Sur le codage quantique sans perte avec pénalisation exponentielle

Steeve ZOZOR[1], Gustavo M. BOSYK[2], Guido BELLOMO[2] et Federico HOLIK[2]

[1]GIPSA-Lab, 11 rue des Mathématiques, 38402 Saint Martin d'Hères, France

[2]Instituto de Física La Plata, UNLP, CONICET, Facultad de Ciencias Exactas, 1900 La Plata, Argentina

steeve.zozor@gipsa-lab.grenoble-inp.fr, (gbosyk,gbellomo,holik)@fisica.unlp.edu.ar

Résumé – Dans cet article nous étudions le problème du codage source quantique sans perte. Nous nous appuyons pour cela sur un schéma d'encodage satisfaisant à une version quantique de l'inégalité de Kraft-McMillan. Tandis que dans le cadre standard l'objectif est de minimiser la moyenne arithmétique des longueurs des mots code quantiques, nous nous intéressons à la minimisation d'une moyenne exponentielle afin de pénaliser les mots code de grande longueur. Nous montrons que, à l'image du cas classique, la longueur moyenne exponentielle du code optimum est liée à la version quantique de l'entropie de Rényi de la source, le cas von Neumann (équivalent quantique de Shannon) étant le cas particulier correspondant à la pénalisation linéaire. La longueur moyenne usuelle est, elle, reliée à la fois à l'entropie de Rényi et de von Neumann.

Abstract – In this paper, we study the lossless quantum data coding problem. To this end, we appeal to an encoding scheme that satisfies a quantum version of the Kraft-McMillan inequality. Whereas in the standard situation the goal is to minimize the arithmetic average length of the quantum codewords, we are interested in the minimization of an exponential type average, in order to penalize the large codeword lengths. We show that, similarly to the classical context, the exponential average length of the optimal code is related to the quantum Rényi entropy of the source, the von Neumann case (quantum equivalent of Shannon) being the particular case corresponding to the linear penalization. The usual average length is then linked to both the Rényi and the von Neumann entropies.

1 Introduction

Une préoccupation importante du traitement de l'information classique ou quantique est celui du codage d'une source en utilisant le moins de ressources possibles. Les fondations du codage source classique remontent aux travaux célèbres de Shannon [1]. Étant donnée une source $S = \{p_n, s_n\}_{i=1}^N$ de symboles s_n de probabilités d'occurrence p_n, le problème consiste à affecter à chaque s_n un mot code $c(s_n)$, séquence de ℓ_n lettres d'un alphabet $A = \{0, \ldots, k-1\}$. Les ℓ_n étant non nécessairement égaux, on parle de code de longueur variable. En général, on s'intéresse aux codes uniquement décodables (à une séquence de lettres de A ne peut correspondre qu'une seule séquence de symboles), qui soit de longueur moyenne $L = \sum_n p_n \ell_n$ minimale. La contrainte d'unique décodabilité impose aux longueurs de satisfaire à la célèbre inégalité de Kraft-McMillan [2] : $\sum_n k^{-\ell_n} \le 1$. Un résultat remarquable est que la longueur moyenne minimale d'un tel code est liée à l'entropie de Shannon de la source $H(p) = -\sum_n p_n \log_k p_n$. (théorème du codage source [2]).

Le codage optimum dû à Huffman [3], assigne des mots code courts aux symboles à forte probabilité d'occurrence, et longs aux symboles rares. Ce codage peut poser soucis si l'on dispose par exemple d'une mémoire ne permettant pas de stocker des mots code trop longs [4]. Nous nous penchons ici sur l'approche de Campbell, basée sur une pénalisation non linéaire des longueurs des mots code en considérant la longueur moyenne t-exponentielle $L_t = \frac{1}{t} \log_k \sum_n p_n k^{t\ell_n}$, le cas usuel étant retrouvé quand $t \to 0$ [5]. À l'image du théorème de codage source, la longueur t-exponentielle minimale est liée à l'entropie de Rényi $H_\alpha(p) = \frac{1}{1-\alpha} \log_k \sum_n p_n^\alpha$ de la source [6], d'index $\alpha = \frac{1}{1+t}$.

