Au delà du déterminisme dans le calcul par consommation d'intrication

Luc Pellissier,
encadré par Simon Perdrix,
Laboratoire d'informatique de Grenoble
22 Août 2011

Le contexte général. Le calcul par consommation d'intrication est un formalisme alternatif de l'ordinateur quantique. Son fonctionnement est le suivant : on place un système dans un état intriqué, où l'information n'est pas localisée, que l'on détruit progressivement en effectuant des mesures paramétrées par un angle. Ce faisant, l'information est « poussée » d'éléments que l'on interprète comme des entrées vers d'autres que l'on interprète comme des sorties. Cependant, les postulats de la mécanique quantique nous indiquent qu'une mesure ne produit pas de résultat déterministe. Ainsi, il est nécessaire après chaque mesure d'effectuer des corrections dépendant du résultat de la mesure pour récupérer un système déterministe. Il est donc intéressant d'étudier quels types d'intrication et quels types de correction sont suffisantes pour réaliser tous les calculs que l'on peut désirer faire, tout en étant réalisable physiquement et en garantissant le déterminisme.

Le problème étudié. La question posée est la suivante : on peut représenter l'état de certains systèmes intriqués par un graphe. Il a été démontré que, en se limitant à une certaine famille de correcteurs (les opérateurs de Pauli), un système possède une exécution déterministe (des corrections à appliquer avec chaque mesure quelque soit l'angle des mesures tel que l'état final ne dépende que de l'état initial) si et seulement si le graphe le représentant satisfait une certaine condition. De même un système possède une exécution préservant l'information (des corrections à appliquer après chaque mesure telles que, en ayant l'état final et en sachant quelles corrections ont été appliquées, on puisse reconstituer l'état initial) si et seulement si une autre condition graphique est satisfaite. Ces deux conditions ne sont pas équivalentes : il existe des calculs préservant l'information sans être déterministes. Ce n'est pas satisfaisant, et j'ai cherché à modifier l'ensemble des corrections pour faire se joindre ces deux notions. Connaître une bonne famille de corrections permet de poser avec plus de précision la question de la réalisabilité d'un ordinateur quantique selon ce modèle.

La contribution proposée. Notre démarche a été d'étudier systématiquement un graphe préservant l'information mais ne garantissant pas le déterminisme : regarder les états dans lesquels il se trouvait après les mesures, observer des stratégies de corrections quand certains angles sont fixés. Le but avoué était de reconnaître dans la correction devant être faite dans le cas général une combinaison linéaire (dont les coefficients soient fonction des angles de mesure) de corrections devant être faites dans les cas particuliers, et ainsi une méthode de construction de la correction générale en partant des cas particuliers qui puisse être encore opérante pour d'autres graphes. Cette démarche a partiellement réussi : on reconnait bien certaines une somme pondérée des corrections particulières (trouvées par des méthodes graphiques) dans la correction générale (obtenue par le calcul). Cependant, il n'est pas encore clair de voir la valeur des coefficients, notamment pourquoi certains sont nuls.

Les arguments en faveur de sa validité. Bien que le lien entre la correction générale et les corrections particulières ne soient pas élucidé, la forme recherchée des solutions est optimale : nous avons démontré qu'une correction plus simple (ne dépendant pas des angles de mesure, où n'étant pas une combinaison linéaire) ne pouvait pas permettre de corriger les états dans certains états particuliers. De plus, l'ensemble des corrections considérées est suffisamment large. Ainsi, la démarche est confirmée par des résultats d'impossibilité.

Le bilan et les perspectives. Mon travail n'a été qu'une étude préliminaire : on sait mieux quel genre de corrections chercher, il est clair qu'elles ont un lien avec des corrections trouvables graphiquement, mais aucune conjecture n'a été complètement formulée, et encore moins démontrée. Ainsi, l'étape suivant ce travail sera de vérifier si ses conclusions tiennent encore dans d'autres cas, puis, le cas échéant les démontrer. Enfin, il pourra être utile de faire un travail analogue dans un formalisme plus manipulable, le *measurement calculus*, en y ajoutant des combinaisons linéaires.

Au-delà du déterminisme dans le calcul par consommation d'intrication

Stage de L3

Juin — Juillet 2011

Luc Pellissier
Luc.Pellissier@dptinfo.ens-cachan.fr

Encadré par Simon Perdrix
Simon.Perdrix@imag.fr

Remerciements

Je tiens à remercier Simon Perdrix pour m'avoir proposé un sujet et accepté comme stagiaire. Ses explications, nombreuses et didactiques, m'ont fait découvrir des domaines nouveaux. Les autres membres de l'équipe, parmi lesquels Medhi Mallah, Alejandro Diaz-Carro ou Jérome Javelle doivent être aussi être cités pour leurs conversations stimulantes, et en général, l'ambiance qu'ils apportèrent à ces deux mois.

Je tiens aussi à mentionner Ali Assaf qui, stagiaire lui aussi, partagea mon bureau pendant mon premier mois. Puisse-t-il avoir une belle continuation.

Table des matières

Introduction

J'ai fait mon stage dans l'équipe CAPP (Calculs, Algorithmes, Programmes et Preuves), l'équipe d'informatique théorique du Laboratoire d'Informatique de Grenoble (`http://www.liglab.fr`) sous la direction de Simon Perdrix. Comme son nom l'indique, l'équipe regroupe tous les aspect de l'informatique théorique. En son sein, un groupe travaille en particulier sur l'informatique quantique, et c'est ce groupe que j'ai rejoint pendant deux mois. Le domaine est riche, et située à la croisée de plusieurs disciplines : les problématiques sont informatiques, le formalisme est mathématique et les contraintes physiques. Ainsi, mon stage a contenu des graphes, des systèmes de réécritures, de l'algèbre linéaire et bilinéaire, et (à dose homéopathique) des catégories.

Depuis maintenant une trentaine d'années, la communauté scientifique s'est penchée sur les promesses calculatoires de la physique quantique. En effet, des calculs réalisés de manière extrêmement simple par des dispositifs physiques quantiques ne peuvent être simulés classiquement que par de lourds produits matriciels. L'usage de propriétés quantiques (la principale étant, dans le domaine de l'information, l'intrication) a permis des résultats éclatants, tels l'algorithme de Shor [Sho95] réalisant la factorisation en nombres premiers en temps polynomial. Bien que l'on soit loin de réalisations à grande échelle d'ordinateurs capables de faire tourner de tels algorithmes, leurs propriétés théoriques sont impressionnantes, et, comme l'informatique classique avant la Seconde Guerre Mondiale, l'informatique quantique se cherche des formalismes pour être exprimée naturellement.

Le formalisme que j'ai étudié dans mon stage est celui du calcul par mesure (*measurement-calculus*, [DKP07]), qui est un cas particulier de calcul par consommation d'intrication. Dans ce formalisme, on effectue des mesures sur l'état d'un dispositif préalablement préparé, et on effectue des opérations sur le dispositif selon le résultat de ces mesures. Pour rendre cette idée précise, un peu de formalisme quantique est nécessaire. Traditionnellement, depuis l'article fondateur de Von Neumann ([Neu32]), les espaces de Hilbert sont utilisés à cette fin. On décrit l'état d'un système comme un vecteur dans un espace particulier, dont une base orthonormée fournit une base d'états classiques. Ainsi, le dispositif quantique le plus simple, le qubit, ne possédant que deux états classiques (notés respectivement 0 et 1) sera représenté par un vecteur normé dans un espace de Hilbert complexe à deux dimensions, dont la base canonique est traditionnellement appelée base calculatoire et notée $(|0\rangle, |1\rangle)$. Mesurer un système dans une base orthonormée donnée le projette sur un des vecteurs de la base avec une probabilité dépendant du coefficient de ce vecteur dans ladite base.

Le système créé par la réunion de deux systèmes est décrit par le produit tensoriel des espaces décrivant chacun des systèmes (cf section 1.1.3). Considérons le cas le plus simple : si on note $|\varphi\rangle$ l'état d'un qubit, il est décrit par $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, où α et β sont deux complexes tels que $|\alpha|^2 + |\beta|^2 = 1$. Un système à deux qubits sera donc décrit par $\alpha|0\rangle \otimes |0\rangle + \beta|0\rangle \otimes |1\rangle + \gamma|1\rangle \otimes |0\rangle + \delta|1\rangle \otimes |1\rangle$, où $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. On remarque que tous les états ne se décomposent pas en produits tensoriels d'états sur un qubit. De tels états sont appelés intriqués.

