STABILISATEUR QUANTIQUE

PHILIPPE LANGEVIN

Résumé. Dans cette note, je décris la notion de code quantique. La littérature francophone sur le sujet est assez étroite. Je me suis initié à la question au travers d'un exposé de Gilles Zémor, les slides de Jean-Pierre Tillich, le mémoire de master de Anne Marin, quelques blogs sur internet. Le cours de Joseph Gruska m'a permis de mieux comprendre certains aspec purement physique. Au final, c'est principalement une partie de la thèse de Daniel Gottesman et une partie du chapitre VII du cours de John Preskill qui sont rapportés dans cette note quelque peu dépouillée de la plupart des aspects physiques.

Quantum Error Correction Sonnet

By Daniel Gottesman

We cannot clone, perforce ; instead, we split
Coherence to protect it from that wrong
That would destroy our valued quantum bit
And make our computation take too long.

Correct a flip and phase - that will suffice.
If in our code another error's bred,
We simply measure it, then God plays dice,
Collapsing it to X or Y or Zed.

We start with noisy seven, nine, or five
And end with perfect one. To better spot
Those flaws we must avoid, we first must strive
To find which ones commute and which do not.

With group and eigenstate, we've learned to fix
Your quantum errors with our quantum tricks.

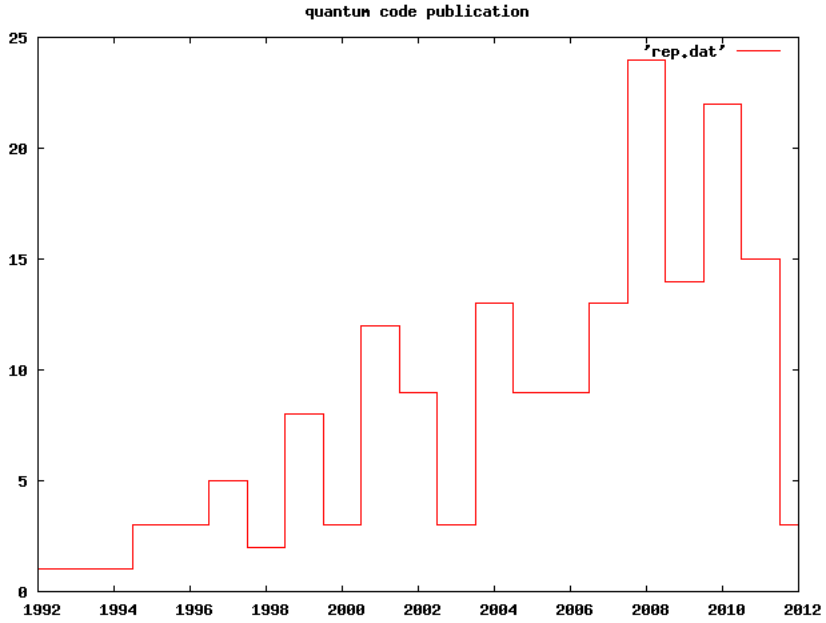
1. Introduction

Il s'agit d'un rapport sur les codes stabilisateurs de Daniel Gottesman que j'ai rédigé pour le Groupe de Travail en Physique Mathématique de Toulon organisé par Walter. Il y a peu, j'ai appris que les codes quantiques sont nécessaires à la conception des machines quantiques. La plupart des codes quantiques dérivent des codes classiques et il peuvent être décrits à partir de sous-espaces de l'espace de Hamming. Depuis l'introduction de cette notion plusieurs centaines d'articles ont été publiés. Cette note termine par la liste des 168 articles référencés dans mathscinet comportant les mots "quantum" et "code", ils sont publiés principalement dans les revues :

IEEE Trans. Inform. Theory (48), Phys. Rev. A (21), Quantum Inf. Comput. (9) et Quantum Inf. Process (7)... L'objectif de cette note est de donner un double aperçu classique et quantique de la théorie des codes. L'essentiel étant d'exposer la construction des codes stabilisateurs proprosée (1997 !) par Daniel Gottesman dans sa thèse.

On peut raisonnablement penser qu'un grand nombre de questions et problèmes ouverts de la théorie des codes correcteurs se traduisent dans le langage des codes quantiques. Pour cette raison, j'ai introduit des notions de codage pour faire un micro panorama du domaine a des fins exploratoires.

Date: Printemps 2012.



Pour terminer cette introduction, je signale que les compléments physiques pourront être trouvés sur web anglophone qui contient pas mal d'information, par exemple :http ://www.quantiki.org.

2. Notations

Les états d'un système quantique sont des vecteurs de norme 1 dans un espace de Hilbert. Les états d'un atome d'hydrogène sont modéliser par les vecteurs de norme 1 de l'espace $\mathcal{H} := \mathbb{C} \times \mathbb{C}$ muni du produit scalaire usuel, les vecteurs de la base canonique sont notés $|0\rangle$ et $|1\rangle$. L'espace $\mathcal{H}$ est un bit quantique (qubit), il peut prendre une infinité de valeurs :

$$\alpha|0\rangle + \beta|1\rangle, \quad |\alpha| + |\beta| = 1, \quad \text{où} \quad |0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1}$$

En physique, la composition des états systèmes quantiques s'obtient par tensorisation. Ainsi, le produit tensoriel itéré $(n-1)$ fois, $\mathcal{H}^{\otimes n} := \mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}$, est l'espace des états d'un registre composé de n qubits. Les états possibles sont représentés par des éléments de norme 1 dans $\mathcal{H}^{\otimes n}$ quand il muni du produit scalaire :

$$\langle x_1 \otimes x_2 \otimes \cdots \otimes x_n \mid y_1 \otimes y_2 \otimes \cdots \otimes y_n \rangle = \prod_{i=1}^{n} \langle x_i \mid y_i \rangle.$$

Il s'agit d'un espace de dimension 2^n une des bases orhogonales s'identifie aux mots de l'espace de Hamming binaire. Pour un mot binaire, $c \in \mathbb{F}_2^n$, on utilise la notation condensée $|c\rangle$ pour désigner le produit $|c_1\rangle \otimes |c_2\rangle \otimes \cdots \otimes |c_n\rangle$. Curieusement c'est dans cette association $c \mapsto |c\rangle$ que les propriétés de correction quantique doivent se déduire de propriétés métriques des espaces de Hamming.

Remarque 1. *Nous discutons principalement de code quantique binaire mais à la fin de cette note il sera question de codes quantique q-aire qui vivent dans des espaces de dimension q^n.*

3. Espace de Hamming

On note K un corps à q éléments.

Remarque 2. *Il est peut-être utile de rapeller que tous les corps finis sont commutatifs ! L'ordre q d'un corps fini K est une puissance d'un premier p qui est la caractéristique de K qui contient un corps isomorphe à $\mathbb{F}_p := \mathbb{Z}/(p)$. Ainsi K est un espace vectoriel sur $\mathbb{F}_p$, si f désigne la dimension alors $q = p^f$, et le corps K est obtenu en adjoignant à $\mathbb{F}_p$ une racine d'un polynôme irréductible de degré f.*

Tous les corps finis d'ordre q sont isomorphes. plus précisément, il existe un seul corps fini d'ordre q dans une clotûre algébrique de $\mathbb{F}_p$, "il" est souvent noté $\mathbb{F}_q$.

Exercice 1. *Décrire le corps $\mathbb{F}_4$ à partir d'une racine ω du polynome $X^2 + X + 1$.*

L'espace K^n est muni de la métrique de Hamming

$$(x, y) \mapsto \mathrm{d_H}(x, y) = \mathrm{wt}\,(y - x).$$

où $\mathrm{wt}\,(z)$ désigne le *poids de Hamming* du mots z i.e. le nombre de composantes non nulle de z. Par définition, un (n, M, d) code correcteur est une partie de cardinal M dans K^n dans laquelle les mots sont distants d'au moins d. On peut utiliser ces codes pour transmettre de l'information sur un canal q-aire bruité. Trés brièvement, l'information est vue comme une suite de messages i.e. un texte sur un alphabet de taille M. Un *encodage* réalise une injection de l'alphabet vers le code correcteur, les symboles codés sont transmis sur le canal bruité, le récepteur décode les mots de K^n qui sont reçus en déterminant un mot de code le plus proche :*décodage*. La capacité de correction de ce dispositif vaut $t = \frac{d-1}{2}$, car un symbole transmis entaché d'au plus t erreurs sera correctement décodé.

Si p désigne la probalité d'erreur sur un symbole transmis, la probabilité d'erreur aprés décodage vérifie :

$$P_{\mathrm{err}} \leq \sum_{w=t+1}^{n} \binom{n}{w} (q-1)^w p^w (1-p)^{n-w} \tag{2}$$

Normalement, il faudrait citer le théorème de Shannon.

