

CENTRALESUPÉLEC

PARCOURS RECHERCHE
RAPPORT

Parcours Recherche

Informatique Quantique

Synthèse de matrices quantiques à l'aide de QMDD

Élève:

Pierrick BOURNEZ

Encadrant :

Renaud VILMART

4 novembre 2024

Table des matières

1	Introduction	1
1.1	Contexte et enjeux	1
1.2	Objectif du projet	1
2	Les Quantum Multiple Decisions Diagram	2
2.1	Définition	2
2.2	Clifford+T	3
2.3	Notre Implémentation Python	3
2.3.1	Réduction de QMDD	3
2.3.2	Réduction de la taille de la QMDD par swapping	4
3	Diagramme ZX	5
4	Vers une synthèse des QMDDs en diagramme ZX	6
4.1	Passer du ZX à des circuits quantiques	6
5	Comparaison pratique de la synthèse des circuits quantiques	8
6	Conclusion et perspectives	9
6.1	Conclusion	9

Chapitre 1

Introduction

1.1 Contexte et enjeux

L'informatique quantique est actuellement en plein essor : les états et les entreprises investissent massivement dans le but de se doter de cette technologie de rupture. En effet, le calcul quantique permettrait de résoudre des problèmes considérés comme très durs : des systèmes de cryptographie deviendraient obsolètes et seraient remplacés par leur homologue quantique ; la simulation de système physique se verrait améliorée de façon drastique, etc.

Pour obtenir cette suprématie quantique, ce domaine utilise un nouveau paradigme issu de l'algèbre linéaire. Pour pouvoir concevoir efficacement de nouveaux algorithmes, il s'agit alors de trouver de nouveaux langages graphiques adaptés à cette nouvelle manière de penser.

1.2 Objectif du projet

Une des problématiques de l'informatique quantique est de trouver le nombre minimal de portes quantiques pour préparer synthétiser des circuits quantiques. Pour cela, nous avons étudié une piste qui consiste à utiliser de Quantum Multiple Decisions Diagrams (QMDDs). Alors que certains auteurs se sont intéressés à la synthèse de QMDD à l'aide de la logique classique [6], nous nous sommes concentrés à traduire le QMDD dans un langage graphique appelé ZX. Notre apport est une implémentation des QMDDs en python, une proposition de synthèse des générateurs des QMDDs et une identification de pistes supplémentaires pour la synthèse en diagramme ZX. Nous allons dans un premier temps introduire tous les outils nécessaires à notre projet, c'est-à-dire les QMDD, les diagrammes ZX et la librairie sur laquelle on travaille (Clifford+T). Nous verrons enfin nos résultats généraux sur la synthèse de QMDD à l'aide de diagramme ZX et enfin nos résultats sur un fragment de cette synthèse.

Chapitre 2

Les Quantum Multiple Decisions Diagram

2.1 Définition

Les QMDD sont des diagrammes de décisions capables de représenter efficacement de grandes matrices, et particulièrement les matrices unitaires, par ces coefficients. Cette représentation est inspirée des Binary Decisions Diagrams (BDD) issus de la logique classique conçu pour représenter des formules SAT .

Un QMDD est la combinaison d'un état-QMDD, sa syntaxe, et de son interprétation. On reprend la plupart des définitions de [9] dont ce passage est fortement inspiré.

Définition 1 (QMDD) *Un état-QMDD est la donnée d'un tuple $(s, V, H, u_0, t, h, E, w)$ tel que :*

- $s \in \mathbb{C}$ est le scalaire global.
- $V \neq \emptyset$ est l'ensemble des sommets.
- $u_0, t \in V$ sont deux sommets distincts, appelés respectivement la racine et le nœud terminal.
- H est la hauteur du QMDD.
- $h : V \rightarrow \llbracket 0, H \rrbracket$ qui associe à chaque sommet sa hauteur dans le QMDD.
- $E : V \setminus \{t\} \rightarrow V^2$ qui associe à chaque sommet non terminal ses fils.
- chaque sommet possède au moins un parent.
- $w : V \rightarrow \mathbb{C}^2$ qui correspond au poids des arêtes.