L'intrication se produisant alors a un intérêt calculatoire : considérons la suite d'opération suivante. On part d'un qubit dans l'état $\alpha|0\rangle + \beta|1\rangle$. On l'intrique avec un autre qubit de manière à obtenir un système dans l'état $\alpha|01\rangle + \beta|10\rangle$ (où $|ij\rangle$ est une abréviation pour $|i\rangle \otimes |j\rangle$). On mesure le premier qubit dans la base calculatoire. Si l'on a mesuré $|0\rangle$, on sait que le système global a été projeté dans l'état $|01\rangle$, et donc que le second qubit est dans l'état $|1\rangle$. De même, si on a mesuré $|1\rangle$ le deuxième qubit est dans l'état $|0\rangle$. L'ensemble de nos opérations (préparation du système et mesure du premier qubit) a ainsi consisté, si l'on considère notre premier qubit comme une entrée et le second comme une sortie, en une porte NON : si le premier qubit était dans un des deux états classiques, le second sera dans l'autre.

Ce type de calcul se nomme le calcul par consommation d'intrication ([RB01]). Dans le modèle utilisé, les qubits ne peuvent être intriqués que par une opération, notée $\wedge$ Z (Contrôle-Z). On s'autorise à faire des mesures dans toutes les bases de la forme $(|+_\alpha\rangle, |-_\alpha\rangle)$ où

$$|+_\alpha\rangle = \frac{|0\rangle + e^{i\alpha}|1\rangle}{\sqrt{2}}$$
$$|-_\alpha\rangle = \frac{|0\rangle - e^{i\alpha}|1\rangle}{\sqrt{2}}$$

et à faire certaines corrections (des corrections de Pauli) dépendant des mesures pour sauvegarder le déterminisme. Il est naturel de représenter les ensembles de qubits par des graphes, où les sommets représentent les qubits, et les arêtes les opérations d'intrication effectuées, comme dans la figure 1. Il a été montré dans [Mha+10] que les intrications de qubits garantissant une exécution déterministe, c'est-à-dire pour lesquels existe une stratégie de correction telle que quelque soient les angles de mesure, le résultat soit déterministe, possèdent une caractérisation graphique. Par ailleurs, le même article montre que les intrications préservant l'information (l'état des entrées peut être reconstruit de l'état des sorties) possèdent elles aussi une caractérisation graphique, différente de celle mentionnée ci-dessus. Le graphe de la figure 1 est de ceux-là : il préserve l'information de son entrée dans ses sorties, mais il n'existe pas de stratégie n'utilisant que des opérateurs de Pauli pour assurer un résultat déterministe.

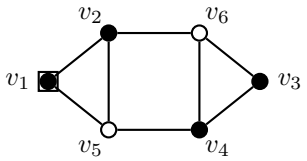

FIGURE 1. Un graphe ouvert. Le sommet encadré est une entrée, les sommets creux sont des sorties

Le but de mon stage était d'étudier la différence entre ces deux notions, éventuellement de proposer une famille de corrections plus large permettant de les faire se rejoindre. Après avoir passé quelques semaines à me familiariser avec l'information quantique, et notamment les différentes formulations concurrentes du calcul par consommation d'intrication (*measurement-calculus* [DKP07], états stabilisés [Got97, p17-30], et la généralisation commune de ce calcul avec le formalisme des circuits quantiques ([Deu89]) : les catégories dagger-compactes closes [CD09]), j'ai étudié en profondeur le graphe ci-dessus, calculé des corrections admissibles avec plus ou moins d'angles de mesure fixés.

1. MÉCANIQUE QUANTIQUE

1.1. **Rappels d'algèbre linéaire.**

Le formalisme standard de la mécanique quantique tel qu'introduit par Von Neumann dans [Neu32] représente les états des systèmes comme des vecteurs de certains espaces, et les transformations comme certaines des applications linéaires de ces espaces. Il est donc important de passer rapidement en revue des définitions et notations de l'algèbre linéaire.

1.1.1. *Notations de Dirac.* Soit $(\mathcal{H}, \langle\cdot|\cdot\rangle)$ un espace de Hilbert complexe de dimension finie n, que l'on rapportera systématiquement à une base orthonormée directe. On confondra les vecteurs et leur expression dans cette base, ainsi que les applications linéaires et leurs matrices dans cette base. On rappelle qu'un espace de Hilbert est un espace vectoriel muni d'un produit scalaire et complet pour la distance induite par celui-ci. Nous utiliserons la notation « bra-ket »de Dirac, c'est à dire que les éléments de $\mathcal{H}$ seront notés de la forme $|\phi\rangle$. Par exemple, la base canonique de $\mathcal{H}$ sera notée $(|0\rangle, |1\rangle, ..., |n-1\rangle)$.

Pour $|\varphi\rangle \in \mathcal{H}$, on pose $\langle\varphi| \in \mathcal{H}^\star$ son élément dual, c'est à dire l'application $\mathcal{H} \to \mathbf{C}, |\psi\rangle \mapsto \langle\varphi|\psi\rangle$. On a alors

$$\begin{aligned}\forall |\varphi\rangle, |\psi\rangle \in \mathcal{H}, \langle\varphi|(|\psi\rangle) &= \langle\phi| \times |\psi\rangle \\ &= \langle\varphi|\psi\rangle \\ &= \sum_{i=0}^{n-1} \overline{\varphi_i}\psi_i\end{aligned}$$

Si $|\varphi\rangle = \begin{bmatrix} \varphi_0 \\ \vdots \\ \varphi_{n-1} \end{bmatrix}$, $\langle\varphi| = [\overline{\varphi_0} \cdots \overline{\varphi_{n-1}}]$, sa trans-conjuguée.

Considérons maintenant, pour $i \in \{0, ..., n-1\}$ l'application $\mathcal{H} \to \mathcal{H}, |\phi\rangle \mapsto \langle i|\phi\rangle |i\rangle$, notée $|i\rangle \langle i|$. Remarquons que

$$\forall j \in \{0, ...n-1\}, (|i\rangle \langle i|) |j\rangle = |i\rangle \langle i|j\rangle = \delta_{ij} |i\rangle$$

(où δ_{ij} est le symbole de Kronecker). Ainsi, $|i\rangle \langle i|$ est la projection sur l'espace vectoriel engendré par $|i\rangle$. On a la décomposition de l'identité suivante : $\sum_{i=0}^{n-1} |i\rangle \langle i| = \mathrm{Id}$.

1.1.2. *Opérateurs.* Soit $U \in \mathcal{L}(\mathcal{H})$ un opérateur linéaire sur $\mathcal{H}$. Il existe un opérateur, noté $U^\dagger$ et dit ADJOINT de U tel que

$$\forall |\varphi\rangle, |\psi\rangle \in \mathcal{H}, \langle\varphi|U\psi\rangle = \left\langle U^\dagger\varphi|\psi\right\rangle$$

On dit que U est UNITAIRE si $UU^\dagger = U^\dagger U = \mathrm{Id}$. L'ensemble des opérateurs unitaires forme un groupe de Lie de dimension n^2. La matrice de $U^\dagger$ est la matrice trans-conjuguée de celle de U.

On dit que U est une isométrie si $U^\dagger U = \mathrm{Id}$.

