A class of quantum LDPC codes: construction and performances under iterative decoding

Thomas Camara
INRIA, Projet Codes,
BP 105, Domaine de Voluceau
F-78153 Le Chesnay, France.
Email: thomas.camara@inria.fr

Harold Ollivier
Perimeter Institute,
31 Caroline St. N, Waterloo,
ON N2L 2Y5, Canada.
Email: harold.ollivier@polytechnique.org

Jean-Pierre Tillich
INRIA, Projet Codes,
BP 105, Domaine de Voluceau
F-78153 Le Chesnay, France.
Email: jean-pierre.tillich@inria.fr

***Abstract*— A generic method for constructing quantum LDPC codes is presented. We first explain how to overcome the difficulty of finding a set of low weight generators for the stabilizer group of the code. Our approach is based on a graph representation of the generators of the stabilizer group and on a simple local rule to ensure commutativity. We provide several specific examples of quantum LDPC codes obtained by our method, together with numerical simulations over the depolarizing channel and the erasure channel.**

I. Introduction

The idea of using quantum systems for processing information has first been suggested by Feynman and it has developed since into an exciting research area with implications ranging from cryptography to complexity theory. As a concrete example, quantum computer would be able to solve efficiently some hard problems such as integer factorization [11].

However, for taking advantage of the quantum nature of physical systems to process information, it is necessary to protect them from unwanted evolutions. Indeed, if quantum registers are not protected from noise, the very fragile superpositions required for efficiently manipulating quantum information tend to disappear exponentially fast with the number of qubits involved. This effect — called decoherence — can nonetheless be reduced by using quantum error correcting codes. The first scheme of this kind has been proposed in 1995 by P. Shor [12]. Since then, quantum error correction has evolved much. Most notable, is the introduction of the stabilizer formalism [6], [3] for defining quantum codes . With this tools at hand, it has been shown that quantum information processing can be done fault-tolerantly (see for instance [1]), i.e. would be feasible even in the presence of qubit errors and gate faults — provided these events are rare enough.

In spite of these important results, properties of quantum channels and of quantum codes are less understood than for their classical counterparts. For instance, the capacity for sending quantum information is unknown even for the depolarizing channel. It is thus of interest to tackle the problem from a pragmatic point of view: devise versatile constructions of quantum codes inspired by the best classical codes, and analyze their performances.

When sending classical information over memoryless classical channels, it has been demonstrated that a very efficient way for approaching the channel capacity is obtained by using LDPC codes with Gallager's iterative decoding algorithm. Generalizing these notions to quantum codes seems a promising way, and has indeed been proposed recently [9]. The approach promoted by these authors is to define quantum LDPC codes using a subclass of stabilizer codes, namely the CSS codes, which can be constructed from a couple of classical binary codes, each of them containing the dual of the other. MacKay *et al.* have shown that it is possible to find sparse classical binary codes which meet this property and use them for defining quantum LDPC codes. Several other papers have followed the same approach by constructing sparse CSS codes, namely [8], [7].

Our work is aimed at improving the aforementioned codes by finding other constructions of LDPC quantum codes using the more general family of stabilizer codes. While a brief introduction to stabilizer codes is provided below, we would like to pinpoint here the main difficulty for finding LDPC stabilizer codes. As explained in [3], every stabilizer code can be viewed as a code over $\mathbb{F}_4$, the field with four elements. However, the converse is not true: to correspond to valid stabilizer codes, these codes must be self-orthogonal for some hermitian trace inner product. Fulfillment of this peculiar constraint makes the usual constructions of LDPC codes useless in the quantum setting.

Our work provides a partial solution to this problem by defining such codes through a group theoretical construction (see Section III). The resulting codes can be viewed as quantum analogues of regular Gallager codes: each qubit is involved in the same number of "parity-check equations", and each parity-check equation involves the same number of qubits. We have decoded these codes with an iterative decoding algorithm applied to a certain Tanner graph associated to our construction and present the results of these numerical simulations in Section V.