La transposition du codage source du monde classique au cadre quantique n'est pas immédiate. Dans le monde quantique, un symbole est un élément d'un espace de Hilbert et à un système donné peut correspondre une infinité de sources. Ce qui est codé est une "source virtuelle", formée de symboles mutuellement orthogonaux, conduisant au même système que la "source réelle". Schumacher et Westmoreland ont été parmi les premiers à proposer une approche générale du problème de codage quantique [7]. Ils ont en particulier obtenu une version quantique de l'inégalité de Kraft-McMillan et montré que dans le codage quantique, l'entropie de von Neumann de la source joue un rôle analogue à celle de Shannon du cadre classique. Cependant, l'approche proposée souffre de la même limitation que le codage de Huffman classique en terme de longueurs des mots code. Ce problème est particulièrement sensible dans le cadre quantique, la manipulation de longues chaînes de qubits étant difficile [8]. Pour y remédier, nous proposons une alternative basée sur la stratégie de Campbell.

2 Codage quantique

2.1 Formalisme quantique en bref

Un système quantique de dimension finie à l'état pur est décrit par un vecteur unitaire $|s\rangle$ d'un espace de Hilbert $\mathcal{H}_\mathcal{S} \equiv \mathbb{C}^d$ de dimension d. Schématiquement, on peut voir $|s\rangle$ comme le moment magnétique d'une particule par exemple (même si ce dernier est plutôt une observable), ou encore comme un signal d'énergie unité. Outre l'état d'un système, on peut s'intéresser à une caractéristique, ou observable, décrite par un opérateur hermitien $A = \sum_{i=1}^{d} a_i \left|a_i\right\rangle\!\left\langle a_i\right| : \mathcal{H}_\mathcal{S} \mapsto \mathcal{H}_\mathcal{S}$. Ses vecteurs propres $|a_i\rangle$ forment une base orthonormée de $\mathcal{H}_\mathcal{S}$, base de représentation si l'on parle d'un signal, et $\langle a_i|$ est l'adjoint de $|a_i\rangle$. Ses valeurs propres a_i sont les valeurs que l'observable peut prendre. Le produit hermitien $\langle a_i|s\rangle$ est donc la composante de $|s\rangle$ sur l'élément de base $|a_i\rangle$. Son module carré, réécrit à l'aide de la trace, $p_i^A = |\langle a_i|s\rangle|^2 = \mathrm{Tr}\left(\left|a_i\right\rangle\!\left\langle a_i\right| \rho\right)$ avec $\rho = |s\rangle\!\langle s|$, représente la probabilité que l'observable prenne la valeur a_i. Un système peut toutefois être dans un état dit mélangé, par exemple composé de moments magnétiques avec différentes orientations, ou classe de signaux avec accès aléatoire, $\mathcal{S} = \{p_n, |s_n\rangle\}_{n=1}^{N}$ avec p_n “proportion” d'éléments $|s_n\rangle$ ou probabilité de tirer le signal $|s_n\rangle$. La probabilité que l'observable prenne la valeur a_i s'écrit donc $p_i^A = \sum_n p_n |\left\langle a_i|s_n\right\rangle|^2 = \mathrm{Tr}\left(\left|a_i\right\rangle\!\left\langle a_i\right| \rho\right)$ avec $\rho = \sum_n p_n \left|s_n\right\rangle\!\left\langle s_n\right|$. Clairement, ρ, hermitien et de trace unité, appelé opérateur densité, caractérise le système quantique $\mathcal{S}$, et lui seul. Sauf dans le cas pur, une infinité de sources peuvent conduire au même ρ, seule “information” disponible sur $\mathcal{S}$. Enfin, la valeur moyenne de l'observable A, s'écrit $\langle A\rangle_\rho = \sum_i a_i p_i^A = \mathrm{Tr}(\rho A)$.

2.2 Codage quantique uniquement décodable

L'objectif du codage quantique est d'encoder une source quantique $\mathcal{S}$ grâce à des mots code formés par des “séquences” d'éléments d'un alphabet quantique $\mathcal{A} = \{|0\rangle, \ldots, |k-1\rangle\} \subset \mathcal{H}_\mathcal{A} \equiv \mathbb{C}^k$, $k \geq 2$, où les $|i\rangle$ forment une base orthonormée de l'espace de Hilbert $\mathcal{H}_\mathcal{A}$ et où la “séquence” formée de $|i\rangle$ et $|j\rangle$ est le produit de Kronecker $|i\rangle \otimes |j\rangle \in \mathcal{H}_\mathcal{A}^{\otimes 2}$, noté $|ij\rangle$. Dans le cas quantique, ces mots code sont donc éléments d'espaces de Hilbert de dimensions différentes. Il en est de même pour deux séquences de longueurs différentes à encoder. Afin de travailler dans un unique espace source et un unique espace code, nous adoptons le formalisme de [9] en considérant les espaces de Fock $\mathcal{F}_\mathcal{S}$ de la source et $\mathcal{F}_\mathcal{A}$ de l'alphabet, avec $\mathcal{F} = \oplus_{\ell=0}^{+\infty} \mathcal{H}^{\otimes \ell}$ somme directe d'espaces de Hilbert.