1.1.3. *Produits tensoriels.* Étant donnés deux espaces vectoriels $\mathcal{H}$ et $\mathcal{G}$, on peut construire leur produit tensoriel $\mathcal{H} \otimes \mathcal{G}$. Si $(|0\rangle_{\mathcal{H}}, ..., |n-1\rangle_{\mathcal{H}})$ et $(|0\rangle_{\mathcal{G}}, ..., |m-1\rangle_{\mathcal{G}})$ sont les bases canoniques respectives de $\mathcal{H}$ et de $\mathcal{G}$, on note, pour $(i,j) \in \{0, ..., n-1\} \times \{0, ..., m-1\}, |ij\rangle = |i\rangle_{\mathcal{H}} \otimes |j\rangle_{\mathcal{G}}$. $\{|ij\rangle, 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant n-1\}$ est par définition une base de $\mathcal{H} \otimes \mathcal{G}$ qui est donc de dimension nm. $\mathcal{H} \times \mathcal{G}$ s'injecte linéairement de manière non-bijective dans $\mathcal{H} \otimes \mathcal{G}$. Si U est un opérateur de $\mathcal{H}$ dans lui-même, et que V en est un de $\mathcal{G}$ dans lui-même, $U \otimes V$ est l'opérateur de $\mathcal{H} \otimes \mathcal{G}$ dans lui-même défini par :

$$\forall (i,j) \in \{0, ..., n-1\} \times \{0, ..., m-1\}, (U \otimes V) |ij\rangle = (U |i\rangle_{\mathcal{H}}) \otimes \left(V |j\rangle_{\mathcal{G}}\right)$$

Le produit tensoriel est associatif. Étant donné $\mathcal{H}$, on notera $\mathcal{H}^{\otimes p}$ le produit tensoriel $\mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}$ p fois. Si U est un opérateur de $\mathcal{H}$ dans lui-même, on notera, pour $1 \leqslant i \leqslant p$, $U_i : \mathcal{H}^{\otimes p} \to \mathcal{H}^{\otimes p}$ l'opérateur $\mathrm{Id} \otimes \mathrm{Id} \otimes \cdots \otimes U \otimes \cdots \otimes \mathrm{Id}$ où le U est à la i-ème position.

1.2. Généralités sur l'informatique quantique.

1.2.1. *Qubit.* En plus des états classiques, observables, les dispositifs quantiques peuvent se placer dans une superposition d'iceux. Ainsi, la plus petite quantité d'information classique (le bit) est celle contenue dans un dispositif ne possédant que deux états stables. De manière analogique, la plus petite quantité d'information quantique est celle contenue dans un dispositif dont on ne peut observer que deux états distincts, et qui est donc dans une superposition de ceux-ci.

Un QUBIT est un dispositif dont l'état $|\psi\rangle$ peut se mettre sous la forme

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, (\alpha, \beta) \in \mathbf{S}^1_{\mathbf{C}}$$

où $|0\rangle$ et $|1\rangle$ sont deux états classiques.

Ainsi, un qubit est un élément de $\mathbf{S}^1_{\mathbf{C}}$ la sphère unité de $\mathbf{C}^2$.

On décrit l'état de n qubits par un élément de la sphère unité de l'ensemble des combinaisons linéaire des produits tensoriels des états de base. Ainsi, la fonction d'onde d'un système de deux qubits se met sous la forme :

$$|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle, (\alpha, \beta, \gamma, \delta) \in \mathbf{S}^3_{\mathbf{C}}$$

où $|ab\rangle = |a\rangle \otimes |b\rangle$.

1.2.2. *Mesures.* Une mesure de qubit se fait selon une base orthonormée. Supposons que l'on veuille mesurer $|\varphi\rangle$ dans la base $(|\psi\rangle, |\theta\rangle)$. Soient $(\alpha, \beta) \in \mathbf{S}^1_{\mathbf{C}}$ tels que $|\varphi\rangle = \alpha |\psi\rangle + \beta |\theta\rangle$. Après la mesure, le qubit a une probabilité $|\alpha|^2$ d'être dans l'état $|\psi\rangle$ et une probabilité $|\beta|^2$ d'être dans l'état $|\theta\rangle$. Ainsi, une mesure altère un qubit et son résultat est probabiliste.

Soit $|\phi\rangle = \alpha |\psi\rangle + \beta |\theta\rangle$ un qubit. Soit $\Phi \in \mathbf{R}$. Considérons le qubit $e^{i\Phi} |\phi\rangle$. La probabilité que $|\phi\rangle$ soit dans l'état $|\psi\rangle$ (respectivement θ) après mesure dans la base $(|\phi\rangle, |\psi\rangle)$ est $|\alpha|^2 = |e^{i\Phi}\alpha|^2$ (respectivement $|\beta|^2 = |e^{i\Phi}\beta|^2$), c'est à dire la même que pour $e^{i\Phi} |\phi\rangle$. Donc les vecteurs $|\phi\rangle$ et $e^{i\Phi} |\phi\rangle$ sont physiquement indiscernables. On considère donc les états d'un système modulo un complexe de module 1, et on appelle RAYON une telle classe d'équivalence. On passera indifféremment d'un rayon à un vecteur le représentant.

1.2.3. *Opérateurs de Pauli.* On utilisera aussi les trois opérateurs X, Y, Z dits OPÉRATEURS DE PAULI définis par :

$$\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{cases} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{cases} = |1\rangle\langle 0| + |0\rangle\langle 1|$$
$$\mathrm{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{cases} |0\rangle \mapsto i\,|1\rangle \\ |1\rangle \mapsto -i\,|0\rangle \end{cases} = i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1|$$
$$\mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{cases} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

Les opérateurs de Pauli forment, avec l'identité, une base de l'ensemble des opérateurs de $\mathbf{C}^2$.

L'ensemble $P = \{I, \mathrm{X}, \mathrm{Y}, \mathrm{Z}, -I, -\mathrm{X}, -\mathrm{Y}, -\mathrm{Z}, iI, i\,\mathrm{X}, i\,\mathrm{Y}, i\,\mathrm{Z}, -iI, -i\,\mathrm{X}, -i\,\mathrm{Y}, -i\,\mathrm{Z}\}$ forme un groupe pour la loi produit, intégralement décrit par l'équation

$$\mathrm{X}^2 = \mathrm{Y}^2 = \mathrm{Z}^2 = -i\,\mathrm{X}\,\mathrm{Y}\,\mathrm{Z} = I$$

1.2.4. *Intrication.* Considérons maintenant deux qubits. Leur état est décrit par les rayons normés de $\mathcal{H} \otimes \mathcal{H}$. En particulier, considérons par exemple l'état (dit état EPR, pour Einstein-Podolsky-Rosen) suivant :

$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Supposons que l'on puisse décrire séparément chacun des qubits de $|\Psi\rangle$, c'est à dire que $|\Psi\rangle = |\phi\rangle \otimes |\psi\rangle$, pour $|\phi\rangle = a\,|0\rangle + b\,|1\rangle$ et $|\psi\rangle = c\,|0\rangle + d\,|1\rangle$. On aurait alors :

$$(a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$\Leftrightarrow \begin{cases} ac = \frac{1}{\sqrt{2}} \\ ad = 0 \\ bc = 0 \\ bd = \frac{1}{\sqrt{2}} \end{cases} \Rightarrow abcd = 0 \,\&\, abcd = \frac{1}{2}$$

Ce qui est absurde. La description séparée des deux qubits est impossible. On dit que leurs états sont INTRIQUÉS.

Une manière d'intriquer deux qubits que nous utiliserons par la suite est l'opérateur nommé Contrôle-Z, noté $\wedge\,\mathrm{Z}$ et défini par

$$\wedge\,\mathrm{Z} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

En généralisant, l'état d'un ensemble de n qubits se met donc sous la forme $\sum \alpha_x\,|x\rangle$, quand x parcourt l'ensemble des mots binaires de longueur n, où $\sum |\alpha_x|^2 = 1$. Si x est un mot binaire de longueur n, on définit le support de x $\mathrm{supp}(x)$ comme l'ensemble des positions i telles que $x_i = 1$. Ce sont les qubits dans l'état classique $|1\rangle$ si l'ensemble de n qubits est dans l'état classique $|x\rangle$.

2. Le calcul par consommation d'intrication

Comme on l'a présenté dans l'introduction, le calcul par consommation d'intrication contient trois types d'opérations : des Contrôle-Z réalisant les intrications, des mesures selon les bases $(|+_\alpha\rangle, |-_\alpha\rangle)$ où

$$|+_\alpha\rangle = \frac{|0\rangle + e^{i\alpha}\,|1\rangle}{\sqrt{2}}$$
$$|-_\alpha\rangle = \frac{|0\rangle - e^{i\alpha}\,|1\rangle}{\sqrt{2}}$$

et des corrections de Pauli X et Z pouvant dépendre des résultats de mesure, ainsi que la préparation de qubits auxiliaires dans l'état $|+\rangle = |+_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$. De plus, il a été démontré dans [Dan+10] qu'une suite de telles opérations peut toujours être mise sous forme standard, c'est à dire d'abord d'une suite de création de qubits auxiliaires, suivie par une série d'intrications, suivi enfin par des mesures et leurs corrections conditionnelles associées.

