Comparaison des performances des algorithmes classiques et quantiques pour la détection dans un système NOMA

Muhammad Idham HABIBIE, Jihad HAMIE, Claire GOURSAUD

Université de Lyon, INSA Lyon, INRIA
CITI EA 3720
F-69621 Villeurbanne, France
muhammad-idham.habibie@insa-lyon.fr, jihad.hamie@insa-lyon.fr
claire.goursaud@insa-lyon.fr

Résumé – L'un des freins des systèmes NOMA *(Non orthogonal Multiple access)* est la complexité de détection des utilisateurs actifs *(AUD: Active User Detection)*. Nous proposons dans cet article d'utiliser une version adaptée de l'algorithme quantique de Grover pour la détection des utilisateurs actifs afin de tirer partie de l'accélération apportée par la superposition d'états dans les architectures quantiques, Notre version adaptée de l'algorithme de Grover est comparée aux deux récepteurs classiques de référence : le récepteur optimal du maximum de vraisemblance *(ML: Maximum Likelihood)* et le récepteur basique d'intercorrelation conventionnel *(CCR: Conventional Correlation Receiver)*. La probabilité de détection des utilisateurs actifs est évaluée en fonction du SNR *(Signal to Noise Ratio)* du signal reçu, où les résultats obtenus prouvent que notre algorithme de Grover adapté est très prometteur sous un faible niveau de bruit.

Abstract – The complexity of *Active User Detection* (AUD) is considered an essential problem in the *Non-Orthogonal Multiple Access* (NOMA) systems. Thanks to the superposition property of quantum architecture, the goal of this paper is to adapt and apply the quantum Grover algorithm for AUD purpose in the context of NOMA, to alleviate the search complexity. Our adapted Grover's algorithm is compared with some basic classical AUD receivers such as the optimal *Maximum Likelihood* (ML) and the *Conventional Correlation Receiver* (CCR). The success probability of AUD is assessed as a function of the *Signal to Noise Ratio* (SNR) of the received signal, where the obtained results prove that our adapted Grover's algorithm is very promising under a low noise level.

1 Introduction

Récemment, le nombre d'appareils mobiles connectés a fait l'objet d'une forte croissance qui va encore s'accélérer d'ici quelques années pour atteindre des milliards d'objets. En effet, leur utilisation s'est répandue dans de nombreuses applications de la vie courante telles que le multimédia amélioré, les transmissions de données à haut débit, ainsi que les communications entre machines [1]. Dans ce contexte, le partage des ressources est devenu une fonctionnalité clé permettant l'utilisation simultanée des ressources du réseau entre plusieurs utilisateurs ou appareils [2]. Ces solutions d'accès multiples sont classées en deux familles. Dans la première, l'accès multiple se fait de façon orthogonale *(OMA : Orthogonal Multiple Access)* et permet d'attribuer une ressource spécifique à chacun des nœuds émetteurs sans (ou presque sans) interférence entre utilisateurs. Cependant, le nombre des nœuds actifs est limité au nombre de ressources et une sélection aléatoire basée sur la contention d'accès est nécessaire pour allouer ces ressources aux nœuds qui demandent à transmettre à cet instant.

Ces deux contraintes conduisent à un gaspillage des ressources car chaque émetteur peut ne pas être en mesure d'exploiter pleinement la capacité de sa ressource assignée, tandis qu'un surcoût de signalisation élevé (souvent supérieur à la quantité de donnée à transmettre) est nécessaire pour établir la connexion [3]. En conséquence, l'accès multiple non orthogonal *(NOMA : Non Orthogonal Multiple Access)* a été proposé pour surmonter ces inconvénients [3]. L'idée principale est de permettre aux utilisateurs de partager les mêmes ressources d'une manière non orthogonale afin de relâcher la contrainte due au nombre limité de ressources, ainsi que de surdimmensionner le réseau pour s'approcher de sa capacité.

Dans cet article, nous nous concentrons sur l'accès NOMA par codes ((Code Domain) CD NOMA) où chaque appareil est identifié par son code et aucune information préalable n'est nécessaire avant la transmission [4]. En outre, CD NOMA permet d'avoir une transmission efficace puisque l'identifiant de l'appareil émetteur est fourni par la séquence de code, sur laquelle les données peuvent être mappées. Dans ce cas, le challenge se porte sur la capacité de détecter en temps réel l'ensemble des utilisateurs actifs parmi tous les appareils existants AUD *(Active User Detection)*.