Des points de vues pratique et théorique, il est important de donner des classes de codes effectivement constructibles permettant d'obtenir des suites de codes (N_i, M_i, d_i) avec des paramétres strictement croissants et tels que

$$\lim_{i \mapsto \infty} \left(\frac{d_i}{N_i}, \frac{\log_q(M_i)}{N_i}\right) \neq (1, 0) \quad \text{ou} \quad (0, 1),$$

on parle de *classe de bons codes*. Du point ve vue pratique, il est important de connaitre les codes optimaux c'est à dire qui réalise les meilleurs paramètres quand la dimension ou la distance minimale est fixée, on parle de *codes optimaux*.

4. Code linéaire

En pratique, il est difficile de décrire des codes de grandes taille sans utiliser un minimum d'algèbre pour réaliser les opérations d'encodage et de décodage. On se place dans le cadre des espaces vectoriels sur un corps fini. On dit que $C \subseteq K^n$, est un $[n,k,d]_q$-code si c'est un sous-espace vectoriel de dimension k dont la distance minimale est plus grande que d.

Dans le langage des codes, les éléments de K^n sont des *mots*, et ils sont notés par des vecteur lignes. Une matrice $k \times n$ dont les lignes forment une base du code est dite *génératrice*.

On vérifie que le groupe des matrices monomiales correspond au groupe des isométries de K^n. On dit que deux codes sont équivalents s'il existe une isométrie de K^n qui envoie l'un sur l'autre. Notons au passage qu'un théorème de V. Pless affirme qu'une isométrie d'un sous-espace sur un sous-espace se prolonge en une isométrie de K^n, conséquence de la théorie des caractères.

A une permutation de colonnes prés, la matrice génératrice d'une $[n,k]$-code peut prendre une forme normalisée :

$$G = [I_k : A]$$

où A est une matrice $k \times (n-k)$. Les k sont les symboles d'information, les $r := n-k$ derniers sont des symboles de parités ou redondances.

L'espace de Hamming est muni du produit scalaire usuel, si G désigne une matrice génératrice de C et H une matrice génératrice de $C^\perp$ alors $GH^t = 0$. Dans le cas normal,

$$G = [I_k : A], \quad H = [-A^t : I_r]$$

Les mots du code sont caractérisés par H, on parle de *matrice de contrôle* :

$$\forall y \in K^n, \quad y \in C \iff Hy^t = 0.$$

D'une manière générale $\mathrm{syn}\,(y) = Hy^t$ est le syndrome de y i.e. l'ensemble des symptomes caractéristiques de la présence d'un mot code !

Un code de matrice de contrôle H est t correcteur si et seulement si l'application $y \mapsto \mathrm{syn}\,(y)$ est une inejection de la boule de rayon t dans l'espace K^{n-k}.

On peut caractériser géométriquement, un code de distance minimale d et de redondance r comme un ensemble de vecteur de K^r ne contenant pas de système lié de cardinal stricement inférieur à d. Typiquement, l'espace projectif $\mathbb{P}^r(K)$ définit un code de longueur $n = \frac{q^{r+1}-1}{q-1}$, de dimension $r+1$ et de distance minimale 3. C'est la famille des 1-correcteurs de Hamming.

Exercice 2. *Les points de droite projective $\mathbb{P}^1(\mathbb{F}_4)$ mis en colonne forment une matrice de contrôle*

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \omega^2 \end{pmatrix}$$

d'un $[5,3,3]_4$ code correcteur parfait.

5. Enumérateur de poids

L'énumérateur des poids de C est :

$$W_C(X,Y) = \sum_{c\in C} X^{n-\mathrm{wt}\,(c)} Y^{\mathrm{wt}\,(c)} \in \mathbb{Z}[X,Y] \tag{3}$$

Un premier fait remarquable de la théorie des codes relie la distribution des distances d'un code avec celle de son dual

$$W_{C^\perp}(X,Y) = \frac{1}{q^k} W_C(X+(q-1)Y, X-Y) \tag{4}$$

cette relation de MacWilliams est bien sûr une formule de Poisson.

6. Deux bornes classiques

Traditionnelement, on note $A(n,d)$ le cardinal du plus grand code q-aire de longueur n et de distance minimale au moins d. On dispose immédiatement d'une borne supérieure (Singleton) :

$$d \leq n - \log_q A(n,d) + 1 \tag{5}$$

Quand il y a égalité, le code est dit MDS.

Par ailleurs, pour des raisons d'empilements, il est facile de voir que l'existence d'un $[n,k,d]$-code linéaire maximal donne une borne inférieure (Varshamov-Gilbert) :

$$V_q(n,d-1)q^k \geq q^n$$

où $V_q(n,r)$ désigne le cardinal d'une boule de rayon r dans l'espace de Hamming

$$V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

On introduit la *fonction d'entropie* de Shanon H_q

$$H_q(t) = t\log_q(q-1) - t\log_q(t) - (1-t)\log_q(1-t)$$

Il est facile de vérifier que pour $0 < t \leq \frac{q-1}{q}$:

$$\lim_{n\mapsto\infty} \frac{1}{n} t \log_q V_q(n,nt) = H_q(t)$$

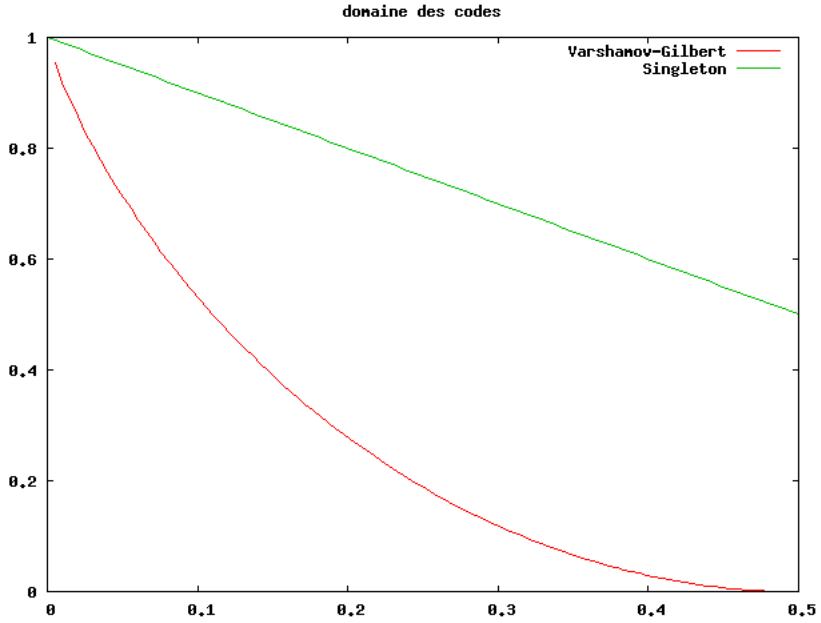
Pour mesurer l'efficacité des constructions, on introduit les asymptotiques :

$$\alpha(\delta) = \lim_{n\mapsto\infty} \frac{1}{n} \log_q A(n,\delta n)$$

Les bornes ci-dessus deviennent :

$$1 - H_q(\delta) \leq \alpha(\delta) \leq 1 - \delta$$

On peut écrire de nombreuses majorations : Hamming, Plotkin, Elias etc... Mais les faits marquants sont d'une part la conjecture MDS et les constructions issues de la géométrie algébrique qui dépassent VGB.



7. Codes MDS

Dans le cas linéaire, (5) devient :

$$d \leq n - k + 1 \tag{6}$$

Les codes satisfaisant l'égalité sont dit à distance de séparation maximale (MDS). Les codes MDS triviaux correspondent aux paramètres $k \leq 1$ ou $k \geq n - 1$.

Exercice 3. *Montrer que le dual d'un code linéaire MDS est un code MDS.*

Plus précisément, on peut utiliser les relations de MacWilliams pour déterminer complétement la distribution de poids d'un code MDS. Le nombre de mots de poids w d'un $[n, k]_q$-code MDS est :

$$A_w = \binom{n}{w}(q-1)\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j} \tag{7}$$

En particulier

$$A_d = \binom{n}{k-1}(q-1), \quad A_{d+1} = \binom{n}{k-2}(q-1)(q-n+k-1)$$

L'intérêt de la théorie des corps finis dans le contexte des codes est illustré par ce qui suit. Considérons $a_1, a_2, \ldots, a_q$ les éléments des corps à q éléments.