On voit sous cette forme standard que toutes les créations de qubits et intrications peuvent être faites avant les mesures. Ainsi, l'idée de représenter les qubits par des sommets et les intrications par des arêtes dans un graphe est justifiée : la géométrie du graphe est fixée une fois pour toute et ne dépend pas de l'exécution. Par la suite, on appellera GRAPHE OUVERT la donnée d'un graphe non-orienté G et de deux ensembles distingués de sommets, les entrées et les sorties, notés respectivement I et O.

Pour décrire l'exécution, il nous faut aussi la liste des angles de mesure de tous les sommets non-sorties, ainsi que, pour chaque sommet mesuré, les corrections à appliquer sur les autres sommets. Ceci motive la description suivante d'un calcul par consommation d'intrication :

(i) Un graphe ouvert (G, I, O) ;

(ii) Une application $\alpha : O^c \to [0; 2\pi[, u \mapsto \alpha_u$;

(iii) Une application de correction $\mathtt{P} : O^c \to P^{V(G)}$ (où P est le groupe engendré par les opérateurs de Pauli) qui associe à chaque sommet l'ensemble des corrections à appliquer sur les autres sommets pour rendre l'exécution déterministe.

Pour que la séquence soit exécutable, il faut de plus qu'il existe un ordre partiel $\prec$ tel que pour tout sommet $u \in O^c$, tous les sommets tels que $\mathtt{P}(u)$ soit différent de l'identité soient supérieurs à u, c'est-à-dire que les corrections dépendant de mesures aient lieu après celles-ci, et non anachroniquement.

2.0.1. *Exemple.* Considérons le graphe de la figure 2, où de plus $\alpha : v_1 \mapsto 0$ et $\mathtt{P} : v_1 \mapsto \mathrm{X}_2$. Supposons que v_1 était dans l'état $|\varphi\rangle = a\,|0\rangle + b\,|1\rangle$. La préparation et l'intrication met le graphe dans l'état $\frac{1}{\sqrt{2}}\left(a\,|00\rangle + a\,|01\rangle + b\,|10\rangle - b\,|11\rangle\right) = \frac{1}{2}\left((a+b)\,|{+}0\rangle + (a-b)\,|{+}1\rangle + (a-b)\,|{-}0\rangle + (a+b)\,|{-}1\rangle\right)$. Ainsi, si $|+\rangle$ a été mesuré, une fois v_1 mesuré, le graphe est dans l'état $|\varphi_{\text{final}}\rangle\ \frac{1}{\sqrt{2}}\left((a+b)\,|0\rangle + (a-b)\,|1\rangle\right)$. Si $|-\rangle$ a été mesuré, on applique $\mathtt{P}(v_1) = \mathrm{X}_2$, ce qui met le graphe dans l'état $|\varphi_{\text{final}}\rangle$. Ainsi, on a dans tous les cas réalisé l'opérateur d'Hadamard $\mathrm{H} = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right] : |\varphi_{\text{final}}\rangle = \mathrm{H}\,|\varphi\rangle$.

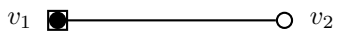

FIGURE 2. Un calcul par consommation d'intrication : l'opérateur d'Hadamard

2.1. **La préparation.** Intéressons nous à l'opération de préparation. Elle consiste à initialiser les qubits différents des entrées à $|+\rangle$, puis à réaliser les intrications régies par le graphe. L'état d'un ensemble de n qubits initialisés à l'état $|+\rangle$ est

$$\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle$$

Ainsi, si les p qubits d'entrée sont dans un état $|\varphi\rangle = \sum_{x\in\{0,1\}^p} a_x\,|x\rangle$, l'ensemble du graphe se retrouve dans l'état

$$\left(\sum_{x\in\{0,1\}^n} a_x\,|x\rangle\right) \otimes \left(\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} |y\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{\substack{y\in\{0,1\}^n\\ x\in\{0,1\}^p}} a_x\,|xy\rangle$$

$$= \left(\frac{1}{\sqrt{2^n}} \sum_{\substack{y\in\{0,1\}^n\\ x\in\{0,1\}^p}} |xy\rangle\,\langle x|\right)|\varphi\rangle$$

Considérons maintenant l'étape d'intrication. On applique un $\wedge$ Z entre deux qubits si et seulement si il y a une arête entre les sommets les représentant dans le graphe d'intrication. Un $\wedge$ Z change le signe de l'état de deux qubits uniquement s'ils sont tous deux dans l'état $|1\rangle$. Donc, si un ensemble de qubits est dans l'état $|x\rangle$ où x est un mot binaire, un $\wedge$ Z entre les qubits i et j sera différent de l'identité si et seulement si $(i,j) \in \mathrm{supp}(x)^2$. Comme on a appliqué le $\wedge$ Z uniquement si $(i,j) \in E(G)$, on ne fait un changement de signe que si $(i,j) \in E(G) \cap \mathrm{supp}(x)^2$. Donc, appliquer des $\wedge$ Z à l'image d'un graphe revient à appliquer l'application définie par $|x\rangle \mapsto (-1)^{|E(G)\cap supp(x)^2|}\,|x\rangle$ pour x un mot binaire.

Ainsi, l'application N de préparation du graphe s'écrit

$$N = \frac{1}{\sqrt{2^n}} \sum_{\substack{y\in\{0,1\}^n\\ x\in\{0,1\}^p}} (-1)^{|E(G)\cap supp(x)^2|}\,|xy\rangle\,\langle x|$$

2.2. **Les mesures.** Une mesure applique de façon non-déterministe une projection parmi deux possibles. Pour chaque qubit u mesuré, on convient de poser $s_u = 0$ si le résultat de la mesure de u selon l'angle α_u est $|{+}_{\alpha_u}\rangle$, et $s_u = 1$, sinon. Mesurer le

qubit u (pour simplifier, on va supposer $u = 1$) selon α_u revient à appliquer $\langle +_{\alpha_u}|$ ou $\langle -_{\alpha_u}|$ sur u est l'identité ailleurs :

$$\begin{aligned}
\langle +_{\alpha_u}| \otimes \left(\sum_{y\in\{0;1\}^n} |y\rangle \langle y| \right) &= \left(\frac{\langle 0| + e^{-i\alpha_u} \langle 1|}{\sqrt{2}} \right) \otimes \left(\sum_{y\in\{0;1\}^n} |y\rangle \langle y| \right) \\
&= \left(\sum_{y\in\{0;1\}^{n-1}} |y\rangle \langle 0y| \right) + \left(\sum_{y\in\{0;1\}^{n-1}} e^{-i\alpha_u} |y\rangle \langle 1y| \right) \\
&= \sum_{\substack{y\in\{0;1\}^{n-1} \\ x\in\{0;1\}}} e^{-ix\alpha_u} |y\rangle \langle xy| \\
\langle -_{\alpha_u}| \otimes \left(\sum_{y\in\{0;1\}^n} |y\rangle \langle y| \right) &= \left(\frac{\langle 0| - e^{-i\alpha_u} \langle 1|}{\sqrt{2}} \right) \otimes \left(\sum_{y\in\{0;1\}^n} |y\rangle \langle y| \right) \\
&= \left(\sum_{y\in\{0;1\}^{n-1}} |y\rangle \langle 0y| \right) - \left(\sum_{y\in\{0;1\}^{n-1}} e^{-i\alpha_u} |y\rangle \langle 1y| \right) \\
&= \sum_{\substack{y\in\{0;1\}^{n-1} \\ x\in\{0;1\}}} (-1)^x e^{-ix\alpha_u} |y\rangle \langle xy|
\end{aligned}$$

Ainsi, l'opérateur suivant réalise une mesure avec l'angle α sur le qubit 1, où le résultat classique de la mesure est s_1 :

$$M_{1,s_1}(\alpha) = \sum_{\substack{y\in\{0;1\}^{n-1} \\ x\in\{0;1\}}} (-1)^{x\cdot s_1} \frac{e^{-ix\alpha}}{\sqrt{2}} |y\rangle \langle xy|$$

Considérons la mesure d'un unique qubit selon un angle α. Si $s = 0$, la projection réalisée est $\langle +_\alpha|$. Considérons l'opération $\langle -_\alpha| \mathrm{Z}$.

$$\begin{aligned}
\langle -_\alpha| \mathrm{Z} &= \begin{bmatrix} 1 & -e^{-i\alpha} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & e^{-i\alpha} \end{bmatrix} \\
&= \langle +_\alpha|
\end{aligned}$$

On en déduit donc que $M_{1,s_1}(\alpha)\, \mathrm{Z}_1^{s_1}$ est déterministe.

