.

On peut appliquer le même calcul à l'autre multidistributions. Et on retrouve ainsi les mêmes mémoires et les mêmes probabilités. □

Lemme 3.3.2. *Soit $e \in \mathscr{E}$ et $(m_0, m_1) \in MDST(\mathscr{E})^2$ tel que $e \rightarrow m_0$ et $e \rightarrow m_1$.*
Alors :
$\Rightarrow$ soit : $m_0 = m_1$
$\Rightarrow$ soit : pour tout $e' \in m_0$, et tout $e'' \in m_1$, il existe $(m', m'') \in MDST(\mathscr{E})$ tel que $e' \rightarrow m'$ et $e'' \rightarrow m''$

Démonstration. Soit $e \in \mathscr{E}$ et $(m_0, m_1) \in MDST(\mathscr{E})^2$ tel que $e \rightarrow m_0$ et $e \rightarrow m_1$.

Si les réductions $\rightarrow$ se font sur le même REDEX, alors clairement $m_0 = m_1$.

Si l'on parle de deux REDEX différents, si les deux réductions $\rightarrow$ sont des β-réduction, q_{init}, U_A alors par le Corollaire 1.4.3, on conclut.

Passons donc pour les réductions avec mesure avec une réduction non-mesure. Faisons une induction sur $\mathscr{T}(e)$.

(1) Terme simple -¿ ok

(2) si $\mathscr{T}(e) = $ M N (*) Si les deux réductions se font toutes les deux dans M ou dans N alors pas de problème.

(**) Si l'une se fait dans M l'autre dans N, alors les deux multidistribution qui en résulte n'ont pas leur état sous forme normale de $\rightarrow$.

(***) Si M N est directement impliqué dans la réduction, c'est à dire que la deuxième réduction est une β-réduction.
Donc que $MN = (\lambda x.M_0)N$.

$\Rightarrow$ si la réduction meas se fait dans N
La réduction linéaire ne peut pas supprimer le terme N.
Il apparaît forcément une fois dans M_0. Donc après β-réduction on pourra faire la réduction meas. C'est ok pour l'inverse. Donc on conclut.

$\Rightarrow$ si la réduction meas se fait dans M
Une variable abstrait par λ-abstraction linéaire apparaît forcément une fois dans les "branches" du meas. Donc après réduction meas on pourra faire la β-réduction, dans les deux états. C'est ok pour l'inverse. Donc on conclut. □

3.3.1 Confluence

Théorème 3.3.3 (Confluence 2.0)**.** *La relation* $(MDST(\mathscr{E}^{emeas}), \rightrightarrows)$ *est confluente.*

Chapter 4

Calcul quantique avec récursion

Nous définissons ici un langage quantique que l'on dénote $Q^!$. Nous enrichissons le calcul précédent avec un nouveau constructeur qui permet la récursion.

4.1 Langage

En suivant le calcul de Simpson [8], on va rajouter un constructeur "!" qui intuitivement va enfermer nos termes dans des boites. Cela va correspondre au bang de la logique linéaire. Le bang freeze les termes qui donc ne peuvent pas être réduit. Par contre les termes sous un bang peuvent être copier ou effacer. Dualement, nous rajoutons une lambda-abstraction et une beta-réduction non linéaire.

Définition 4.1.1 (Définition de termes $\mathscr{T}^!$)**.**

$$M, N ::= x \mid !M \mid \lambda x.M \mid \lambda^! x.M \mid MN \mid (U_A)_{A \in Matrice} \mid r_i \mid q_{init} \mid \texttt{meas}(R, M, N)$$

On note $\mathscr{T}^!$ l'ensemble des termes.

Nous remarquons que mesure et récursion sont tous les deux présents.

4.1.1 Bonne formation de termes

Il faut ensuite rajouter une règle de bonne construction des termes avec bang, ainsi que de l'abstraction. Il est important de ne pas pouvoir dupliquer les registres, on se restreint donc de mettre des registres à l'intérieur d'un bang.

Définition 4.1.2 (bonne formation de !)**.** On a $\vdash !M$, si $\vdash M$ et que $RE(M) = \emptyset$.

Définition 4.1.3 (bonne formation de $\lambda^!$)**.** On a $\vdash \lambda^! x.M$, si $\vdash M$.

Puisque le langage est plus riche, il faut réviser la règle de bonne formation pour l'abstraction linéaire λ.

Définition 4.1.4 (Bonne formation de λ 3.0)**.** On a $\vdash \lambda x.M$ si $\vdash M$ et pour tout sous-terme de M de la forme $!M_0$, alors x n'est pas libre dans M_0. De plus, on doit respecter une des deux conditions suivantes :

- x est linéaire dans M (si M ne possède aucun sous terme de la forme $\texttt{meas}(R, M, N)$)

- il existe un unique sous terme de la forme $\texttt{meas}(R, M, N)$, tel que :
  - x est linéaire dans R mais n'est libre ni dans M ni dans N
  - x est linéaire dans M et dans N mais n'est pas libre dans R

4.2 Sémantique opérationnelle

4.2.1 Etat $\mathscr{E}^!$

Définissons les états avec les termes $\mathscr{T}^!$.

Définition 4.2.1 (état $\mathscr{E}^!$)**.** Un état est un couple $[Q_n, M]$ avec $Q_n \in \mathscr{Q}$ memoire (de taille $n \in \mathbb{N}$) et $M \in \mathscr{T}^!$ terme, tel que :

- $\vdash M$
- $RE(M) = \{k \in \mathbb{N} \mid 0 \leqslant k \leqslant n-1\}$

Exemple. (1) $[|10\rangle, !\texttt{meas}(q_{init}, x, y)]$ (2) $\left[|10\rangle, (\lambda^! x.!\texttt{meas}(q_{init}, xx, y)\right])!q_{init}$

4.2.2 Réduction

Nous allons définir deux relations de reduction :

- une relation $\rightarrow_{Q^!} \subset \mathscr{E}^! \times MDST\left(\mathscr{E}^!\right)$
- une relation $\rightrightarrows_{Q^!} \subset MDST\left(\mathscr{E}^!\right) \times MDST\left(\mathscr{E}^!\right)$, qui lift $\rightarrow_{Q^!}$ comme en Définition 3.2.7.

4.2.3 Relation $\rightarrow_{Q^!}$

Avant d'introduire la relation $\rightarrow_{Q^!}$, nous devons revoir la définition de contexte de surface. On s'interdit de réduire à l'intérieur d'un terme bangué en ne rajoutant pas de terme bangué dans le contexte de surface.

Définition 4.2.2 (Contexte de Surface 3.0)**.** On définit le contexte de surface par la grammaire :

$$\mathbf{S} ::= \square \mid \lambda x.S \mid \lambda^! x.S \mid SN \mid MS \mid \texttt{meas}(S, M, N)$$

La relation $\rightarrow_{Q^!} := \rightarrow_{Q^{meas}} \cup \rightarrow_!$ est l'union de $\rightarrow_{Q^{meas}}$, qui est défini comme au Chapitre 2 (en tenant compte de la définition des termes $\mathscr{T}^!$) et $\rightarrow_!$, qui est défini comme suit :

Définition 4.2.3 (Réduction $\rightarrow_{Q^!}$)**.** On définit une beta-réduction non linéaire :

$$\left[Q_n, \mathbf{S}\left((\lambda^! x.M)!N\right)\right] \rightarrow_! \{[Q_n, \mathbf{S}(M[x := N])]\}$$

Elle n'autorise que les termes bangués à être possiblement dupliquer.

4.2.4 Relation $\rightrightarrows_{Q^!}$

La réduction $\rightarrow_{Q^!}$ est un sous-ensemble de $\mathscr{E}^! \times MDST(\mathscr{E}^!)$. On va lifter cette relation de la façon la plus naturelle possible sur $MDST(\mathscr{E}^!) \times MDST(\mathscr{E}^!)$.
Cette réduction va pouvoir nous permettre de réduire chaque élément de la multidistribution en une seule étape de réécriture, de plus celle-ci va nous servir à exprimer correctement la propriété de confluence sur les multidistribution d'état.

Par abus de notation, dans la suite du chapitre, on notera $\rightarrow$ la flèche $\rightarrow_{Q^!}$ et $\rightrightarrows$ la flèche $\rightrightarrows_{Q^!}$.

Définition 4.2.4 (Liftage de $\rightrightarrows$)**.** On définit la relation $\rightrightarrows$ ($\subset MDST(\mathscr{E}) \times MDST(\mathscr{E})$) à partir de la réduction $\rightarrow$ ($\subset \mathscr{E} \times MDST(\mathscr{E})$) par :
(1) si $e \not\rightarrow$ alors $\{e\} \rightrightarrows \{e\}$
(2) si $e \rightarrow m$ alors $\{e\} \rightrightarrows m$
(3) si $(\{e_i\} \rightrightarrows m_i)_{i \in I}$ alors $\{p_i e_i | i \in I\} \rightrightarrows \sum_{i \in I} p_i m_i$

Définition 4.2.5. Le calcul $Q^!$ est le système de réécriture $(\mathscr{E}^!, \rightrightarrows_{Q^!})$.

4.3 Propriété de la réduction

Dans cette section, on va prouver que la réduction $\rightrightarrows_{Q^!}$ est confluente en prouvant une propriété plus forte, le quasi-diamand (voir Def. 1.2.6 et Prop. 1.2.7), que l'on utilisera au chapitre 5.

Proposition 4.3.1 (Propriété du quasi-diamant 3)**.** *Soient $e \in \mathscr{E}$ et $(m_0, m_1) \in MDST(\mathscr{E})^2$, tels que $e \rightarrow_{Q^!} m_0$ et $e \rightarrow_{Q^!} m_1$, alors il existe $m' \in MDST(\mathscr{E})$ tel que $m_0 \rightrightarrows m'$ et $m_1 \rightrightarrows m'$.*

Démonstration. Soient $e \in \mathscr{E}$ et $(m_0, m_1) \in MDST(\mathscr{E})^2$, tels que $e \rightarrow_{Q^!} m_0$ et $e \rightarrow_{Q^!} m_1$.

Si l'on a $e \rightarrow_{Q^{meas}} m_0$ et $e \rightarrow_{Q^{meas}} m_1$, on conclut en utilisant la propriété du quasi-diamant 2.

On peut donc supposer qu'au moins l'une des deux réductions est une réduction $\rightarrow_!$, supposons que :
- $e \rightarrow_! m_0$

Faisons une induction sur e.

Si $\mathscr{T}(e) = x$, il n'y a pas de réduction possible, donc les hypothèses ne tiennent pas.
Si $\mathscr{T}(e) = U_A$, il n'y a pas de réduction possible, donc les hypothèses ne tiennent pas.
Si $\mathscr{T}(e) = r_i$, il n'y a pas de réduction possible, donc les hypothèses ne tiennent pas.
Si $\mathscr{T}(e) = !M$, il n'y a pas de réduction possible (on ne peut pas réduire à l'intérieur d'un "!"), donc les hypothèses ne tiennent pas.
Si $\mathscr{T}(e) = \lambda^! x.M$, alors par hypothèse d'induction, on conclut.
Si $\mathscr{T}(e) = \lambda x.M$, alors par hypothèse d'induction, on conclut.
Si $\mathscr{T}(e) = q_{init}$, il n'y a pas de réduction $\rightarrow_!$ possible, cela contredit l'hypothèse. Si $\mathscr{T}(e) = \texttt{meas}(R, M, N)$, alors :
- soit les deux réductions se font dans R (impossible dans M ou N) alors par hypothèse

d'induction on conclut.
- soit il n'y a qu'une seul réduction possible $\rightarrow_{meas}$ et cela contredit l'hypothèse.
Si $\mathscr{T}(e) = MN$ alors plusieurs possibilités :
- soit les deux réductions ont lieu dans M ou N et on conclut par hypothèse d'induction.
- soit une réduction a lieu dans M et l'autre dans N. Alors on conclut par clôture de chaque relation.