Le récepteur basé sur le maximum de vraisemblance *(ML : maximum likelihood)* est l'AUD optimal [5], mais au prix d'une grande complexité. Ainsi, plusieurs algorithmes moins complexes ont été proposés tels que le SIC *(Serial Interference Cancellation)*, le PIC *(Parallel Interference Cancellation)* et le CCR *(Conventional Correlation Receiver)* [6], mais en dégradant les performances.

D'un autre côté, les algorithmes quantiques tirent partie de

la superposition d'états, ce qui permet d'évaluer tous les cas simultanément. Des algorithmes quantiques ont été utilisés dans [7] pour décoder conjointement les symboles transmis par tous les émetteurs. À noter que dans [7], la détection multi-utilisateurs (MUD) a été faite pour récupérer des données, alors que dans cet article nous considérons la détection d'activité.

La contribution de cet article est l'adaptation de l'algorithme quantique de Grover [8] pour la détection de l'ensemble des utilisateurs actifs dans un schéma de communication CDMA non orthogonal, où les familles des codes unipolaires et bipolaires sont adressées. Notre algorithme quantique est comparé avec le détecteur classique ML, ainsi qu'avec le CCR. En outre, nous évaluons la probabilité de succès de détection des utilisateurs actifs en fonction du SNR du signal reçu.

Le reste de l'article est organisé comme suit : La section 2 introduit les principes de base du quantum et l'algorithme de Grover. La section 3 présente l'adaptation de l'algorithme de Grover pour l'AUD. La section 4 présente le dispositif de simulation et les résultats obtenus. Enfin, la section 5 conclut l'article.

2 Algorithmie quantique

2.1 Principes quantiques

Les algorithmes quantiques ont suscité un grand intérêt ces dernières années, car ils permettent l'accélération des calculs. En particulier, l'algorithme de Grover n'a besoin que de $\mathcal{O}(\sqrt{N})$ opérations pour rechercher une valeur dans une base de données de taille N [7], tandis que l'approche classique nécessite $\mathcal{O}(N)$. En effet, une superposition des états en quantique permet d'avoir deux bits différents 0 et 1 codés simultanément sur un nouveau type de bits nommé qubit comme suit :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

où α et β sont des nombres complexes normalisés et vérifiant $|\alpha|^2 + |\beta|^2 = 1$. α^2 et β^2 sont les probabilités d'être respectivement dans les états $|0\rangle$ et $|1\rangle$.

2.2 Algorithme de Grover

L'algorithme de Grover est la référence en quantique pour rechercher une valeur dans une base de données non triée. Il est basé sur deux parties principales ; 1) Oracle et 2) Diffuseur (cf Fig. 1). L' oracle U_δ vise à marquer (avec un signe négatif) les états qui vérifient une contrainte donnée (adresse qui contient la valeur désirée (δ) pour une base de données, ou la solution d'une fonction) comme suit :

$$U_\delta|x\rangle = \begin{cases} -|x\rangle & \text{if } f(x) = \delta \\ |x\rangle & \text{if } f(x) \neq \delta \end{cases} \tag{2}$$

Puis le diffuseur amplifie les amplitudes des états marqués par l'utilisation de la moyenne inverse [8]. Les solutions attendues sont partiellement mises en évidence, et plusieurs itérations de l'oracle et du diffuseur sont nécessaires.

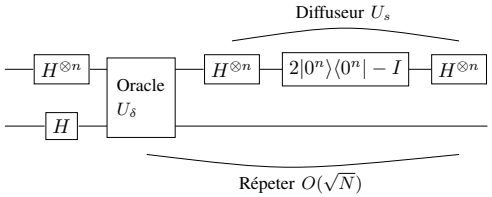

FIGURE 1 – Schéma Grover

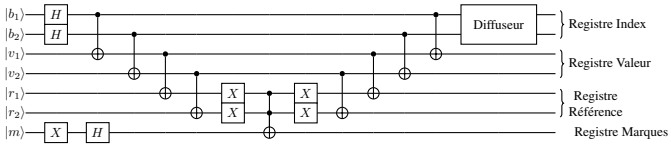

FIGURE 2 – Circuit de Grover avec 2 qubits

Le diffuseur s'obtient avec $|s\rangle$ le déphaseur conditionnel, et I la matrice identité.

$$U_s = H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n} = 2|s\rangle\langle s| - I \tag{3}$$

où $H^{\otimes n}$ et $2|0^n\rangle\langle 0^n| - I$ sont l'opérateur de Hadamard et de réflexion. La figure 2 illustre le circuit de Grover avec 2 qubits. l'Oracle de Grover s'appuie sur quatre registres différents [7]. Le registre d'index contient l'argument de la fonction f et stockera la solution à la fin de l'algorithme. Le registre des valeurs contient les résultats de la fonction appliquée aux états du registre d'index. Le registre de référence correspond à la valeur cible δ. Finalement, le registre des marques fournit le signe négatif dans le calcul pour marquer les états valides.