Pour tout entier $0 < k < q$, les vecteurs lignes de la matrice

$$G = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 0 \\ a_1 & a_2 & a_3 & \ldots & a_q & 0 \\ a_1^2 & a_2^2 & a_3^2 & \ldots & a_q^2 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1^{k-1} & a_2^{k-1} & a_3^{k-1} & \ldots & a_q^{k-1} & 1 \end{pmatrix}$$

engendrent un code MDS.

Si la caractéristique du corps est paire alors on peut faire un code MDS plus long en dimension 3 :

$$G = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 0 & 0 \\ a_1 & a_2 & a_3 & \dots & a_q & 0 & 1 \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_q^2 & 1 & 0 \end{pmatrix}$$

La conjecture MDS affirme qu'un $[n, k, d]_q$-code MDS non trivial vérifie $n \leq q+1$ ou $n \leq q+2$ en fonction de la parité de q. Un résultat récent de Ball et De Beule affirme que si la dimension d'un code MDS sur un corps de caractéristique p vérifie $k \leq 2p-2$ alors sa longueur est au plus $q+1$.

Exercice 4. *Utiliser la forme normale d'un code pour faire une traduction algébrique de la notion de code MDS.*

8. Transformation de Hadamard

L'opérateur de Hadamard, est l'opérateur unitaire de matrice $H_n := H^{\otimes n}$ où H désigne la matrice de Hadamard $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} +1 & +1 \\ +1 & -1 \end{smallmatrix}\right)$, il agit par

$$|v\rangle \mapsto \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} (-1)^{uv} |u\rangle$$

Pour une fonction $f \colon \mathbb{F}_2^n \to \mathbb{C}$, on pose

$$\hat{f}(y) = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{xy}$$

Il s'agit de la transformée de Fourier de f. Pour tout sous-espace C de $\mathbb{F}_2^n$, la relation de Poisson :

$$\sum_{y \in C^\perp}^{\star} (-1)^{yt} \hat{f}(y) = \sum_{x \in C}^{\star} f(x+t) \tag{8}$$

On introduit les $\star$ indique une somme normalisées :

$$\sum_{x \in C}^{\star} f(x) := \frac{1}{\sqrt{|C|}} \sum_{x \in C} f(x)$$

Ainsi, si le code $C^\perp$ à une capacité de correction t, il sera possible de corriger les inversions de phase, en corrigeant les inversions de bit dans le système de Hadamard puis de revenir dans la base naturelle.

Proposition 1. *Si W est un code t-correcteur contenant un sous code C de co-dimension k dont le dual est t-correcteur alors il existe un $[[n, k]]$-code quantique t-correcteur.*

Une manière de faire est d'utiliser des codes autoduaux i.e. incluent dans leur dual. Pour illustrer cet construction, nous construisons le $[[9, 1, 3]]$-code de Shor.

9. Groupe de Pauli

Sur le canal de dépolarisation, on admet que les états de $\mathcal{H}^{\otimes n}$ sont altérés par des opérateurs de Pauli qui agissent de façon indépendante sur les n qubits d'un registre quantique. Trois type d'erreurs peuvent de produire sur un qubit : le bit flip, le phase flip ou les deux simultanéments. Le résultat de cette erreur correspond à appliquer l'opérateur unitaire X, Z ou iY.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Les matrices réelles vérifient

$$X^2 = Z^2 = I, \quad Y^2 = -I \quad ZX = Y = -XZ$$

elles engendrent un groupe non commutatif, d'ordre 8 dont le centre est d'ordre 2 et

$$\{\pm I, \pm X, \pm Y, \pm Z\} = \pm\{I, X, Y, Z\}$$

Plus généralement, les produits tensoriels d'ordre n de ces éléments forment un groupe $\mathcal{P}^{\otimes n}$, un élément $E \in \mathcal{P}^{\otimes n}$ s'écrit :

$$E = E_1 \otimes E_2 \otimes \cdots \otimes E_n, \quad \forall i E_i \in \mathcal{P}$$

au signe prés, tout élément s'écrit de manière unique avec toutes les composantes $E_i \in \{I, X, Y, Z\}$, on peut alors définir le poids d'une erreur de Pauli par

$$\mathrm{wp}\,(E) = \sharp\{i \mid E_i \neq I\}$$

Chaque élément de $\mathcal{P}^{\otimes n}$ modulo $\pm$ s'écrit de manière unique

$$Z^\alpha X^\beta := \otimes_{i=1}^n Z^{\alpha_i} . \otimes_{i=1}^n X^{\beta_i}$$

Le groupe de Pauli des n-qubits est une extension centrale de $\mathbb{F}_2^n$ par $\mathbb{Z}/2\mathbb{Z}$, son ordre est 2^{2n+1}.

10. Code quantique binaire

Soit $d \leq 2t + 1$. On souhaite corriger l'ensemble des motifs d'erreurs :

$$\mathcal{E} = \{E \in \mathcal{P}^{\otimes n} \mid \mathrm{wp}\,(E) \leq t\}$$

Un $[[n, k, d]]$-code quantique permet de corriger t erreurs de Pauli par un encodage de $\mathcal{H}^{\otimes k}$ dans $\mathcal{H}^{\otimes n}$. Il s'agit d'un code binaire classique C auquel on associe l'espace de dimension 2^k

$$Q = \sum_{c \in C} \mathbb{C}.|c\rangle \subseteq \mathcal{H}^{\otimes n}$$

De sorte que les sous-espaces $E.Q$, avec $E \in \mathcal{E}$, soient deux à deux orthogonaux. Il est alors possible de mesurer un état, par rapport à cette décomposition orthogonale, si ce dernier correspond à un vecteur $|\psi\rangle \in Q$ entaché de moins de t erreurs, le résultat de la mesure permet de déterminer le motif d'erreur unitaire E, il suffit alors d'appliquer $E^\dagger$ pour retrouver l'état $|\psi\rangle$.

Observant la dimension, l'inégalité de Hamming :

$$2^k \sum_{i=0}^{t} \binom{i}{n} 3^i \leq 2^n$$

Dans l'article original de Shor, un code $[[9,1,3]]$ est construit, puis un code $[[7,1,3]]$, en fait il existe un un code $[[5,1,3]]$ qui est parfait et donc optimal.

11. Codes CSS

Il s'agit de la première classe de codes quantiques proposée par Calderbank-Shor et Stean en 1995-96. La construction est fondée sur l'utilisation de codes binaires autoduaux.

Soit e un mot de $\mathbb{F}_2^n$. Notons X^e un opérateur d'erreur produisant des inversions de bit aux positions du support de e. L'action produit une translation :

$$X^e|c\rangle = |c+e\rangle.$$

Il suffit donc d'utiliser un code t-correcteur pour obtenir un code quantique corrigeant t inversions de bit.

Considérons maintenant Z^e un opérateur d'erreur produisant des inversions de phase. L'action produit une modulation :

$$Z^e|c\rangle = (-1)^{ec}|c\rangle.$$

L'idée de base est d'utiliser la formule de Poisson pour voir les erreurs de phase comme des inversions. Pour cela, on choisit un $[n,k]$-code C, un système de représentants de l'espace quotient K^n/C, et pour $w \in K^n/C$, on pose :

$$|w\rangle = \sum_{c\in C}^{\star} |w+c\rangle$$

Par la formule de Poisson (8)

$$H_n Z^e|w\rangle = \sum_{c\perp C}^{\star} (-1)^{wc}|c+e\rangle \tag{9}$$

12. Stabilisateur

Le groupe de Pauli est dans le groupe unitaire. Deux éléments commutent ou bien anticommutent. Les carrés sont dans le groupe $\pm I$. Plus précisément, si $E^2 = I$ alors E est symétrique et le nombre de composantes Y dans E est pair sinon il est impair et E et antisymétrique.

Soit S un sous-groupe abélien du groupe de Pauli. On suppose que $-I \notin S$. L'espace stabilisé par S est :

$$\operatorname{stab}(S) = \{|\psi\rangle \in \mathcal{H}^{\otimes n} \mid \forall E \in S, \quad E|\psi\rangle = |\psi\rangle\}$$

Proposition 2. *Le groupe S possède un système de générateurs indépendants et*

$$\dim_{\mathbb{C}} \operatorname{stab}(S) \times |S| = 2^n$$

Démonstration. Nous procédons par induction sur la $\mathbb{F}_2$-dimension de S. Considérons un groupe d'ordre 2^{r+1} avec $r \geq 0$. Le centre de $\mathcal{P}^{\otimes n}$ étant réduit à $\pm I$, il existe un élément A qui n'est pas dans le centralisateur de S. Les éléments x de S qui commutent avec A forment un sous-groupe S' d'indice 2 dans S. Notons T un supplémentaire de S' dans S. Par hypothèse d'induction, l'espace stable V de S' est de dimension $n-r$. Par ailleurs, pour $|\psi\rangle \in V$, nous avons :

$$T|\psi\rangle = |\psi\rangle \Rightarrow AT|\psi\rangle = A|\psi\rangle \Rightarrow -TA|\psi\rangle = A|\psi\rangle$$

□

En particulier, la dimension du stabilisateur de S est bien 2^{n-r-1}.