1-4244-1429-6/07/$25.00 ©2007 IEEE

II. STABILIZER CODES

An $[n,k]$ quantum code is a subspace of dimension 2^k of the Hilbert space $\mathcal{H}_n \cong (C^2)^{\otimes n}$ of n qubits. Such a space allows to encode k qubits and the rate of this code is defined to be $\frac{k}{n}$. While defining such code subspace can be done in many different ways, a particularly useful method is known as the stabilizer formalism, which we now briefly review [6].

Preliminaries: Stabilizer codes rely heavily on properties of $\mathcal{G}_n$, the n-qubit Pauli group. This group is defined in terms of the Pauli matrices for a single qubit: $\mathcal{I} = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \mathcal{X} = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \mathcal{Y} = \left(\begin{smallmatrix}0&-i\\i&0\end{smallmatrix}\right), \mathcal{Z} = \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$. The group $\mathcal{G}_n$ is the multiplicative group generated by the n-fold tensor products of single qubit Pauli matrices. The crucial fact about $\mathcal{G}_n$, is that any pair of elements either commutes or anti-commutes.

For our purpose here, phases are irrelevant and it will be more convenient to work with the effective Pauli group $G_n \stackrel{\text{def}}{=} \mathcal{G}_n / \{\pm\mathcal{I}^{\otimes n}; \pm i\mathcal{I}^{\otimes n}\}$ (see [3]). There are 4 elements in G_1 which are $[\mathcal{I}]$, $[\mathcal{X}]$, $[\mathcal{Y}]$, and $[\mathcal{Z}]$. Here, $[\mathcal{P}]$ denotes the equivalence class of $\mathcal{P} \in \mathcal{G}_n$, that is $\{\pm\mathcal{P}, \pm i\mathcal{P}\}$.

Definition of the code subspace: The code subspace C of an $[n,k]$ stabilizer code is the largest subspace stabilized by the action of $\mathcal{S}$, an Abelian subgroup of $\mathcal{G}_n$. If $-\mathcal{I}^{\otimes n} \notin \mathcal{S}$ and if $\mathcal{S}$ is generated by $n-k$ independent operators $\mathcal{S}_j$, then the associated code is of rate $\frac{k}{n}$. The code subspace is equivalently defined by $n-k$ eigenvalue equations: $|\psi\rangle \in C$ if and only if $\forall j \in \{1,\ldots,n-k\},\ \mathcal{S}_j |\psi\rangle = |\psi\rangle$. It is sufficient to represent the set of generators of the stabilizer group $\{\mathcal{S}_j\}_j$ by the set of equivalence classes $\{S_j\}$ where $S_j = [\mathcal{S}_j]$ which generate a subgroup S of G_n. Using a slight abuse in terminology, we also call S the stabilizer group of the code and $\{S_j\}_j$ the stabilizer set of the code.

Error model: Since any error recovery procedure is a linear operation, it is sufficient to describe it for an error basis. This basis can be chosen to be the set of elements $\mathcal{E}^1 \otimes \mathcal{E}^2 \otimes \cdots \otimes \mathcal{E}^n$, where the $\mathcal{E}^i$'s belong to $\{\mathcal{I}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$. An error $\mathcal{E}$ is viewed as an element of $\mathcal{G}_n$ which acts on a vector $|\psi\rangle$ of the code subspace. The *depolarizing channel with crossover probability* p is an error model where the $\mathcal{E}_i$'s are chosen independently of each other, $\mathcal{E}^i$ being equal to $\mathcal{I}$ with probability $1-p$ and $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ with probability $p/3$. The *quantum erasure channel with erasure probability* p is an error model where each qubit is erased with probability p and the receiver knows which qubit has been erased or not. When the i-th qubit is erased, $\mathcal{E}^i$ is equal to $\mathcal{I}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$, each with probability $1/4$ and when it is not, $\mathcal{E}^i$ is equal to $\mathcal{I}$.

Capacity: Similarly to the classical setting, there is a notion of capacity. For a given quantum channel it is the supremum of the rate of a quantum code with fidelity arbitrarily close to 1 after decoding as the length goes to infinity. There is basically just one non-classical channel where the capacity is known exactly, namely the quantum erasure channel which has capacity $1-2p$ [2]. Even for the depolarizing channel there are only lower and upper bounds which do not match. It is known [1] that its capacity is greater than $1 + p\log_2 p + (1-p)\log_2(1-p) - p\log_2 3$. On the other hand, the no-cloning theorem implies that for $p \geq \frac{1}{4}$, the capacity is equal to 0.