Définition 1. Un code source quantique uniquement décodable de la source $\mathcal{S} = \{p_n, |s_n\rangle\}_{n=1}^{N}$ sur un alphabet $\mathcal{A} = \{|0\rangle, \ldots, |k-1\rangle\}$, est une isométrie linéaire $U : \mathcal{F}_\mathcal{S} \to \mathcal{F}_\mathcal{A}$. Le codage de chaque élément de $\mathcal{S}$ étant $U|s_n\rangle$, l'opérateur densité de la source codée s'écrit $C(\rho) = U\rho U^\dagger$ avec $U^\dagger$ opérateur adjoint de U.

U étant une isométrie, elle est injective et $U^\dagger U = I$ identité. Si $|\omega_M\rangle \in \mathcal{F}_\mathcal{A}$ est le codage d'une séquence $\otimes_{m=1}^{M} |s_{i_m}\rangle \in \mathcal{F}_\mathcal{S}$, cette séquence s'obtient sans ambiguïté par $U^\dagger |\omega_M\rangle$.

Par la suite nous suivons le schéma de codage proposé dans [9], s'appuyant sur le principe de codage uniquement décodable classique d'une source $S = \{1, \ldots, d\}$ sur un alphabet $A = \{0, \ldots, k-1\}$. En notant $F_A = \bigcup_{\ell=0}^{\infty} A^\ell$, un code classique $c : S \to F_A$ est uniquement décodable si et seulement si toute concaténation $c^M(i_1, \ldots, i_M) = c(i_1) \cdots c(i_M)$ de M mots code est une fonction injective [2]. Nous considérons ainsi les isométries U de la forme [9],

$$U = \sum_{i=1}^{d} \left|c(i)\right\rangle\!\left\langle e_i\right|, \qquad (1)$$

où $\{|e_i\rangle\}_{i=1}^{d}$ est une base orthonormée de $\mathcal{H}_\mathcal{S}$ et c un code classique uniquement décodable de S. $|c(i)\rangle \in \mathcal{H}_\mathcal{A}^{\otimes \ell_i} \subset \mathcal{F}_\mathcal{A}$ avec ℓ_i longueur du mot code classique $c(i)$ et les $\{|c(i)\rangle\}$ forment un ensemble orthonormé, de sorte que $U^\dagger U = I$.

Contrairement au cas classique, les $|c(i)\rangle$ n'encodent pas les mots $|s_n\rangle$ de la source (auxquels on n'a pas accès), mais la base $|e_i\rangle$. En particulier, $U|s_n\rangle$ n'appartient pas forcément à un sous espace de la forme $\mathcal{H}_\mathcal{A}^{\otimes \ell}$, de sorte que l'on ne parle plus de code de longueur variable, mais de code de longueur indéterminée.

On peut étendre l'encodage pour des séquences de M de mots source par $U^{\otimes M}$ et l'opérateur $U^\infty = \sum_{M=1}^{\infty} U^{\otimes M}$ répond ainsi à la définition 1 d'un codage sans perte. Par la suite, nous nous concentrons sur le schéma d'encodage (1).

2.3 Observable longueur et inégalité de Kraft-McMillan quantique

Dans le cas du codage classique, l'inégalité de Kraft-McMillan donne une condition nécessaire (et suffisante) d'existence d'un code source uniquement décodable [2]. Ce résultat a été étendu dans le cadre du codage quantique [7], repris ici avec le formalisme que nous avons adopté.

Dans un premier temps, il est nécessaire de définir une notion de longueur compatible avec le cadre quantique. Elle se définit naturellement comme étant une observable du système.

Définition 2. L'observable longueur Λ, opérateur agissant sur l'espace $\mathcal{F}_\mathcal{A}$, est définie par

$$\Lambda \equiv \sum_{\ell=0}^{\infty} \ell\, \Pi_\ell, \qquad (2)$$

où Π_ℓ est le projecteur orthogonal sur le sous espace $\mathcal{H}_\mathcal{A}^{\otimes \ell}$.