Pour dessiner un état-QMDD, on place tous les sommets à la même hauteur h dans l'état-QMDD à la même hauteur dans la représentation graphique. De plus, on omet la pondération sur une arête si elle vaut un et à la place d'écrire le nom de chaque nœud, on écrit plutôt la hauteur sur ledit nœud. Une représentation graphique est donnée figure 2.1

On souligne la racine par un fil entrant et on distingue le nœud terminal par un carré en opposition au cercle pour les autres nœuds.

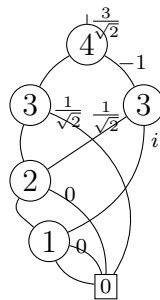
Pour D un état-QMDD on définit $\ell(D)$ le diagramme de décision défini comme le fils gauche de la racine et $r(D)$ le diagramme de décision défini comme le fils droit de la racine. On définit l'interprétation d'un QMDD inductivement :

Définition 2 (Interprétation d'un QMDD) *Pour tous état-QMDD D ,*

$\llbracket D \rrbracket$ *est l'état quantique (non normalisé) définit inductivement par :*

- $\llbracket \begin{smallmatrix} s \\ 0 \end{smallmatrix} \rrbracket = s = s | \rangle$
- $\llbracket \mathcal{D} \rrbracket = |0\rangle \otimes \llbracket \ell(\mathcal{D}) \rrbracket + |1\rangle \otimes \llbracket r(\mathcal{D}) \rrbracket$

Ce diagramme D :



Est une représentation graphique d'un SQMDD d'interprétation.

$$\llbracket \mathcal{D} \rrbracket = \frac{3}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \end{pmatrix}^T$$

On notera que les QMDD représentent initialement des vecteurs, mais que cette restriction n'est qu'un jeu de convention en adoptant une bijection idoine entre les matrices et les vecteurs.

A priori, il n'y a aucune restriction sur les valeurs prises par les coefficients sur les arêtes. Pour indiquer que nous synthétisons uniquement des circuits quantiques, nous allons nous restreindre à des coefficients utilisés dans une librairie quantique Clifford+T.

2.2 Clifford+T

Clifford+T est une suite de portes populaire pour les circuits quantiques. En effet, elle a l'avantage d'être universelle, i.e n'importe quelle matrice unitaire peut être approximés par une matrice de Clifford+T. De plus, elle est aussi résistante aux erreurs.

la librairie de Clifford+T est généré par les 3 portes du groupe de Clifford Hadamard (H), C-NOT et S

$$\begin{aligned} \text{--- H} &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ \text{--- CNOT} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \text{--- S} &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} \end{aligned}$$

L'universalité est donnée par la porte $T = \begin{pmatrix} 1 & 0 \\ 0 & \exp i\frac{\pi}{4} \end{pmatrix}$.

Une mesure du cout de réalisation d'un circuit en clifford+T est le nombre de T utilisé dans un circuit quantique, le cout de chaque circuit quantiques est donné en Figure 2.2 issue de [7]. Giles et Selinger ont aussi prouvé dans qu'une matrice unitaire dans Clifford+T avait l'aide d'un qbit ancillaire est de la forme $\frac{1}{\sqrt{2}^k}(a\omega^3 + b\omega^2 + c\omega + d$ avec $a, b, c, d, k \in \mathbb{Z}$ et $\omega = \exp i\frac{\pi}{4}$

#CONTROLS	CNOT	H	T
0	0	0	1
1	0	1	5
2	2	7	21
3	12	21	33
4	32	33	69
5	68	69	105
6	104	105	129
⋮	+24 per add. control		

Figure 2.2 : Nombre de porte T nécessaire pour faire une porte quantique avec n qbit de contrôle