Syndrome measurement: It is readily checked that for a stabilizer code, there are physical measurements revealing the binary vector $s(\mathcal{E}) = (s_1(\mathcal{E}), \ldots, s_{n-k}(\mathcal{E}))$, where $s_i(\mathcal{E})$ is equal to 0 iff $\mathcal{S}_j$ and $\mathcal{E}$ commute and to 1 otherwise. $s(\mathcal{E})$ is called the *syndrome* of $\mathcal{E}$. This allows to cast errors in three categories: (i) the *detectable errors* which have non-zero syndrome; (ii) the *harmless undetectable errors* which have zero syndrome, but belong to $\mathcal{S}$; (iii) the *harmful undetectable errors* which have zero syndrome, those that belong to $N(\mathcal{S}) - \mathcal{S}$, where $N(\mathcal{S})$ is the normalizer of $\mathcal{S}$.

Minimum distance: It is defined as the smallest Hamming weight of a harmful undetectable error.

Stabilizer codes as codes over $\mathbb{F}_4$: For the purpose of establishing a correspondance between quantum and classical codes, it is useful to view stabilizer codes as codes over $\mathbb{F}_4$ [3]. This duality is due to the additive structure of $\mathbb{F}_4$ which echoes the additive structure of the effective Pauli group G_1. The mapping between them is given by $[\mathcal{I}] \leftrightarrow 0$, $[\mathcal{X}] \leftrightarrow \omega$, $[\mathcal{Z}] \leftrightarrow \bar{\omega}$ and $[\mathcal{Y}] \leftrightarrow 1$, where $\bar{\omega} \stackrel{\text{def}}{=} \omega^2$ is the conjugate of ω. Elements of G_n will in turn be associated to vectors of $\mathbb{F}_4^n$ in an obvious way. It can then be checked that two Pauli operators $\mathcal{P}$ and $\mathcal{Q}$ commute iff the two elements $\mathbf{P}$ and $\mathbf{Q}$ of $\mathbb{F}_4$ associated to $[\mathcal{P}]$ and $[\mathcal{Q}]$ satisfy $\mathbf{tr}(\mathbf{P}\bar{\mathbf{Q}}) = 0$, and anti-commute iff $\mathbf{tr}(\mathbf{P}\bar{\mathbf{Q}}) = 1$. Here, $\mathbf{tr}(\mathbf{U}) \stackrel{\text{def}}{=} \mathbf{U} + \bar{\mathbf{U}} = \mathbf{U} + \mathbf{U}^2$ is the trace operator in $\mathbb{F}_4$. This motivates the definition of the following inner product over $\mathbb{F}_4^n$:

$$\mathbf{U} \star \mathbf{V} \stackrel{\text{def}}{=} \mathbf{tr} \sum_{i=1}^{n} \mathbf{U}^i \bar{\mathbf{V}}^i.$$

The generators of a stabilizer code, when expressed as row-vectors of $\mathbb{F}_4^n$, form a matrix $\mathbf{S}$ which will be called a *parity-check matrix* of the stabilizer code. In the following, a row $\mathbf{S}_j$ of $\mathbf{S}$ is associated to the j-th element S_j of the stabilizer set. By construction, the rows of $\mathbf{S}$ are orthogonal with respect to the inner product "$\star$". The converse is also true: any $(n-k)\times n$ matrix over $\mathbb{F}_4$ with orthogonal rows defines a stabilizer code over n qubits.