En d'autres termes, à tout état de $\mathcal{H}_\mathcal{A}^{\otimes \ell_i}$ (dont $|c(i)\rangle$) correspond l'occurrence longueur ℓ_i. On obtient alors la version quantique de l'inégalité de Kraft-McMillan suivante.

Théorème 1. Pour tout encodage quantique (1), l'inégalité

$$\mathrm{Tr}\left(U^\dagger k^{-\Lambda} U\right) \leq 1. \qquad (3)$$

est nécessairement satisfaite [1].

Démonstration. $\langle c(i)|\,\Pi_\ell\,|c(i')\rangle = \delta_{\ell,\ell_{i'}}\, \delta_{i,i'}$, avec ℓ_i longueur du mot code classique $c(i)$, et donc $U^\dagger k^{-\Lambda} U = \sum_{i=1}^{d} k^{-\ell_i} \left|e_i\right\rangle\!\left\langle e_i\right|$. Il en vient $\mathrm{Tr}\left(U^\dagger k^{-\Lambda} U\right) = \sum_{i=1}^{d} k^{-\ell_i}$. c étant un code classique uniquement décodable, le résultat est conséquence de l'inégalité de Kraft-McMillan classique. □

1. La fonction f d'un opérateur O s'écrit via la série entière de f, *i.e.*, par diagonalisation $O = \sum_i o_i \left|o_i\right\rangle\!\left\langle o_i\right|$, $f(O) = \sum_i f(o_i) \left|o_i\right\rangle\!\left\langle o_i\right|$.

3 Codage quantique à la Campbell

Nous ne reprenons pas ici la version quantique du codage de type Huffman, cas limite du codage à la Campbell.

3.1 Longueurs moyennes du code quantique

Afin de construire un code qui minimise les ressources nécessaires au codage, il faut définir ce que l'on entend par ressource. On peut considérer naturellement la valeur moyenne de l'observable Λ sur le système après codage.

Définition 3. Par définition, la longueur moyenne du système après codage, $C(\rho) = U\rho U^\dagger$, est

$$\ell(C(\rho)) = \mathrm{Tr}(C(\rho)\Lambda) \tag{4}$$

Schumacher et Westmoreland [7] ou Hayashi [9] ont étudié le codage (1) qui minimise la longueur moyenne (4). Toutefois, comme dans le cadre classique, ce code peut être gourmand en terme de taille de registre. Pour y remédier, nous nous intéressons ici à la minimisation d'une moyenne exponentielle, à l'image de celle de Campbell du cadre classique [5].

Définition 4. La longueur moyenne t-exponentielle de la source codée $C(\rho) = U\rho U^\dagger$ est définie par

$$\ell_t(C(\rho)) \;\equiv\; \frac{1}{t}\log_k \mathrm{Tr}\left(C(\rho)k^{t\Lambda}\right) \tag{5}$$

où $t \geq 0$ gère la pénalisation affectant les mots code longs.

$t \mapsto \ell_t(C(\rho))$ est continue et croissante pour $t \in [0\,;+\infty)$, de $\ell_0(C(\rho)) = \ell(C(\rho))$ longueur moyenne de la source codée, à $\ell_\infty(C(\rho)) = \max_i \ell_i$, longueur du mot code classique le plus long : minimiser ℓ_t aboutit à chercher un compromis entre longueur moyenne et longueur maximale.

Nous avons à présent tous les ingrédients pour étudier le problème de codage quantique sans perte optimum au sens de la longueur moyenne t-exponentielle minimale.

3.2 Code quantique optimum et longueur moyenne t-exponentielle minimale

Définition 5. Un codage quantique (1) de $\mathcal{S}$, est t-exponentiel optimum s'il minimise $\ell_t(C(\rho))$ sous contrainte de l'inégalité de Kraft-McMillan quantique,

$$U^{\mathrm{opt}} \equiv \underset{\mathrm{Tr}(U^\dagger k^{-\Lambda}U)\leq 1}{\mathrm{argmin}} \; \ell_t(C(\rho)) \tag{6}$$

Le problème du codage uniquement décodable d'une source classique $S = \{1, \ldots, d\}$ de probabilités ρ_i, minimisant la longueur de Campbell $L_t = \sum_i \rho_i k^{t\ell_i}$ a été solutionné dans [10], se réduisant au célèbre code de Huffman [3] pour $t \to 0$. Dans le cadre quantique, il est également possible de déterminer l'encodage quantique (1) t-exponentiel optimum.