Cet opérateur n'est toutefois pas physiquement réalisable : il demande à connaitre le résultat de la mesure avant de l'effectuer pour en corriger le non-déterminisme. Dans certaines conditions dépendant de l'intrication, c'est-à-dire de la géométrie du graphe, la correction anachronique peut être remplacée par une action, notée $\mathsf{P}(u)$ agissant exclusivement sur des qubits non mesurés et ayant la même action.

Ainsi, l'exécution totale du graphe sera représentée par l'opérateur, où $s = (s_u)_{u\in O^c}$ est le vecteur des résultats de mesure, $\chi_s : \mathbf{C}^{2^{|I|}} \to \mathbf{C}^{2^{|O|}}$

$$\chi_s = \prod_{u\in O^c}^{\prec} \mathsf{P}(u)^{s_u} M_{u,s_u}(\alpha_u) N$$

où $\prod^{\prec}$ signifie que le produit est fait dans l'ordre de $\prec$. Le graphe implémente donc la famille d'opérations $(\chi_s)_{s\in\{0,1\}^{O^c}}$. Si quelque soit s, χ_s est le même opérateur, la calcul est déterministe : il ne dépend pas du résultat classique. Si quelque soit s, $\chi_s^\dagger \chi_s = 2^{-n}$ Id, l'évolution est équiprobable : chaque résultat classique a même probabilité et le calcul est réversible.

On a l'importante propriété suivante :

$$\begin{aligned}
\sum_{s\in\{0;1\}^{O^c}} \chi_s^\dagger \chi_s &= \sum_{s\in\{0;1\}^{O^c}} N^\dagger \prod_{u\in O^c}^{\succ} M_{u,s_u}^\dagger(\alpha_u) \left(\mathsf{P}(u)^{s_u}\right)^\dagger \prod_{u\in O^c}^{\prec} \mathsf{P}(u)^{s_u} M_{u,s_u}(\alpha_u) N \\
&= \mathrm{Id}
\end{aligned}$$

$(\chi_s)_{s\in\{0;1\}^{O^c}}$ est donc une opération quantique valide ([Neu32]).

2.3. **Conditions graphiques.** Il est intéressant de savoir si l'application P existe et est dépendante ou non des angles de mesure des qubits, étant donné seulement le graphe d'intrication. Pour cela, on va utiliser une propriété fondamentale des états descriptible par les graphes : l'état décrit par le graphe est point fixe de l'opérateur $X_u \otimes \mathrm{Z}_{\mathcal{N}(u)}$, où u est un qubit qui n'est pas une entrée et $\mathcal{N}(u)$ l'ensemble de ses voisins. En effet, un qubit dans l'état $|+\rangle$ est stabilisé par X ($|+\rangle$ est vecteur propre de X pour la valeur propre 1), et donc l'ensemble des qubits constituant le graphe est avant intrication stabilisé par X_u. Donc, après intrication, le graphe est stabilisé par l'opérateur $\prod_{v\in\mathcal{N}(u)} \wedge \mathrm{Z}_{uv}\ X_u\ (\wedge \mathrm{Z}_{uv})^\dagger = X_u \otimes \prod_{v\in\mathcal{N}(u)} \mathrm{Z}_v$ (voir [BB06] pour des explications plus générales). Ainsi, on peut toujours pré-composer toute application sur le graphe par l'action de X sur un sommet non-entrée et Z sur ses voisins sans changer l'application.

Ainsi, pour supprimer l'action anachronique d'un Z sur un sommet, tel qu'on l'a introduit dans l'opérateur M_{u,s_u}, on peut, à condition que ce sommet ait un voisin non-mesuré dont tous les voisins sont non-mesurés, effectuer un X sur ce voisin, et Z sur ses voisins. On obtient ainsi une exécution déterministe. C'est cette idée qui est formalisée par la notion de *gflow*.

2.3.1. *Déterminisme et gflow.* Étant donné un graphe ouvert (G, I, O), on dit que $(g : O^c \to \mathcal{P}(I^c), \prec)$ est un GFLOW de (G, I, O) si

- si $v \in g(u)$, alors $u \prec v$
- un nombre impair de sommets de $g(u)$ sont voisins de u
- tous les sommets v tels qu'un nombre impair de sommets de $g(u)$ soient voisins de v sont tels que $u \prec v$.

Théorème 1 ([Bro+07]). *Si un graphe ouvert admet un gflow, il garantit une exécution déterministe ne dépendant pas des angles de mesures, c'est à dire qu'il existe une application* P *telle que, quel que soit α, le calcul constitué du graphe munit de α et de* P *soit déterministe.*

On peut interpréter l'ensemble $g(u)$ comme l'ensemble des sommets sur lesquels on applique un X pour corriger u. Qu'un nombre impair de sommets de $g(u)$ soient voisins de u assure que u soit corrigé. La troisième condition assure que les effets de bords (les Z sur les voisins) ne touchent que des qubits non encore mesurés.

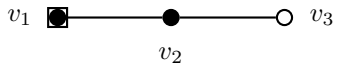

FIGURE 3. Un graphe admettant un *gflow*

2.3.2. *Exemple.* Le graphe de la figure 3, mesuré dans l'ordre $1 \prec 2 \prec 3$ admet un *gflow*. Il suffit de mesurer le sommet v_1, le corriger en faisant un X sur v_2 et un Z sur v_3, mesurer v_2, et le corriger en faisant un X sur v_3. L'application P est donc $v_1 \mapsto \mathrm{X}_2\,\mathrm{Z}_3, v_2 \mapsto \mathrm{X}_3$.

2.3.3. *Équi-probabilité et ensembles violants.* On peut aussi s'intéresser à une classe de graphes plus large : ceux qui garantissent que le calcul préserve l'information : on dit qu'un calcul par consommation d'intrication PRÉSERVE L'INFORMATION si, étant donné l'état du système après le calcul et le vecteur s des résultats classiques, on peut retrouver l'état initial. Une classe particulière de graphe garantissant la préservation de l'information est celle des graphes garantissant l'équiprobabilité, c'est à dire que pour tous angles α, le graphe sans correction muni de α soit équiprobable, c'est à dire que tous les vecteurs s de résultats classiques soient équiprobables.

Théorème 2 ([Mha+10]). *Étant donné un graphe ouvert (G, I, O), si tout sous-ensemble de sommets n'étant pas des sorties possède un voisinage impair n'étant pas contenu dans la réunion des entrées et de lui-même, alors ce graphe garantit l'équiprobabilité, c'est à dire que pour tous angles α de mesure, le graphe muni des angles α a une exécution équiprobable.*

L'existence, pour tout ensemble, d'un voisinage impair non inclus dans la réunion des entrées et de lui-même garantit qu'il puisse être utilisé pour corriger des sommets : son voisinage impair.

On peut s'intéresser à des graphes garantissant l'équiprobabilité, mais pas le déterminisme, et éventuellement, à modifier le co-domaine de l'application P (l'ensemble des corrections faisables) pour faire coïncider les deux notions. L'exemple le plus simple de graphe dans ce cas là est celui de la figure 4. En effet, mesurons le dans l'ordre $v_1 \prec v_2 \prec v_3 \prec v_4$. On peut se servir de v_2 ou de v_5 pour corriger v_1. On ne peut pas se servir de v_5 pour corriger v_2 car cela ferait un effet de bord sur v_1, déjà mesuré. On doit donc se servir de v_6. Pour corriger v_3, on doit de même utiliser v_4 (car utiliser v_6 ferait un effet de bord sur v_2). Et on ne peut pas corriger v_4 : v_3 est déjà mesuré donc ne peut être utilisé et empêche d'utiliser v_6, et on ne peut utiliser v_5 sous peine d'avoir des effets de bord sur v_1 et v_2. Il est aisé de voir qu'il en est de même quel que soit l'ordre. On vérifie de même qu'il satisfait la condition du théorème 2.