On peut alors définir le syndrome d'un d'opérateur de Pauli $\operatorname{syn} E$ comme un mot de r-bits

$$\operatorname{syn} E = s \in \mathbb{F}_2^r, \quad \text{tel que} \quad ES_i = (-1)^{s_i} S_i E$$

Pour chaque syndrome $s = (s_i)_{i=1}^r$, on définit l'espace

$$C(s) = \{|\psi\rangle \mid S_i|\psi\rangle = (-1)^{s_i}|\psi\rangle\}$$

En particulier, $C(0)$ n'est autre que le code stabilisé par S et les éléments de $C(s)$ sont les altérations des états de $C(0)$ par une erreur de syndrome s. Les espaces $C(s)$ sont deux à deux orthogonaux, et pour des questions de dimension :

$$\mathcal{H}^{\otimes n} = \oplus^{\perp}_{s\in\mathbb{F}_2^r} C(s)$$

Au final la condition de décodage est donnée par :

Quelques soient les motifs d'erreurs E_a et E_b dans $\mathcal{E}$, une des conditions est satisfaites

(1) $E_a^\dagger E_b \in S$

(2) Il existe A dans S tel que S anticommute avec $E_a^\dagger E_b$.

Le code est dit dégénéré si (1) est satisfaite par certaine paire de motifs.

Le code est dit de distance d si tous les opérateurs d'erreurs de poids inférieur à d sont dans le stabilisateur ou anticommutent avec un des générateurs du stabilisateur. Le code est dit non dgénéré si le stabilisateur de contient pas d'elément de poids inférieur à t.

La non dégénérécence du code peut-être forlulée de plusieurs manières :

(1) Pour tous les motifs d'erreurs à corriger

$$\langle \psi_i \mid E_a^* E_b \mid \psi_j \rangle = c_{a,b}\delta_{i,j}$$

où la matrice $c_{a,b}$ est inversible.

(2) Les vecteurs $E_a|\psi_i\rangle$ sont indépendants.

(3) Le poids minimum du groupe S est supérieur à $2t$.

13. Approche symplectique

Le quotient du groupe de Pauli par son centre $\mathbb{Z}/2\mathbb{Z}$ est isomorphe à $\mathbb{F}_2^n \times \mathbb{F}_2^n$, autrement dit c'est une extension de $\mathbb{F}_2^n \times \mathbb{F}_2^n$ par $\mathbb{Z}/2\mathbb{Z}$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathcal{P}^{\otimes n} & \longrightarrow & \mathcal{P}^{\otimes n}/\mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & & & & & \downarrow & & \\ & & & & & & \mathbb{F}_2^{2n} & & \end{array}$$

Et dans ce contexte les co-facteurs sont décrit par une forme symplectique. Dans le cas, du groupe de Pauli, le co-facteur $Z^\alpha X^\beta . Z^{\alpha'} X^{\beta'}$ est décrit par la forme symplectique :

$$(\alpha : \beta, \alpha' : \beta') \mapsto \alpha\beta' + \alpha'\beta' \tag{10}$$

car en effet,

$$Z^{\alpha}X^{\beta}.Z^{\alpha'}X^{\beta'} = (-1)^{\alpha'.\beta}Z^{\alpha+\alpha'}X^{\beta+\beta'}$$

Par ailleurs, on peut observer que

$$\mathrm{wp}\,(Z^{\alpha}X^{\beta}) = \mathrm{wt}\,(\alpha \vee \beta)$$

On définit $S^{\perp}$ l'orthogonal de S, c'est donc le normalisateur de S dans le groupe de Pauli, comme S est abélien il contient S et la condition de t-correction se traduit en une nouvelle alternative :

si ce dernier est moins que $2t+1$ alors (α, β) est dans S ou bien est en dehors de $S^{\perp}$.

Au final, un code est caractérisé par son stabilisateur qui lui même est caractérisé par une matrice rn ,

$$H = (H_Z \mid H_X)$$

Le syndrome d'un opérateur d'erreur $E = (\alpha, \beta)$ est un vecteur de $\mathbb{F}_2^r$

$$\mathrm{syn}\,(E) = (\alpha.\beta_i + \alpha_i.\beta)_{1 \leq i \leq r}.$$

Enfin le cas non dégénéré est caractérisé par des syndromes différents sur les motifs d'erreurs.

14. Les codes CSS

De ce qui précède, nous pouvons construire un $[[7, 1, 3]]$-code. En effet, partant de la matrice de contrôle H du code de Hamming binaire $[7, 4, 3]$, nous

$$S = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix}$$

Le syndrome d'un opérateur d'erreur (α, β) est $(H\alpha^t, H\beta^t)$, on voit que les erreurs de poids au plus 1 ont des syndromes distincts, le code est bien 1-correcteur.

Il s'agit d'un cas particulier d'une situation remarquée indépendament par Calderbank-Shor et Stean. Pour définir un code CSS, on écrit une matrice de contrôle

$$S = \begin{pmatrix} H_Z & 0 \\ 0 & H_X \end{pmatrix}$$

Le groupe S doit être abélien. En particulier, la commutation d'une ligne supérieure $(\alpha, 0)$ avec une ligne inférieure $(0, \beta)$ est équivalente à $\alpha.\beta = 0$.

$$H_Z H_X^t = H_X H_Z^t = 0$$

En particulier, si nous notons C_X et C_Z les codes controlés par les matrices H_X et H_Z alors $C_Z^{\perp} \subseteq C_X$ et $C_X^{\perp} \subseteq C_Z$.

15. Le 5-qubit code

La borne de Singleton quantique ne contrarie pas l'existence d'un $[[5, 1, 3]]$-code. En fait, il existe bel et bien un stabilisateur quantique avec ces paramètres mais ce n'est pas un code CSS. Notons au passage que la découverte de ce code par énumumération exhausitive est tout à fait possible avec une machine classique, le facteur de travail est de l'ordre de 2^{40}. Il n'est pas difficile de vérifier à posteriori que le groupe engendré par les 4 lignes suivantes définit bien un $[[5, 1, 3]]$-code.

$$H = \begin{pmatrix} X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \\ Z & X & I & X & Z \end{pmatrix} = \begin{pmatrix} 01100 & 10010 \\ 00110 & 01001 \\ 00011 & 10100 \\ 10001 & 01010 \end{pmatrix} \tag{11}$$

Les syndromes des opérateurs de poids 1 X_i puis Y_j sont tous différents :

	X_1	X_2	X_3	X_4	X_5
L_1	0	1	1	0	0
L_2	0	0	1	1	0
L_3	0	0	0	1	1
L_4	1	0	0	0	1

	Y_1	Y_2	Y_3	Y_4	Y_5
L_1	0	1	1	0	0
L_2	0	0	1	1	0
L_3	0	0	0	1	1
L_4	1	0	0	0	1

Exercice 5. *Calculer les syndromes des erreurs de Y_i, pour $1 \leq i \leq 5$. En déduire que le code stabilisé par (11) est un code 1-correcteur parfait.*

16. Code hermitien sur $\mathbb{F}_4$

Il est possible d'interpréter la forme biliéaire en introduisant les codes sur le corps à 4 éléments. Le produit hermitien de deux vecteurs γ et γ' de $\mathbb{F}_4^n$ est :

$$\gamma\prime * \gamma = \sum_{i=1}^{n} \gamma_i' \bar{\gamma}_i \tag{12}$$

En identifiant $(\alpha : \beta)$ avec le vecteur quaternaire $\gamma := \alpha + \omega\beta \in \mathbb{F}_4^n$, on réalise que :

$$\begin{aligned} \gamma' * \gamma &= \sum_{i=1}^{n} (\alpha_i' + \omega\beta_i')(\alpha_i + \bar{\omega}\beta_i) \\ &= \alpha'\alpha + \beta'\beta + \alpha'\beta + (\gamma', \gamma)\omega \end{aligned}$$

Ainsi, la dualité hermitienne est plus forte que la dualité symplectique. On en déduit que si C désigne un $\mathbb{F}_2$-espace vectoriel de dimension r dont le dual est t-correcteur alors le code stabiisé par une matrice de controle de C est $[[n, k, d]]$.

Ainsi, si nous partons du $[5, 2, 3]$ code quaternaire de (2), nous constatons que ce code est autodual hermitien. Le code quantique correspondant n'est rien d'autre que le fameux $[[5, 1, 3]]$ binaire.

