Revue RAMReS – Sciences Appliquées et de l'Ingénieur
RAMReS 2024 - *Published Online 2024* - http://publication.lecames.org/
Vol. 6(1), pp. 48 - 53, Online July 2024

Vol. 6
ISSN 2630-1164
June 2024

Full Length Research Paper

Détection et correction des erreurs de calculs quantiques par algorithme quantique de code Gray

Jean Paul Latyr Faye [1*] and Serigne Bira Gueye [1]

[1]Département de Physique, Faculté des Sciences et Techniques, Cheikh Anta Diop Université, Dakar, 5005 Dakar-Fann, Sénégal

Received April 2024 – Accepted June 2024

**Corresponding author. jeanpaullatyr.faye@ucad.edu.sn*

Résumé:
L'informatique quantique a le potentiel de résoudre des problèmes trop complexes pour les ordinateurs classiques, mais elle est vulnérable au bruit et à la décohérence. Pour résoudre ce problème, la détection et la correction des erreurs quantiques sont des éléments essentiels. Cet article présente le concept de code Gray quantique, destiné à résoudre les problèmes de détection et de correction des erreurs quantiques. Une approche méthodique est proposée pour créer un algorithme de code Gray quantique. Ce dernier présente une technique de codage d'informations dans les systèmes quantiques et permet des mesures à la fois dans la base canonique et dans la base de Gray, ce qui permet la détection et la correction efficaces des erreurs quantiques. L'algorithme de code Gray proposé a été implémenté sur un ordinateur quantique IBM. Les résultats obtenus prouvent la détection et la correction des erreurs quantique, et montrent une très bonne résistance au bruit quantique.

Mots clés: Informatique quantique, Détection d'erreurs quantiques, Correction d'erreurs quantiques, Algorithmes quantiques, Code Gray, Dispositifs NISQ

Cite this article:
Jean Paul Latyr Faye , Serigne Bira Gueye (2024). Détection et correction des erreurs de calculs quantiques par algorithme quantique de code Gray. Revue RAMReS – Sci. Appl. & de l'Ing., Vol. 6(1), pp. 48-53. ISSN 2630-1164.

1. Introduction

L'émergence de l'informatique quantique [1] a fait sensation dans de nombreux domaines, offrant le potentiel d'une accélération exponentielle des tâches telles que la factorisation de grands nombres, la simulation des systèmes quantiques, et la résolution de problèmes d'optimisation [2]. Cependant, la vulnérabilité inhérente des systèmes quantiques aux bruits, la décohérence et les erreurs de mesure nécessitent le développement de techniques robustes de correction d'erreurs quantiques [3,4]. Les techniques traditionnelles de correction d'erreurs, telles que les codes de Hamming et Reed-Solomon [5] ont réussi à atténuer les erreurs dans les systèmes informatiques classiques. Cependant, ces méthodes ne sont pas adaptées à la correction des erreurs dans les systèmes quantiques en raison de la nature délicate des états quantiques décrits par la mécanique quantique. La mécanique quantique décrit des systèmes physiques aux niveaux atomique et subatomique, dans lesquels des particules telles que des électrons et des photons possèdent des caractéristiques ondulatoires et peuvent exister simultanément dans une combinaison de plusieurs états. Cela permet aux ordinateurs quantiques d'effectuer des calculs en parallèle, offrant potentiellement une accélération exponentielle par rapport aux ordinateurs classiques pour certaines tâches complexes. Cependant, les phases quantiques fragiles de cette superposition sont facilement perturbées, même par la moindre interaction avec leur environnement, entraînant une décohérence et du bruit. La décohérence est la perte de cohérence dans un système quantique, où l'information quantique est perdue en raison de l'intrication avec l'environnement. Le bruit, qui peut être provoqué par des fluctuations thermiques ou des imperfections du matériel quantique, complique encore le problème en introduisant des erreurs dans les états quantiques lors du calcul ou de la communication.