2.3 Notre Implémentation Python

Concernant l'implémentation des QMDD, il existait déjà une implémentation en C++ des QMDD [10] mais aucune documentation n'était disponible. De plus, le ralentissement intrinsèque à python est acceptable, car le temps d'exécution en C++ des algorithmes développés étaient relativement limités.[6]. Nous avons implémenté une version standalone des QMDD qui comprend des fonctionnalités comme la réduction de QMDD par swap de qbit [5], des fonctions pour pouvoir charger les QMDD et la simplification de scalaire avec un algorithme particulier pour Clifford+T

2.3.1 Réduction de QMDD

Pour réduire la taille d'un QMDD, les deux problématiques essentielles sont la remontée des coefficients sur les arêtes et un algorithme de simplification de QMDD. Pour la première probléma-

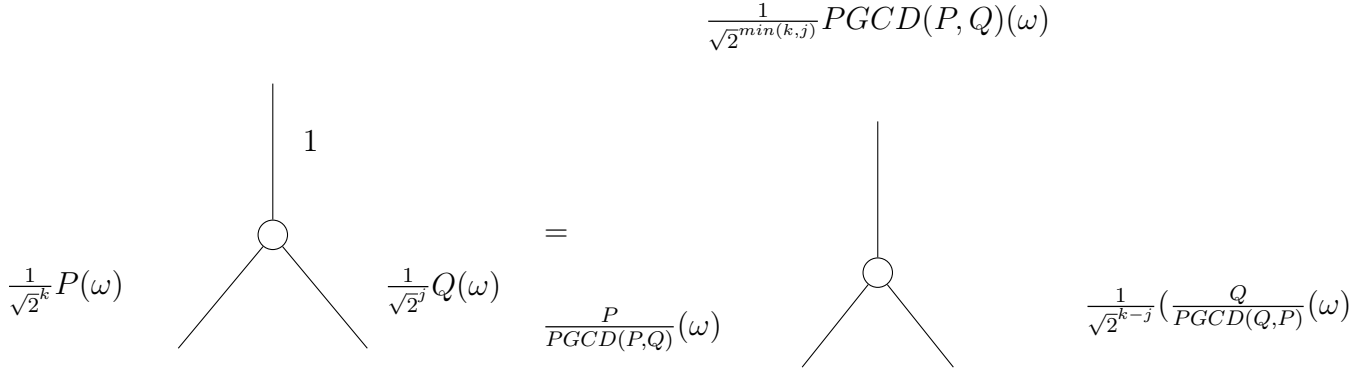


FIGURE 2.1 – factorisation des coefficients dans le cas où $k > j$

tique, nous avons implémenté une fonction de factorisation des QMDD adapté à Clifford+T. On peut remarquer que l'ensemble des coefficients des matrices de Clifford+T est

$$\left\{ \frac{1}{\sqrt{2^k}} (a\omega^3 + b\omega^2 + c\omega + d, a, b, c, d, k \in \mathbb{Z}) \right\} = \frac{1}{\sqrt{2^k}} \mathbb{Z}[\omega]$$

pour $k \in \mathbb{Z}$ avec $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{Z} . Nous pouvons aussi noter que nous pouvons nous restreindre à des polynômes de degré 3, car le polynôme annulateur de ω dans $\mathbb{Z}[X]$ est $X^4 - 1$. Nous allons expliciter le principe de notre factorisation.

Soit $g = \frac{1}{\sqrt{2^k}} P(\omega)$ et $f = \frac{1}{\sqrt{2^j}} Q(\omega)$ deux éléments de Clifford+T. On va alors factoriser P et Q avec une division euclidienne dans $\mathbb{Z}[X]$ $P = RK$ et $Q = RL$. On va alors remonter $\frac{1}{\sqrt{2^{\min(k,j)}}} * R(w)$. Une explication graphique est donnée figure 2.3.1

La factorisation revient donc à faire remonter les scalaires obtenus par cette factorisation et à regarder quelles sont les nœuds qui ont les mêmes coefficients sur les nœuds fils.