On peut toutefois, pour un ensemble d'angles définis, trouver une correction qui rende déterministe le calcul. Supposons par exemple que l'angle de mesure d'un qubit isolé soit 0. L'action d'un X sur lui est gratuite. En effet, notons son état $a\,|+\rangle + b\,|-\rangle$. Le mesurer avec l'angle 0 a pour résultat $s = 0$ avec probabilité $|a|^2$ et $s = 1$ avec probabilité $|b|^2$. Avant mesure, l'action de X le met dans l'état $a\,|+\rangle - b\,|-\rangle$ ($|+\rangle$ et $|-\rangle$ sont vecteurs propres de X respectivement pour les valeurs propres 1 et -1), ce

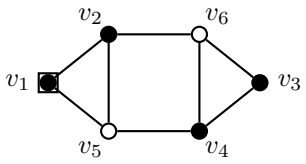

FIGURE 4. Un graphe garantissant l'équiprobabilité, mais pas le déterminisme

qui après mesure, a une probabilité $|a|^2$ de donner $s = 0$ et $|-b|^2$ de donner $s = 1$. Ce qui est la même chose que ci-dessus. Par linéarité, c'est encore le cas pour un qubit intriqué. Ainsi, un sommet mesuré avec l'angle 0 peut être corrigé aussi bien avec l'action de Z qu'avec celle de $-i$ Y (le produit de X et de Z). De même, un angle mesuré selon $\pi/2$ pourra être corrigé par un Z comme par un X.

α_2	α_3	α_4	Corrections après la mesure de v_4
0	0	0	$\mathrm{Z}_6{}^{(3)}/-i\mathrm{X}_5\mathrm{Y}_6{}^{(2,3,4,5,6)}$
0	0	$\pi/2$	$\mathrm{Z}_6{}^{(3)}/-i\mathrm{X}_5\mathrm{X}_6{}^{(2,4,5,6)}$
0	$\pi/2$	0	$\mathrm{Y}_5\mathrm{X}_6{}^{(2,3,5,6)}/i\mathrm{Z}_5{}^{(3,4)}$
0	$\pi/2$	$\pi/2$	$-i\mathrm{X}_5\mathrm{X}_6{}^{(2,4,5,6)}/\mathrm{Y}_5\mathrm{X}_6{}^{(2,3,5,6)}$
$\pi/2$	0	0	$\mathrm{Z}_6{}^{(3)}/\mathrm{Y}_5\mathrm{Z}_6{}^{(2,5)}$
$\pi/2$	0	$\pi/2$	$\mathrm{Z}_6{}^{(3)}/\mathrm{Y}_5\mathrm{Z}_6{}^{(2,5)}$
$\pi/2$	$\pi/2$	0	$i\mathrm{Z}_5{}^{(3,4)}/\mathrm{Y}_5\mathrm{Z}_6{}^{(2,5)}$
$\pi/2$	$\pi/2$	$\pi/2$	$-i\mathrm{X}_5\mathrm{Z}_6{}^{(2,3,4,5)}/\mathrm{Y}_5\mathrm{Z}_6{}^{(2,5)}$

FIGURE 5. Les différentes corrections, selon les angles

Considérons par exemple que v_1 soit mesuré avec un angle quelconque, v_2, v_3 et v_4 tous avec l'angle 0, dans l'ordre $v_1 \prec v_2 \prec v_3 \prec v_4$. Comme v_3 est mesuré avec l'angle 0, on peut se servir de lui pour corriger gratuitement (en faisant un X sur v_3 et un Z sur ses voisins v_4 et v_6) le quatrième qubit. Ainsi, on a une stratégie de correction. Elles sont toutes résumées dans le tableau de la figure 2.3.3, avec en exposant les sommets sur lesquels on applique une correction.

3. Extension de la correction

3.1. **Résultats d'impossibilité.** Avant de rechercher une correction fonctionnant quelque soient les angles de mesure des qubits, intéressons-nous aux contraintes que nous avons ou non sur elle. En effet, dans la définition que nous avons donnée plus haut, les corrections sont uniformes (elles ne dépendent pas des angles de mesure) et locales (elles agissent sur chaque qubit séparément : aucune intrication nouvelle n'est créée ou détruite en correction aux mesures). Nous allons voir qu'il n'est pas possible de garder ces deux contraintes.

3.1.1. *Non-uniformité de la correction.* Nous allons montrer que la correction doit nécessairement dépendre des angles de mesure. Considérons, pour cela, l'état du système désigné par le graphe après les mesures de v_1, v_2 et v_3 toutes faites avec un angle π et où $s_1 = s_2 = s_3 = 0$. Mesurons maintenant v_4 avec un angle θ quelconque. Si le résultat de la mesure est $s_4 = 0$, alors le système est dans l'état

$$-\frac{\beta}{\sqrt{2}}|00\rangle + \frac{\alpha e^{-i\theta}}{\sqrt{2}}|01\rangle - \frac{\alpha e^{-i\theta}}{\sqrt{2}}|10\rangle + \frac{\beta}{\sqrt{2}}|11\rangle$$

où le qubit d'entrée était dans l'état $\alpha|0\rangle + \beta|1\rangle$.
Tandis que si le résultat de la mesure est $s_4 = 1$, alors le système est dans l'état

$$\frac{\beta e^{-i\theta}}{\sqrt{2}}|00\rangle + \frac{\theta}{\sqrt{2}}|01\rangle + \frac{\alpha}{\sqrt{2}}|10\rangle + \frac{\beta e^{-i\theta}}{\sqrt{2}}|11\rangle$$

Supposons qu'il existe une correction uniforme. Cela se traduit par l'existence d'une application linéaire U dont la matrice est de la forme $\begin{bmatrix} a & e & q & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{bmatrix}$, où les coefficients sont des constantes complexes telle que

$$\forall \theta \in \mathbf{R}, \forall (\alpha, \beta) \in \mathbf{S^1_C}, U \begin{bmatrix} \beta e^{-i\theta} \\ \alpha \\ \alpha \\ \beta e^{-i\theta} \end{bmatrix} = \begin{bmatrix} -\beta \\ \alpha e^{-i\theta} \\ -\alpha e^{-i\theta} \\ \beta \end{bmatrix}$$

$$\Leftrightarrow \begin{cases} a\beta e^{-i\theta} + e\alpha + q\alpha + m\beta e^{-i\theta} = -\beta \\ b\beta e^{-i\theta} + f\alpha + j\alpha + n\beta e^{-i\theta} = \alpha e^{-i\theta} \\ c\beta e^{-i\theta} + g\alpha + k\alpha + o\beta e^{-i\theta} = -\alpha e^{-i\theta} \\ d\beta e^{-i\theta} + h\alpha + l\alpha + p\beta e^{-i\theta} = \beta \end{cases}$$

La première ligne équivaut à $\forall \theta \in \mathbf{R}, \forall (\alpha, \beta) \in \mathbf{S^1_C}, (a+m)\beta e^{-i\theta} = -\beta + (e+q)\alpha$. Le membre de gauche étant une fonction de θ et pas le membre de droite, $a + m = 0$ et $e + q = -\frac{\beta}{\alpha}$. Ce qui est absurde, cette dernière égalité devant être vraie quelque soient α et β, en particulier avec $\frac{\beta}{\alpha}$ nul ou non.

La correction est donc nécessairement non-uniforme, dans le cas où v_4 est mesuré en dernier. Un calcul identique montre qu'il n'y a pas de correction uniforme si un autre qubit est mesuré en dernier.