Des recherches sont menées intensément pour protéger l'information quantique de la décohérence et du bruit. Cela a conduit au développement de codes de correction d'erreurs quantiques qui se distinguent de la correction d'erreur classique. Contrairement à la correction d'erreurs classique, la correction d'erreurs quantiques n'implique pas la copie directe de

l'information quantique. Cela est dû au théorème de non-clonage selon lequel il est impossible de faire une copie exacte d'un état quantique inconnu et arbitraire. Cela présente un défi pour l'utilisation des techniques classiques pour corriger les erreurs dans les systèmes quantiques, puisque la correction d'erreurs classique repose sur la redondance et la copie de bits pour la détection et la correction des erreurs. La correction d'erreurs quantiques est un élément clé de l'informatique quantique, car elle est conçue pour contrecarrer les effets du bruit et de la décohérence sur les états quantiques. Cette technique vise à protéger l'information quantique des perturbations externes, permettant ainsi un calcul et une communication quantique plus fiables. En utilisant la correction d'erreurs quantiques, il est possible de maintenir l'intégrité des états quantiques, permettant ainsi une informatique quantique plus précise et plus fiable.

Une approche bien connue pour la correction des erreurs quantiques est celle des codes stabilisateurs [6]. Ces codes sont basés sur un ensemble d'opérateurs (stabilisateurs) qui commutent entre eux et avec l'état codé. Lorsque ces stabilisateurs sont mesurés, il est possible de détecter des erreurs et de déterminer leur emplacement. Néanmoins, cette technique nécessite l'utilisation de nombreux qubits auxiliaires pour détecter et corriger les erreurs d'un seul qubit, ce qui ajoute de la complexité à l'informatique quantique actuelle, où les ordinateurs quantiques disponibles ne disposent que de quelques dizaines de qubits.

Le code Gray s'est bien illustré dans le traitement de l'information classique comme étant une méthode de codage permettant de détecter et de corriger des erreurs de beaucoup de systèmes. Il doit sa renommée entre autres, à sa distance Hamming qui est égale à l'unité.

Dans ce travail, nous proposons un algorithme de code Gray quantique dans le but d'améliorer les performances des ordinateurs quantiques. Notre algorithme quantique de code Gray tire parti des propriétés quantiques telles que la superposition, le parallélisme et la projection quantique pour améliorer la détection, la correction des erreurs et le codage de l'information quantique. Nous utilisons le code Gray comme base de calcul quantique et explorons son utilisation dans les circuits quantiques, la production d'intrication et les protocoles de communication quantique. Pour prouver la résilience de l'algorithme face au bruit, nous avons utilisé un véritable ordinateur quantique de la compagnie IBM pour confirmer que les résultats attendus étaient bien produits.

Ce papier est structuré comme suit. La section 1 fournit une introduction et explique les avantages potentiels du code Gray quantique en matière de détection et de correction d'erreurs. Dans la section 2, nous couvrons les matériels et les méthodes menant à la construction du code Gray quantique. Nous introduisons aussi dans cette section l'informatique quantique ainsi que les opérateurs quantiques. Dans la section 3, nous présentons nos résultats et concluons dans la section 4.

2. Matériels et méthodes

Dans cette section, nous explorons les principes fondamentaux de l'informatique quantique et certaines des portes quantiques ou opérateurs unitaires utilisés dans l'élaboration de l'algorithme du code Gray.

2.1. Informatique quantique

En informatique traditionnelle, le processus est prévisible, ce qui signifie qu'il est possible de déterminer l'état interne de l'ordinateur en avance : l'informatique quantique est déterministe. Cependant, en informatique quantique, en raison du théorème de non-clonage, il n'est pas possible de connaître l'état actuel d'un ordinateur quantique : l'informatique quantique est probabiliste, comme le démontrent les principes de la mécanique quantique.

L'unité de base du traitement de l'information en informatique classique est le bit classique, qui peut prendre l'une des valeurs '0' ou '1', ce qui signifie que les bits ne peuvent être que dans un de ces deux états. Toutes les informations classiques peuvent être représentées sous forme d'une chaîne de bits. Quant à l'informatique quantique, elle utilise des bits quantiques, appelés qubits [7] pour le traitement de l'information. Ainsi, l'unité fondamentale du traitement de l'information en informatique quantique est le qubit. Les qubits sont mathématiquement représentés par des états quantiques bidimensionnels, généralement désignés par $|0\rangle$ et $|1\rangle$ (similaires aux bits classiques '0' et '1'). Ces deux états $|0\rangle$ et $|1\rangle$ constituent la base de calcul en informatique quantique. Contrairement à l'informatique classique, les qubits peuvent exister dans une combinaison des deux états, qui peuvent être exprimés par $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, où α et β sont des nombres complexes : il s'agit de la superposition. Les amplitudes $|\alpha|2$ et $|\beta|2$ représentent la probabilité que le qubit soit respectivement dans l'état $|0\rangle$ ou $|1\rangle$. De plus, un qubit peut être écrit sous la forme $|\psi\rangle = e^{i\gamma}\,[\cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle]$, où γ, φ et θ sont des nombres réels.