2.3.2 Réduction de la taille de la QMDD par swapping


pour réduire la taille des QMDD, nous nous inspirons de [5] pour simplifier les QMDD. L'algorithme consiste à échanger la place de deux variables itérativement, puis à effectuer une opération de la logique classique qui est encore possible en informatique quantique et à regarder la taille de la QMDD obtenue. Si elle est plus petite, on garde cette transformation, sinon on continue à échanger deux nouvelles variables. Cet algorithme polynomial en le nombre de qbits permet potentiellement de réduire fortement le nombre de nœuds nécessaire à la représentation de la QMDD [4]

Chapitre 3

Diagramme ZX

Le diagramme ZX, introduit par Coecke et Duncan [1] est une extension des circuits quantiques visant à créer une représentation graphique des circuits quantiques pour pouvoir les manipuler plus aisément. Un diagramme ZX est composé de file et de *spiders*. Les fils à gauche sont appelés les fils entrants et ceux à droite les fils sortants. On peut les composer horizontalement ou par des produits de tenseurs.

Les diagrammes ZX sont générés par des nœuds vert et rouge et les porte Hadamard dont on donne leur interprétation :

-  appelé la porte Hadamard
- $n \text{ --- } \alpha \text{ --- } m := |+\dots+\rangle\langle +\dots+| + e^{i\alpha} |-\dots-\rangle\langle -\dots-|$ appelé les X-spiders
- $n \text{ --- } \alpha \text{ --- } m := |0\dots0\rangle\langle 0\dots0| + \exp(i\alpha) |1\dots1\rangle\langle 1\dots1|$ appelé les Z-spiders

L'intérêt fondamental des diagrammes ZX est de donner des relations entre les générateurs pour simplifier des diagrammes ZX.

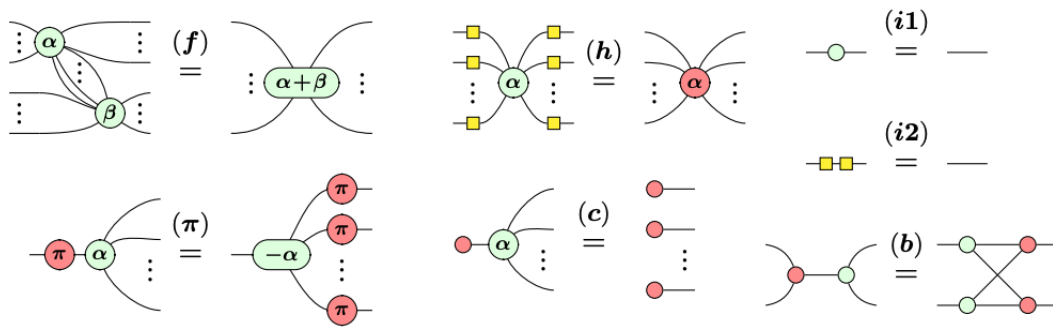
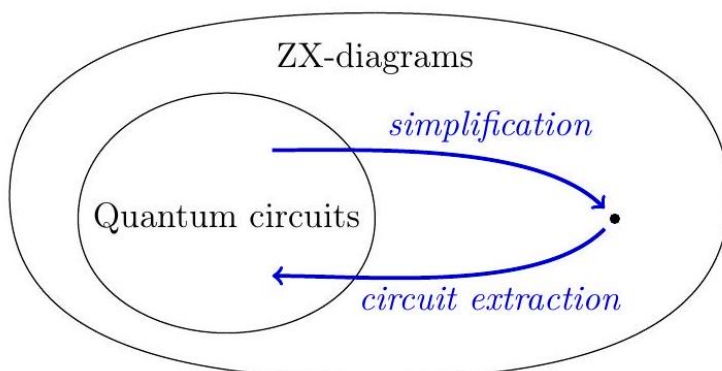


FIGURE 3.1 – Règle d'interactions des diagrammes ZX

Un diagramme ZX se lit de gauche à droite, les entrées se connectent aux fils de gauche et les sorties se lisent sur les fils de droits.