17. Suggestions

L'entropie de von Neuman permet détablir que les paramètres d'un code quantique satisfont à une inégalité de type Singleton :

$$2(d-1) \leq n - k \tag{13}$$

Pour la suite, je suggère de faire le point sur cette inégalité pour vérifier si cette dernière peut donner lieu à une définition de code MDS qui déboucherait sur un analogue quantique de la conjecture MDS.

Dernière modification :

P. Langevin à Toulon, juillet 2012.

Références

[ABC+03] G. Alber, Th. Beth, Ch. Charnes, A. Delgado, M. Grassl, and M. Mussinger, *Detected-jump-error-correcting quantum codes, quantum error designs, and quantum computation*, Phys. Rev. A (3) **68** (2003), no. 1, 012316, 10.

[AC08] Vaneet Aggarwal and A. Robert Calderbank, *Boolean functions, projection operators, and quantum error correcting codes*, IEEE Trans. Inform. Theory **54** (2008), no. 4, 1700–1707.

[ADM01] G. Alber, A. Delgado, and M. Mussinger, *Quantum error correction and quantum computation with detected-jump correcting quantum codes*, Fortschr. Phys. **49** (2001), no. 10-11, 901–908.

[AGP06] Panos Aliferis, Daniel Gottesman, and John Preskill, *Quantum accuracy threshold for concatenated distance-3 codes*, Quantum Inf. Comput. **6** (2006), no. 2, 97–165.

[AK01] Alexei Ashikhmin and Emanuel Knill, *Nonbinary quantum stabilizer codes*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 3065–3072.

[AKP04] V. Arvind, Piyush P. Kurur, and K. R. Parthasarathy, *Non-stabilizer quantum codes from abelian subgroups of the error group*, Quantum Inf. Comput. **4** (2004), no. 6-7, 411–436.

[AKS07] Salah A. Aly, Andreas Klappenecker, and Pradeep Kiran Sarvepalli, *On quantum and classical BCH codes*, IEEE Trans. Inform. Theory **53** (2007), no. 3, 1183–1188.

[AL99] Alexei Ashikhmin and Simon Litsyn, *Upper bounds on the size of quantum codes*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1206–1215.

[Ami10] Massoud Amini, *Quantum error-correction codes on abelian groups*, Iran. J. Math. Sci. Inform. **5** (2010), no. 1, 55–67, 76.

[APS09] C. D. Albuquerque, R. Palazzo, Jr., and E. B. Silva, *Topological quantum codes on compact surfaces with genus $g \geq 2$*, J. Math. Phys. **50** (2009), no. 2, 023513, 20.

[APS10] ———, *New classes of topological quantum codes associated with self-dual, quasi self-dual and denser tessellations*, Quantum Inf. Comput. **10** (2010), no. 11-12, 956–970.

[Arb01] I. M. Arbekov, *Key secrecy in a quantum cryptography system that uses correcting codes*, Problemy Peredachi Informatsii **37** (2001), no. 1, 89–94.

[BCG+11] Salman Beigi, Isaac Chuang, Markus Grassl, Peter Shor, and Bei Zeng, *Graph concatenation for quantum codes*, J. Math. Phys. **52** (2011), no. 2, 022201, 23.

[BE00] Jürgen Bierbrauer and Yves Edel, *Quantum twisted codes*, J. Combin. Des. **8** (2000), no. 3, 174–188.

[BFG+08] Jürgen Bierbrauer, Giorgio Faina, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco, *The geometry of quantum codes*, Innov. Incidence Geom. **6/7** (2007/08), 53–71.

[BFMP11] Jürgen Bierbrauer, Richard Fears, Stefano Marcugini, and Fernanda Pambianco, *The nonexistence of a $[[13, 5, 4]]$-quantum stabilizer code*, IEEE Trans. Inform. Theory **57** (2011), no. 7, 4788–4793.

[BKMD09] H. Bombin, M. Kargarian, and M. A. Martin-Delgado, *Quantum 2-body Hamiltonian for topological color codes*, Fortschr. Phys. **57** (2009), no. 11-12, 1103–1110.

[BMD07] H. Bombin and M. A. Martin-Delgado, *Homological error correction : classical and quantum codes*, J. Math. Phys. **48** (2007), no. 5, 052105, 35.

[BMD09] ———, *Quantum measurements and gates by code deformation*, J. Phys. A **42** (2009), no. 9, 095302, 13.

[BT07] Sundeep B and Andrew Thangaraj, *Self-orthogonality of q-ary images of q^m-ary codes and quantum code construction*, IEEE Trans. Inform. Theory **53** (2007), no. 7, 2480–2489.

[CC97] Nicolas J. Cerf and Richard Cleve, *Information-theoretic interpretation of quantum error-correcting codes*, Phys. Rev. A (3) **56** (1997), no. 3, 1721–1732.

[CCS+09] Isaac Chuang, Andrew Cross, Graeme Smith, John Smolin, and Bei Zeng, *Codeword stabilized quantum codes : algorithm and structure*, J. Math. Phys. **50** (2009), no. 4, 042109, 17.

[CDT09] Andrew W. Cross, David P. DiVincenzo, and Barbara M. Terhal, *A comparative code study for quantum fault tolerance*, Quantum Inf. Comput. **9** (2009), no. 7-8, 541–572.

[CEL99] Gérard Cohen, Sylvia Encheva, and Simon Litsyn, *On binary constructions of quantum codes*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2495–2498.

[CH11] H. F. Chau and K. H. Ho, *Practical entanglement distillation scheme using recurrence method and quantum low density parity check codes*, Quantum Inf. Process. **10** (2011), no. 2, 213–229.

[Cha98] H. F. Chau, *Quantum convolutional error-correcting codes*, Phys. Rev. A (3) **58** (1998), no. 2, 905–909.

[Cha05] ———, *Reply to : "Comment on 'Quantum convolutional error-correcting codes'" [Phys. Rev. A (3) **72** (2005), no. 2, part B, 026301, 2 pp. ; mr2169975] by A. C. A. de Almeida and R. Palazzo, Jr*, Phys. Rev. A (3) **72** (2005), no. 2, part B, 026302, 1.

[Che01] Hao Chen, *Some good quantum error-correcting codes from algebraic-geometric codes*, IEEE Trans. Inform. Theory **47** (2001), no. 5, 2059–2061.

[CKŻ06] Man-Duen Choi, David W. Kribs, and Karol Życzkowski, *Quantum error correcting codes from the compression formalism*, Rep. Math. Phys. **58** (2006), no. 1, 77–91.

[Cle97] Richard Cleve, *Quantum stabilizer codes and classical linear codes*, Phys. Rev. A (3) **55** (1997), no. 6, 4054–4059.

[CLLM11] Carlo Cafaro, Sonia L'Innocente, Cosmo Lupo, and Stefano Mancini, *Quantifying the performance of quantum codes*, Open Syst. Inf. Dyn. **18** (2011), no. 1, 1–31.

[CLX01] Hao Chen, San Ling, and Chaoping Xing, *Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound*, IEEE Trans. Inform. Theory **47** (2001), no. 5, 2055–2058.

[CLX05] ———, *Quantum codes from concatenated algebraic-geometric codes*, IEEE Trans. Inform. Theory **51** (2005), no. 8, 2915–2920.

[CM10] Carlo Cafaro and Stefano Mancini, *Repetition versus noiseless quantum codes for correlated errors*, Phys. Lett. A **374** (2010), no. 26, 2688–2700.

[Cra04] Nuno Crato, *Undecipherable codes, secure messages. Alice, Bob and the meddler. Quantum cryptography*, Boll. Unione Mat. Ital. Sez. A Mat. Soc. Cult. (8) **7** (2004), no. 2, 275–289, Translated from the English by Pierluigi Contucci.

[CRSS98] A. Robert Calderbank, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane, *Quantum error correction via codes over* GF(4), IEEE Trans. Inform. Theory **44** (1998), no. 4, 1369–1387.

[CSSZ09] Andrew Cross, Graeme Smith, John A. Smolin, and Bei Zeng, *Codeword stabilized quantum codes*, IEEE Trans. Inform. Theory **55** (2009), no. 1, 433–438.

[CT12] David Clark and Vladimir D. Tonchev, *Nonbinary quantum codes derived from finite geometries*, Finite Fields Appl. **18** (2012), no. 1, 63–69.

[CX11] Han Wu Chen and Fang Ying Xiao, *Construction of quantum codes based on elementary transformations*, J. Southeast Univ. Nat. Sci. **41** (2011), no. 5, 934–937.