We now review the complete correspondence between stabilizer codes and self-orthogonal codes over $\mathbb{F}_4$:
- An error $\mathcal{E}$ is associated to a vector $\mathbf{E}$ of $\mathbb{F}_4^n$;
- The stabilizer group S is associated to the vector space over $\mathbb{F}_2$ generated by $\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_{n-k}$—i.e. $\text{span}_{\mathbb{F}_2}\{\mathbf{S}_j\}$;
- The syndrome associated to an error $\mathcal{E}$ is the binary vector $(\mathbf{E} \star \mathbf{S}_i)_{i=1}^{n-k}$;
- Harmless undetectable errors are associated to elements of $\mathbb{F}_4^n$ with zero syndrome and belonging to $\text{span}_{\mathbb{F}_2}\{\mathbf{S}_j\}$;
- Harmful undetectable errors are associated to elements of $\mathbb{F}_4^n$ with zero syndrome which do not belong to $\text{span}_{\mathbb{F}_2}\{\mathbf{S}_j\}$;
- A successful decoding of the error $\mathcal{E}$ is reached when the decoding algorithm outputs an error vector $\mathbf{E}'$ such that $\mathbf{E}+\mathbf{E}'$ is a harmless undetectable error, that is $\mathbf{E}+\mathbf{E}' \in \text{span}_{\mathbb{F}_2}\{\mathbf{S}_j\}$.

[1] Actually a slightly better bound holds from [13], [14], but the improvement is quite small.

Quantum LDPC codes: With this definition of parity-check matrix for stabilizer codes, it is natural to define quantum LDPC codes as stabilizer codes which have a sparse parity check matrix. In this article we are going to construct regular LDPC codes.

Definition 1: A quantum regular LDPC code of type (a, b) is a stabilizer code which has a parity-check matrix $\mathbf{S}$ with a non-zero entries per column and b non-zero entries per row. When the number of ω's, $\bar{\omega}$'s and 1's is fixed per column, and equal respectively to $a_\omega, a_{\bar{\omega}}, a_1$ we say that it is of detailed type $([a_\omega, a_{\bar{\omega}}, a_1], b)$.

III. A GENERIC CONSTRUCTION OF (a, b) QUANTUM LDPC CODES

In the following we restrict our attention to quantum LDPC codes having only two kind of non-zero entries, ω and $\bar{\omega}$.

Generic construction of the Tanner graph of (a, b) quantum LDPC codes: We use the following Tanner graph associated to a parity check matrix $\mathbf{S}$. It is a bipartite graph with vertex set $A \cup B$, where A is the set of variables nodes (i.e. the qubits of the code, or the columns of $\mathbf{S}$) and B is the set of check nodes (i.e. the generators of the stabilizer group, or the rows of $\mathbf{S}$). There is an edge between $\alpha \in A$ and $\beta \in B$ iff the corresponding entry in $\mathbf{S}$, that is $\mathbf{S}^\alpha_\beta$ is non zero. We label this edge with the entry $\mathbf{S}^\alpha_\beta$.

We start our construction by choosing a group G with cardinality equal to a multiple of the length of the code we are interested in. Then we choose two subgroups H and K of G, with $|K| \geq |H|$. The cosets xH are associated to variable nodes whereas the cosets yK are associated to check nodes. In other words, the length n and the number of rows $n-k$ in the parity check matrix are given by $n = \frac{|G|}{|H|}$ and $n-k = \frac{|G|}{|K|}$.

We then pick up a set of generators Γ of G which can be partitioned into two sets $\Gamma = \Gamma_\omega \cup \Gamma_{\bar{\omega}}$ satisfying the 3 following properties:

$$(\Gamma_\omega)^{-1} = \Gamma_\omega, \quad (\Gamma_{\bar{\omega}})^{-1} = \Gamma_{\bar{\omega}}; \tag{1}$$

$$\forall (g_\omega, g_{\bar{\omega}}, h) \in \Gamma_\omega \times \Gamma_{\bar{\omega}} \times H, \exists (h', k', k'') \in H \times K^2 \text{ s.t.,}$$

$$h g_\omega k' g_{\bar{\omega}} = g_{\bar{\omega}} k'' g_\omega h'; \tag{2}$$

$$hgk = h'g'k', g, g' \in \Gamma, h, h' \in H, k, k' \in K, \implies g = g'. \tag{3}$$

We put an edge between xH and yK iff there exists a $g \in \Gamma$ such that $xHg \cap yK \neq \emptyset$, or equivalently iff there exist $h \in H$, $k \in K$ and $g \in \Gamma$ such that $y = xhgk$. We label this edge with ω if the corresponding g belongs to Γ_ω and with $\bar{\omega}$ otherwise. It can be checked that the degree of any vertex xH is equal to $a \stackrel{\text{def}}{=} \sum_{g \in \Gamma} \frac{|H|}{|H_g \cap K|}$ and the degree of any vertex yK is equal to $b \stackrel{\text{def}}{=} \sum_{g \in \Gamma} \frac{|K|}{|H_g \cap K|}$, where $H_g \stackrel{\text{def}}{=} g^{-1} H g$. This is a simple consequence of

Lemma 1: H_g is a subgroup of G and either $xH_g \cap yK = \emptyset$ or $xH_g \cap yK = z(H_g \cap K)$ for some $z \in G$.