On peut considérer n ≥2 qubits notés $|q_0\rangle$, $|q_1\rangle$,⋯,$|q_{n-1}\rangle$, dont chacun est dans l'état $|0\rangle$ ou $|1\rangle$, ou une superposition de ces états $|0\rangle$ et $|1\rangle$. L'état final est un produit tensoriel et s'exprime sous la forme : $|q_0\rangle \otimes |q_1\rangle \otimes \cdots |\otimes q_{n-1}\rangle$. L'espace de Hilbert pour n qubits a une dimension de $N=2^n$.

Les ordinateurs quantiques diffèrent des ordinateurs traditionnels (classiques) en raison de trois caractéristiques principales : la superposition, l'intrication et le parallélisme quantique. Les bits quantiques, similaires aux bits classiques, peuvent être dans l'état $|0\rangle$ ou $|1\rangle$. Cependant, un état quantique $|\psi\rangle$ peut être exprimé sous la forme

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |\psi_i\rangle \qquad \text{[Eq. 1]}$$

où les $\{|\psi_i\rangle\}_{i=0,\cdots,N-1}$ forment une base dans l'espace de Hilbert. L'informatique quantique possède une deuxième caractéristique remarquable : l'intrication ou l'entanglement. Contrairement à la superposition, l'intrication n'a pas d'équivalence en

informatique classique. Les états intriqués semblent former une seule unité et ne peuvent pas être exprimés comme une combinaison de deux états quantiques distincts. Une illustration des états intriqués sont les célèbres états de Bell [8].
L'un de ces états, pour deux qubits, peut s'exprimer comme suit :

$$|\psi_{\text{Bell}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad \text{[Eq. 2]}$$

On peut démontrer que la quantité d'informations contenues dans un état intriqué de n qubits augmente de façon exponentielle plutôt que linéaire, comme c'est le cas pour les bits classiques. Cela signifie que l'informatique quantique peut stocker beaucoup plus de données que ses homologues classiques.
L'informatique quantique a la capacité d'effectuer une multitude d'opérations en même temps, ce qu'on appelle le parallélisme quantique. Ceci est réalisé en allouant certains groupes de qubits pour des calculs spécifiques, ce qui est beaucoup plus efficace qu'avec l'informatique classique.
Théoriquement, les ordinateurs quantiques sont plus puissants que les ordinateurs classiques, mais il reste encore quelques défis à relever avant de pouvoir les utiliser. L'un d'eux est lié à la mise en œuvre physique, avec des technologies potentielles telles que les pièges à ions [9], électrodynamique quantique en cavité [10], photonique [11], points quantiques [12] et technologies supraconductrices [13]. Parmi ceux-ci, ces dernières semblent être le plus prometteuses, comme le démontre l'utilisation par IBM de qubits réels pour tester les simulations. Dans cette étude, nous soumettons nos simulations au dispositif quantique de l'IBM, précisément à l'ordinateur appelé ibm-cairo. Il est important de noter que le nom de ces ordinateurs change progressivement.

2.2. Opérateurs quantiques

Nous devons aujourd'hui résoudre le deuxième problème de l'informatique quantique, à savoir le manque d'algorithmes quantiques existants par rapport aux algorithmes classiques. Pour garantir que les ordinateurs quantiques conservent leur avantage potentiel sur les ordinateurs classiques, de nouveaux algorithmes quantiques doivent être créés. La superposition, l'intrication et le parallélisme quantique sont les caractéristiques clés qui permettent le développement d'algorithmes quantiques importants tels que l'algorithme de factorisation de Shor [14], qui peut être utilisé pour briser le protocole de chiffrement Rivest-Shamir-Adleman (RSA), l'algorithme quantique de recherche de Grover [15], qui est utilisée pour rechercher une base de données non structurée, la transformée de Fourier quantique [16], qui est à la base de nombreux algorithmes, et l'algorithme de Simon Simon [17] conçu pour trouver la période d'une fonction.