Il reste le cas de la β-reduction, transformant ainsi le terme MN.
- soit $\mathscr{T}(e) = (\lambda^! x.M')!(N')$.
La réduction $\rightarrow$ n'a pas lieu dans un "!".
Alors forcément, la réduction $\rightarrow$ a lieu dans le terme M'.
On ne duplique pas ainsi la réduction correspondante : - si la réduction est une beta-reduction linéaire, pas de problème.
- si la réduction est un q_{init}, alors pas de problème.
- si la réduction est un U_A alors pas de problème
- si la réduction est un $meas$, alors la condition R du $\texttt{meas}(R, O, P)$ est indépendante de la réduction !, en effet, sinon, on ne pourrait pas faire de réduction meas en premier (de plus, pour rappel un bang! ne peut pas contenir de registre). Donc pas de problème ici.
- si la réduction est un bang, alors la preuve se termine en utilisant la proposition 3.2 de l'article "Reduction in a linear lambda-calculus with applications to operational semantics", de l'Université d'Edinburgh.
- soit $\mathscr{T}(e) = (\lambda x.M')N'$.
Alors la preuve se termine en utilisant la proposition 3.2 de l'article "Reduction in a linear lambda-calculus with applications to operational semantics", de l'Université d'Edinburgh.
□

Lemme 4.3.2. *Soit $e \in \mathscr{E}$ et $(m_0, m_1) \in MDST(\mathscr{E})^2$ tel que $e \rightarrow m_0$ et $e \rightarrow m_1$.*
Alors :
$\Rightarrow$ soit : $m_0 = m_1$
$\Rightarrow$ soit : pour tout $e' \in m_0$, et tout $e'' \in m_1$, il existe $(m', m'') \in MDST(\mathscr{E})$ tel que $e' \rightarrow m'$ et $e'' \rightarrow m''$

Démonstration. Soit $e \in \mathscr{E}$ et $(m_0, m_1) \in MDST(\mathscr{E})^2$ tel que $e \rightarrow m_0$ et $e \rightarrow m_1$.

Si les réductions $\rightarrow$ se font sur le même REDEX, alors clairement $m_0 = m_1$.

Si l'on parle de deux REDEX différents, si les deux réductions $\rightarrow$ sont des β-réduction, q_{init}, U_A, $meas$ alors par le Corollaire 2.4.2, on conclut.

Traitons donc le cas d'une réduction $\rightarrow_!$ avec une réduction $\rightarrow_{Q^{meas}}$.
Faisons une induction sur $\mathscr{T}(e)$.

(1) Terme simple :
Si $\mathscr{T}(e) = x$, pas de réduction possible, donc les hypothèses ne tiennent pas.
Si $\mathscr{T}(e) = r_i$, pas de réduction possible, donc les hypothèses ne tiennent pas.

Si $\mathscr{T}(e) = U_A$, pas de réduction possible, donc les hypothèses ne tiennent pas.
Si $\mathscr{T}(e) = !M$, pas de réduction possible (pas de réduction autorisée à l'intérieur d'un bang), donc les hypothèses ne tiennent pas.
Si $\mathscr{T}(e) = \lambda x.M$, alors on conclut par hypothèse d'induction.
Si $\mathscr{T}(e) = \lambda^! x.M$, alors on conclut par hypothèse d'induction.

(2) si $\mathscr{T}(e) =$ M N
(*) Si les deux réductions se font toutes les deux dans M ou dans N alors on conclut par hypothèse de récurrence.

(**) Si l'une se fait dans M l'autre dans N, alors les deux multidistribution qui en résulte n'ont pas leur état sous forme normale de $\to$, en effet on peut encore faire une réduction dans N ou dans M.

(***) Si M N est directement impliqué dans la réduction, alors :
- soit $MN = (\lambda x.M')N$
- soit $MN = (\lambda^! x.M')!N'$

Si $MN = (\lambda x.M')N$, alors la réduction $\to_!$ peut se faire soit dans M soit dans N.
Les variables abstraites par le λ et le $\lambda^!$ ne sont pas les mêmes. De plus, ceci est une abstraction linéaire, donc on ne peut pas faire "disparaître" de réduction.
Donc après la β-réduction, on a donc un seul état dans la multidistribution, et le terme de celui-ci n'est pas en forme normale (on peut faire un bang-réduction).
De même, que la réduction non linéaire ne pourra pas faire disparaître la variable x (elle n'est pas dans le bang).
On pourra donc faire encore une réduction après celle non linéaire.
Si $MN = (\lambda^! x.M')!N'$
, alors la réduction $\to_{Q^{meas}}$ se fait dans le terme M' (pas de réduction autorisée dans un terme bangué).
Donc elle ne disparaîtra pas.
Et donc chaque état ne sera pas en forme normale pour $\to$. □

4.3.1 Confluence

Théorème 4.3.3 (Confluence 3.0)**.** *Le système* $\left(MDST\left(\mathscr{E}^!\right), \rightrightarrows\right)$ *est confluent.*

4.3.2 Invariante de la réduction

On observe que le beta-reduction (linéaire ou non) ne change jamais les registres.

Proposition 4.3.4. *Soit* $(e_0, e_1) \in \mathscr{E}^2$.
Si $e_0 \to_! e_1$ *ou* $e_0 \to_\beta e_1$ *alors* $RE(\mathscr{T}(e_0)) = RE(\mathscr{T}(e_1))$.

Proof. Posons $e_0 = [Q_n, M]$ et $e_1 = [Q'_n, M']$. Commençons une induction sur les termes.
Si $M = x$, alors l'hypothèse ne tient pas.
Si $M = U_A$, alors l'hypothèse ne tient pas.
Si $M = q_{init}$, alors l'hypothèse ne tient pas.
Si $M = r_i$, alors l'hypothèse ne tient pas.
Si $M =!T$, alors l'hypothèse ne tient pas.
Si $M = \lambda x.T$, alors la réduction se fait à l'intérieur de T.
Par hypothèse d'induction et définition de RE, on conclut.
Si $M = \lambda^! x.T$, alors la réduction se fait à l'intérieur de T.
Par hypothèse d'induction et définition de RE, on conclut.
Si $M = meas(R, M, N)$, alors la réduction se fait à l'intérieur de R. Par hypothèse d'induction et définition de RE, on conclut.
Si $M = T_0 T_1$, plusieurs cas peuvent se présenter.
(1) si la réduction se fait à l'intérieur de T_0, alors on conclut par hypothèse d'induction et définition de RE, on conclut.
(2) si la réduction se fait à l'intérieur de T_1, alors on conclut par hypothèse d'induction et définition de RE, on conclut.
(3) si la réduction se fait avec T_0 le RE- et T_1 le -DEX.
Deux cas sont possibles :
- soit on a !-réduction
- soit on a β-réduction
Si c'est une β-réduction alors pas de problème car l'abstraction est linéaire, donc si r_i apparaît dans T_1 alors il apparaîtra dans le contractum. □

4.4 Expressivité du langage

4.4.1 Un terme qui termine presque-sûrement

Voyons si nous pouvons construire un terme qui termine presque-sûrement.

Pour cela nous avons besoin de créer de multiples Q-bit (qbit), pour pouvoir ensuite les mesurer et en faire des éléments de notre multidistribution.

q_{init} sert à créer des Q-bit initialiser à 0, des $|0\rangle$.

Seulement, en l'état, ce Q-bit ne sert pas à grand-chose. Il faudrait lui superposer un état $|1\rangle$ pour pouvoir créer de multiples éléments.

On va pour cela utiliser la porte quantique d'Hadamard :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Elle transforme un Q-bit d'état $|0\rangle$ en $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

Prenons donc maintenant le terme Δ $(= \lambda^! x.x!x)$.

Regardons comment se comporte $\Delta!\Delta$.

$$\begin{aligned}\Delta!\Delta &= (\lambda^!x.x!x)!\lambda^!x.x!x\\ &\to (\lambda^!x.x!x)!\lambda^!x.x!x(=\Delta!\Delta)\end{aligned}$$

Transformons un peu ce terme pour pouvoir faire apparaître la mesure :

$$\Delta' = \lambda^!x.\mathtt{meas}(U_A\ q_{init}, \lambda^!x.x, \lambda^!x.z)!(x!x)$$

$$\begin{aligned}[,\Delta'!\Delta'] &= \left[,(\lambda^!x.\mathtt{meas}(U_A\ q_{init}, \lambda^!x.x, \lambda^!x.z)!(x!x))!\Delta'\right]\\ &\longrightarrow \left\{\left[,\mathtt{meas}(U_A\ q_{init}, \lambda^!x.x, \lambda^!x.z)!(\Delta'!\Delta')\right]\right\}\\ &\rightrightarrows \left\{\left[|0\rangle, \mathtt{meas}(U_A\ r_0, \lambda^!x.x, \lambda^!x.z)!(\Delta'!\Delta')\right]\right\}\\ &\rightrightarrows \left\{\left[\frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle, \mathtt{meas}(r_0, \lambda^!x.x, \lambda^!x.z)!(\Delta'!\Delta')\right]\right\}\\ &\rightrightarrows \left\{\frac{1}{2}\left[|0\rangle, (\lambda^!x.x)!(\Delta'!\Delta')\right], \frac{1}{2}\left[|1\rangle, (\lambda^!x.z)!(\Delta'!\Delta')\right]\right\}\\ &\rightrightarrows \left\{\frac{1}{2}\left[|0\rangle, \Delta'!\Delta'\right], \frac{1}{2}\left[|1\rangle, z\right]\right\}\left(=\left\{\frac{1}{2}\left[|0\rangle, \left(\lambda^!x.\mathtt{meas}(U_A\ q_{init}, \lambda^!x.x, \lambda^!x.z)!(x!x)\right)!\Delta'\right], \frac{1}{2}\left[|1\rangle, z\right.\right.\right.\\ &\rightrightarrows \left\{\frac{1}{2}\left[|0\rangle, \mathtt{meas}(U_A\ q_{init}, \lambda^!x.x, \lambda^!x.z)!(\Delta'!\Delta')\right], \frac{1}{2}\left[|1\rangle, z\right]\right\}\\ &\rightrightarrows \left\{\frac{1}{2}\left[|00\rangle, \mathtt{meas}(U_A\ r_1, \lambda^!x.x, \lambda^!x.z)!(\Delta'!\Delta')\right], \frac{1}{2}\left[|1\rangle, z\right]\right\}\\ &\rightrightarrows \left\{\frac{1}{2}\left[\frac{\sqrt{2}}{2}|00\rangle + \frac{\sqrt{2}}{2}|01\rangle, \mathtt{meas}(r_1, \lambda^!x.x, \lambda^!x.z)!(\Delta'!\Delta')\right], \frac{1}{2}\left[|1\rangle, z\right]\right\}\\ &\rightrightarrows \left\{\frac{1}{4}\left[|00\rangle, (\lambda^!x.x)!(\Delta'!\Delta')\right], \frac{1}{4}\left[|01\rangle, (\lambda^!x.z)(\Delta'!\Delta')\right], \frac{1}{2}\left[|1\rangle, z\right]\right\}\\ &\rightrightarrows \left\{\frac{1}{4}\left[|00\rangle, \Delta'!\Delta'\right], \frac{1}{4}\left[|01\rangle, z\right], \frac{1}{2}\left[|1\rangle, z\right]\right\}\end{aligned}$$

Essayons maintenant avec ce terme :

$$\Delta' = \lambda^!x.\mathtt{meas}(U_A\ q_{init}, x!x, I)$$

On a donc :

$$
\begin{aligned}
[, \Delta'!\Delta'] &= \left[, (\lambda^! x.\texttt{meas}(U_A\ q_{init}, x!x, I))!\Delta'\right] \\
&\longrightarrow \{[, \texttt{meas}(U_A\ q_{init}, \Delta'!\Delta', I)]\} \\
&\rightrightarrows \{[|0\rangle, \texttt{meas}(U_A\ r_0, \Delta'!\Delta', I)]\} \\
&\rightrightarrows \left\{\left[\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \texttt{meas}(r_0, \Delta'!\Delta', I)\right]\right\} \\
&\rightrightarrows \left\{\frac{1}{2}[|0\rangle, \Delta'!\Delta'], \frac{1}{2}[|1\rangle, I]\right\} \left(= \left\{\frac{1}{2}\left[|0\rangle, (\lambda^! x.\texttt{meas}(U_A\ q_{init}, x!x, I))!\Delta'\right], \frac{1}{2}[|1\rangle, I]\right\}\right) \\
&\rightrightarrows \left\{\frac{1}{2}[|0\rangle, \texttt{meas}(U_A\ q_{init}, \Delta'!\Delta', I)], \frac{1}{2}[|1\rangle, I]\right\} \\
&\rightrightarrows \left\{\frac{1}{2}[|00\rangle, \texttt{meas}(U_A\ r_1, \Delta'!\Delta', I)], \frac{1}{2}[|1\rangle, I]\right\} \\
&\rightrightarrows \left\{\frac{1}{2}\left[\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle, \texttt{meas}(r_1, \Delta'!\Delta', I)\right], \frac{1}{2}[|1\rangle, I]\right\} \\
&\rightrightarrows \left\{\frac{1}{4}[|00\rangle, \Delta'!\Delta'], \frac{1}{4}[|01\rangle, I], \frac{1}{2}[|1\rangle, I]\right\}
\end{aligned}
$$

On retrouve à chaque fois le même terme I au lieu de la variable z.