3.1.2. *Non-localité de la correction.* Supposons maintenant que U soit locale et ne dépende pas des angles et des corrections précédentes, c'est à dire la composée spatiale de deux opérateurs, chacun sur un qubit : $U = U_1 \otimes U_2$, où $U_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ et $U_2 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, où les coefficients sont des fonctions de θ, l'angle de mesure du troisième qubit, mais ne dépende pas des autres angles de mesure. Ainsi

$$U = \begin{bmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{bmatrix}$$

et, comme ci dessus

$$\forall (\alpha, \beta) \in \mathbf{S^C_1}, U \begin{bmatrix} \beta e^{-i\theta} \\ \alpha \\ \alpha \\ \beta e^{-i\theta} \end{bmatrix} = \begin{bmatrix} -\beta \\ \alpha e^{-i\theta} \\ -\alpha e^{-i\theta} \\ \beta \end{bmatrix}$$

Ce qui implique

$$ae\beta e^{-i\theta} + af\alpha + be\alpha + bf\beta e^{-i\theta} = -\beta$$
$$\Leftrightarrow (af + be)\alpha = -\beta(1 + aee^{-i\theta} + bfe^{-i\theta})$$

Si $af + be \neq 0$, l'égalité précédente implique

$$\forall \theta \in \mathbf{R}, \forall (\alpha, \beta) \in \mathbf{S^C_1}, \alpha \neq 0, \frac{1 + aee^{-i\theta} + bfe^{-i\theta}}{af + be} = -\frac{\beta}{\alpha}$$

Or, le membre gauche dépend de θ mais pas des coordonnées du qubit d'entrée, et le membre de droite dépend de ces coordonnées, mais pas de θ. C'est donc absurde, et $af + be = 0$ et $ae + bf = -e^{i\theta}$.

En raisonnant aussi sur les autres lignes, on obtient le système suivant :

$$\forall \theta \in \mathbf{R}, \begin{cases} af + be = 0 \\ ae + bf = -e^{i\theta} \\ ch + dg = 0 \\ cg + dh = e^{i\theta} \\ ah + bg = e^{-i\theta} \\ ag + bh = 0 \\ cf + de = -e^{-i\theta} \\ ce + df = 0 \end{cases}$$

qui, pour $\theta = \pi/4$, n'a pas de solutions. Donc a fortiori, ce système n'a pas de solutions quelque soit θ. La correction ne peut pas se formuler comme un produit tensoriel de corrections locales.

3.2. **Des corrections plus générales....** On va chercher à généraliser ces corrections, en les rendant dépendantes de certains angles. Tout d'abord, on remarque les deux identités suivantes : $\forall \alpha \in \mathbf{R}$, $\langle +_\alpha | \, \mathrm{X} = \langle +_{-\alpha}| = \langle +_\alpha | \, (\cos\alpha \mathrm{I} - i \sin\alpha \, \mathrm{Z})$. En effet :

$$\begin{aligned}
\langle +_\alpha | \begin{bmatrix} e^{-i\alpha} & 0 \\ 0 & e^{i\alpha} \end{bmatrix} &= \begin{bmatrix} 1 & e^{-i\alpha} \end{bmatrix} \begin{bmatrix} e^{-i\alpha} & 0 \\ 0 & e^{i\alpha} \end{bmatrix} \\
&= \begin{bmatrix} e^{-i\alpha} & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & e^{i\alpha} \end{bmatrix}, \text{à une phase globale près} \\
&= \langle +_{-\alpha}|
\end{aligned}$$

et de même $\langle -_\alpha | \begin{bmatrix} e^{-i\alpha} & 0 \\ 0 & e^{i\alpha} \end{bmatrix} = \langle -_{-\alpha}|$. On peut ainsi envisager remplacer une mesure selon un angle α précédée de l'action de X par la même mesure précédée par $(\cos\alpha \, \mathrm{I} - i \sin\alpha \, \mathrm{Z})$. En reprenant le graphe de la figure 4, considérons le cas où v_1, v_2 et v_4 sont mesurés selon 0, et v_3 selon un angle quelconque α_3 dans l'ordre $v_1 \prec v_2 \prec v_3 \prec v_4$. L'opérateur réalisant le calcul, jusqu'à la mesure de v_3 est, où $M_{u,s_u} = M_{u,s_u}(0)$,

$$N' = \mathrm{X}_6^{s_2} \, \mathrm{Z}_4^{s_2} \, \mathrm{Z}_3^{s_2} \, M_{2,s_2} \, \mathrm{X}_2^{s_1} \, \mathrm{Z}_5^{s_1} \, \mathrm{Z}_6^{s_1} \, M_{1,s_1} N$$

On mesure le qubit v_3 et on corrige avec v_4. L'opérateur après la correction est

$$\mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3} \, M_{3,s_3} N'$$

On rend la mesure de v_4 qui vient après déterministe de façon anachronique comme suit :

$$M_{4,s_4} \, \mathrm{Z}_4^{s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3} \, M_{3,s_3} N'$$

L'objectif est de transformer ce terme (noté T) en un terme valide. On a $N' = \mathrm{X}_3^{s_4} \, \mathrm{Z}_4^{s_4} \, \mathrm{Z}_6^{s_4} \, N'$. Donc

$$\begin{aligned}
T &= M_{4,s_4} \, \mathrm{Z}_4^{s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3} \, M_{3,s_3} \, \mathrm{X}_3^{s_4} \, \mathrm{Z}_4^{s_4} \, \mathrm{Z}_6^{s_4} \, N' \\
&= M_{4,s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3+s_4} \, M_{3,s_3} \, \mathrm{X}_3^{s_4} \, N' \\
&= M_{4,s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3+s_4} \, M_{3,s_3} \, (\cos\alpha_3 \, \mathrm{I} - i \sin\alpha_3 \, \mathrm{Z}_3)^{s_4} \, N' \\
&= 2^{s_4-1} \cos^{s_4}\alpha_3 \, \mathrm{Z}_6^{s_4} \, M_{4,s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3+s_4} \, M_{3,s_3} N' \\
&\quad + 2^{s_4-1} (-i \sin\alpha_3)^{s_4} \, \mathrm{Z}_6^{s_4} \, M_{4,s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3+s_4} \, M_{3,s_3} \, \mathrm{Z}_3^{s_4} \, N'
\end{aligned}$$

en effet, $(\cos\alpha \, \mathrm{I} - i \sin\alpha \, \mathrm{Z}_3)^s = 2^{s-1} \cos^s\alpha \, \mathrm{I} + 2^{s-1}(-i)^s \sin^s\alpha \, \mathrm{Z}$.

Intéressons nous au second membre T' de la somme. On a $N' = \mathrm{X}_4^{s_4} \, \mathrm{Z}_3^{s_4} \, \mathrm{Z}_5^{s_4} \, \mathrm{Z}_6^{s_4} \, N'$. Donc

$$\begin{aligned}
T' &= 2^{s_4-1} (-i \sin\alpha_3)^{s_4} \, \mathrm{Z}_6^{s_4} \, M_{4,s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3+s_4} \, M_{3,s_3} \, \mathrm{Z}_3^{s_4} \, \mathrm{X}_4^{s_4} \, \mathrm{Z}_3^{s_4} \, \mathrm{Z}_5^{s_4} \, \mathrm{Z}_6^{s_4} \, N' \\
&= 2^{s_4-1} (-i \sin\alpha_3)^{s_4} \, \mathrm{Z}_5^{s_4} \, M_{4,s_4} \, \mathrm{X}_4^{s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3+s_4} \, M_{3,s_3} N'
\end{aligned}$$

Or $M_{4,s_4} \, \mathrm{X}_4^{s_4} = M_{4,s_4}$, donc

$$T = (\cos\alpha_3 \, \mathrm{Z}_6 - i \sin\alpha_3 \, \mathrm{Z}_5)^{s_4} \, M_{4,s_4} \, \mathrm{X}_4^{s_3} \, \mathrm{Z}_5^{s_3} \, \mathrm{Z}_6^{s_3+s_4} \, M_{3,s_3} N'$$

En rajoutant les combinaisons linéaires de corrections, on devient donc capable de corriger quelque chose que l'on ne savait pas faire avant.

3.3. **La correction générale.** Cependant, cette stratégie (fixer un angle à 0 , trouver graphiquement la correction à appliquer, le fixer à $\pi/2$, sommer les deux corrections) échoue lorsqu'on essaye de l'appliquer au graphe entier, et ce, quelque soit le choix fait de corrections (en effet, pour chaque choix d'angle, deux corrections sont possibles). Nous avons donc cherché une correction d'une autre manière. Notons $f_+ : \mathbf{C}^2 \mapsto \mathbf{C}^4$ l'application linéaire qui envoie les coefficients du qubit d'entrée sur ceux du qubits de sortie, dans le cas où les qubits v_1, v_2, v_3, et v_4 ont été mesurés selon les angles α_1, α_2, α_3 et α_4, où les mesures de v_1, v_2, v_3 ont été suivies de corrections appropriées et ou $s_4 = 0$. De même notons f_- l'application linéaire faisant la même chose dans le cas où $s_4 = 1$.