[dAP05] Antonio Carlos Aido de Almeida and Reginaldo Palazzo, Jr., *Comment on : "Quantum convolutional error-correcting codes" [Phys. Rev. A (3) **58** (1998), no. 2, 905–909 ; mr1638225] by H. F. Chau*, Phys. Rev. A (3) **72** (2005), no. 2, part B, 026301, 2.

[dAPdS09] Clarice Dias de Albuquerque, Reginaldo Palazzo, Júnior, and Eduardo Brandani da Silva, *On toric quantum codes*, Int. J. Pure Appl. Math. **50** (2009), no. 2, 221–226.

[ELS11] Martianus Frederic Ezerman, San Ling, and Patrick Solé, *Additive asymmetric quantum codes*, IEEE Trans. Inform. Theory **57** (2011), no. 8, 5536–5550.

[ELSY11] Martianus Frederic Ezerman, San Ling, Patrick Solé, and Olfa Yemen, *From skew-cyclic codes to asymmetric quantum codes*, Adv. Math. Commun. **5** (2011), no. 1, 41–57.

[Fen02] Keqin Feng, *Quantum codes* $[[6,2,3]]_p$ *and* $[[7,3,3]]_p$ $(p \geq 3)$ *exist*, IEEE Trans. Inform. Theory **48** (2002), no. 8, 2384–2391.

[FGG07] G. David Forney, Jr., Markus Grassl, and Saikat Guha, *Convolutional and tail-biting quantum error-correcting codes*, IEEE Trans. Inform. Theory **53** (2007), no. 3, 865–880.

[FKSS06] Jesse Fern, Julia Kempe, Slobodan N. Simić, and Shankar Sastry, *Generalized performance of concatenated quantum codes—a dynamical systems approach*, IEEE Trans. Automat. Control **51** (2006), no. 3, 448–459.

[FLX06] Keqin Feng, San Ling, and Chaoping Xing, *Asymptotic bounds on quantum codes from algebraic geometry codes*, IEEE Trans. Inform. Theory **52** (2006), no. 3, 986–991.

[FM01] Michael H. Freedman and David A. Meyer, *Projective plane and planar quantum codes*, Found. Comput. Math. **1** (2001), no. 3, 325–332.

[FM04] Keqin Feng and Zhi Ma, *A finite Gilbert-Varshamov bound for pure stabilizer quantum codes*, IEEE Trans. Inform. Theory **50** (2004), no. 12, 3323–3325.

[FSS01] L. Frappat, P. Sorba, and A. Stsiarrino, *Quantum groups and the genetic code*, Teoret. Mat. Fiz. **128** (2001), no. 1, 27–42.

[FWH11] Austin G. Fowler, David S. Wang, and Lloyd C. L. Hollenberg, *Surface code quantum error correction incorporating accurate error propagation*, Quantum Inf. Comput. **11** (2011), no. 1-2, 8–18.

[FX08] Keqin Feng and Chaoping Xing, *A new construction of quantum error-correcting codes*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 2007–2019.

[GB00] Markus Grassl and Thomas Beth, *Cyclic quantum error-correcting codes and quantum shift registers*, R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci. **456** (2000), no. 2003, 2689–2706.

[GBP97] M. Grassl, Th. Beth, and T. Pellizzari, *Codes for the quantum erasure channel*, Phys. Rev. A (3) **56** (1997), no. 1, 33–38.

[GL10] Ying Guo and Moon Ho Lee, *Erratum to : "Fast quantum codes based on Pauli block jacket matrices" [mr2540481]*, Quantum Inf. Process. **9** (2010), no. 5, 663–666.

[Got96] Daniel Gottesman, *Class of quantum error-correcting codes saturating the quantum Hamming bound*, Phys. Rev. A (3) **54** (1996), no. 3, 1862–1868.

[GPL09] Ying Guo, Jun Peng, and Moon Ho Lee, *Fast quantum codes based on Pauli block jacket matrices*, Quantum Inf. Process. **8** (2009), no. 5, 361–378.

[GRB03] Markus Grassl, Martin Rötteler, and Thomas Beth, *Efficient quantum circuits for non-qubit quantum error-correcting codes*, Internat. J. Found. Comput. Sci. **14** (2003), no. 5, 757–775, Quantum computing.

[GSS+09] Markus Grassl, Peter Shor, Graeme Smith, John Smolin, and Bei Zeng, *Generalized concatenated quantum codes*, Phys. Rev. A (3) **79** (2009), no. 5, 050306, 4.

[GZL10] Ying Guo, Guihu Zeng, and MoonHo Lee, *Fast constructions of quantum codes based on residues Pauli block matrices*, Adv. Math. Phys. (2010), Art. ID 469124, 12.

[Ham04] Mitsuru Hamada, *Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution*, J. Phys. A **37** (2004), no. 34, 8303–8328.

[Ham05] ———, *Information rates achievable with algebraic codes on quantum discrete memoryless channels*, IEEE Trans. Inform. Theory **51** (2005), no. 12, 4263–4277.

[Ham08] ———, *Concatenated quantum codes constructible in polynomial time : efficient decoding and error correction*, IEEE Trans. Inform. Theory **54** (2008), no. 12, 5689–5704.

[HR08] Henry L. Haselgrove and Peter P. Rohde, *Trade-off between the tolerance of located and unlocated errors in nondegenerate quantum error-correcting codes*, Quantum Inf. Comput. **8** (2008), no. 5, 399–410.

[HSW08] Patrick Hayden, Peter W. Shor, and Andreas Winter, *Random quantum codes from Gaussian ensembles and an uncertainty relation*, Open Syst. Inf. Dyn. **15** (2008), no. 1, 71–89.

[HYH11] Min-Hsiu Hsieh, Wen-Tai Yen, and Li-Yi Hsu, *High performance entanglement-assisted quantum LDPC codes need little entanglement*, IEEE Trans. Inform. Theory **57** (2011), no. 3, 1761–1769.

[IM07] Lev Ioffe and Marc Mézard, *Asymmetric quantum error-correcting codes*, Phys. Rev. A (3) **75** (2007), no. 3, 032345, 4.

[JFS06] Stephen P. Jordan, Edward Farhi, and Peter W. Shor, *Error-correcting codes for adiabatic quantum computation*, Phys. Rev. A (3) **74** (2006), no. 5, 052322, 5.

[JLLX10] Lingfei Jin, San Ling, Jinquan Luo, and Chaoping Xing, *Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes*, IEEE Trans. Inform. Theory **56** (2010), no. 9, 4735–4740.

[Kau93] Louis H. Kauffman, *Gauss codes, quantum groups and ribbon Hopf algebras*, Rev. Math. Phys. **5** (1993), no. 4, 735–773.

[Kaz08] A. Ya. Kazakov, *An elementary constructive approach to the higher-rank numerical ranges of unitary matrices and quantum error-correcting codes*, J. Phys. A **41** (2008), no. 25, 255306, 9.

[KBMD10] M. Kargarian, H. Bombin, and M. A. Martin-Delgado, *Topological color codes and two-body quantum lattice Hamiltonians*, New J. Phys. **12** (2010), no. February, 025018, 40.

[KdW04] Iordanis Kerenidis and Ronald de Wolf, *Exponential lower bound for 2-query locally decodable codes via a quantum argument*, J. Comput. System Sci. **69** (2004), no. 3, 395–420.

[KKR10] Robert Koenig, Greg Kuperberg, and Ben W. Reichardt, *Quantum computation with Turaev-Viro codes*, Ann. Physics **325** (2010), no. 12, 2707–2749.

[KL97] Emanuel Knill and Raymond Laflamme, *Theory of quantum error-correcting codes*, Phys. Rev. A (3) **55** (1997), no. 2, 900–911.

[KLZ10] W. F. Ke, K. F. Lai, and R. B. Zhang, *Quantum codes from Hadamard matrices*, Linear Multilinear Algebra **58** (2010), no. 7-8, 847–854.

[Kou09] Su-Peng Kou, *Realization of topological quantum computation with planar codes*, Phys. Rev. A (3) **80** (2009), no. 5, 052317, 9.

[KPŻ08] David W. Kribs, Aron Pasieka, and Karol Życzkowski, *Entropy of a quantum error correction code*, Open Syst. Inf. Dyn. **15** (2008), no. 4, 329–343.

[KS07] Andreas Klappenecker and Pradeep Kiran Sarvepalli, *On subsystem codes beating the quantum Hamming or Singleton bound*, Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **463** (2007), no. 2087, 2887–2905.

[KS08] ———, *Clifford code constructions of operator quantum error-correcting codes*, IEEE Trans. Inform. Theory **54** (2008), no. 12, 5760–5765.

[KW08] Jon-Lark Kim and Judy Walker, *Nonbinary quantum error-correcting codes from algebraic curves*, Discrete Math. **308** (2008), no. 14, 3115–3124.