4.4.2 Paires usuelles

Dans le lambda calcul, on peut définir les paires, comme ceci :

$$\langle a, b\rangle = \lambda f.fab$$

On a aussi la projection de la 1er et 2ième coordonnée :

$$fst := \lambda x.\lambda y.x$$

$$snd := \lambda x.\lambda y.y$$

On aimerait bien redéfinir ces termes avec notre calcul en utilisant le bang ("!").

Il faut déjà modifier fst et snd pour que ce soit des termes correctes. En effet, dans fst, le y n'est pas linéaire, de même que le x dans le snd.

$$fst := \lambda x.\lambda^! y.x$$

$$snd := \lambda^! x.\lambda y.y$$

Mais alors il faut modifier le constructeur de paire :

$$\langle a, b\rangle = \lambda f.f!a!b$$

Et ainsi les deux destructeurs :

$$fst := \lambda^! x.\lambda^! y.x$$

$$snd := \lambda^! x.\lambda^! y.y$$

Chapter 5

Terminaison probabiliste

5.1 Terminaison et Probabilité

Donnée une multidistribution m, qui représente un système quantique, on définit sa probabilité d'être en forme normale ($\mathbb{P}$) comme :

Définition 5.1.1 (probabilité d'être en forme normale $\mathbb{P}$)**.** On définit $\mathbb{P} : MDST(\mathscr{E}) \to [0,1]$ comme :

$$\mathbb{P}(m) = \sum_{\substack{p_e e \in m \\ \mathscr{T}(e) \text{ normal}}} p_e$$

Exemple. 1) $m_1 = \left\{\frac{3}{4}\left[|010\rangle, r_0\right], \frac{1}{4}\left[|1\rangle, \Delta!\Delta\right]\right\}$
On a $\mathbb{P}(m) = \frac{3}{4}$

2) $m_2 = \left\{\frac{1}{4}\left[|00\rangle, \Delta'!\Delta'\right], \frac{1}{4}\left[|01\rangle, I\right], \frac{1}{2}\left[|1\rangle, I\right]\right\}$
On a $\mathbb{P}(m) = \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$.

Remarque. L'intervalle $[0,1] \subseteq \mathbb{R}$ est fermé donc pour toute suite croissantes $(x_n)_{n\in\mathbb{N}}(0 \leq x_n \leq 1)$ $sup_{n\in\mathbb{N}}\ x_n \in [0,1]$. $[0,1]$ avec l'ordre usuel est un ω-*cpo*.

Lemme 5.1.2 (Croissance de $\mathbb{P}$)**.** *Soit* $(m, m') \in MDST(\mathscr{E})^2$,

$$si\ m \rightrightarrows m'\ alors\ \mathbb{P}(m) \leqslant \mathbb{P}(m')$$

Corollaire 5.1.3 (Existence du Sup)**.** *Soit une réduction de séquence* $(m_n)_{n\in\mathbb{N}}$*, alors la séquence* $(\mathbb{P}(m_n))_{n\in\mathbb{N}}$ *est monotone et croissante.*
De plus, le $sup_{n\in\mathbb{N}}(\mathbb{P}(m_n))$ *existe.*

Ce corollaire nous permet de bien définir la terminologie suivante :

Définition 5.1.4 (Probabilité de terminaison)**.** Soit $(m_n)_{n\in\mathbb{N}}$ une séquence de réduction.
On définit :
$(m_n) \Downarrow p$ si $sup_{n\in\mathbb{N}}(\mathbb{P}(m_n)) = p$

Dans la prochaine section, nous allons prouver le Théorème 5.3.5 qui nous dit qu'étant donné deux séquences de réduction (m_n) et (r_n) à partir du même état $e \in \mathscr{E}^!$, la séquence $(\mathbb{P}(m_n))$ est égale à la séquence $(\mathbb{P}((r_n))$. En conséquence, toutes les séquences de réduction à partir d'un même état ($e \in \mathscr{E}^!$) ont la même limite (le même sup).

Ceci nous permet la définition suivante.

Définition 5.1.5. Soit $e \in \mathscr{E}^!$, on définit $e \Downarrow p$ comme étant l'unique sup d'une séquence de réduction à partir de $\{e\}$.

Dans la prochaine section, on va prouver cette propriété.

5.2 Observations

On va prouver une propriété plus forte que la propriété voulue. On définit la restriction aux formes normales de la multidistribution m :

Définition 5.2.1 (*obs*)**.** On définit $obs : MDST(\mathscr{E}^!) \to MDST(\mathscr{E}^!)$ comme :

$$obs\,(m) = \{p_e\ e \mid e \in m \text{ et } \mathscr{T}\,(e)\ \text{normal}\}$$

La fonction *obs* est croissante (avec le respect de l'inclusion des multidistributions) :

Proposition 5.2.2 (Croissance de *obs*)**.** *Soit $e \in \mathscr{E}^!$ et $m \in MDST(\mathscr{E}^!)$,*

$$\textit{si } \{e\} \rightrightarrows m \textit{ alors } obs(\{e\}) \subseteq obs(m)$$

Démonstration. Si $\mathscr{T}\,(e)$ est en forme normale alors $\{e\} = m$ et donc $obs(\{e\}) = obs(m)$.

Si $\mathscr{T}\,(e)$ n'est pas en forme normale alors $obs(\{e\}) = \emptyset$.
Et donc $obs(\{e\}) \subseteq obs(m)$. □

Lemme 5.2.3. *Les propriétés sur obs implique les propriétés sur $\mathbb{P}$.*

5.3 Déterminisme essentiel et limite unique

Définition 5.3.1 (Diamant pointé)**.** Soit $e \in \mathscr{E}^!$, on dit que e a la propriété du diamant pointé si :

$$t \leftarrow e \to s \Rightarrow obs(t) = obs(s)\ \text{, et il existe } r \in MDST\left(\mathscr{E}^!\right) \text{ tel que } t \rightrightarrows r\ \&\ s \rightrightarrows r.$$

Ce qui suit généralise la définition de Random Descent que nous avions donné au Chapitre 1.

Définition 5.3.2 (Random Descent)**.** Soit $e \in \mathscr{E}^!$, soit deux séquences de réductions $(m_n)_{n\in\mathbb{N}}$ et $(r_n)_{n\in\mathbb{N}}$ à partir de e alors la séquence $(obs(m_n))_{n\in\mathbb{N}}$ est égale à la séquence $(obs(r_n))_{n\in\mathbb{N}}$.

Proposition 5.3.3. *La propriété de Diamant pointé implique la propriété de la Random Descent.*

Démonstration. La preuve est donnée dans l'article "Probabilistic Rewriting: on Normalization, Termination, and Unique Normal Forms" de Claudia Faggian. □

Proposition 5.3.4. *Le calcul $Q^!$ satisfait la propriété du diamant pointé.*

Remarque. Donc $Q^!$ a la prop de la random descent.
Donc le sup est unique.

Théorème 5.3.5. *Étant donné un état $e \in \mathscr{E}^!$, toute séquence de réduction à partir de e a la même limite. C'est à dire : si $(m_n), (r_n)$ sont deux séquences de réductions à partir de $\{e\} = m_0 = r_0$ alors : $(m_n) \Downarrow p$ si et seulement si $(r_n) \Downarrow p$.*

Chapter 6

Résumé

6.1 Le calcul $Q = (\mathscr{E}, \rightarrow_Q)$

Beta-réduction linéaire	
remplacement de variable	$[Q_n, \mathbf{S}\,((\lambda x.M)\,N)] \rightarrow_\beta [Q_n, \mathbf{S}\,(M\,[x := N])]$
Réduction quantique	
création d'un Q-Bit	$[Q_n, \mathbf{S}\,(q_{init})] \rightarrow_q [Q_n \otimes \left\|0\right\rangle, \mathbf{S}\,(r_n)]$
application de U_A : qbit $\rightarrow$ qbit	$[Q_n, \mathbf{S}\,(U_A r_i)] \rightarrow_{U_A^{(1)}} \left[I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n, \mathbf{S}\,(r_i)\right]$
application de U_A : qbit $\times$ qbit $\rightarrow$ qbit $\times$ qbit	$[Q_n, \mathbf{S}\,(U_A \langle r_i, r_j\rangle)] \rightarrow_{U_A^{(2)}} \left[(A \otimes I^{\otimes n-2} Q_n^{\sigma_{i,j}})^{\sigma_{i,j}}, \mathbf{S}\,(\langle r_i, r_j\rangle)\right]$

Table 6.1: Réduction $\rightarrow_Q \;:=\; \rightarrow_\beta \cup \rightarrow_q \cup \rightarrow_{U_A^{(1)}} \cup \rightarrow_{U_A^{(2)}}$

6.2 Lifting d'une relation $\rightarrow \subset \mathscr{E} \times MDST\,(\mathscr{E})$

Pour toute relation $\rightarrow \subset \mathscr{E} \times MDST\,(\mathscr{E})$, réduisant un état à une multidistribution d'état, on peut définir son lifting dans une relation $\rightrightarrows \subset MDST\,(\mathscr{E}) \times MDST\,(\mathscr{E})$:

Lifting de $\to$	
Forme normale	$\dfrac{e \not\to}{\{e\} \rightrightarrows \{e\}}$
Règle de mise en forme	$\dfrac{e \to m}{\{e\} \rightrightarrows m}$
Règle de la somme	$\dfrac{(\{e_i\} \rightrightarrows m_i)_{i \in I}}{\{p_i e_i \mid i \in I\} \rightrightarrows \sum_{i \in I} p_i m_i}$

Table 6.2: Réduction $\rightrightarrows$

Dans les deux prochaines sections, on va instancier la flèche $\to$ par $\to_{Q^{meas}}$ et $\to_{Q^!}$.

6.3 Le calcul $Q^{meas} = (MDST(\mathscr{E}^{meas}), \rightrightarrows_{Q^{meas}})$

$\mathscr{E}^{meas}$ est l'ensemble des états, comme défini en 3.2.1.

La relation $\rightrightarrows_{Q^{meas}} \subset MDST(\mathscr{E}^{meas}) \times MDST(\mathscr{E}^{meas})$ est le lifting (comme défini en 3.2.7) de la relation $\to_{Q^{meas}} \subset \mathscr{E}^{meas} \times MDST(\mathscr{E}^{meas})$ comme défini ci-dessous.

Beta-réduction linéaire	
remplacement de variable	$[Q_n, \mathbf{S}\left((\lambda x.M)\, N\right)] \rightarrow_\beta \{[Q_n, \mathbf{S}\left(M\left[x := N\right]\right)]\}$
Réduction quantique	
création d'un Q-Bit	$[Q_n, \mathbf{S}\left(q_{init}\right)] \rightarrow_q \{[Q_n \otimes \left\|0\right\rangle, \mathbf{S}\left(r_n\right)]\}$
application de U_A : qbit $\rightarrow$ qbit	$[Q_n, \mathbf{S}\left(U_A r_i\right)] \rightarrow_{U_A^{(1)}} \left\{\left[I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n, \mathbf{S}\left(r_i\right)\right]\right\}$
application de U_A : qbit $\times$ qbit $\rightarrow$ qbit $\times$ qbit	$[Q_n, \mathbf{S}\left(U_A \langle r_i, r_j\rangle\right)] \rightarrow_{U_A^{(2)}} \left\{\left[(A \otimes I^{\otimes n-2} Q_n^{\sigma_{i,j}})^{\sigma_{i,j}}, \mathbf{S}\left(\langle r_i, r_j\rangle\right)\right]\right\}$

Table 6.3: $\rightarrow_Q \subset \mathscr{E} \times MDST\left(\mathscr{E}\right)$

Mesure de Q-Bit	
Mesure d'un Q-Bit	$[Q_n, \mathbf{S}\left(\texttt{meas}(r_i, M, N)\right)] \rightarrow_{meas} \left\{\left\|\alpha\right\|^2 [L_n, \mathbf{S}\left(M\right)], \left\|\beta\right\|^2 [R_n, \mathbf{S}\left(N\right)]\right\}$

Table 6.4: Réduction $\rightarrow_{meas}$

On définit :

$$\rightarrow_{Q^{meas}} \quad := \quad \rightarrow_\beta \cup \rightarrow_q \cup \rightarrow_{U_A^{(1)}} \cup \rightarrow_{U_A^{(2)}} \cup \rightarrow_{meas}$$

6.4 Le calcul $Q^! = (\mathscr{E}^!, \rightrightarrows_{Q^!})$

$\mathscr{E}^!$ est l'ensemble des états, comme défini en 4.2.1.