Dans cet article, nous profitons de certaines propriétés de l'informatique quantique telles que la superposition, l'intrication et le parallélisme pour introduire une nouvelle implémentation quantique de l'algorithme du code Gray. Notre circuit quantique a une complexité de O(1) et peut être exécuté efficacement sur les ordinateurs quantiques actuels.
Avant de discuter de notre nouvelle implémentation quantique de l'algorithme du code Gray, nous examinerons les principales portes quantiques nécessaires à cet article. Ces dernières, également appelées opérateurs quantiques, doivent être des opérateurs unitaires puisque la longueur des vecteurs doit être préservée après l'évolution de l'état quantique. Un opérateur U est un opérateur unitaire s'il satisfait la relation UU† = I, où I désigne la matrice unité.
Considérons d'abord l'opérateur de Pauli X agissant sur un seul qubit. Sa représentation matricielle est donnée par :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{[Eq. 3]}$$

L'action de cette porte X sur une qubit donne :

$$X|x\rangle = |1-x\rangle \quad \text{pour} \quad x = 0,1 \qquad \text{[Eq. 4]}$$

Classiquement, cela équivaut à la porte NOT.
Nous examinerons la deuxième porte quantique : la porte de Hadamard H. Il s'agit d'une porte à un qubit, et sa matrice peut être représentée comme :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{[Eq. 5]}$$

L'action de la porte Hadamard sur la base informatique est la suivante :

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle \qquad \text{[Eq. 6]}$$

Ainsi, la porte Hadamard permet de mettre une base de calcul en superposition. Pour n qubits, tous initialisés à l'état fondamental |0⟩, les actions de l'opérateur Hadamard se généralisent à :

$$H \otimes \cdots \otimes H\,(|0\rangle \cdots \otimes |0\rangle) = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{k=0}^{2^n-1} |B^k\rangle \qquad \text{[Eq. 7]}$$

avec $\quad |B^k\rangle = |b_{n-1}^k b_{n-2}^k \cdots b_1^k b_0^k\rangle$

où les |b⟩ représentent les états de la base.

Nous devons parler de la troisième porte quantique, la porte CNOT, également connue sous le nom de porte contrôlée X. Il s'agit d'une porte à deux qubits, le premier qubit agissant comme commande et le deuxième comme cible. Lorsque le qubit de commande est dans l'état |1⟩, la porte X est appliquée au qubit cible. La représentation matricielle de la porte contrôlée X, notée CNOT est donnée par :

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{[Eq. 8]}$$

Nous utilisons des propriétés et des opérateurs quantiques pour construire un circuit de code Gray quantique, qui peut être utilisé à la place de la base de calcul. Dans la section suivante, nous présenterons et analyserons nos résultats

3. Résultats

3.1. Circuit du code Quantum Gray

Cette section présente et examine un circuit quantique pour implémenter le code Gray et les résultats obtenus à partir de la simulation sur un véritable dispositif supraconducteur de d'IBM. Comme la majeure partie des ordinateurs quantiques actuels, les ordinateurs d'IBM ne sont soumis à aucune correction quantique. L'algorithme 1, illustré dans la Figure 1, ci-après, décrit l'algorithme quantique que nous proposons pour le code Gray. Nous avons en entrée un circuit quantique obtenu par l'application d'un opérateur unitaire UB. Notre but est de mesurer l'état résultant dans la base du code Gray, et non dans la base de calcul quantique. Nous appliquons d'abord la porte quantique CNOT dont les qubits de contrôle sont les qubits de sortie du circuit UB, et les cibles sont des qubits auxiliaires. Ces opérations transfèrent les informations quantiques des qubits physiques, vers les qubits auxiliaires, que nous appelons ancillas. Après cette transformation, il va falloir appliquer un opérateur code Gray U_G pour convertir la base de calcul en base du code Gray. Cependant, la conception de l'opérateur U_G du circuit quantique Gray est moins évident et constitue l'un des résultats majeurs de cette étude. Avant de démontrer comment une mesure basée sur le code Gray peut réduire la détection et permettre la correction des erreurs quantiques,