Les auteurs dans [8] ont défini et exprimé le nombre optimal d'itérations (L_{opt}) pour trouver une solution spécifique dans une base de données, en fonction du nombre de solutions valides (S) et de la taille de la base de données N :

$$L_{opt} = \lfloor \pi/4(\sqrt{N/S}) \rfloor \tag{4}$$

3 Proposition d'algorithme pour l'AUD

3.1 Modélisation du système

L'objectif principal de cet article est d'adapter l'algorithme quantique de Grover à des fins d'AUD dans un système CD NOMA. Dans ce contexte, on considère un réseau avec N utilisateurs communiquant avec la station de base (BS). Leurs données sont portées par un code contenant SF slots, où SF est le facteur d'étalement. Ces utilisateurs sont principalement en mode de veille et initient la transmission uniquement lorsque cela est nécessaire.

Nous nous concentrons sur l'initialisation de la transmission, où les utilisateurs envoient leur code unique c_i pour identification. Puisque tous les utilisateurs partagent le même canal, le signal reçu résultant est la somme de tous les codes des utilisateurs actifs. Pour simplifier les simulations, nous nous plaçons dans le pire cas où le canal est le même pour tous les utilisateurs avec un gain normalisé à $h = 1$, accompagné d'un bruit gaussien blanc additif *(AWGN : Additive White Gaussian Noise)*

désigné par n. Dans ce cas, le signal reçu $\tilde{y}$ peut être donné par l'équation suivante :

$$\tilde{y} = \sum_{i=1}^{K} b_i c_i + n \tag{5}$$

où K est le nombre d'utilisateurs, $b_i \in \{0, 1\}$ est le statut d'activité de l'utilisateur i, c_i est le mot de code correspondant et n est le bruit gaussien de loi $\mathcal{N}(0, \sigma^2)$. À des fins de comparaison, deux familles de codes seront retenues. La première (resp. deuxième) est formée par les codes bipolaires (resp unipolaires), où la composante de chaque code c_i appartient à l'ensemble $\{-1, 1\}$ (resp $\{0, 1\}$).

Etant donné le signal reçu et l'ensemble des codes utilisateurs, le récepteur AUD doit détecter l'ensemble des utilisateurs actifs ayant $b_i = 1$. Notons que le canal de transmission est toujours classique et que l'algorithme quantique est exécuté seulement du côté récepteur.

3.2 Adaptation de Grover pour l'AUD

Notre algorithme est basé sur celui de Grover. Chaque qubit du registre d'index correspond au statut d'activité d'un utilisateur. Ils sont tous initialisés avec l'état de superposition $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Nous utilisons ensuite des portes quantiques, afin de calculer toutes les signatures de signal possibles (une pour chaque ensemble d'activité utilisateur). Le registre de valeur contient alors ces signatures d'une manière superposée. Enfin, le signal reçu, fourni dans le registre de référence, est comparé à l'ensemble des états du registre de valeur. L'état identique est marqué avec un signe négatif, avant amplification comme expliqué dans 2.2. Cependant, avant d'être introduit dans le registre de référence, le signal reçu doit être prétraité.

En effet, le circuit de Grover ne peut être alimenté qu'avec des données binaires alors que notre signal reçu est un vecteur réel. Pour résoudre ce problème, une méthode simple consiste à transformer $\tilde{y}$ en prenant la valeur entière la plus proche dans l'ensemble des valeurs attendues théoriques, puis de le convertir en binaire. En accord avec les familles de codes concernées (unipolaires et bipolaires), la partie entière de $\tilde{y}$ notée $\tilde{y}_{pr}$ est obtenue de la façon suivante :

$$\tilde{y}_{pr} = \begin{cases} \min(\max(0, \text{round}(\tilde{y})), 2^m - 1) & c \in \{0, 1\} \\ \min(\max(\text{round}(\tilde{y}), -2^m - 1), 2^m - 1) & c \in \{-1, 1\} \end{cases} \tag{6}$$

où m est le nombre de bits utilisés pour représenter chaque composante de $\tilde{y}_{pr}$, et définit l'échelle des valeurs traitées.