La traduction d'un circuit quantique en un diagramme ZX est directe, en revanche, il faut noter que n'importe quels diagrammes ZX ne peut pas se synthétiser en un circuit quantique. En effet, les diagrammes ZX sont universelles, c'est-à-dire qu'ils permettent de synthétiser une matrice quelconque. De plus, il a été prouvé que l'extraction de circuit quantique à partir de diagramme ZX peut être très difficile [2]



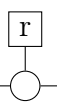


Chapitre 4

Vers une synthèse des QMDDs en diagramme ZX

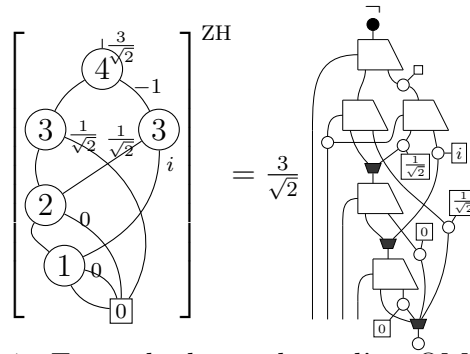
Notre premier objectif est de synthétiser des QMDD en diagramme ZX pour retrouver un circuit. Sachant la difficulté de synthétiser un diagramme ZX en circuit quantique, il faut trouver une représentation adéquate. Un QMDD étant composé d'un nœud, de fils et de poids sur les arêtes, il suffit d'être capable de synthétiser chacun de ces éléments.

[9] a introduit en ZH les générateurs suivants :

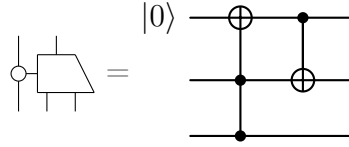
- Le premier générateur  d'interprétation $\begin{bmatrix} \text{symbol} \end{bmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$
-  d'interprétation $\begin{bmatrix} \text{symbol} \end{bmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.
-  d'interprétation : $\begin{bmatrix} \text{symbol} \end{bmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}$.

Nous renvoyons le lecteur intéressé à [9] pour l'expression explicite de ces générateurs en ZH. Comme le ZH et le ZX représentent tous les deux le même concept, mais ne prennent pas les mêmes générateurs, il existe aussi une définition de ces générateurs en diagrammes ZX.

Un exemple de la traduction de QMDD en ZH est donnée en exemple 4

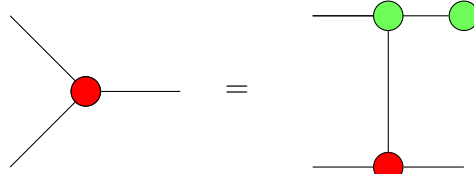


juste en une porte Toffoli et un CNOT . Rigoureusement, pour obtenir le générateur avec un unique-
ment un fil vers le haut, il suffit d'appliquer un nœud blanc à la première sortie ou un nœud blanc
sur l'entrée si on veut obtenir le générateur équivalent



Traduction en circuit quantique du générateur des nœuds des QMDDs

-Pour les arêtes, ce générateur en ZX n'est pas synthétisable en circuit quantique, car ce n'est
pas une isométrie. En revanche, on peut remarquer la propriété suivante :



Réécriture du générateur des arêtes en ZX

Cette reformulation à première vue ésotérique signifie juste que cet opérateur correspond à une
mesure du second qubit avec une sélection sur le second qubit par $|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Cela signifie que
ce générateur correspond à une mesure et on ne sélectionne que les qbits qui ont la bonne valeur.
Cette information nous invite vers la voie du Measurement based quantum Correction (*MBQC*).