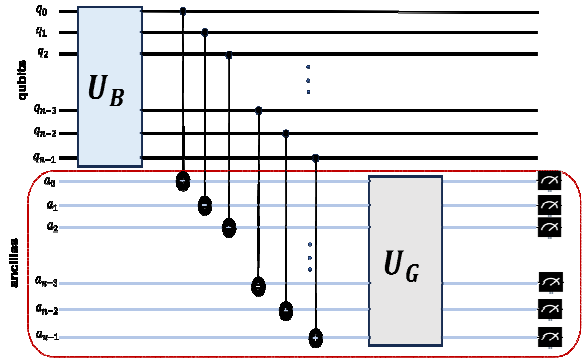

Figure 1 : **Circuits quantiques utilisés dans ce travail pour obtenir le code Gray quantique et la mesure dans la base du code Gray. On nous donne un circuit quantique UB que nous avons l'intention de mesurer selon la base du code Gray. On applique ensuite la porte CNOT, avec les qubits de contrôle appartenant au circuit quantique UB. Ces opérations transfèrent les informations quantiques des qubits réels, que nous appelons uniquement qubits, vers les qubits auxiliaires, que nous appelons ancillas. Après cette transformation, nous appliquons le code Gray quantique pour convertir la base de calcul en base du code Gray. Les qubits auxiliaires ont été mesurés et les résultats ont été enregistrés dans la base du code Gray.**

Algorithme 1 : L'algorithme du code Quantum Gray utilise deux registres quantiques Q and A pour coder les états $|\psi_B\rangle$ $|\psi_G\rangle$ respectivement. Chaque registre est composé de de n.

Entrée : registre quantique Q de n qubits q
Entrée : registre quantique A de n qubits a auxiliaires.

Entrée : $|\psi_B\rangle \leftarrow U_B^r|q[r]\rangle$ pour $r = 0, \cdots, n-1$

Pour $i = 0, \cdots, n-1$ **Faire**

$$|\psi_{B'}\rangle = \text{CNOT}_{(q[i],a[i])}|\psi_B\rangle$$

Fin Pour

$$|\psi_G\rangle \leftarrow U_G|\psi_{B'}\rangle$$

Pour $i = 0, \cdots,$ n-2 **Faire**

Si n % 2 == 0 **Alors**
Pour $i = 0, \cdots,$ n-2 **Faire**

$$|\psi_{G_1}\rangle = \text{CNOT}_{(a[i],a[i+2])}|\psi_{G_0}\rangle$$

Fin Pour

Pour $i = 0, \cdots,$ n-3 **Faire**

$$|\psi_G\rangle = \text{CNOT}_{(a[i],a[n-1])}|\psi_{G_1}\rangle$$

Fin Pour

Fin Si

Nous démontrerons d'abord que notre circuit quantique produit le code Gray correct lorsqu'il utilise un véritable ordinateur quantique.
Nous considérons le circuit quantique UB dans un état de superposition uniforme avec trois qubits. Ceci est réalisé en appliquant une porte Hadamard à chaque qubit. Dans le cas de trois qubits, nous avons un état quantique sous la forme :

$$|\psi_B\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

Nous utilisons ibmq-cairo, qui est l'un des processeurs de l'IBM Quantum. Il s'agit d'un ordinateur quantique de 27 qubits. Nous utilisons Qiskit [18] pour modéliser nos circuits quantiques proposés. Pour démontrer que notre code Gray de circuit quantique fonctionne, nous utilisons des chaînes binaires de trois et huit bits. Nous précisons qu'il s'agit d'un exemple de preuve, mais le circuit quantique peut être utilisé avec n'importe quelle chaîne de bit. Les résultats sont représentés sur la Figure 2. Il est évident que la probabilité d'obtenir le bon code Gray pour un état binaire donné est plus élevée. Comme le montre la Figure 3 (en bas à gauche), la probabilité d'obtenir 101, par exemple, après plusieurs mesures, est proche de 90 %. Cela démontre que le circuit quantique proposé pour obtenir le code Gray est efficace sur les ordinateurs NISQ (Noisy Intermediate Scale Quantum).

Les résultats pour le cas de huit bits sont représentés dans la Figures 3 (a) et (b) pour un état d'entrée:

$$\frac{1}{\sqrt{2}}(|11111111\rangle + |00001111\rangle$$

Nous observons que la probabilité d'obtenir le code Gray exact est nettement supérieure à celle des autres états, bien que nous ayons utilisé un vrai ordinateur quantique (IBMQ Cairo de 27 qubits). Cependant, les résultats de tous les 256 états, que nous avons obtenus, indiquent une probabilité importante (supérieure à 80%) pour chaque code Gray correspondant.