Soundness of the construction: This defines the Tanner graph of our stabilizer code and therefore also its parity-check matrix. The point of this construction is that property (2), which expresses some weak commutation of g_ω and $g_{\bar{\omega}}$ modulo elements of H and K, implies the orthogonality of the rows of the associated parity-check matrix (so that it represents a valid parity-check matrix of a stabilizer code). Property (3) is used to show that there are no multiples edges in the graph.

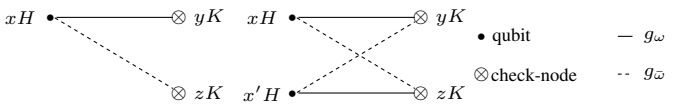


Fig. 1. Subgraph showing that each qubit xH of the second type (involved in the $\mathbf{S}_i$ corresponding to yK with an ω and in the $\mathbf{S}_j$ corresponding to zK with an $\bar{\omega}$) is necessarily part of a 4-cycle with another qubit of the second type.

Proposition 1: The parity-check matrix $\mathbf{S}$ associated to the Tanner graph given by this construction has orthogonal rows.

Proof: Given two rows $\mathbf{S}_i$ and $\mathbf{S}_j$ of $\mathbf{S}$, the set of qubits can be partitioned in two classes : qubits k for which $\mathbf{S}^k_i \star \mathbf{S}^k_j = 0$ and those for which $\mathbf{S}^k_i \star \mathbf{S}^k_j = 1$. $\mathbf{S}_i$ and $\mathbf{S}_j$ are orthogonal iff the number of qubits of the second type is even. Equivalently, and this is how our construction is tailored, we must show that qubits of the second type can be paired together.

Consider a qubit belonging to the second class; say it corresponds to xH and that rows $\mathbf{S}_i$ and $\mathbf{S}_j$ correspond to yK and zK. Then necessarily one of these two rows has an ω at the entry corresponding to xH and the other one has an $\bar{\omega}$. W.l.o.g. we may assume that the subgraph of the Tanner graph induced by xH, yK and zK is as in Fig. 1

In other words there exist $g_\omega \in \Gamma_\omega$, $g_{\bar{\omega}} \in \Gamma_{\bar{\omega}}$ such that $xHg_\omega \cap yK \neq \emptyset$ and $xHg_{\bar{\omega}} \cap zK \neq \emptyset$. That is, there exist h_1, h_2 in H and k_1, k_2 in K such that

$$\begin{aligned} y &= x h_1 g_\omega k_1 \\ z &= x h_2 g_{\bar{\omega}} k_2. \end{aligned}$$

From Property 2, there exists $(h', k', k'') \in H \times K^2$ such that, $h_1 g_\omega k' g_{\bar{\omega}} = h_2 g_{\bar{\omega}} k'' g_\omega h'$. Let $x' \stackrel{\text{def}}{=} x h_1 g_\omega k' g_{\bar{\omega}}$, then we have the following equalities:

$$\begin{aligned} x' g_{\bar{\omega}}^{-1} k'^{-1} k_1 &= x h_1 g_\omega k' g_{\bar{\omega}} g_{\bar{\omega}}^{-1} k'^{-1} k_1 = y, \\ &\text{and} \\ x' h'^{-1} g_\omega^{-1} k''^{-1} k_2 &= x h_1 g_\omega k' g_{\bar{\omega}} h'^{-1} g_\omega^{-1} k''^{-1} k_2 \\ &= x h_2 g_{\bar{\omega}} k'' g_\omega h' h'^{-1} g_\omega^{-1} k''^{-1} k_2 \\ &= z. \end{aligned}$$