Théorème 2. Le code quantique (1) t-exponentielle optimum pour $\mathcal{S} = \{p_n, |s_n\rangle\}_{n=1}^N$, d'opérateur densité $\rho = \sum_{n=1}^N p_n\,|s_n\rangle\langle s_n|$ écrit sous forme diagonale $\rho = \sum_{i=1}^d \rho_i\,|\rho_i\rangle\langle\rho_i|$ est donné par

$$U_t^{\mathrm{opt}} = \sum_{i=1}^d |c_t^{\mathrm{opt}}(i)\rangle\langle\rho_i|\,, \tag{7}$$

où $c_t^{\mathrm{opt}}(i)$ est le code classique uniquement décodable minimisant la longueur de Campbell L_t associée aux probabilités ρ_i. Par la suite on notera $C_t^{\mathrm{opt}}(\rho) = U_t^{\mathrm{opt}}\rho\, U_t^{\mathrm{opt}\dagger}$.

Démonstration. L'inégalité de Kraft-McMillan quantique étant indépendante de la base $\{|e_i\rangle\}$ du schéma (1), commençons par minimiser $\mathrm{Tr}(C(\rho)k^{t\Lambda}) = \sum_{i,j} k^{t\ell_i}\rho_j|\langle e_i|\rho_j\rangle|^2$ sur l'ensemble des bases de $\mathcal{H}_\mathcal{S}$ à c fixé. Soit la matrice doublement stochastique D de composantes $D_{i,j} \equiv |\langle e_i|\rho_j\rangle|^2$. On veut alors minimiser $\kappa_t D r^T$ sur l'ensemble des matrices doublement stochastiques, avec $\kappa_t = \left[k^{t\ell_1}\ldots k^{t\ell_d}\right]$ et $r = [\rho_1 \ldots \rho_d]$. D'après le théorème de Birkhoff [11], D est combinaison convexe des matrices P_q de permutation, $D = \sum_q \alpha_q P_q$. Soit $q' = \mathrm{argmin}_q\, \kappa_t P_q \rho^T$. Alors $\kappa_t D r^T \geq \kappa_t P_{q'} r^T$ avec égalité si $\alpha_q = \delta_{q,q'}$: le minimum est atteint pour $D = P_{q'}$. Ainsi, la base $\{|e_i\rangle\}$ coïncide avec la base $\{|\rho_j\rangle\}$ à une permutation près. Cette permutation peut être reportée dans les ℓ_i de sorte que l'on peut choisir $|e_i\rangle = |\rho_i\rangle$ et $U = \sum_i |c(i)\rangle\langle\rho_i|$. Le problème consiste alors à minimiser $\ell_t(C(\rho))$ sous contrainte d'inégalité de Kraft-McMillan quantique. Or $\ell_t(C(\rho)) = \frac{1}{t}\log_k\left(\sum_i \rho_i k^{t\ell_i}\right)$, longueur de Campbell L_t du code classique c pour les probabilités ρ_i, minimum pour $c_t^{\mathrm{opt}}(i)$, optimum de Campbell. $\square$

Clairement, U_t^{opt} ne code pas les états $|s_n\rangle$ de la source, auxquels on n'a pas accès, mais les états propres $|\rho_i\rangle$ de l'opérateur densité. Cela revient à coder la seule source (virtuelle) d'états orthonormés conduisant à l'opérateur densité ρ, ce qui différencie fondamentalement codage classique et codage quantique.

L'algorithme [10], comme celui de Huffman [3], ne fournit pas analytiquement les ℓ_i optimaux. On montre cependant que les réels ℓ_i minimisant L_t sous contrainte d'inégalité de Kraft-McMillan sont $\ell_i = -\log_k \rho_{t\,i}$ avec $\rho_{t\,i}$ “probabilités compagnes”, valeurs propres de “l'opérateur densité compagne”

$$\rho_t \equiv \frac{\rho^{\frac{1}{1+t}}}{\mathrm{Tr}\,\rho^{\frac{1}{1+t}}} \quad \text{et} \quad \rho_{t\,i} = \frac{\rho_i^{\frac{1}{1+t}}}{\sum_j \rho_j^{\frac{1}{1+t}}}, \tag{8}$$

(voir [12] pour ce qui est du cas classique). On pourrait choisir $\ell_i = \lceil -\log_k \rho_{t\,i}\rceil$, longueurs satisfaisant à l'inégalité de Kraft-McMillan, et construire le code correspondant, code dit de Shannon (ici pour les probabilités compagnes) [2]. Ce code n'est pas optimum en général, sauf si tous les $-\log_k \rho_{t\,i}$ sont entiers (voir par exemple [2] dans le cadre usuel $t = 0$; l'approche dans le cadre présent est scrupuleusement la même).