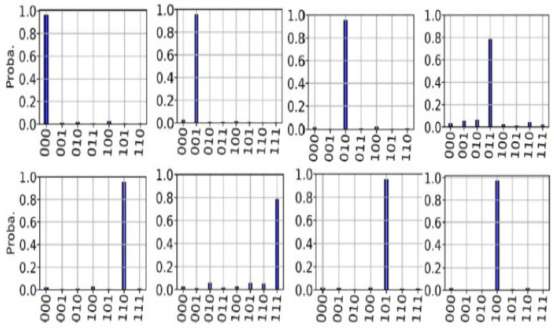

Figure 2: Nous démontrons l'efficacité de notre algorithme quantique de Gray en examinant l'état $|\psi B\rangle$ généré par le circuit quantique UB. En utilisant un véritable appareil NISQ (IBMQCairo (27 qubits)), nous observons que la probabilité d'obtenir le code Gray correspondant pour trois bits est nettement supérieure aux probabilités d'obtenir d'autres bits. Malgré le bruit de l'appareil réel, les probabilités d'obtenir d'autres bits sont encore suffisamment faibles pour conclure que nos algorithmes quantiques de Gray peuvent être utilisés dans les appareils NISQ

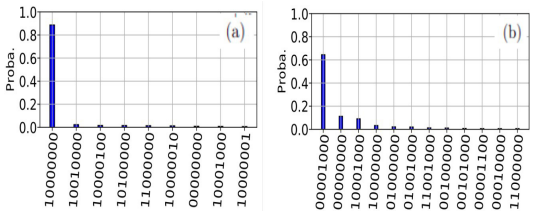

Figure 3 : Distribution de probabilité pour les entrées à huit bits : $\frac{1}{\sqrt{2}}(|11111111\rangle + |00001111\rangle$

La Figure 4 montre la densité pour un état intriqué au maximum. Dans (a), nous n'introduisons pas de bit flip (bit d'erreur) et l'utilisons comme référence. Dans (b), (c) et (d), nous faisons respectivement une inversion logique (corruption de bit) des premier, deuxième et troisième qubits pour générer un bit-flip.

Il apparait que la base du code Gray a une distance de Hamming de 1, alors que cette distance est supérieure ou égale à l'unité dans la base de calcul. Par conséquent, travailler avec une base de code Gray permet de simplifier l'identification des erreurs quantiques, et facilite leur correction.

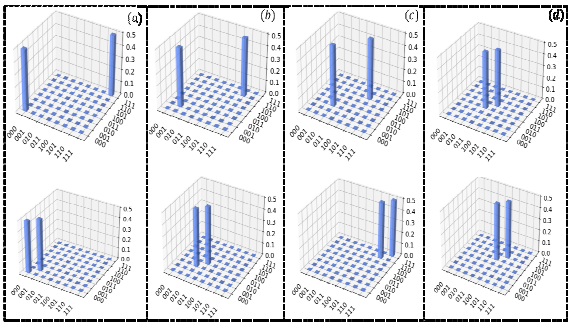

Figure 4 : La matrice de densité dans la base de calcul est présentée en dessus, et celle dans la base du code Gray en dessous. Dans (a), nous n'introduisons pas le bit flip et l'utilisons comme référence. Dans (b), (c) et (d), nous changeons respectivement les états du premier, deuxième et troisième qubit.

Il est à noter que la sortie du premier qubit reste la même, qu'il soit inversé ou non. Si le premier qubit est corrompu, cette corruption est détectée dans le deuxième qubit. Lorsque le deuxième qubit est corrompu, alors l'erreur est détectée à l'aide du premier et du troisième qubits qui sont ses voisins directs et dont chacun de leurs états ont été inversés. Si seul le troisième qubit est corrompu, l'erreur est détectée au niveau du qubit précédent dont l'état est inversé. Ainsi, quel que soit le cas, l'erreur survenue au niveau du qubit n se manifeste sur les qubits voisins n-1 ans n+1. Ainsi, une mesure dans la base du code Gray permet une détection efficace et très simple de l'erreur. La correction se fait simplement par l'action de la porte X sur le qubit dont l'erreur a été détectée. Ceci prouve un avantage du code Gray en informatique quantique.