This implies that there is an edge labeled by $\bar{\omega}$ between $x'H$ and yK, and an edge labeled ω between $x'H$ and zK, i.e. xH and $x'H$ are involved in a 4-cycle (see Fig. 1. Using property (3), it is easy to show that qubits of the second type are paired in a unique fashion through the 4-cycles described above. ∎

IV. ON THE NECESSITY OF HAVING 4-CYCLES IN THE TANNER GRAPH

It can be noticed that there are 4-cycles in the construction we suggest. Indeed, we wish to point out that this is not a characteristic of our construction, but rather that *any* stabilizer code which detects all single qubit errors necessarily has a

Tanner graph with 4-cycles. This comes from the fact that: (i) in order to detect such errors, each column of the parity-check matrix must contain at least two different non-zero entries; and that (ii) two rows which differ in some position by having two different non-zero entries, must differ in the same way in at least one other position in order to commute.

It will be convenient to bring in the following definition.

Definition 1: The *4-cycle graph* associated to a Tanner graph is the graph with vertex set the qubits and with edges connecting two qubits each time they are involved in a 4-cycle in the Tanner graph.

For several examples, the (a, b) quantum LDPC codes we construct are of detailed type $([a/2, a/2, 0], b)$. Point (ii) above implies that the vertices of the associated 4-cycle graph have *at least* degree $a^2/4$. A simple calculation shows that the examples we provide have 4-cycles graph which are $a^2/4$-regular. Therefore, they meet this lower bound for every vertex. On the contrary, quantum codes of detailed type $([a/2, a/2, 0], b)$ obtained from the CSS-construction based on dual-containing codes, as is the case in [9], have 4-cycle graphs of minimum degree at least $a^2/4+a(a/2-1)$, which is significantly larger.

This 4-cycle graph contains other useful information about the possible performance of the codes. For instance, one should avoid generators which involve qubits which induce a subgraph of the 4-cycle graph which has more than one connected component. Such a configuration yields a potentially harmful undetected error of small Hamming weight.

Lemma 1: Consider a row $\mathbf{S}_i$ of the parity-check matrix $\mathbf{S}$ of the code and the set of positions j such that $\mathbf{S}_i^j \neq 0$. A connected component of the subgraph of the 4-cycle graph induced by those j's yields an undetected error $\mathbf{E}$ of Hamming weight the size of the subgraph. This element is obtained by giving at each qubit position j involved in the subgraph its value taken by $\mathbf{S}_i$, that is $\mathbf{S}_i^j$ and 0 elsewhere.

Proof: We just have to prove that $\mathbf{E}$ is orthogonal to each row of $\mathbf{S}$. First of all, it is orthogonal to $\mathbf{S}_i$. Second, it obviously commutes with all rows $\mathbf{S}_j$ which have no overlap with $\mathbf{E}$. Third, consider an $\mathbf{S}_j$ which overlaps with $\mathbf{E}$ at position k. All the positions of overlap between $\mathbf{S}_i$ and $\mathbf{S}_j$ are adjacent to k in the subgraph of the 4-cycle graph, thus they are also in $\mathbf{E}$. Since $\mathbf{S}_i$ and $\mathbf{S}_j$ are orthogonal, $\mathbf{E}$ and $\mathbf{S}_j$ are also orthogonal. ∎

V. Results

We present simulation results of several quantum LDPC codes under iterative decoding (namely the SUM-PRODUCT algorithm applied to their Tanner Graph in their syndrome decoding form) on the depolarizing channel and the quantum erasure channel. We use here two different groups as ingredients in our construction.

$\mathbb{I}$ is here a generic notation for the identity of a group. The group it refers to will depend on the context. The first one is a semi-direct product $\mathbb{Z}/30\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, which has for presentation $\{\rho, \tau \mid \rho^{30} = \tau^2 = \mathbb{I}, \tau\rho\tau = \rho^{19}\}$. The last group $\mathcal{S}_4$ is the symmetric group on 4 elements. We use these groups in the following constructions :