La relation $\rightrightarrows_{Q^!} \subset MDST\left(\mathscr{E}^!\right) \times MDST\left(\mathscr{E}^!\right)$ est le lifting (comme défini en 4.2.4) de la relation $\rightarrow_{Q^!} \subset \mathscr{E}^! \times MDST\left(\mathscr{E}^!\right)$ comme défini ci-dessous.

Beta réduction non-linéaire	
remplacement de variable bang	$\left[Q_n, \mathbf{S}\left((\lambda^! x.M)!N\right)\right] \to_! \{[Q_n, \mathbf{S}\left(M[x := N]\right)]\}$

Table 6.5: Réduction $\to_!$

On définit :

$$\to_{Q^!} \quad := \quad \to_{Q^{meas}} \cup \to_!$$

Appendix A

Produit tensoriel

A.1 Commutativité de la mémoire

(Géométrie of parrallelism , screenshot sur la mémoire commutative) On démontre ici que toutes les opérations sur la mémoires sont commutatives. =¿ Prendre le diagramme de Benoît.

Lemme A.1.1 (q_{init} et q_{init})**.** *Les modifications sur la mémoire dû à q_{init} et q_{init} (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. On a $|0\rangle \otimes |0\rangle =$ Et à permutation des registres près, on a le même terme (σ-équivalence). □

Lemme A.1.2 (q_{init} et $U_A^{(1)}$)**.** *Les modifications sur la mémoire dû à q_{init} et $U_A^{(1)}$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. On a que :

$$\begin{aligned}
(I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i+1})(Q_n \otimes |0\rangle) &= (I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i+1})\left(\left(\sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b\rangle\right) \otimes |0\rangle\right) \\
&= (I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i+1})\left(\sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b (|b\rangle \otimes |0\rangle)\right) \\
&= (I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i+1})\left(\sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b_0 \ldots b_{n-1}0\rangle\right) \\
&= \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b(|b_0 \ldots b_{i-1}\rangle \otimes A |b_i\rangle \otimes |b_{i+1} \ldots b_{n-1}0\rangle)
\end{aligned}$$

et que :

$$
\begin{aligned}
(I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} Q_n) \otimes |0\rangle &= (I^{\otimes i-1} \otimes A \otimes I^{\otimes n-i} \left(\sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b_0 \ldots b_{n-1}\rangle \right)) \otimes |0\rangle \\
&= \left(\sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b_0 \ldots b_{i-1}\rangle \otimes A |b_i\rangle \otimes |b_{i+1} \ldots b_{n-1}\rangle \right) \otimes |0\rangle \\
&= \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b_0 \ldots b_{i-1}\rangle \otimes A |b_i\rangle \otimes |b_{i+1} \ldots b_{n-1}\rangle \otimes |0\rangle \\
&= \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b_0 \ldots b_{i-1}\rangle \otimes A |b_i\rangle \otimes |b_{i+1} \ldots b_{n-1} 0\rangle
\end{aligned}
$$

□

Lemme A.1.3 (q_{init} et $U_A^{(2)}$)**.** *Les modifications sur la mémoire dû à q_{init} et $U_A^{(2)}$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. On a :

$$
\begin{aligned}
((A \otimes I^{\otimes (n+1)-2}(Q_n \otimes |0\rangle)^{\sigma_{i,j}})^{\sigma_{i,j}} &= ((A \otimes I^{\otimes (n+1)-2}(\sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b |b0\rangle)^{\sigma_{i,j}})^{\sigma_{i,j}} \\
&= (A \otimes I^{\otimes (n+1)-2} \sum_{b'=(b_{\sigma_{i,j}(0)},\ldots,b_{\sigma_{i,j}(n-1)})} \alpha_b |b'0\rangle)^{\sigma_{i,j}} \\
&= (A \otimes I^{\otimes (n-1)} \sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\ldots,b_{\sigma_{i,j}(n-1)})} \alpha_b |b_i\ b_j\rangle \otimes |b_{\sigma_{i,j}(2)} \ldots b_{\sigma_{i,j}(n-1)}\ 0\rangle)^{\sigma_{i,j}} \\
&= (\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\ldots,b_{\sigma_{i,j}(n-1)})} \alpha_b A |b_i\ b_j\rangle \otimes |b_{\sigma_{i,j}(2)} \ldots b_{\sigma_{i,j}(n-1)}\ 0\rangle)^{\sigma_{i,j}}
\end{aligned}
$$

De plus :

$$
\begin{aligned}
((A \otimes I^{\otimes n-2} Q_n^{\sigma_{i,j}})^{\sigma_{i,j}}) \otimes |0\rangle &= ((A \otimes I^{\otimes n-2} \sum_{b'=(b_{\sigma_{i,j}(0)},\ldots,b_{\sigma_{i,j}(n-1)})} \alpha_b |b'\rangle)^{\sigma_{i,j}}) \otimes |0\rangle \\
&= ((\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\ldots,b_{\sigma_{i,j}(n-1)})} \alpha_b A |b_i\ b_j\rangle \otimes |b_{\sigma_{i,j}(2)} \ldots b_{\sigma_{i,j}(n-1)}\rangle)^{\sigma_{i,j}}) \otimes |0\rangle \\
&= (\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\ldots,b_{\sigma_{i,j}(n-1)})} \alpha_b A |b_i\ b_j\rangle \otimes |b_{\sigma_{i,j}(2)} \ldots b_{\sigma_{i,j}(n-1)}\ 0\rangle)^{\sigma_{i,j}}
\end{aligned}
$$

$(car\ j < n\ et\ i < n)$

□

Lemme A.1.4 (q_{init} et $\texttt{meas}(\cdot,\cdot,\cdot)$)**.** *Les modifications sur la mémoire dû à q_{init} et $\texttt{meas}(\cdot,\cdot,\cdot)$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. La réduction de q_{init} crée à chaque fois un nouveau qbit, on a donc $i \neq n$. Donc le qbit mesuré à 0 ou 1 (séparant ainsi la mémoire e) ne peut être le n-ième qbit. Posons :

$$Q_n = \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b \left|b\right\rangle$$

Alors, pour la réduction (2), on a :

$$L_n = \sum_{b'=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b'}}{\alpha} \left|b'\right\rangle$$

et que :

$$R_n = \sum_{b''=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b''}}{\beta} \left|b''\right\rangle$$

On a donc que :

$$\begin{aligned} L_n \otimes \left|0\right\rangle &= \left(\sum_{b'=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b'}}{\alpha} \left|b'\right\rangle \right) \otimes \left|0\right\rangle \\ &= \sum_{b'=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b'}}{\alpha} \left|b'\right\rangle \otimes \left|0\right\rangle \\ &= \sum_{b'=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b'}}{\alpha} \left|b'\ 0\right\rangle \end{aligned}$$

et que :

$$\begin{aligned} R_n \otimes \left|0\right\rangle &= \left(\sum_{b''=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b''}}{\beta} \left|b''\right\rangle \right) \otimes \left|0\right\rangle \\ &= \sum_{b''=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b''}}{\beta} \left|b''\right\rangle \otimes \left|0\right\rangle \\ &= \sum_{b''=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{n-1})} \frac{\alpha_{b''}}{\beta} \left|b''\ 0\right\rangle \end{aligned}$$

En ce qui concerne la réduction (1), on a :

$$\begin{aligned} Q_n \otimes \left|0\right\rangle &= \left(\sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b \left|b\right\rangle \right) \otimes \left|0\right\rangle \\ &= \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b \left|b\right\rangle \otimes \left|0\right\rangle \\ &= \sum_{b=(b_0,\ldots,b_{n-1})} \alpha_b \left|b\ 0\right\rangle \end{aligned}$$

L'espace de probabilité qui en résulte est le même que pour Q_n (les coefficients α_b sont les mêmes). En appliquant à cette mémoire la réduction meas pour le qbit i, on obtient d'une part :

$$\sum_{b'=(b_0,...,b_{i-1},0,b_{i+1},...,b_{n-1})} \alpha_{b'} \left|b'\ 0\right\rangle$$

Et l'on retrouve $L_n \otimes |0\rangle$. Et de l'autre part :

$$\sum_{b''=(b_0,...,b_{i-1},1,b_{i+1},...,b_{n-1})} \alpha_{b''} \left|b''\ 0\right\rangle$$

Et l'on retrouve $R_n \otimes |0\rangle$.
On a donc :

$$\{[Q_n \otimes |0\rangle, \mathscr{C}(r_n, \texttt{meas}(r_i, M, N))]\} \rightrightarrows \left\{|\alpha|^2 [L_n \otimes |0\rangle, \mathscr{C}(r_n, M)], |\beta|^2 [R_n \otimes |0\rangle, \mathscr{C}(r_n, N)]\right\}$$

□

Lemme A.1.5 ($U_{A_1}^{(1)}$ et $U_{A_2}^{(1)}$)**.** *Les modifications sur la mémoire dû à $U_{A_1}^{(1)}$ et $U_{A_2}^{(1)}$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. On a que :

$$\begin{aligned}
&I^{\otimes i_2-1} \otimes A_2 \otimes I^{\otimes n-i_2}(I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1} Q_n \\
&= I^{\otimes i_2-1} \otimes A_2 \otimes I^{\otimes n-i_2} \left(\sum_{b=(b_0,...,b_{n-1})} \alpha_b \left|b_0...b_{i_1-1}\right\rangle \otimes A_1 \left|b_{i_1}\right\rangle \otimes \left|b_{i_1+1}, ..., b_{n-1}\right\rangle \right) \\
= &\sum_{b=(b_0,...,b_{n-1})} \alpha_b \left|b_0...b_{i_1-1}\right\rangle \otimes A_1 \left|b_{i_1}\right\rangle \otimes \left|b_{i_1+1}, ..., b_{i_2-1}\right\rangle \otimes A_2 \left|b_{i_2}\right\rangle \otimes \left|b_{i_2+1}, ..., b_{n-1}\right\rangle
\end{aligned}$$

Et que :

$$\begin{aligned}
&I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1}(I^{\otimes i_2-1} \otimes A_2 \otimes I^{\otimes n-i_2} Q_n \\
&= I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1} \left(\sum_{b=(b_0,...,b_{n-1})} \alpha_b \left|b_0...b_{i_2-1}\right\rangle \otimes A_2 \left|b_{i_2}\right\rangle \otimes \left|b_{i_2+1}, ..., b_{n-1}\right\rangle \right) \\
= &\sum_{b=(b_0,...,b_{n-1})} \alpha_b \left|b_0...b_{i_1-1}\right\rangle \otimes A_1 \left|b_{i_1}\right\rangle \otimes \left|b_{i_1+1}, ..., b_{i_2-1}\right\rangle \otimes A_2 \left|b_{i_2}\right\rangle \otimes \left|b_{i_2+1}, ..., b_{n-1}\right\rangle
\end{aligned}$$