Toutefois, indépendamment de l'expression explicite des longueurs optimales, on peut borner la longueur minimale $\ell_t(C_t^{\mathrm{opt}}(\rho))$ comme pour le code de Huffmann classique ($t = 0$) [2] ou celui de Campbell $t \geq 0$ [5, 12].

Théorème 3. La moyenne t-exponentielle minimale vérifie

$$S_{\frac{1}{1+t}}(\rho) \;\leq\; \ell_t(C_t^{\mathrm{opt}}(\rho)) \;<\; S_{\frac{1}{1+t}}(\rho) + 1, \tag{9}$$

où $S_\alpha(\rho) = \frac{1}{1-\alpha} \log_k \operatorname{Tr} \rho^\alpha,\ \alpha \geq 0$, est l'entropie de Rényi quantique de l'opérateur densité ρ de la source avec, pour $\alpha \to 1$, $S_\alpha(\rho) \to S(\rho) = -\operatorname{Tr}(\rho \log_k \rho)$ entropie de von Neumann.

Démonstration. La preuve est similaire à celle du cadre classique et s'appuie sur l'opérateur densité σ,

$$\sigma \equiv \frac{U^\dagger k^{-\Lambda} U}{\beta} \qquad \text{avec} \qquad \beta \equiv \operatorname{Tr}\left(U^\dagger k^{-\Lambda} U\right) \tag{10}$$

Pour un code quelconque (1), $\rho U^\dagger k^{t\Lambda} U = \rho \left(U^\dagger k^{-\Lambda} U\right)^{-t} = \rho_t^{1+t} \sigma^{-t} \left[\operatorname{Tr}\left(\rho^{\frac{1}{1+t}}\right)\right]^{1+t} \beta^{-t}$, d'où $\ell_t(C(\rho)) = S_{\frac{1}{1+t}}(\rho) + S_{1+t}(\rho_t \| \sigma) - \log_k \beta$, avec $S_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1} \log_k \operatorname{Tr} \rho^\alpha \sigma^{1-\alpha}$ divergence quantique de Rényi [13]. Celle-ci étant positive, et l'inégalité de Kraft-McMillan impliquant $\log_k \beta \leq 0$, il vient $\ell_t(C(\rho)) \geq S_{\frac{1}{1+t}}(\rho)$ pour tout U, et donc pour U_t^{opt}.

Soit à présent le code de Shannon quantique $U = \sum_{i=1}^d |c(i)\rangle\langle\rho_i|$ de l'opérateur densité compagne ρ_t, de longueurs $\ell_i = \lceil -\log_k \rho_{t\,i} \rceil$ des $c(i)$. De $\lceil -\log_k \rho_{t\,i} \rceil < -\log_k \rho_{t\,i} + 1$ il vient, par définition de l'optimum $\ell_t(C_t^{\mathrm{opt}}(\rho)) \leq \ell_t(C(\rho)) = \frac{1}{t} \log_k \left(\sum_{i=1}^d \rho_i k^{t\lceil -\log_k \rho_{t\,i} \rceil}\right) < S_{\frac{1}{1+t}}(\rho) + 1$. □

Ce résultat est similaire à celui du codage classique, à la Huffman ou à la Campbell [2, 5, 12], où l'entropie quantique de Rényi remplace l'entropie classique. On montre de plus que pour tout opérateur densité $\rho = \sum_n p_n |s_n\rangle\langle s_n|$, on a $S_\alpha(\rho) \leq H_\alpha(p)$ avec H_α entropie classique de Rényi [14]. Le codage d'une source quantique s'avère plus "économique" que celui d'une source classique de symboles de probabilités $\{p_n\}$, exploitant implicitement le fait que les symboles quantiques $|s_n\rangle$ n'étant pas orthonormés partagent de "l'information".