Code A of type (6,12):
-length : 34560, rate $1/2$,
-$G = \mathcal{S}_4 \times \mathbb{Z}/30\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4$.
-$H = \{\mathbb{I}\}$ and $K = \{\mathbb{I}, u\}$ with $u = ((2,3), \tau, (2,3))$
- $\Gamma_\omega = \{g_1, g_1^{-1}, g_2\}$,with $g_2^2 = \mathbb{I}$, $g_1 = \big((1,2,3), \rho^5, \mathbb{I}\big)$, and $g_2 = \big((1,4), \rho^3\tau, \mathbb{I}\big)$
- $\Gamma_{\bar\omega} = \{g_3, g_3^{-1}, g_4\}$,with $g_4^2 = \mathbb{I}$, $g_3 = \big(\mathbb{I}, \rho^{10}, (1,2,3)\big)$ and $g_4 = \big(\rho^6\tau, \mathbb{I}, (1,4)\big)$.
Code B of type (8,16):
-length : 34560, rate $1/2$,
-$G = \mathcal{S}_4 \times \mathbb{Z}/30\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4$.
-$H = \{\mathbb{I}\}$ and $K = \{\mathbb{I}, u\}$ with $u = ((2,3), \tau, (2,3))$
- $\Gamma_\omega = \{g_1, g_2, g_1^{-1}\}$,with $g_2^2 = \mathbb{I}$, $g_1 = \big((1,2,3,4), \rho^5, \mathbb{I}\big)$, $g_2 = \big((1,4), \rho^3\tau, \mathbb{I}\big)$,
- $\Gamma_{\bar\omega} = \{g_3, g_4, g_5, g_3^{-1}, g_4^{-1}\}$,with g_3=$\big(\mathbb{I}, \rho^{10}, (1,2,3,4)\big)$, $g_4 = \big(\mathbb{I}, \rho^3\tau, (1,3,4)\big)$ and $g_5 = \big(\mathbb{I}, \rho^6\tau, (1,4)\big)$. Note that $g_5^2 = \mathbb{I}$. In the last example, the Tanner graph displays some irregularity, it is of detailed type $([3,5,0], 16)$.

Code C : The two previous codes have been found to be of distance 12. There is a simple way to increase the minimum distance by using concatenation which works in the same way as classical concatenated codes. We refer to [10], [4] for more details about this topic. We found it useful to concatenate the previous code B with a quantum generalization of the parity-code of length 4 given by the parity-check matrix

$$\begin{pmatrix} \omega & \omega & \omega & \omega \\ \bar\omega & \bar\omega & \bar\omega & \bar\omega \end{pmatrix}$$

The inner code is the code of length 4 and the outer code is B. The length of the concatenated code is the product of the lengths, namely 138240 and the rate the product of the rates, that is $\frac{1}{4}$.

Such a code can be decoded in the same way as classical serial turbo-codes. Its quantum version has been presented in [10].

The following figures display the performances of iterative decoding of these codes over the erasure channel(resp. the depolarizing channel). We plot here the block error after iterative decoding against the erasure probability (resp. crossover probability) of the channel.

Fig. 2. Performances of A and B over the erasure channel

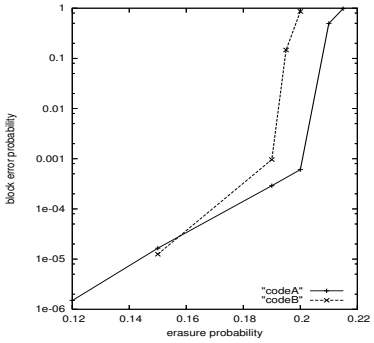


Fig. 3. Performances of A and B over the depolarizing channel

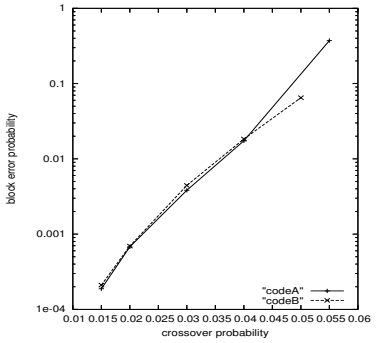
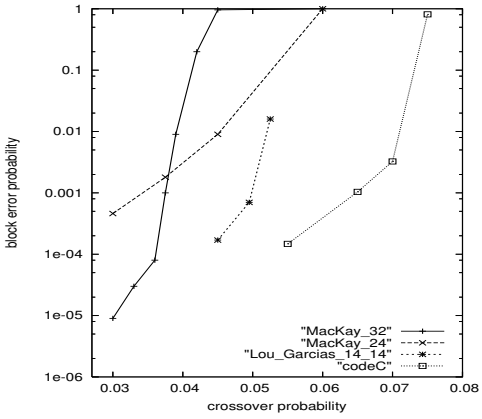