□

Lemme A.1.6 ($U_{A_1}^{(1)}$ et $U_{A_2}^{(2)}$)**.** *Les modifications sur la mémoire dû à $U_{A_1}^{(1)}$ et $U_{A_2}^{(2)}$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. On a :

$$(A_2 \otimes I^{\otimes n-2}(I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1} Q_n)^{\sigma_{i,j}})^{\sigma_{i,j}}$$

$$= (A_2 \otimes I^{\otimes n-2}(\sum_{b=(b_0,\dots,b_{n-1})} \alpha_b \left|b_0 \dots b_{i_1-1}\right\rangle \otimes A_1 \left|b_{i_1}\right\rangle \otimes \left|b_{i_1+1} \dots b_{n-1}\right\rangle)^{\sigma_{i,j}})^{\sigma_{i,j}}$$

$$= (A_2 \otimes I^{\otimes n-2} \sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)} \dots, b_{\sigma_{i,j}(n-1)})} \alpha_b \left|b_i, b_j, b_{\sigma_{i,j}(2)}, \dots b_{\sigma_{i,j}(i_1-1)}\right\rangle \otimes A_1 \left|b_{i_1}\right\rangle \otimes \left|b_{\sigma_{i,j}(i_1+1)} \dots b_{\sigma_{i,j}(n-1)}\right\rangle)^{\sigma_{i,j}}$$

$$= (\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)} \dots, b_{\sigma_{i,j}(n-1)})} \alpha_b A_2 \left|b_i, b_j\right\rangle \otimes \left|b_{\sigma_{i,j}(2)}, \dots b_{\sigma_{i,j}(i_1-1)}\right\rangle \otimes A_1 \left|b_{i_1}\right\rangle \otimes \left|b_{\sigma_{i,j}(i_1+1)} \dots b_{\sigma_{i,j}(n-1)}\right\rangle)^{\sigma_{i,j}}$$

D'autre part :

$$I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1}(A_2 \otimes I^{\otimes n-2} Q_n^{\sigma_{i,j}})^{\sigma_{i,j}}$$

$$= I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1}(A_2 \otimes I^{\otimes n-2} \sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\dots,b_{\sigma_{i,j}(n-1)})} \alpha_b \left|b_i\ b_j\ b_{\sigma_{i,j}(2)} \dots b_{\sigma_{i,j}(n-1)}\right\rangle)^{\sigma_{i,j}}$$

$$= I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1}(\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\dots,b_{\sigma_{i,j}(n-1)})} \alpha_b A \left|b_i\ b_j\ \right\rangle \otimes \left|b_{\sigma_{i,j}(2)} \dots b_{\sigma_{i,j}(n-1)}\right\rangle)^{\sigma_{i,j}}$$

$$= I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1}(\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\dots,b_{\sigma_{i,j}(n-1)})} \alpha_b A_2 \left|b_i\ b_j\ \right\rangle \otimes \left|b_{\sigma_{i,j}(2)} \dots b_{\sigma_{i,j}(i_1-1)}\right\rangle \otimes \left|b_{\sigma_{i,j}(i_1)}\right\rangle \otimes$$
$$\left|b_{\sigma_{i,j}(i_1+1)} \dots b_{\sigma_{i,j}(n-1)}\right\rangle)^{\sigma_{i,j}}$$

$$= I^{\otimes i_1-1} \otimes A_1 \otimes I^{\otimes n-i_1}(\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\dots,b_{\sigma_{i,j}(n-1)})} \alpha_b A_2 \left|b_i\ b_j\ \right\rangle \otimes \left|b_{\sigma_{i,j}(2)} \dots b_{\sigma_{i,j}(i_1-1)}\right\rangle \otimes \left|b_{i_1}\right\rangle \otimes$$
$$\left|b_{\sigma_{i,j}(i_1+1)} \dots b_{\sigma_{i,j}(n-1)}\right\rangle)^{\sigma_{i,j}}$$

$$= (\sum_{b'=(b_i,b_j,b_{\sigma_{i,j}(2)},\dots,b_{\sigma_{i,j}(n-1)})} \alpha_b A_2 \left|b_i\ b_j\ \right\rangle \otimes \left|b_{\sigma_{i,j}(2)} \dots b_{\sigma_{i,j}(i_1-1)}\right\rangle \otimes A_1 \left|b_{i_1}\right\rangle \otimes \left|b_{\sigma_{i,j}(i_1+1)} \dots b_{\sigma_{i,j}(n-1)}\right\rangle)^{\sigma_{i,j}}$$

□

Lemme A.1.7 ($U_A^{(1)}$ et $\texttt{meas}(\cdot,\cdot,\cdot)$)**.** *Les modifications sur la mémoire dû à $U_A^{(1)}$ et $\texttt{meas}(\cdot,\cdot,\cdot)$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. Il faut donc vérifier que les probabilités α' et β' issus de cette réduction sont les mêmes que dans la multidistribution $\left\{|\alpha|^2 \left[I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} L_n, \mathscr{C}(r_j, M)\right], |\beta|^2 \left[I^{\otimes j-1} \otimes A \otimes I^{\right.}\right.$ c'est à dire que $\alpha = \alpha'$ et que $\beta = \beta'$.

Ensuite, il nous suffira de voir que :

$$L'_n = I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} L_n$$

et

$$R'_n = I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} R_n$$

Deux cas possible, $i < j$ ou $j < i$.
Sans perte de généralité, admettons que $i < j$.

$I^{j-1} \otimes A \otimes I^{n-j} Q_n$

$= I^{j-1} \otimes A \otimes I^{n-j} \sum_{b=(b_0,...,b_{n-1})} \alpha_b |b\rangle$

$= \sum_{b=(b_0,...,b_{n-1})} \alpha_b |b_0...b_{j-1}\rangle \otimes A|b_j\rangle \otimes |b_{j+1}...b_{n-1}\rangle$

$= \sum_{b=(b_0,...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ b_i\ b_{i+1}...b_{j-1}\rangle \otimes A|b_j\rangle \otimes |b_{j+1}...b_{n-1}\rangle$

$= \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes A|b_j\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes A|b_j\rangle \otimes |b_{j+1}...b_{n-1}\rangle$

$= \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes A|0\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes A|1\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes A|0\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes A|1\rangle \otimes |b_{j+1}...b_{n-1}\rangle$

Supposons que A = $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$

$= \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes (a_{1,1}|0\rangle + a_{2,1}|1\rangle) \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes (a_{1,2}|0\rangle + a_{2,2}|1\rangle) \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes (a_{1,1}|0\rangle + a_{2,1}|1\rangle) \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes (a_{1,2}|0\rangle + a_{2,2}|1\rangle) \otimes |b_{j+1}...b_{n-1}\rangle$

$= \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes a_{1,1}|0\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes a_{2,1}|1\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes a_{1,2}|0\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},0,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\rangle \otimes a_{2,2}|1\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes a_{1,1}|0\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},0,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes a_{2,1}|1\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes a_{1,2}|0\rangle \otimes |b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b=(b_0,...,b_{i-1},1,b_{i+1},...,b_{j-1},1,b_{j+1},...,b_{n-1})} \alpha_b |b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\rangle \otimes a_{2,2}|1\rangle \otimes |b_{j+1}...b_{n-1}\rangle$

$$
\begin{aligned}
&= \sum_{b=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{j-1},0,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{1,1} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{j-1},0,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{2,1} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{j-1},1,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{1,2} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b=(b_0,\ldots,b_{i-1},0,b_{i+1},\ldots,b_{j-1},1,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{2,2} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{j-1},0,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{1,1} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{j-1},0,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{2,1} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{j-1},1,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{1,2} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b=(b_0,\ldots,b_{i-1},1,b_{i+1},\ldots,b_{j-1},1,b_{j+1},\ldots,b_{n-1})} \alpha_b a_{2,2} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{1,1} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1},\ldots,b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{2,1} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1}\ \ldots\ b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{1,2} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{2,2} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1},\ldots,b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{1,1} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{2,1} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{1,2} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{2,2} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{1,1} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1}\ \ldots\ b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{1,2} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1},\ldots,b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{2,1} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{2,2} \left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1},\ldots,b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{1,1} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{1,2} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{2,1} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \alpha_{b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{2,2} \left|b_0 \ldots b_{i-1}\ 1\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}\right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} (\alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{1,1} + \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1}\ \ldots\ b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{1,2}) \\
&\left|b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}\right\rangle \\
&+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} (\alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1},\ldots,b_{j-1}\ 0\ b_{j+1} \ldots b_{n-1}} a_{2,1} + \alpha_{b_0 \ldots b_{i-1}\ 0\ b_{i+1} \ldots b_{j-1}\ 1\ b_{j+1} \ldots b_{n-1}} a_{2,2})
\end{aligned}
$$

$|b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} (\alpha_{b_0...b_{i-1}\ 1\ b_{i+1},...,b_{j-1}\ 0\ b_{j+1}...b_{n-1}} a_{1,1} + \alpha_{b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}} a_{1,2})$
$|b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\ 0\ b_{j+1}...b_{n-1}\rangle$
$+ \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} (\alpha_{b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\ 0\ b_{j+1}...b_{n-1}} a_{2,1} + \alpha_{b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}} a_{2,2})$
$|b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}\rangle$

Prouvons maintenant que $\alpha = \alpha'$.
On pose $b' = b_0...b_{i-1}\ 0\ b_{i+1}, ..., b_{j-1}\ 0\ b_{j+1}...b_{n-1}$ Et $b'' = b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}$

$$\begin{aligned}
\alpha' &= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'} a_{1,1} + \alpha_{b''} a_{1,2}|^2 + \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'} a_{2,1} + \alpha_{b''} a_{2,2}|^2} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'} a_{1,1} + \alpha_{b''} a_{1,2}|^2 + |\alpha_{b'} a_{2,1} + \alpha_{b''} a_{2,2}|^2} \\
&= \sqrt{\sum_{b',b''} |\alpha_{b'} a_{1,1}|^2 + |\alpha_{b''} a_{1,2}|^2 + \alpha_{b'} a_{1,1} \overline{\alpha_{b''} a_{1,2}} + \overline{\alpha_{b'} a_{1,1}} \alpha_{b''} a_{1,2} + |\alpha_{b'} a_{2,1}|^2 + |\alpha_{b''} a_{2,2}|^2 + \alpha_{b'} a_{2,1} \overline{\alpha_{b''} a_{2,2}} + \overline{\alpha_{b'} a_{2,1}} \alpha_{b''} a_{2,2}} \\
&= \sqrt{\sum_{b',b''} |\alpha_{b'}|^2 |a_{1,1}|^2 + |\alpha_{b''}|^2 |a_{1,2}|^2 + \alpha_{b'} a_{1,1} \overline{\alpha_{b''} a_{1,2}} + \overline{\alpha_{b'} a_{1,1}} \alpha_{b''} a_{1,2} + |\alpha_{b'}|^2 |a_{2,1}|^2 + |\alpha_{b''}|^2 |a_{2,2}|^2 + \alpha_{b'} a_{2,1} \overline{\alpha_{b''} a_{2,2}} + \overline{\alpha_{b'} a_{2,1}} \alpha_{b''} a_{2,2}} \\
&= \sqrt{\sum_{b',b''} |\alpha_{b'}|^2 (|a_{1,1}|^2 + |a_{2,1}|^2) + |\alpha_{b''}|^2 (|a_{1,2}|^2 + |a_{2,2}|^2) + \alpha_{b'} \overline{\alpha_{b''}} (a_{1,1} \overline{a_{1,2}} + a_{2,1} \overline{a_{2,2}}) + \overline{\alpha_{b'}} \alpha_{b''} (\overline{a_{1,1}} a_{1,2} + \overline{a_{2,1}} a_{2,2})}
\end{aligned}$$

On sait que A est une porte quantique, c'est à dire que A est une matrice unitaire. Autrement dit, que $A^*A = I_2$. Ce qui veut dire que :

$$\begin{aligned}
A^*A &= \begin{pmatrix} \overline{a_{1,1}} & \overline{a_{2,1}} \\ \overline{a_{1,2}} & \overline{a_{2,2}} \end{pmatrix} \times \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \\
&= \begin{pmatrix} |a_{1,1}|^2 + |a_{2,1}|^2 & \overline{a_{1,1}} a_{1,2} + \overline{a_{2,1}} a_{2,2} \\ \overline{a_{1,2}} a_{1,1} + \overline{a_{2,2}} a_{2,1} & |a_{1,2}|^2 + |a_{2,2}|^2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

On a donc :

$$\begin{aligned}
\alpha' &= \sqrt{\sum_{b',b''} |\alpha_{b'}|^2 (|a_{1,1}|^2 + |a_{2,1}|^2) + |\alpha_{b''}|^2 (|a_{1,2}|^2 + |a_{2,2}|^2) + \alpha_{b'} \overline{\alpha_{b''}} (a_{1,1} \overline{a_{1,2}} + a_{2,1} \overline{a_{2,2}}) + \overline{\alpha_{b'}} \alpha_{b''} (\overline{a_{1,1}} a_{1,2} + \overline{a_{2,1}} a_{2,2})} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'}|^2 \times 1 + |\alpha_{b''}|^2 \times 1 + \alpha_{b'} \overline{\alpha_{b''}} \times 0 + \overline{\alpha_{b'}} \alpha_{b''} \times 0} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'}|^2 + |\alpha_{b''}|^2} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_j,b_{j+1},...,b_{n-1}} \left|\alpha_{b_0...b_{i-1}\ 0\ b_{i+1},...,b_{j-1}\ b_j\ b_{j+1}...b_{n-1}}\right|^2} \\
&= \alpha \qquad \text{(d'après la propriété 5.6)}
\end{aligned}$$

Prouvons maintenant que $\beta = \beta'$.