Considérons à présent le code quantique de Shannon $U = \sum_{i=1}^d |c(i)\rangle\langle\rho_i|$ construit sur l'opérateur compagne ρ_t. Si tous les $-\log_k \rho_{t\,i}$ sont entiers, ce code coïncidant avec C_t^{opt}, la borne inférieure de (9) est atteinte. De plus, de $-\log_k \rho_{t\,i} = \frac{1}{1+t}(-\log_k \rho_i) + \frac{t}{1+t} S_{\frac{1}{1+t}}(\rho)$, on s'aperçoit que la longueur moyenne usuelle du code de Shannon quantique de l'opérateur densité compagne ρ_t est bornée de la manière suivante :

$$0 \leq \ell(C(\rho)) - \left[\frac{1}{1+t} S(\rho) + \frac{t}{1+t} S_{\frac{1}{1+t}}(\rho)\right] < 1 \tag{11}$$

où la borne inférieure est atteinte pour le code optimum C_t^{opt} lorsque tous les $-\log_k \rho_{t\,i}$ sont entiers. Le compromis longueur moyenne et maximale réalisé par la pénalisation t-exponentielle est illustré par la longueur moyenne usuelle du code quantique, au travers de la combinaison convexe de l'entropie de von Neuman –longueur moyenne minimale–, et de l'entropie quantique de Rényi –moyenne t-exponentielle minimale–.

4 Discussions

Dans cet article nous nous sommes intéressés au codage source quantique sans perte Si l'approche suit le canevas général du codage source classique, le cadre quantique montre quelques subtilités. En particulier, nous n'avons pas accès aux symboles, mais à l'état global du système, de sorte que c'est une source équivalente particulière qui est codée. Nous nous sommes également placés dans le cadre de la prise en compte de ressources quantiques limitées, le problème de traiter des chaînes de qubits en pratique étant plus difficile que celui de chaînes de bits. Cette étude révèle qu'aux entropies classiques caractérisant les longueurs moyennes des codes, se substituent leur contrepartie quantique et non les entropies classiques des probabilités associées aux symboles quantiques.

À l'image des travaux de [10], nous étudions à présent la notion de probabilité de dépassement de mémoire dans le cadre quantique, et le choix de t garantissant qu'elle n'est pas trop forte. Nous étudions également des pénalisations générales, de type $\phi^{-1}\left(\operatorname{Tr}\left(\rho\, \phi(\Lambda)\right)\right)$ avec ϕ croissante (et convexe), offrant une plus large gamme de pénalisations des longs mots code.

Références

[1] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. Journal*, 27(4) :379, 1948.

[2] T. M. Cover and J. A. Thomas. *Elements of information theory*. John Wiley & Sons, 2006.

[3] D. A. Huffman. A method for the construction of minimum-redundancy codes. *Proc. of the IRE*, 40(9) :1098, 1952.

[4] F. Jelinek. Buffer overflow in variable length coding of fixed rate sources. *IEEE Transactions on Information Theory*, 14(3) :490–501, May 1968.

[5] L. L. Campbell. A coding theorem and Rényi's entropy. *Information and Control*, 8(4) :423, 1965.

[6] A. Rényi. On measures of entropy and information. In *Proc. of the 4th Berkeley symposium on mathematical statistics and probability*, volume 1, page 547, 1961.

[7] B. Schumacher and M. D. Westmoreland. Indeterminate-length quantum coding. *Phys. Rev. A*, 64(4) :042304, 2001.

[8] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe. Experimental comparison of two quantum computing architectures. *PNAS*, 114(13) :3305–3310, March 2017.

[9] M. Hayashi. *A Group Theoretic Approach to Quantum Information*. Springer, Berlin, 2017.

[10] P. A. Humblet. Generalization of the Huffman coding to minimize the probability of buffer overflow. *IEEE Trans. on Information Theory*, 27(2) :230, 1981.

[11] R. Bhatia. *Matrix Analysis*. Springer, 1997.

[12] J.-F. Bercher. Source coding with escort distributions and Rényi entropy bounds. *Phys. Let. A*, 373(36) :3235, 2009.

[13] D. Petz. Quasi-entropies for finite quantum systems. *Reports on Mathematical Physics*, 23(1) :57–65, 1986.

[14] G. M. Bosyk, S. Zozor, F. Holik, M. Portesi, and P. W. Lamberti. A family of generalized quantum entropies : definition and properties. *Quantum Information Processing*, 15(8) :3393, 2016.