4. Conclusion

Il existe un grand enthousiasme pour la création d'algorithmes quantiques en raison des applications potentielles et de l'accélération exponentielle que peuvent offrir les ordinateurs quantiques. Néanmoins, les ordinateurs quantiques actuels présentent certaines restrictions en termes de temps de cohérence des qubits et de bruit. Cet article présente une nouvelle implémentation quantique de l'algorithme du code Gray qui tire parti des propriétés de l'informatique quantique telles que la superposition, l'intrication et le parallélisme. En effet il peut être utilisé comme base de calcul permettant une détection simple et efficace des erreurs quantiques et leur correction. Nos simulations sur un dispositif quantique réel démontrent que le circuit conçu est efficace sur les ordinateurs quantiques actuels et produit une forte probabilité de trouver la bonne solution.

Acknowledgements

Nous tenons à remercier le Réseau national de conception du Canada (CNDN) pour avoir facilité cette recherche, en particulier par le biais de l'adhésion d'IBM Quantum Hub au PIQ2.

Nous tenons également à remercier les collègues Alassane Traoré et Mor Ndiaye pour leur soutien et encouragement.

REFERENCES

[1] T.D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J.L. O'Brien, Quantum computers. nature 464(7285), 45–53 (2010)

[2] Y. Wang, J.E. Kim, K. Suresh, Opportunities and challenges of quantum computing for engineering optimization. Journal of Computing and Information Science in Engineering pp. 1–10 (2023)

[3] J. Roffe, Quantum error correction: an introductory guide. Contemporary Physics 60(3), 226–245 (2019)

[4] V. Sivak, A. Eickbusch, B. Royer, S. Singh, I. Tsioutsios, S. Ganjam, A. Miano, B. Brock, A. Ding, L. Frunzio, et al., Real-time quantum error correction beyond break-even. Nature 616(7955), 50–55 (2023)

[5] S. Gao, in Communications, information and network security (Springer, 2003), pp. 55–68

[6] A. Antipov, E. Kiktenko, A. Fedorov, Realizing a class of stabilizer quantum error correction codes using a single ancilla and circular connectivity. Physical Review A 107(3), 032403 (2023)

[7] M. Nielsen, I. Chuang. Quantum computation and quantum information, 10th anniversary cambridge university press (2010)

[8] H. Weinfurter, Experimental bell-state analysis. Europhysics Letters 25(8), 559 (1994)

[9] I. Pogorelov, T. Feldker, C.D. Marciniak, L. Postler, G. Jacob, O. Krieglsteiner,
V. Podlesnic, M. Meth, V. Negnevitsky, M. Stadler, B. H¨ofer, C. W¨achter, K. Lakhmanskiy, R. Blatt, P. Schindler, T. Monz, Compact ion-trap quantum computing demonstrator. PRX Quantum 2, 020343 (2021). https://doi. org/10.1103/PRXQuantum.2.020343. URL https://link.aps.org/doi/10.1103/ PRXQuantum.2.020343

[10] S. Haroche, D. Kleppner, Cavity quantum electrodynamics. Phys. Today 42(1), 24–30 (1989)

[11] J.L. O'Brien, Optical quantum computing. Science 318(5856),1567–1570(2007).
https://doi.org/10.1126/science.1142892.URhttps://www.science.org/doi/abs/10.1126/science.1142892.

[12] C. Kloeffel, D. Loss, Prospects for spin-based quantum computing in quantum dots. Annu. Rev. Condens. Matter Phys. 4(1), 51–81 (2013)

[13] W. et al., Strong quantum computational advantage using a superconducting quantum processor. Phys. Rev. Lett. 127,180501(2021)
https://doi.org/10.1103/PhysRevLett.127.180501.

[14] P.W. Shor, in Proceedings 35th annual symposium on foundations of computer science (Ieee, 1994), pp. 124–134

[15] L.K. Grover, in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (1996), pp. 212–219

[16] C. Moore, D. Rockmore, A. Russell, Generic quantum fourier transforms. ACM Transactions on Algorithms (TALG) 2(4), 707–723 (2006)

[17] D.R. Simon, On the power of quantum computation. SIAM journal on computing 26(5), 1474–1483 (1997)

[18]à G. Aleksandrowicz, T. Alexander, P. Barkoutsos, L. Bello, Y. Ben-Haim, D. Bucher, F.J. Cabrera-Hern´andez, J. Carballo-Franquis, A. Chen, C.F. Chen, et al., Qiskit: An open-source framework for quantum computing. Accessed on: Mar 16 (2019)