On pose $b' = b_0...b_{i-1}\ 1\ b_{i+1},...,b_{j-1}\ 0\ b_{j+1}...b_{n-1}$ Et $b'' = b_0...b_{i-1}\ 1\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}$

$$\begin{aligned}
\beta' &= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'}a_{1,1} + \alpha_{b''}a_{1,2}|^2 + \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'}a_{2,1} + \alpha_{b''}a_{2,2}|^2} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'}a_{1,1} + \alpha_{b''}a_{1,2}|^2 + |\alpha_{b'}a_{2,1} + \alpha_{b''}a_{2,2}|^2} \\
&= \sqrt{\sum_{b',b''} |\alpha_{b'}a_{1,1}|^2 + |\alpha_{b''}a_{1,2}|^2 + \alpha_{b'}a_{1,1}\overline{\alpha_{b''}a_{1,2}} + \overline{\alpha_{b'}a_{1,1}}\alpha_{b''}a_{1,2} + |\alpha_{b'}a_{2,1}|^2 + |\alpha_{b''}a_{2,2}|^2 + \alpha_{b'}a_{2,1}\overline{\alpha_{b''}a_{2,2}} + \overline{\alpha_{b'}a_{2,1}}\alpha_{b''}a_{2,2}} \\
&= \sqrt{\sum_{b',b''} |\alpha_{b'}|^2 |a_{1,1}|^2 + |\alpha_{b''}|^2 |a_{1,2}|^2 + \alpha_{b'}a_{1,1}\overline{\alpha_{b''}a_{1,2}} + \overline{\alpha_{b'}a_{1,1}}\alpha_{b''}a_{1,2} + |\alpha_{b'}|^2 |a_{2,1}|^2 + |\alpha_{b''}|^2 |a_{2,2}|^2 + \alpha_{b'}a_{2,1}\overline{\alpha_{b''}a_{2,2}} + \overline{\alpha_{b'}a_{2,1}}\alpha_{b''}a_{2,2}} \\
&= \sqrt{\sum_{b',b''} |\alpha_{b'}|^2 (|a_{1,1}|^2 + |a_{2,1}|^2) + |\alpha_{b''}|^2 (|a_{1,2}|^2 + |a_{2,2}|^2) + \alpha_{b'}\overline{\alpha_{b''}}(a_{1,1}\overline{a_{1,2}} + a_{2,1}\overline{a_{2,2}}) + \overline{\alpha_{b'}}\alpha_{b''}(\overline{a_{1,1}}a_{1,2} + \overline{a_{2,1}}a_{2,2})}
\end{aligned}$$

Rappel : On sait que A est une porte quantique.
On a donc :

$$\begin{aligned}
\beta' &= \sqrt{\sum_{b',b''} |\alpha_{b'}|^2 (|a_{1,1}|^2 + |a_{2,1}|^2) + |\alpha_{b''}|^2 (|a_{1,2}|^2 + |a_{2,2}|^2) + \alpha_{b'}\overline{\alpha_{b''}}(a_{1,1}\overline{a_{1,2}} + a_{2,1}\overline{a_{2,2}}) + \overline{\alpha_{b'}}\alpha_{b''}(\overline{a_{1,1}}a_{1,2} + \overline{a_{2,1}}a_{2,2})} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'}|^2 \times 1 + |\alpha_{b''}|^2 \times 1 + \alpha_{b'}\overline{\alpha_{b''}} \times 0 + \overline{\alpha_{b'}}\alpha_{b''} \times 0} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} |\alpha_{b'}|^2 + |\alpha_{b''}|^2} \\
&= \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_j,b_{j+1},...,b_{n-1}} \left|\alpha_{b_0...b_{i-1}\ 0\ b_{i+1},...,b_{j-1}\ b_j\ b_{j+1}...b_{n-1}}\right|^2} \\
&= \beta \qquad \text{(d'après la propriété 5.6)}
\end{aligned}$$

On a donc les mêmes probabilités, il reste à vérifier que :

$$L'_n = I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} L_n$$

et

$$R'_n = I^{\otimes j-1} \otimes A \otimes I^{\otimes n-j} R_n$$

D'après les calculs précédents, on a :

$$\begin{aligned}
L'_n = &\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} \frac{\alpha_{b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\ 0\ b_{j+1}...b_{n-1}}a_{1,1} + \alpha_{b_0...b_{i-1}\ 0\ b_{i+1}\ ...\ b_{j-1}\ 1\ b_{j+1}...b_{n-1}}a_{1,2}}{\alpha} \\
&|b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\ 0\ b_{j+1}...b_{n-1}\rangle \\
&+ \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} \frac{\alpha_{b_0...b_{i-1}\ 0\ b_{i+1},...,b_{j-1}\ 0\ b_{j+1}...b_{n-1}}a_{2,1} + \alpha_{b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}}a_{2,2}}{\alpha} \\
&|b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\ 1\ b_{j+1}...b_{n-1}\rangle
\end{aligned}$$

Et on a :

$$\begin{aligned}
&I^{j-1} \otimes A \otimes I^{n-j} L_n \\
&= I^{j-1} \otimes A \otimes I^{n-j} \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \frac{\alpha_{b_0,...b_{i-1}\ 0\ b_{i+1}...b_{n-1}}}{\alpha} |b_0...b_{i-1}\ 0\ b_{i+1}...b_{n-1}\rangle
\end{aligned}$$

$$= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{n-1}}}{\alpha} |b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\rangle \otimes A|b_j\rangle \otimes |b_{j+1}\ldots b_{n-1}\rangle$$

$$= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}}{\alpha} |b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\rangle \otimes A|0\rangle \otimes |b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\alpha} |b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\rangle \otimes A|1\rangle \otimes |b_{j+1}\ldots b_{n-1}\rangle$$

$$= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\rangle \otimes (a_{1,1}|0\rangle + a_{2,1}|1\rangle) \otimes |b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\rangle \otimes (a_{1,2}|0\rangle + a_{2,2}|1\rangle) \otimes |b_{j+1}\ldots b_{n-1}\rangle$$

$$= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}} a_{1,1}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}} a_{2,1}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}} a_{1,2}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}} a_{2,2}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}\rangle$$

$$= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}} a_{1,1}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}} a_{2,1}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}} a_{1,2}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}} a_{2,2}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}\rangle$$

$$= \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}} a_{1,1} + \alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}} a_{1,2}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}\rangle$$
$$+ \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}} a_{2,1} + \alpha_{b_0,\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}} a_{2,2}}{\alpha}$$
$$|b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}\rangle$$

$= L'_n$

De même, pour les coefficients de R'_n. □

Lemme A.1.8 ($U_{A_1}^{(2)}$ et $U_{A_1}^{(2)}$)**.** *Les modifications sur la mémoire dû à $U_A^{(2)}$ et $U_A^{(2)}$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. Vu que les registres ne peuvent pas être présent plus d'une fois dans chaque terme, on a donc que i_1, j_1, i_2, j_2 sont deux à deux distincts.

On a donc d'une part :

$$(A_2 \otimes I^{\otimes n-2}((A_1 \otimes I^{\otimes n-2} Q_n^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}})^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2}((A_1 \otimes I^{\otimes n-2} \sum_{b'} \alpha_b \left|b_{i_1}\ b_{j_1}\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}})^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2}((\sum_{b'} \alpha_b A_1 \left|b_{i_1}\ b_{j_1}\right\rangle \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}})^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2}((\sum_{b'} \alpha_b(\beta_1^{(b)} \left|00\right\rangle + \beta_2^{(b)} \left|01\right\rangle + \beta_1^{(b)} \left|10\right\rangle + \beta_1^{(b)} \left|11\right\rangle) \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}})^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2}((\sum_{b'} \alpha_b(\beta_1^{(b)} \left|00 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle + \beta_2^{(b)} \left|01 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle$$
$$+ \beta_3^{(b)} \left|10 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle + \beta_4^{(b)} \left|11 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle))^{\sigma_{i_1,j_1}})^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2}((\sum_{b'} \alpha_b\beta_1^{(b)} \left|00 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle + \alpha_b\beta_2^{(b)} \left|01 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_3^{(b)} \left|10 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle + \alpha_b\beta_4^{(b)} \left|11 b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle))^{\sigma_{i_1,j_1}})^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2}(\sum_{b} \alpha_b\beta_1^{(b)} \left|b_0...b_{i_1-1}\ 0\ b_{i_1+1}...b_{j_1-1}\ 0\ b_{j_1+1}...b_{n-1}\right\rangle + \alpha_b\beta_2^{(b)} \left|b_0...b_{i_1-1}\ 0\ b_{i_1+1}...b_{j_1-1}\ 1\ b_{j_1+1}...b_{n-}$$
$$+ \alpha_b\beta_3^{(b)} \left|b_0...b_{i_1-1}\ 1\ b_{i_1+1}...b_{j_1-1}\ 0\ b_{j_1+1}...b_{n-1}\right\rangle + \alpha_b\beta_4^{(b)} \left|b_0...b_{i_1-1}\ 1\ b_{i_1+1}...b_{j_1-1}\ 1\ b_{j_1+1}...b_{n-1}\right\rangle)^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2} \sum_{b'} \alpha_b\beta_1^{(b)} \left|b_{\sigma_{i_2,j_2}(0)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_2^{(b)} \left|b_{\sigma_{i_2,j_2}(0)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_3^{(b)} \left|b_{\sigma_{i_2,j_2}(0)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_4^{(b)} \left|b_{\sigma_{i_2,j_2}(0)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle)^{\sigma_{i_2,j_2}}$$

$$= (A_2 \otimes I^{\otimes n-2} \sum_{b'} \alpha_b\beta_1^{(b)} \left|b_{i_2}\ b_{j_2}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_2^{(b)} \left|b_{i_2}\ b_{j_2}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_3^{(b)} \left|b_{i_2}\ b_{j_2}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_4^{(b)} \left|b_{i_2}\ b_{j_2}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle)^{\sigma_{i_2,j_2}}$$

$$= (\sum_{b'} \alpha_b\beta_1^{(b)} A_2 \left|b_{i_2}\ b_{j_2}\right\rangle \otimes \left|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_2^{(b)} A_2 \left|b_{i_2}\ b_{j_2}\right\rangle \otimes \left|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_3^{(b)} A_2 \left|b_{i_2}\ b_{j_2}\right\rangle \otimes \left|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_4^{(b)} A_2 \left|b_{i_2}\ b_{j_2}\right\rangle \otimes \left|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle)^{\sigma_{i_2,j_2}}$$

$$= (\sum_{b'} \alpha_b\beta_1^{(b)}(\gamma_1^{(b)} \left|00\right\rangle + \gamma_2^{(b)} \left|01\right\rangle + \gamma_3^{(b)} \left|10\right\rangle + \gamma_4^{(b)} \left|11\right\rangle) \otimes \left|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$
$$+ \alpha_b\beta_2^{(b)}(\gamma_1^{(b)} \left|00\right\rangle + \gamma_2^{(b)} \left|01\right\rangle + \gamma_3^{(b)} \left|10\right\rangle + \gamma_4^{(b)} \left|11\right\rangle) \otimes \left|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\right\rangle$$