Ces opérations de calibration du signal sont effectuées avec des dispositifs classiques. Le calcul quantique se limite à l'algorithme de Grover. L'algorithme de Grover est appliqué pour le nombre optimal d'itérations préalablement défini L_{opt} afin de détecter l'ensemble des utilisateurs actifs à partir de $\tilde{y}_{pr}$.

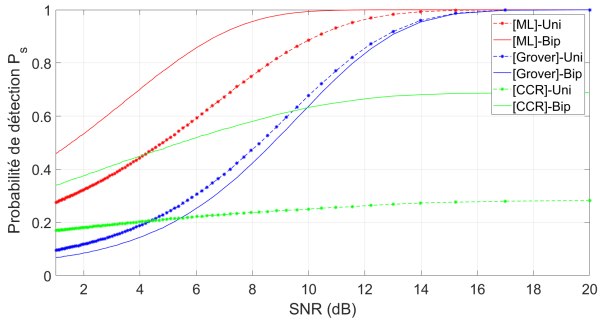

FIGURE 3 – Probabilité de détection en fonction du SNR.

4 Simulations et Résultats

4.1 Paramètres

Afin d'obtenir les performances de notre algorithme, nous avons utilisé la bibliothèque Qiskit en Python pour effectuer des simulations. Ainsi, le comportement quantique est émulé avec un circuit classique, donc très consommateur en ressources de calculs. En conséquence, sans perte de généralité, nous utilisons des configurations de réseaux réduits pour valider notre approche. Nous avons ainsi sélectionné une famille de codes avec SF $= 4$ et $K = 5$. Ces conditions fournissent bien des codes non orthogonaux puisque le nombre de codes est supérieur à la dimension des codes. Les codes unipolaires utilisés sont : $c_1 = [0, 1, 0, 1]$, $c_2 = [1, 0, 0, 1]$, $c_3 = [0, 1, 1, 0]$, $c_4 = [1, 1, 1, 0]$ et $c_5 = [0, 0, 1, 1]$. D'autre part, les codes bipolaires utilisés sont $c_1 = [-1, -1, 1, 1]$, $c_2 = [1, 1, 1, -1]$, $c_3 = [-1, -1, -1, -1]$, $c_4 = [1, -1, -1, 1]$ et $c_5 = [1, -1, 1, -1]$. Ces codes ont été sélectionnés car ils fournissent un nombre maximum d'utilisateurs, tout en gardant une signature unique pour chaque ensemble d'utilisateurs actifs. Avec cette contrainte, dans un canal sans bruit, la probabilité d'erreur de l'AUD est nulle.

Afin de calculer les signatures possibles, il faut sommer les codes de chaque utilisateur actif grâce à un additionneur quantique [9]. La particularité des codes bipolaires, qui contiennent des composantes négatives, nécessite un codage binaire en complément binaire à deux.

4.2 Résultats

Dans cet article, un succès est obtenu quand l'ensemble exact des utilisateurs actifs est récupéré. Ainsi, une fausse alarme, ou une mauvaise détection au sein de l'ensemble entraîne une erreur sur l'ensemble entier.

La figure 3 présente l'évolution de la *Probabilité de succès (Ps)*, en fonction du SNR, pour les récepteurs classiques de référence (ML, CCR) et notre algorithme quantique, lorsque le système utilise des codes unipolaires, ainsi que des codes bipolaires. Notons ici que Ps est moyennée sur 4000 réalisations indépendantes de bruit.

Tout d'abord, nous pouvons vérifier que les performances s'améliorent lorsque le SNR augmente, quel que soient le ré-

cépteur et la famille de codes utilisées. Néanmoins, on peut observer que l'amélioration des performances est plus franche pour l'algorithme quantique que pour les algorithmes classiques. Ceci est dû au processus de recherche utilisé dans notre algorithme quantique, où l'oracle cherche les états vérifiant exactement $f(x) = \delta$. Or, en cas de bruit important, la signature est modifiée et n'est plus valide. Dans ce cas, l'oracle échoue à trouver une solution pour $f(x) = \delta$. L'algorithme de Grover conduit donc à la sélection aléatoire et équiprobable des utilisateurs actifs parmi l'ensemble des 2^K solutions possibles. Ce qui amène à une probabilité de succès faible. A l'inverse, pour de faibles bruits, l'algorithme de pré-traitement permet généralement de retrouver la séquence émise, en annulant la contribution de bruit. L'augmentation du SNR permet de se retrouver beaucoup plus fréquemment dans cette deuxième situation, et donc d'améliorer significativement les performances.