[LD07] Zhicheng Luo and Igor Devetak, *Efficiently implementable codes for quantum key expansion*, Phys. Rev. A (3) **75** (2007), no. 1, 010303, 4.

[LDP10] Yunfan Li, Ilya Dumer, and Leonid P. Pryadko, *Clustered error correction of codeword-stabilized quantum codes*, Phys. Rev. Lett. **104** (2010), no. 19, 190501, 4.

[LG11a] Giuliano G. La Guardia, *New families of asymmetric quantum BCH codes*, Quantum Inf. Comput. **11** (2011), no. 3-4, 239–252.

[LG11b] ———, *New quantum MDS codes*, IEEE Trans. Inform. Theory **57** (2011), no. 8, 5551–5554.

[LGPL10] Giuliano G. La Guardia, Reginaldo Palazzo, Jr., and Carlile Lavor, *Nonbinary quantum Reed-Solomon codes*, Int. J. Pure Appl. Math. **65** (2010), no. 1, 55–63.

[Lin04] Xiaoyan Lin, *Quantum cyclic and constacyclic codes*, IEEE Trans. Inform. Theory **50** (2004), no. 3, 547–549.

[LL04] Ruihu Li and Xueliang Li, *Binary construction of quantum codes of minimum distance three and four*, IEEE Trans. Inform. Theory **50** (2004), no. 6, 1331–1336.

[LL08] ———, *Binary construction of quantum codes of minimum distances five and six*, Discrete Math. **308** (2008), no. 9, 1603–1611.

[LL11] Ching-Yi Lai and Chung-Chin Lu, *A construction of quantum stabilizer codes based on syndrome assignment by classical parity-check matrices*, IEEE Trans. Inform. Theory **57** (2011), no. 10, 7163–7179.

[LLX10] San Ling, Jinquan Luo, and Chaoping Xing, *Generalization of Steane's enlargement construction of quantum codes and applications*, IEEE Trans. Inform. Theory **56** (2010), no. 8, 4080–4084.

[LMF06] Xin Lü, Zhi Ma, and Deng Guo Feng, *Quantum secure direct communication using quantum Calderbank-Shor-Steane error correcting codes*, J. Softw. **17** (2006), no. 3, 509–515.

[LS08] Debbie Leung and Graeme Smith, *Communicating over adversarial quantum channels using quantum list codes*, IEEE Trans. Inform. Theory **54** (2008), no. 2, 883–887.

[LW08] Tai Lin Liu and Qiao Yan Wen, *Isometries and equivalences of quantum codes*, Acta Math. Sinica (Chin. Ser.) **51** (2008), no. 1, 1–10.

[LWB02] Daniel A. Lidar, Lian-Ao Wu, and Alexandre Blais, *Quantum codes for simplifying design and suppressing decoherence in superconducting phase-qubits*, Quantum Inf. Process. **1** (2002), no. 3, 155–182.

[LWL05] Tailin Liu, Qiaoyan Wen, and Zihui Liu, *Construction of nonbinary quantum cyclic codes by using graph method*, Sci. China Ser. F **48** (2005), no. 6, 693–702.

[LX01] Fang Qiong Li and Hong Xi, *A theory of the quantum error-correcting codes*, Xinan Shifan Daxue Xuebao Ziran Kexue Ban **26** (2001), no. 4, 416–419.

[LX07] Zhuo Li and Li Juan Xing, *A family of asymptotically good quantum codes based on code concatenation*, Acta Phys. Sinica **56** (2007), no. 10, 5602–5606.

[LX08] ———, *Quantum generalized Reed-Solomon codes*, Acta Phys. Sinica **57** (2008), no. 1, 28–30.

[LX10a] Ruihu Li and Zongben Xu, *Construction of $[[n, n-4, 3]]_q$ quantum codes for odd prime power q*, Phys. Rev. A (3) **82** (2010), no. 5, 052316, 4.

[LX10b] Zhuo Li and Lijuan Xing, *On a problem concerning the quantum Hamming bound for impure quantum codes*, IEEE Trans. Inform. Theory **56** (2010), no. 9, 4731–4734.

[LXL08] Ruihu Li, Zongben Xu, and Xueliang Li, *Standard forms of stabilizer and normalizer matrices for additive quantum codes*, IEEE Trans. Inform. Theory **54** (2008), no. 8, 3775–3778.

[LXS12] Yuan Li, Mantao Xu, and Qiang Sun, *Graphical quantum error-correcting codes based on entanglement of subgraphs*, Internat. J. Modern Phys. B **26** (2012), no. 4, 1250024, 16.

[LXW08] Zhuo Li, Li-Juan Xing, and Xin-Mei Wang, *Quantum generalized Reed-Solomon codes : unified framework for quantum maximum-distance-separable codes*, Phys. Rev. A (3) **77** (2008), no. 1, 012308, 4.

[LXW09] Zhuo Li, Lijuan Xing, and Xinmei Wang, *A family of asymptotically good quantum codes based on code concatenation*, IEEE Trans. Inform. Theory **55** (2009), no. 8, 3821–3824.

[Ma08] Yuefei Ma, *The asymptotic probability distribution of the relative distance of additive quantum codes*, J. Math. Anal. Appl. **340** (2008), no. 1, 550–557.

[Mar04] William J. Martin, *A physics-free introduction to quantum error correcting codes*, Util. Math. **65** (2004), 133–158.

[Mat02] Ryutaroh Matsumoto, *Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes*, IEEE Trans. Inform. Theory **48** (2002), no. 7, 2122–2124.

[Mat03] ———, *Conversion of a general quantum stabilizer code to an entanglement distillation protocol*, J. Phys. A **36** (2003), no. 29, 8113–8127.

[MFZL07] Yuena Ma, Youqian Feng, Xuejun Zhao, and Ruihu Li, *Large quaternary cyclic codes of length 85 and related quantum error-correcting*, Sci. Magna **3** (2007), no. 2, 9–14.

[MMM04] David J. C. MacKay, Graeme Mitchison, and Paul L. McFadden, *Sparse-graph codes for quantum error correction*, IEEE Trans. Inform. Theory **50** (2004), no. 10, 2315–2330.

[MN02] Cristopher Moore and Martin Nilsson, *Parallel quantum computation and quantum codes*, SIAM J. Comput. **31** (2001/02), no. 3, 799–815.

[DMO01] Micho Durdevich, Hanna E. Makaruk, and Robert Owczarek, *Generalized noiseless quantum codes utilizing quantum enveloping algebras*, J. Phys. A **34** (2001), no. 7, 1423–1437.

[MZLF08] Yue Na Ma, Xue Jun Zhao, Rui Hu Li, and You Qian Feng, *Self-orthogonal caps in* $\mathrm{PG}(k-1,4)$ *and construction of quantum codes*, J. Northwest Univ. **38** (2008), no. 2, 210–212.

[Nie07] Annika Niehage, *Nonbinary quantum Goppa codes exceeding the quantum Gilbert-Varshamov bound*, Quantum Inf. Process. **6** (2007), no. 3, 143–158.

[ON07] Tomohiro Ogawa and Hiroshi Nagaoka, *Making good codes for classical-quantum channel coding via quantum hypothesis testing*, IEEE Trans. Inform. Theory **53** (2007), no. 6, 2261–2266.

[Par01] K. R. Parthasarathy, *An inducing construction of quantum codes from classical error correcting codes*, J. Appl. Probab. **38A** (2001), 27–32, Probability, statistics and seismology.

[Par02] ———, *The Bush matrix over a Galois field and error correcting quantum codes*, Linear Algebra Appl. **341** (2002), 23–34, Special issue dedicated to Professor T. Ando.

[PC08] David Poulin and Yeojin Chung, *On the iterative decoding of sparse quantum codes*, Quantum Inf. Comput. **8** (2008), no. 10, 987–1000.

[PR04] Harriet Pollatsek and Mary Beth Ruskai, *Permutationally invariant codes for quantum error correction*, Linear Algebra Appl. **392** (2004), 255–288.

[PTO09] David Poulin, Jean-Pierre Tillich, and Harold Ollivier, *Quantum serial turbo codes*, IEEE Trans. Inform. Theory **55** (2009), no. 6, 2776–2798.

[Rag02] Maxim Raginsky, *Almost any quantum spin system with short-range interactions can support toric codes*, Phys. Lett. A **294** (2002), no. 3-4, 153–157.

[Rai99a] Eric M. Rains, *Nonbinary quantum codes*, IEEE Trans. Inform. Theory **45** (1999), no. 6, 1827–1832.

[Rai99b] ———, *Quantum codes of minimum distance two*, IEEE Trans. Inform. Theory **45** (1999), no. 1, 266–271.