-Le dernier générateur à traiter est le générateur qui représente les coefficients de matrice

$$\left\| \begin{array}{c} \boxed{r} \\ \text{---} \text{---} \text{---} \end{array} \right\| = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix}.$$

Si le coefficient r est à priori quelconque, il n'est pas possible d'obtenir ni un circuit quantique ni
une mesure post-sélection, car la matrice ne serait pas unitaire. Pour pouvoir retrouver un circuit
quantique, nous devons donc nous restreindre à des éléments de \mathbb{C} particuliers. Nous allons donc nous
restreindre par la suite au cas $|r| = 1$ qui rend exactement la matrice unitaire. Plus précisément,
nous allons dans ce rapport nous restreindre à *Clifford+T* et ces unitaires typiques de la forme ω^n
avec $\omega = e^{i\frac{\pi}{4}}$.Cela revient à imposer que les coefficients du QMDD soient uniquement à valeur de la
forme ω^n

Avec toutes ces informations, nous pouvons alors synthétiser une matrice avec des coefficients
idoines représentant un circuit quantique en un circuit avec des mesures post-sélections. En effet,
nous traduisons dans un premier la matrice sous la forme d'un QMDD, puis nous synthétisons le
QMDD avec leurs équivalents donnés lors de ce chapitre et cela renvoie alors un circuit quantique
avec des mesures post-sélections.

En conclusion de ce chapitre, sous certaines hypothèses, nous pouvons synthétiser à l'aide du ZH
des QMDDs à l'aide de mesure post-sélections et en se restreignant à des QMDD à valeurs dans ω^n

Chapitre 5

Comparaison pratique de la synthèse des circuits quantiques

Nous voulons enfin tester nos résultats pour le comparer à la littérature. Pour cela, nous nous sommes restreints à un type particulier de matrice : les matrices diagonales avec des puissances en ω^n . L'intérêt est que ces matrices diagonales émergent naturellement dans un algorithme de synthèse de matrices diagonales [6] de Clifford+T. Nous avons donc comparé le nombre de portes T nécessaire avec la méthode usuelle et notre méthode de synthèse présentées au chapitre 4.4. Concernant l'implémentation de [6], ils synthétisent ces matrices diagonales en traitant itérativement les coefficients $1, i, -i$ en les considérant comme une *Exclusive Sum of Product*. N'ayant pas trouvé l'implémentation initiale, nous avons implémenté une version alternative inspirée de [8] nous même une synthèse qui n'utilise uniquement Exorlink1 et Exorlink2 mais permettent déjà de faire des réductions décentes du nombre de cubes. Nous avons pris pour pour différents qbits 300 matrices diagonales complètement aléatoires à coefficient idoine et nous avons calculé le nombre de portes T nécessaire et de mesure pour chacun des deux algorithmes. Le temps d'exécutions était négligeable, de l'ordre de la dizaine de secondes. Les résultats sont présents au tableau 5.1

nombre qbit	nombre porte T ESOP	nombre porte T pour notre algorithme	nombre mesure associée
1	20	6	2
2	128	12	7
3	315	27	17
4	1171	50	37
5	3807	105	76
6	11257	205	155
7	51823	396	312

TABLE 5.1 – Résultat de notre benchmark

les résultats sont relativement impressionnants, le nombre de Portes T pour la synthèse est parfois diminué d'un facteur 100 voir plus et le nombre de mesures est du même niveau que le nombre de portes T. Toutefois ces résultats impressionnants sont à relativiser, la première donnée est qu'il faudrait calculer la probabilité d'obtenir le résultat final en fonction du nombre de mesures, il est possible que la probabilité d'obtenir toutes ces mesures soit très négligeable. De plus, l'intérêt de Clifford+T est justement son caractère *fault Tolerant* et la mesure post correction n'est pas un outil usuel de cette librairie.