De plus, en comparant les performances des codes unipolaires et bipolaires, nous pouvons remarquer que la précision de détection des algorithmes classiques est meilleure lors de l'utilisation des codes bipolaires. Ceci vient du fait que la distance euclidienne est plus élevée entre les composantes des codes bipolaires, rendant la détection de signature plus fiable pour un même niveau de bruit. Cependant, l'écart de performances est fortement réduit en utilisant l'algorithme quantique. En effet, comme expliqué précédemment, le détecteur est perturbé lorsqu'il reçoit une séquence non valide. Cependant, la probabilité d'erreur est la même quel que soit l'écart entre la séquence reçue et la séquence émise. L'avantage concernant la distance euclidienne pour les codes bipolaires avec les récepteurs classiques ne s'applique donc plus dans ce cas.

D'autre part, en comparant les performances des différents récepteurs, on peut observer que notre algorithme quantique est moins performant que le CCR à bas SNR. A l'inverse, pour de forts SNR, il le surpasse largement et converge rapidement vers le ML optimal, pour les 2 familles de codes ; tandis que le CCR plafonne à cause de l'interférence. En effet, comme les codes ne sont pas orthogonaux, le CCR fait des erreurs à cause de l'interférence résiduelle sur la variable décisionnelle de chaque utilisateur. A l'inverse, le ML, que ce soit en version classique ou quantique, parvient à s'en affranchir en considérant l'ensemble des utilisateurs dans leur globalité.

Enfin, notre algorithme quantique se caractérise par une plus faible complexité, puisqu'il nécessite $\mathcal{O}(\sqrt{2^K})$ itérations, là où le ML classique en nécessite $\mathcal{O}(2^K)$, (mais le CCR $\mathcal{O}K$). Cette étude prouve donc que ce ML quantique permet de réduire significativement la complexité par rapport au ML classique, tout en conservant les mêmes performances de détection si le SNR est suffisant. Nous devrions pouvoir améliorer les performances, en améliorant l'oracle, et recherchant les états qui minimisent l'écart , i.e. vérifiant $min||f(x) - \delta||$ (au lieu de $f(x) = \delta$ actuellement).

5 Conclusion

Dans cet article, nous avons proposé l'adaptation de l'algorithme quantique de Grover pour la détection des utilisateurs actifs dans un réseau CD NOMA. Nous proposons une méthode de prétraitement du signal reçu, avant d'utiliser l'algorithme de Grover personnalisé pour l'AUD. Nous avons comparé notre algorithme de Grover aux récepteurs classiques ML et CCR pour des codes CD NOMA unipolaires et bipolaires, pour démontrer l'intérêt de ce concept. Nous avons montré que cette approche quantique permet, dans le régime à fort SNR, d'atteindre les mêmes performances que le récepteur optimal ML, tout en réduisant le nombre d'itérations. Cela ouvre la porte à de belles perspectives pour le quantique dans la résolution plus efficace de problèmes de détection d'utilisateurs actifs, mais de façon plus générale, de traitement de signal dans les réseaux de communication massifs.

Références

[1] Ericsson, Mobile cellular subscriptions, 2019. [Online].Available : https ://www.ericsson.com/en/press-releases/ 7/2019/ericsson-mobility-report-5g-uptake-even-faster- than-expected (visited on 04/30/2021)

[2] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5g networks for the in ternet of things : Communication technologies and chal- lenges," IEEE access, vol. 6, pp. 3619–3647, 2017

[3] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (noma) for cellular future radio access," in 2013 IEEE 77th Vehicular Technology Conference (VTC Spring), 2013, pp. 1–5

[4] H. Nikopour and H. Baligh, "Sparse code multiple access," 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2013, pp. 332-336

[5] D. Duchemin, L. Chetot, J. Gorce, and C. Goursaud, "Coded random access for massive MTC under statistical channel knowledge," in 2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2019, pp. 1–5

[6] E. V. Rogozhnikov, K. V. Savenko, A. K. Movchan and E. M. Dmitriyev, "The Study of Correlation Receivers," 2019 20th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM), 2019, pp. 155-159

[7] P. Botsinis, S. X. Ng and L. Hanzo, "Quantum Search Algorithms, Quantum Wireless, and a Low-Complexity Maximum Likelihood Iterative Quantum Multi-User Detector Design," in IEEE Access, vol. 1, pp. 94-122, 2013

[8] M. Vogel, Review of Quantum Computation and Quantum Information, by M.A. Nielsen and I.L. Chuang, 6.2011, vol. 52, pp. 604–605

[9] Y. Kang and J. Heo, "Quantum Minimum Searching Algorithm and Circuit Implementation," 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 214-219.