$+\alpha_b\beta_3^{(b)}(\gamma_1^{(b)}\,|00\rangle+\gamma_2^{(b)}\,|01\rangle+\gamma_3^{(b)}\,|10\rangle+\gamma_4^{(b)}\,|11\rangle)\otimes|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\alpha_b\beta_4^{(b)}(\gamma_1^{(b)}\,|00\rangle+\gamma_2^{(b)}\,|01\rangle+\gamma_3^{(b)}\,|10\rangle+\gamma_4^{(b)}\,|11\rangle)\otimes|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle)^{\sigma_{i_2,j_2}}$

$= (\sum_{b'}\alpha_b\beta_1^{(b)}\gamma_1^{(b)}\,|00\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_1^{(b)}\gamma_2^{(b)}\,|01\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_1^{(b)}\gamma_3^{(b)}\,|10\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_1^{(b)}\gamma_4^{(b)}\,|11\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_2^{(b)}\gamma_1^{(b)}\,|00\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_2^{(b)}\gamma_2^{(b)}\,|01\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_2^{(b)}\gamma_3^{(b)}\,|10\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_2^{(b)}\gamma_4^{(b)}\,|11\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_3^{(b)}\gamma_1^{(b)}\,|00\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_3^{(b)}\gamma_2^{(b)}\,|01\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_3^{(b)}\gamma_3^{(b)}\,|10\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_3^{(b)}\gamma_4^{(b)}\,|11\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 0\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_4^{(b)}\gamma_1^{(b)}\,|00\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_4^{(b)}\gamma_2^{(b)}\,|01\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\beta_4^{(b)}\gamma_3^{(b)}\,|10\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\alpha_b\beta_4^{(b)}\gamma_4^{(b)}\,|11\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(i_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(i_1+1)}...b_{\sigma_{i_2,j_2}(j_1-1)}\ 1\ b_{\sigma_{i_2,j_2}(j_1+1)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle)^{\sigma_{i_2,j_2}}$

D'autre part, on a :

$(A_1\otimes I^{\otimes n-2}((A_2\otimes I^{\otimes n-2}Q_n^{\sigma_{i_2,j_2}})^{\sigma_{i_2,j_2}})^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}$

$= (A_1\otimes I^{\otimes n-2}((A_2\otimes I^{\otimes n-2}\sum_{b'}\alpha_b\,|b_{i_2}\ b_{j_2}\ b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle)^{\sigma_{i_2,j_2}})^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}$

$= (A_1\otimes I^{\otimes n-2}((\sum_{b'}\alpha_b A_2\,|b_{i_2}\ b_{j_2}\rangle\otimes|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle)^{\sigma_{i_2,j_2}})^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}$

$= (A_1\otimes I^{\otimes n-2}((\sum_{b'}\alpha_b(\gamma_1^{(b)}\,|00\rangle+\gamma_2^{(b)}\,|01\rangle+\gamma_1^{(b)}\,|10\rangle+\gamma_1^{(b)}\,|11\rangle)\otimes|b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle)^{\sigma_{i_2,j_2}})^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}$

$= (A_1\otimes I^{\otimes n-2}((\sum_{b'}\alpha_b(\gamma_1^{(b)}\,|00b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle+\gamma_2^{(b)}\,|01b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \gamma_3^{(b)}\,|10b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle+\gamma_4^{(b)}\,|11b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle)^{\sigma_{i_2,j_2}})^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}$

$= (A_1\otimes I^{\otimes n-2}((\sum_{b'}\alpha_b\gamma_1^{(b)}\,|00b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle+\alpha_b\gamma_2^{(b)}\,|01b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle$
$+\ \alpha_b\gamma_3^{(b)}\,|10b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle+\alpha_b\gamma_4^{(b)}\,|11b_{\sigma_{i_2,j_2}(2)}...b_{\sigma_{i_2,j_2}(n-1)}\rangle)^{\sigma_{i_2,j_2}})^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}$

$= (A_1\otimes I^{\otimes n-2}(\sum_{b}\alpha_b\gamma_1^{(b)}\,|b_0...b_{i_2-1}\ 0\ b_{i_2+1}...b_{j_2-1}\ 0\ b_{j_2+1}...b_{n-1}\rangle+\alpha_b\gamma_2^{(b)}\,|b_0...b_{i_2-1}\ 0\ b_{i_2+1}...b_{j_2-1}\ 1\ b_{j_2+1}...b_{n-}$
$+\alpha_b\gamma_3^{(b)}\,|b_0...b_{i_2-1}\ 1\ b_{i_2+1}...b_{j_2-1}\ 0\ b_{j_2+1}...b_{n-1}\rangle+\alpha_b\gamma_4^{(b)}\,|b_0...b_{i_2-1}\ 1\ b_{i_2+1}...b_{j_2-1}\ 1\ b_{j_2+1}...b_{n-1}\rangle)^{\sigma_{i_1,j_1}})^{\sigma_{i_1,j_1}}$

$= (A_1\otimes I^{\otimes n-2}\sum_{b'}\alpha_b\gamma_1^{(b)}\,|b_{\sigma_{i_1,j_1}(0)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle$

$$
\begin{aligned}
&+ \alpha_b\gamma_2^{(b)} \left|b_{\sigma_{i_1,j_1}(0)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)} \left|b_{\sigma_{i_1,j_1}(0)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)} \left|b_{\sigma_{i_1,j_1}(0)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}}
\end{aligned}
$$

$$
\begin{aligned}
&= (A_1\otimes I^{\otimes n-2} \sum_{b'} \alpha_b\gamma_1^{(b)} \left|b_{i_1}\ b_{j_1}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_2^{(b)} \left|b_{i_1}\ b_{j_1}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)} \left|b_{i_1}\ b_{j_1}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)} \left|b_{i_1}\ b_{j_1}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}}
\end{aligned}
$$

$$
\begin{aligned}
&= (\sum_{b'} \alpha_b\gamma_1^{(b)} A_1 \left|b_{i_1}\ b_{j_1}\right\rangle \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_2^{(b)} A_2 \left|b_{i_1}\ b_{j_1}\right\rangle \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)} A_2 \left|b_{i_1}\ b_{j_1}\right\rangle \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)} A_2 \left|b_{i_1}\ b_{j_1}\right\rangle \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}}
\end{aligned}
$$

$$
\begin{aligned}
&= (\sum_{b'} \alpha_b\gamma_1^{(b)} (\beta_1^{(b)} \left|00\right\rangle + \beta_2^{(b)} \left|01\right\rangle + \beta_3^{(b)} \left|10\right\rangle + \beta_4^{(b)} \left|11\right\rangle) \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_2^{(b)} (\beta_1^{(b)} \left|00\right\rangle + \beta_2^{(b)} \left|01\right\rangle + \beta_3^{(b)} \left|10\right\rangle + \beta_4^{(b)} \left|11\right\rangle) \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)} (\beta_1^{(b)} \left|00\right\rangle + \beta_2^{(b)} \left|01\right\rangle + \beta_3^{(b)} \left|10\right\rangle + \beta_4^{(b)} \left|11\right\rangle) \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)} (\beta_1^{(b)} \left|00\right\rangle + \beta_2^{(b)} \left|01\right\rangle + \beta_3^{(b)} \left|10\right\rangle + \beta_4^{(b)} \left|11\right\rangle) \otimes \left|b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}}
\end{aligned}
$$

$$
\begin{aligned}
&= (\sum_{b'} \alpha_b\gamma_1^{(b)}\beta_1^{(b)} \left|00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_1^{(b)}\beta_2^{(b)} \left|01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_1^{(b)}\beta_3^{(b)} \left|10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_1^{(b)}\beta_4^{(b)} \left|11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_2^{(b)}\beta_1^{(b)} \left|00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_2^{(b)}\beta_2^{(b)} \left|01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_2^{(b)}\beta_3^{(b)} \left|10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_2^{(b)}\beta_4^{(b)} \left|11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)}\beta_1^{(b)} \left|00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)}\beta_2^{(b)} \left|01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)}\beta_3^{(b)} \left|10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_3^{(b)}\beta_4^{(b)} \left|11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)}\beta_1^{(b)} \left|00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)}\beta_2^{(b)} \left|01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)}\beta_3^{(b)} \left|10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\gamma_4^{(b)}\beta_4^{(b)} \left|11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle)^{\sigma_{i_1,j_1}}
\end{aligned}
$$

$$
\begin{aligned}
&= (\sum_{b'} \alpha_b\beta_1^{(b)}\gamma_1^{(b)} \left|00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle \\
&+ \alpha_b\beta_1^{(b)}\gamma_2^{(b)} \left|01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&+ \alpha_b\beta_1^{(b)}\gamma_3^{(b)} |10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_1^{(b)}\gamma_4^{(b)} |11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_2^{(b)}\gamma_1^{(b)} |00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_2^{(b)}\gamma_2^{(b)} |01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_2^{(b)}\gamma_3^{(b)} |10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_2^{(b)}\gamma_4^{(b)} |11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_3^{(b)}\gamma_1^{(b)} |00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_3^{(b)}\gamma_2^{(b)} |01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_3^{(b)}\gamma_3^{(b)} |10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_3^{(b)}\gamma_4^{(b)} |11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 0\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_4^{(b)}\gamma_1^{(b)} |00\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_4^{(b)}\gamma_2^{(b)} |01\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_4^{(b)}\gamma_3^{(b)} |10\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle\\
&+ \alpha_b\beta_4^{(b)}\gamma_4^{(b)} |11\ b_{\sigma_{i_1,j_1}(2)}...b_{\sigma_{i_1,j_1}(i_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(i_2+1)}...b_{\sigma_{i_1,j_1}(j_2-1)}\ 1\ b_{\sigma_{i_1,j_1}(j_2+1)}...b_{\sigma_{i_1,j_1}(n-1)}\rangle)^{\sigma_{i_1,j_1}}
\end{aligned}
$$

On a que i_1,j_1,i_2 et j_2 sont deux à deux distincts, donc les bit de chaque qbit sont mis au bon endroit pour chaque permutation restante dans les calculs précédents.
De plus, les β_k et γ_l sont commutatifs ($\forall(k,l) \in \{1,2,3,4\}$).

□

Lemme A.1.9 ($U_A^{(2)}$ et $\texttt{meas}(\cdot,\cdot,\cdot)$)**.** *Les modifications sur la mémoire dû à $U_A^{(2)}$ et $\texttt{meas}(\cdot,\cdot,\cdot)$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. Comme dans le cas de $U_A^{(1)}$, on utilise le fait que A soit une matrice unitaire.

Autrement dit, si $\mathrm{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{2,1} & a_{2,2} & a_{3,3} & a_{3,4} \\ a_{2,1} & a_{2,2} & a_{4,3} & a_{4,4} \end{pmatrix}$

On ait $A^* \times A = I_4$.