Chapitre 6

Conclusion et perspectives

6.1 Conclusion

Lors de ce pôle projet, nous avons pu étudier la synthèse de circuit quantique à l'aide des QMDDs. Pour cela, nous avons d'abord réimplémenté les QMDDs en python pour pouvoir être manipulable avec une documentation clair, puis nous avons trouvé des équivalents en ZX des éléments fondamentaux des QMDDs. Ces générateurs peuvent se traduire en informatique quantique au prix de mesures post-sélections. Nous avons obtenu des résultats à première vue prometteurs, mais qui nécessiterait des travaux supplémentaires. En effet, il faudrait réussir à quantifier la probabilité d'obtenir le résultat à l'aide de nos mesures post-sélections et nous pourrions aussi regarder nos résultats avec des bibliothèques qui utilisent déjà les mesures post-sélections. Concernant les QMDDs en tant que tel, je pense qu'ils existent plusieurs pistes d'amélioration.

- Il faudrait réussir à mieux comprendre l'interaction entre les QMDD et la synthèse des coefficients sur les arêtes. Pour cela, on pourrait étudier leurs interactions en ZH pour essayer de trouver des représentations intermédiaires pour faire de simplifier ces coefficients.
- On pourrait aussi regarder à quelles conditions sur les arêtes un QMDD possède ou non un g-flow [3], ce qui devrait être possible, car dans certains cas, il existe une traduction en circuit quantique de ces QMDDs.
- Enfin, une autre piste d'amélioration serait de creuser l'interaction entre les QMDDs et les BDDs. Une voie serait de regarder s'il est possible de voir à quelles conditions nous pourrions utiliser les mêmes algorithmes que les BDDs mais appliqué sur les QMDDs.

Nous pensons que ces différentes voies permettraient d'améliorer nos résultats obtenus lors de ce parcours recherche

Bibliographie

- [1] Bob Coecke and Ross Duncan. Interacting quantum observables : categorical algebra and diagrammatics. *New Journal of Physics*, 13(4) :043016, 2011.
- [2] Niel de Beaudrap, Aleks Kissinger, and John van de Wetering. Circuit extraction for zx-diagrams can be# p-hard. *arXiv preprint arXiv :2202.09194*, 2022.
- [3] Ross Duncan, Aleks Kissinger, Simon Perdrix, and John Van De Wetering. Graph-theoretic simplification of quantum circuits with the zx-calculus. *Quantum*, 4 :279, 2020.
- [4] Stefan Hillmich, Lukas Burgholzer, Florian Stögmüller, and Robert Wille. Reordering decision diagrams for quantum computing is harder than you might think. In *Reversible Computation : 14th International Conference, RC 2022, Urbino, Italy, July 5–6, 2022, Proceedings*, pages 93–107. Springer, 2022.
- [5] Christoph Meinel, Fabio Somenzi, and Thorsten Theobald. Linear sifting of decision diagrams and its application in synthesis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 19(5) :521–533, 2000.
- [6] Philipp Niemann, Robert Wille, and Rolf Drechsler. Advanced exact synthesis of clifford+t circuits. 19(9) :317.
- [7] Philipp Niemann, Robert Wille, and Rolf Drechsler. Advanced exact synthesis of clifford+ t circuits. *Quantum Information Processing*, 19 :1–23, 2020.
- [8] Ning Song and Marek A Perkowski. Minimization of exclusive sum-of-products expressions for multiple-valued input, incompletely specified functions. *IEEE transactions on computer-aided design of integrated circuits and systems*, 15(4) :385–395, 1996.
- [9] Renaud Vilmart. Quantum multiple-valued decision diagrams in graphical calculi. *arXiv preprint arXiv :2107.01186*, 2021.
- [10] Alwin Zulehner, Stefan Hillmich, and Robert Wille. How to efficiently handle complex values ? implementing decision diagrams for quantum computing. *International Conference on Computer Aided Design (ICCAD)*, 2019.