[Rai00] ———, *Polynomial invariants of quantum codes*, IEEE Trans. Inform. Theory **46** (2000), no. 1, 54–59.

[Rei05] Ben W. Reichardt, *Quantum universality from magic states distillation applied to CSS codes*, Quantum Inf. Process. **4** (2005), no. 3, 251–264.

[Ren05] Joseph M. Renes, *Equiangular spherical codes in quantum cryptography*, Quantum Inf. Comput. **5** (2005), no. 1, 81–92.

[Sch04] Dirk-M. Schlingemann, *Error syndrome calculation for graph codes on a one-way quantum computer : towards a quantum memory*, J. Math. Phys. **45** (2004), no. 11, 4322–4333.

[SEDH08] Ashley M. Stephens, Zachary W. E. Evans, Simon J. Devitt, and Lloyd C. L. Hollenberg, *Asymmetric quantum error correction via code conversion*, Phys. Rev. A (3) **77** (2008), no. 6, 062335, 5.

[SGL10] Ronghua Shi, Ying Guo, and Moon Ho Lee, *Quantum codes based on fast Pauli block transforms in the finite field*, Quantum Inf. Process. **9** (2010), no. 5, 611–628.

[Sid01] V. M. Sidel'nikov, *On a class of quantum codes*, Dokl. Akad. Nauk **381** (2001), no. 1, 27–30.

[Sid02] ———, *Quantum codes and abelian subgroups of the extra-special group*, Problemy Peredachi Informatsii **38** (2002), no. 3, 34–44.

[SKR09] Pradeep Kiran Sarvepalli, Andreas Klappenecker, and Martin Rötteler, *Asymmetric quantum codes : constructions, bounds and performance*, Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **465** (2009), no. 2105, 1645–1672.

[SP06] P. J. Salas-Peralta, *Introduction to error correcting codes in quantum computers*, Rev. Mex. Fís. E **52** (2006), no. 2, 218–243.

[SSSZ11] Peter W. Shor, Graeme Smith, John A. Smolin, and Bei Zeng, *High performance single-error-correcting quantum codes for amplitude damping*, IEEE Trans. Inform. Theory **57** (2011), no. 10, 7180–7188.

[SSW07] John A. Smolin, Graeme Smith, and Stephanie Wehner, *Simple family of nonadditive quantum codes*, Phys. Rev. Lett. **99** (2007), no. 13, 130505, 4.

[Ste96a] A. M. Steane, *Error correcting codes in quantum theory*, Phys. Rev. Lett. **77** (1996), no. 5, 793–797.

[Ste96b] ———, *Simple quantum error-correcting codes*, Phys. Rev. A (3) **54** (1996), no. 6, 4741–4751.

[Ste99a] Andrew M. Steane, *Enlargement of Calderbank-Shor-Steane quantum codes*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2492–2495.

[Ste99b] ———, *Quantum Reed-Muller codes*, IEEE Trans. Inform. Theory **45** (1999), no. 5, 1701–1703.

[Sun06] Guang Ren Sun, *A new construction of quantum error-correcting codes from a condition of equivalence*, J. Univ. Sci. Technol. China **36** (2006), no. 9, 946–950.

[Svo04] Karl Svozil, *Eutactic quantum codes*, Phys. Rev. A (3) **69** (2004), no. 3, 034303, 3.

[TL10] Peiyu Tan and Jing Li, *Efficient quantum stabilizer codes : LDPC and LDPC-convolutional constructions*, IEEE Trans. Inform. Theory **56** (2010), no. 1, 476–491.

[TLL05] Li Ming Tang, Wei Hua Liu, and Huan Ping Liu, *Some conclusions about the existence of quantum codes*, Natur. Sci. J. Harbin Normal Univ. **21** (2005), no. 2, 12–13.

[TLL06] Li-ming Tang, Huan-ping Liu, and Xue-qin Lü, *A new description of the additive quantum codes*, Northeast. Math. J. **22** (2006), no. 3, 285–290.

[TM01] Andrew Thangaraj and Steven W. McLaughlin, *Quantum codes from cyclic codes over* $\mathrm{GF}(4^m)$, IEEE Trans. Inform. Theory **47** (2001), no. 3, 1176–1178.

[TN04] Koujin Takeda and Hidetoshi Nishimori, *Self-dual random-plaquette gauge model and the quantum toric code*, Nuclear Phys. B **686** (2004), no. 3, 377–396.

[TN05] ———, *Duality of the random model and the quantum toric code*, Progr. Theoret. Phys. Suppl. (2005), no. 157, 237–240.

[Ton02] Vladimir D. Tonchev, *A Varshamov-Gilbert bound for a class of formally self-dual codes and related quantum codes*, IEEE Trans. Inform. Theory **48** (2002), no. 4, 975–977.

[Ton08] ———, *Quantum codes from caps*, Discrete Math. **308** (2008), no. 24, 6368–6372.

[Tsu07] Makoto Tsubota, *Quantum turbulence—another Da Vinci code*, Progr. Theoret. Phys. Suppl. (2007), no. 166, 152–158.

[VRA99] Farrokh Vatan, Vwani P. Roychowdhury, and M. P. Anantram, *Spatially correlated qubit errors and burst-correcting quantum codes*, IEEE Trans. Inform. Theory **45** (1999), no. 5, 1703–1708.

[vWB10] G. von Winckel and A. Borzì, *QUCON : a fast Krylov-Newton code for dipole quantum control problems*, Comput. Phys. Comm. **181** (2010), no. 12, 2158–2163.

[WFF10] WeiYang Wang, RongQuan Feng, and KeQin Feng, *Inhomogenous quantum codes (I) : additive case*, Sci. China Math. **53** (2010), no. 9, 2501–2510.

[WFLX10] Long Wang, Keqin Feng, San Ling, and Chaoping Xing, *Asymmetric quantum codes : characterization and constructions*, IEEE Trans. Inform. Theory **56** (2010), no. 6, 2938–2945.

[Wil09] Mark M. Wilde, *Logical operators of quantum codes*, Phys. Rev. A (3) **79** (2009), no. 6, 062322, 5.

[WSBW12] Yun-Jiang Wang, Barry C. Sanders, Bao-Ming Bai, and Xin-Mei Wang, *Enhanced feedback iterative decoding of sparse quantum codes*, IEEE Trans. Inform. Theory **58** (2012), no. 2, 1231–1241.

[XC08] Li Qing Xu and Hao Chen, *Construction of asymptotically good* p^m*-ary quantum codes*, Chinese Ann. Math. Ser. A **29** (2008), no. 3, 343–348.

[XC10] Fang Ying Xiao and Han Wu Chen, *Generating of seed generators for quantum stabilizer codes*, J. Southeast Univ. Nat. Sci. **40** (2010), no. 1, 52–57.

[XCZ+10] Mei Ju Xing, Han Wu Chen, Jin Hua Zhang, Fang Ying Xiao, and Shuo Xing Wang, *A class of quantum codes over finite fields*, J. Southeast Univ. Nat. Sci. **40** (2010), no. 2, 282–284.

[YCLO08] Sixia Yu, Qing Chen, C. H. Lai, and C. H. Oh, *Nonadditive quantum error-correcting code*, Phys. Rev. Lett. **101** (2008), no. 9, 090501, 4.

[Yos11] Beni Yoshida, *Classification of quantum phases and topology of logical operators in an exactly solved model of quantum codes*, Ann. Physics **326** (2011), no. 1, 15–95.

[Zan99] Paolo Zanardi, *Computation on an error-avoiding quantum code and symmetrization*, Phys. Rev. A (3) **60** (1999), no. 2, R729–R732.

[ZCC11] Bei Zeng, Andrew Cross, and Isaac L. Chuang, *Transversality versus universality for additive quantum codes*, IEEE Trans. Inform. Theory **57** (2011), no. 9, 6272–6284.

[ZLGL08] Guihua Zeng, Yuan Li, Ying Guo, and Moon Ho Lee, *Stabilizer quantum codes over the Clifford algebra*, J. Phys. A **41** (2008), no. 14, 145304, 8.

[ZMX10] ShuQin Zhong, Zhi Ma, and YaJie Xu, *Constructing quantum error correcting code via logic function*, Sci. China Inf. Sci. **53** (2010), no. 3, 515–523.

[ZR97] Paolo Zanardi and Mario Rasetti, *Error avoiding quantum codes*, Modern Phys. Lett. B **11** (1997), no. 25, 1085–1093.

[ZZT02] Quan Zhang, Er Yang Zhang, and Chao Jing Tang, *Quantum error-avoiding code based on the decoherence-free subspace*, Acta Phys. Sinica **51** (2002), no. 8, 1675–1683.

Imath, université du sud Toulon Var.