Pour voir que les probabilités et les mémoires sont égales. □

Lemme A.1.10 ($\texttt{meas}(\cdot,\cdot,\cdot)$ et $\texttt{meas}(\cdot,\cdot,\cdot)$)**.** *Les modifications sur la mémoire dû à $\texttt{meas}(\cdot,\cdot,\cdot)$ et $\texttt{meas}(\cdot,\cdot,\cdot)$ (avec des registres différents) ne dépendent pas de l'ordre des réductions.*

Démonstration. Toujours d'après 5.6, on a :

$$\gamma = \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{j-1},b_{j+1},...,b_{n-1}} \left| \frac{\alpha_{b_0...b_{i-1}\ 0\ b_{i+1}...b_{j-1}\ 0\ b_{j+1}...b_{n-1}}}{\alpha} \right|^2}$$

$$LL_n = \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}}{\alpha\gamma} |b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}\rangle$$

$$\xi = \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\frac{\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\alpha}\right|^2}$$

$$LR_n = \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\alpha\xi} |b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}\rangle$$

$$\gamma' = \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\frac{\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}}{\beta}\right|^2}$$

$$RL_n = \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}}{\beta\gamma'} |b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}\rangle$$

$$\xi' = \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\frac{\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\beta}\right|^2}$$

$$RR_n = \sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\beta\xi'} |b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}\rangle$$

Simplifions un peu tout cela :

$$\begin{aligned}
\alpha\gamma &= \alpha\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\frac{\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}}{\alpha}\right|^2} \\
&= \alpha\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\left|\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}\right|^2}{|\alpha|^2}} \\
&= \alpha\sqrt{\frac{1}{\alpha^2}\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}\right|^2} \\
&= \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}\right|^2}
\end{aligned}$$

$$\begin{aligned}
\alpha\xi &= \alpha\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\frac{\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\alpha}\right|^2} \\
&= \alpha\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\left|\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}\right|^2}{|\alpha|^2}} \\
&= \alpha\sqrt{\frac{1}{\alpha^2}\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}\right|^2} \\
&= \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 0\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}\right|^2}
\end{aligned}$$

$$\begin{aligned}
\beta\gamma' &= \beta\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\frac{\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}}{\beta}\right|^2} \\
&= \beta\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\left|\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}\right|^2}{|\beta|^2}} \\
&= \beta\sqrt{\frac{1}{\beta^2}\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}\right|^2} \\
&= \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 0\ b_{j+1}\ldots b_{n-1}}\right|^2}
\end{aligned}$$

$$\begin{aligned}
\beta\xi' &= \beta\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\frac{\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}}{\beta}\right|^2} \\
&= \beta\sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \frac{\left|\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}\right|^2}{|\beta|^2}} \\
&= \beta\sqrt{\frac{1}{\beta^2}\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}\right|^2} \\
&= \sqrt{\sum_{b_0,\ldots,b_{i-1},b_{i+1},\ldots,b_{j-1},b_{j+1},\ldots,b_{n-1}} \left|\alpha_{b_0\ldots b_{i-1}\ 1\ b_{i+1}\ldots b_{j-1}\ 1\ b_{j+1}\ldots b_{n-1}}\right|^2}
\end{aligned}$$

□

Proposition A.1.11. *Soit $n \neq 0$, pour tout $Q_n \in \mathscr{M}$, pour tout $i \leqslant n$ on peut décomposer Q_n de la façon suivante :*

$$Q_n = \alpha \underbrace{\sum_{b'=(b_0...b_{i-1}\ 0\ b_{i+1}...b_{n-1})} \gamma_{b'} \left|b_0...b_{i-1}\ 0\ b_{i+1}...b_{n-1}\right\rangle}_{L_n} + \beta \underbrace{\sum_{b''=(b_0...b_{i-1}\ 1\ b_{i+1}...b_{n-1})} \gamma_{b''} \left|b_0...b_{i-1}\ 1\ b_{i+1}...b_{n-1}\right\rangle}_{R_n}$$

avec :

$$\alpha = \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \left|\alpha_{b_0...b_{i-1}\ 0\ b_{i+1}...b_{n-1}}\right|^2}$$

$$\beta = \sqrt{\sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \left|\alpha_{b_0...b_{i-1}\ 1\ b_{i+1}...b_{n-1}}\right|^2}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$(L_n, R_n) \in \mathscr{Q}$$

Démonstration. Soit $Q_n \in \mathscr{M}$, on pose $Q_n = \sum_{b=(b_0,...,b_{n-1})} \alpha_b \left|b\right\rangle$.

On a :

$$\begin{aligned}
Q_n &= \sum_{b_0,...,b_{i-1},b_i,b_{i+1},...,b_{n-1}} \alpha_{b_0...b_{i-1}\ b_i\ b_{i+1}...b_{n-1}} \left|b_0...b_{i-1}\ b_i\ b_{i+1}...b_{n-1}\right\rangle \\
&= \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \alpha_{b'} \left|b'\right\rangle + \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \alpha_{b''} \left|b''\right\rangle \\
&(b' = b_0...b_{i-1}\ 0\ b_{i+1}...b_{n-1} \text{ et } b'' = b_0...b_{i-1}\ 1\ b_{i+1}...b_{n-1}) \\
&= \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \alpha \frac{\alpha_{b'}}{\alpha} \left|b'\right\rangle + \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \beta \frac{\alpha_{b''}}{\beta} \left|b''\right\rangle \\
&= \alpha \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \frac{\alpha_{b'}}{\alpha} \left|b'\right\rangle + \beta \sum_{b_0,...,b_{i-1},b_{i+1},...,b_{n-1}} \frac{\alpha_{b''}}{\beta} \left|b''\right\rangle
\end{aligned}$$

Il suffit maintenant de vérifier que :
- $\left(\sqrt{\sum_{b'} \left|\alpha_{b''}\right|^2}\right)^2 + \left(\sqrt{\sum_{b'''} \left|\alpha_{b''}\right|^2}\right)^2 = 1$
- $L_{n-1} \in \mathscr{Q}$ - $R_{n-1} \in \mathscr{Q}$

$$\begin{aligned}
\left(\sqrt{\sum_{b'} \left|\alpha_{b'}\right|^2}\right)^2 + \left(\sqrt{\sum_{b''} \left|\alpha_{b''}\right|^2}\right)^2 &= \sum_{b'} \left|\alpha_{b'}\right|^2 + \sum_{b''} \left|\alpha_{b''}\right|^2 \\
&= \sum_{b} \left|\alpha_{b}\right|^2 \\
&= 1 (\text{car } Q_n \in \mathscr{Q})
\end{aligned}$$

De plus,

$$\begin{aligned}
\|L_{n-1}\| &= \sum_{b'} \left| \frac{\alpha_{b'}}{\sqrt{\sum\limits_{b''} |\alpha_{b'}|^2}} \right|^2 \\
&= \sum_{b'} \frac{|\alpha_{b'}|^2}{\left| \sqrt{\sum\limits_{b'} |\alpha_{b'}|^2} \right|^2} \\
&= \sum_{b'} \frac{|\alpha_{b'}|^2}{\sum\limits_{b''} |\alpha_{b'}|^2} \\
&= \frac{\sum\limits_{b'} |\alpha_{b'}|^2}{\sum\limits_{b'} |\alpha_{b'}|^2} \\
&= 1
\end{aligned}$$

Donc $L_{n-1} \in \mathscr{Q}$.

$$\begin{aligned}
\|R_{n-1}\| &= \sum_{b''} \left| \frac{\alpha_{b''}}{\sqrt{\sum\limits_{b''} |\alpha_{b''}|^2}} \right|^2 \\
&= \sum_{b''} \frac{|\alpha_{b''}|^2}{\left| \sqrt{\sum\limits_{b'''} |\alpha_{b''}|^2} \right|^2} \\
&= \sum_{b''} \frac{|\alpha_{b''}|^2}{\sum\limits_{b''} |\alpha_{b''}|^2} \\
&= \frac{\sum\limits_{b''} |\alpha_{b''}|^2}{\sum\limits_{b''} |\alpha_{b''}|^2} \\
&= 1
\end{aligned}$$

Donc $R_{n-1} \in \mathscr{Q}$. □

Appendix B

Définition formelle

Définition B.0.1 (Registre d'un terme)**.** L'ensemble $RE(M)$ des registres d'un terme $M \in \mathscr{T}$ se laissent définir par induction structurelle sur M à l'aide des clauses suivantes :

- Si M est une variable x, alors $RE(M) = \emptyset$.
- Si $M = \lambda x.M_0$, alors $RE(M) = RE(M_0)$.
- Si $M = M_1M_2$, alors $RE(M) = RE(M_1) \cup RE(M_2)$.
- Si $M = U_A$ ou q_{init}, alors $RE(M) = \emptyset$.
- Si $M = r_i$, alors $RE(M) = \{i\}$.

Définition B.0.2 (variable libre et liée)**.** L'ensemble $FV(M)$ des variables libres de $M \in \mathscr{T}$ et l'ensemble $BV(M)$ de ses variables liées se laissent définir par induction structurelle sur M à l'aide des clauses suivantes :
⇒Si M est une variable x, alors $FV(M) = \{x\}$.
⇒Si $M = \lambda x.M_0$, alors $FV(M) = FV(M_0) \setminus \{x\}$.
⇒Si $M = M_1M_2$, alors $FV(M) = FV(M_1) \cup FV(M_2)$.
⇒Si $M = U_A$ ou r_i ou q_{init}, alors $FV(M) = \emptyset$.

⇒Si M est une variable, alors $BV(M) = \emptyset$.
⇒Si $M = \lambda x.M_0$, alors $BV(M) = BV(M_0) \cup \{x\}$.
⇒Si $M = M_1M_2$, alors $BV(M) = BV(M_1) \cup BV(M_2)$.
⇒Si $M = U_A$ ou r_i ou q_{init}, alors $BV(M) = \emptyset$.

Exemple. (1) Si $M_1 = \lambda x.\lambda y.xyzz$ alors $FV(M_1) = \{z\}$.
(2) si $M_2 = \lambda x.r_1x$ alors $BV(M_2) = \{x\}$.

Définition B.0.3 (Indicateur de variable linéaire)**.** Soit x une variable libre, on définit l'indicateur de variable linéaire (si la variable apparaît une fois (1) ou autre (0)) sur les termes par induction :
- $Ind_x(x) = 1$
- $Ind_x(y) = 0$
- $Ind_x(\lambda x.M) = 0$
- $Ind_x(\lambda y.M) = Ind_x(M)$

- $Ind_x(MN) = \begin{cases} 0 \text{ si } Ind_x(M) = Ind_x(N) \\ 1 \text{ sinon} \end{cases}$
- $Ind_x(\lambda y.M) = 0$
- $Ind_x(r_i) = 0$
- $Ind_x(q_{init}) = 0$
- $Ind_x(U_A) = 0$

Définition B.0.4. Soit $M \in \mathscr{T}$, on définit $\vdash M$ (M est un terme valide) par :
Règle de U ($\forall A \in$ Matrice unitaire à coefficients dans $\mathbb{C}$):

$$\frac{}{\vdash U_A}\ U$$

Règle de q_{init} :

$$\frac{}{\vdash q_{init}}\ init$$

Variable libre :

$$\frac{x \ \ variable \ \ libre}{\vdash x}\ ax$$

Registre ($\forall i \in \mathbb{N}$):

$$\frac{}{\vdash r_i}\ r$$

Application :

$$\frac{\vdash M \quad \vdash N \quad RE(M) \cap RE(N) = \emptyset}{\vdash MN}$$

Abstration :

$$\frac{\vdash M \quad Ind_x(M) = 1}{\vdash \lambda x.M}\ \lambda$$

Définition B.0.5. On ajoute ainsi une règle de bonne formation de $\texttt{meas}(\cdot,\cdot,\cdot)$:

$$\frac{\vdash R \quad \vdash M \quad \vdash N \quad RE(M) \cap RE(R) = \emptyset \quad RE(M) = RE(N)}{\vdash \texttt{meas}(R, M, N)}$$

Définition B.0.6 (bonne formation de ! et de $\lambda^!$)**.** Voici nos deux règle, celle de $!M$:

$$\frac{\vdash M \quad RE(M) = \emptyset}{\vdash !M}$$

et celle de $\lambda^!$:

$$\frac{\vdash M}{\vdash \lambda^! x.M}$$

Appendix C

Bibliographie

[1] Ugo Dal Lago, Claudia Faggian, Benoit Valiron, and Akira Yoshimizu. The geometry of parallelism: classical, probabilistic, and quantum effects. In POPL 2017: 833–845.

[2] Peter Selinger and Benoit Valiron. A lambda calculus for quantum computation with classical control. Math. Structures Comput. Sci., 16(3):527–552, 2006.

[3] Claudia Faggian and Simona Ronchi Della Rocca. Lambda calculus and probabilistic computation. In LICS 2019: 1-13.

[4] Ugo Dal Lago, Andrea Masini, and Margherita Zorzi. Confluence results for a quantum lambda calculus with measurements. Electr. Notes Theor. Comput. Sci., 270(2):251–261, 2011.

[5] Alejandro Diaz-Caro, Pablo Arrighi, Manuel Gadella, and Jonathan Grattage. Measurements and confluence in quantum lambda calculi with explicit qbits. Electr. Notes Theor. Comput. Sci., 270(1):59–74, 2011.

[6] Claudia Faggian. Probabilistic Rewriting: on Normalization, Termination, and Unique Normal Forms. arXiv:1804.05578v7 [cs.LO] 2 Mar 2020.

[7] Franz Baader, Tobias Nipkow. Term Rewriting and All That-Cambridge University Press. 1998.

[8] Simpson, A. (2005). Reduction in a linear lambda-calculus with applications to operational semantics. In Term Rewriting and Applications. (pp. 219-234).

[9] Semantics for a Higher Order Functional Programming Language for Quantum Computation. Benoît Valiron. 2010.