Trivialement, l'application $f_+ \circ f_-^\dagger$ constitue une correction. Ce n'est pas la seule : le graphe préservant l'information, f_+ et f_- sont injectives. Ainsi, leurs images sont de **C**-dimension 2. Ainsi, l'ensemble des bijections correctrices est un espace vectoriel de **C**-dimension 4, et l'ensemble des transformations unitaires correctrices est une variété différentielle de **R**-dimension 4. Par le calcul, on obtient l'expression suivante :

$$\begin{aligned}
f_+ \circ f_-^\dagger = &\cos(\alpha_3) \, \mathrm{Z}_6 + i \sin(\alpha_3) \cos(\alpha_4) \, \mathrm{Z}_5 \\
&+ \sin(\alpha_2) \, [\mathrm{Y}_5 \, \mathrm{Z}_6 - i \sin(\alpha_3) \sin(\alpha_4) \, \mathrm{X}_5 \, \mathrm{Z}_6] \\
&+ \cos(\alpha_2) \, [-i \cos(\alpha_3) \cos(\alpha_4) \, \mathrm{X}_5 \, \mathrm{Y}_6 - i \sin(\alpha_4) \, \mathrm{X}_5 \, \mathrm{X}_6 + \sin(\alpha_3) \, \mathrm{Y}_5 \, \mathrm{X}_6]
\end{aligned}$$

qui n'est pas unitaire. On ne peut, de plus, pas la mettre sous une forme proche de celle de la section 3.2 : aucun angle ne peut être choisi pour factoriser une partie de ce terme par son sinus, et l'autre par son cosinus.

Par contre on voit clairement que cette expression dégénère en la somme des corrections de la figures 2.3.3 pour peu que l'on choisisse les angles α_2, α_3 et α_4. Ainsi, si $\alpha_2 = \alpha_3 = \alpha_4 = 0$, la correction suggérée est $\mathrm{Z}_6 - i\,\mathrm{X}_5\,\mathrm{Y}_6$, c'est-à-dire la somme des deux corrections de la figure 2.3.3. La somme des deux corrections obtenues graphiquement semble donc plus « canonique » que chacune des deux séparément. Réécrivons le tableau de la figure 2.3.3, mais cette fois en écrivant, pour chaque correction, les angles où elle est valide. On obtient le tableau de la figure 6. En attribuant à chaque correction le coefficient valant 1 dans son domaine minimal et 0 hors de celui-ci, on obtient la correction $f_+ \circ f_-^\dagger$. On a ainsi trouvé une correction canonique, fonctionnant sur ce graphe, combinaison linéaire des corrections particulières, mais n'étant hélas pas unitaire.

Correction	α_2	α_3	α_4	coefficient dans $f_+ \circ f_-^\dagger$
Z_6		0		$\cos(\alpha_3)$
$-i\,\mathrm{X}_5\,\mathrm{Y}_6$	0	0	0	$\cos(\alpha_2)\cos(\alpha_3)\cos(\alpha_4)$
$-i\,\mathrm{X}_5\,\mathrm{X}_6$	0		$\pi/2$	$\cos(\alpha_2)\sin(\alpha_4)$
$\mathrm{Y}_5\,\mathrm{X}_6$	0	$\pi/2$		$\cos(\alpha_2)\sin(\alpha_4)$
$i\,\mathrm{Z}_5$		$\pi/2$	0	$\sin(\alpha_3)\cos(\alpha_4)$
$\mathrm{Y}_5\,\mathrm{Z}_6$	$\pi/2$			$\sin(\alpha_2)$
$-i\,\mathrm{X}_5\,\mathrm{Z}_6$	$\pi/2$	$\pi/2$	$\pi/2$	$\sin(\alpha_2)\sin(\alpha_3)\sin(\alpha_4)$

FIGURE 6. Les domaines minimaux de validité des corrections, en regard des coefficients dans $f_+ \circ f_-^\dagger$

CONCLUSION

Ainsi, on a réussi à étudier certains graphes au-delà de ceux qui étaient connus comme étant déterministes et à comprendre un peu mieux ce qu'il fallait changer aux définitions du calcul pour augmenter le nombre de tels graphes. On sait mieux quels types de corrections ne peuvent pas être utilisés, et, bien que l'on n'aie pas trouvé de correction générale répondant à tous les critères désirables (unitaire, explicable à partir des corrections partielles), on en a trouvé d'assez proche. Ainsi, ce stage s'est révélé n'être qu'un travail préliminaire, sans doute par manque de temps. Il faudrait maintenant étudier un autre graphe équiprobable et non-déterministe, pour tester la validité des conclusions. Il serait aussi intéressant de continuer le travail dans un formalisme plus abstrait et plus léger, le MEASUREMENT CALCULUS ([DKP07],[Dan+10]), un système de réécriture capturant l'essentiel du comportement des opérateurs considérés.

J'ai toutefois apprécié ces deux mois, que ce soit du point de vue de l'ambiance dans l'équipe que du thème, situé à l'intersection entre mathématiques, informatique et physique.

Références

[BB06] Daniel E. Browne et Hans J. Briegel. "One-way Quantum Computation - a tutorial introduction". Dans : *arXiv.org* quant-ph (mar. 2006). URL : http://arxiv.org/abs/quant-ph/0603226v2.

[Bro+07] Daniel E. Browne, Elham Kashefi, Mehdi Mhalla et Simon Perdrix. "Generalized Flow and Determinism in Measurement-based Quantum Computation". Dans : *New Journal of Physics* (fév. 2007), p. 250. DOI : 10.1088/1367-2630/9/8/250. URL : http://arxiv.org/abs/quant-ph/0702212v1.

[CD09] Bob Coecke et Ross Duncan. "Interacting Quantum Observables: Categorical Algebra and Diagrammatics". Dans : *arXiv.org* quant-ph (juin 2009). DOI : 10.1088/1367-2630/13/4/043016. URL : http://arxiv.org/abs/0906.4725v3.

[Dan+10] Vincent Danos, Elham Kashefi, Prakash Panangaden et Simon Perdrix. "Extended Measurement Calculus". English. Dans : *Semantic Techniques in Quantum Computation*. Sous la dir. de Simon Gay et Ian Mackie. Cambridge : Cambridge University Press, juil. 2010, p. 235–310. ISBN : 978-0-521-51374-6.

[Deu89] D. Deutsch. "Quantum Computational Networks". Dans : *Royal Society of London Proceedings Series A* 425 (1989), p. 73–90. DOI : 10.1098/rspa.1989.0099.

[DKP07] Vincent Danos, Elham Kashefi et Prakash Panangaden. "The Measurement Calculus". Dans : *Journal Of The Association Of Computing Machinery* 52.2 (avr. 2007). URL : http://arxiv.org/abs/quant-ph/0412135v1.

[Got97] Daniel Gottesman. "Stabilizer Codes and Quantum Error Correction". Thèse de doct. Pasadena : California Institue of Technology, mai 1997. URL : http://arxiv.org/abs/quant-ph/9705052.

[Mha+10] Mehdi Mhalla, Mio Murao, Simon Perdrix, Masato Someya et Peter S. Turner. "Which graph states are useful for quantum information processing?" Dans : *arXiv.org* quant-ph (juin 2010). URL : http://arxiv.org/abs/1006.2616v2.

[Neu32] John von Neumann. "Mathematische Grundlagen der Quantenmechanik". Dans : *Springer, Berlin* (1932).

[RB01] Robert Raussendorf et Hans J. Briegel. "A One-Way Quantum Computer". Dans : *Physical Review Letter* 86.22 (mai 2001), p. 5188–5191. DOI : 10.1103/PhysRevLett.86.5188.

[Sho95] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". Dans : *arXiv.org* quant-ph (août 1995). URL : http://arxiv.org/abs/quant-ph/9508027v2.