Fig. 4. Performances of C against the performances of other codes of rate $\frac{1}{4}$ taken from [8], [9]



Several remarks can be made here

1) The erasure probability threshold is slightly below 0.2 for the$(8, 16)$-code and slightly above 0.2 for the $(6, 12)$-code. This should be compared with the erasure probability that the best codes of rate $\frac{1}{2}$ can sustain which is 0.25.
2) Code A and B given here show an error-floor which starts at block error probability of order 10^{-4}. This is due to the fact that they all turned out to have a minimum distance which is 12.
3) Code A and B have a rather good block error probability for a crossover probability in the range $(0.05 - 0.055)$. This has to be compared with the crossover probability threshold for random stabilizer codes of rate $\frac{1}{2}$ which is of about 0.0743. Code C gives better performances than the codes of the same rate given in [8], [9].

VI. Conclusion

The quantum $(6, 12)$ and $(8, 16)$-codes of rate $\frac{1}{2}$ constructed here look very much like quantum analogs of classical $(3, 6)$ Gallager codes in terms of the noise values they sustain for moderate block error probabilities (say in the range $(10^{-3}, 10^{-1})$) both on the quantum erasure channel and on the quantum depolarizing channel. They already display quite respectable performances in this range. Unfortunately, the error floor starts much earlier in our case than for the classical $(3, 6)$-code and is due to the rather small minimum distance of our codes. This does not seem to be an unavoidable problem of our general construction. It seems to be due to the particular choice of groups and group generators. It might be quite interesting to study whether a clever choice of families of groups and group generators would yield a linear minimum distance. The quantum LDPC codes constructed in this article also have associated Tanner graphs with several cycles of size 4 (but this was also the case in [8], [9]). However, it should be emphasized that this is not due to the particular construction chosen here, but that it is a characteristic of all stabilizer codes. This affects iterative decoding performances when the usual SUM-PRODUCT or MIN-SUM algorithm is used. It would be interesting to study how variants of this algorithm (see [15] for instance) would overcome this problem.

Finally, we would like to point out that quantum LDPC codes might be good candidates for constructing fault-tolerant architectures. First, we hope that the minimum distance of these codes increases linearly with the block size, as it is the case for most classical LDPC codes. This would warrant that any finite weight error can be corrected for sufficiently large block sizes. Second, the rate of such codes does not decrease to zero, thus possibly improving the overhead requirements over schemes employing concatenation or toric codes [5].

References

[1] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error rate. In *Proc. 29th. Ann. ACM Symp. on Theory of Computing*, 1997. Longer version quant-ph/9906129.
[2] C.H. Bennett, D.P. DiVincenzo, and J.A. Smolin. Capacities of quantum erasure channels. *Phys. Rev. Lett.*, 78:3217, 1997.
[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44:1369, 1998.
[4] T. Camara, H. Ollivier, and J.-P. Tillich. Construction and performance of classes of quantum ldpc codes, 2005.
[5] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *J. Math. Phys.*, quant-ph/0110143(9):4452–4505, 2002.
[6] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, Pasadena, CA, 1997.
[7] L. Ioffe and M. Mézard. Asymmetric quantum error correcting codes, 2006.
[8] H. Lou and J. Garcia-Frias. On the application of error-correcting codes with low-density generator matrix over different quantum channels. In *Proceedings of Turbo-coding 2006*, Munich, April 2006.
[9] D. J. C. MacKay, G. Mitchison, and P. L. McFadden. Sparse graph codes for quantum error-correction. *IEEE Trans. Info. Theory*, 50(10):2315–2330, 2004.
[10] H. Ollivier and J.-P. Tillich. Interleaved serial concatenation of quantum convolutional codes: gate implementation and iterative error estimation algorithm. In *Proceedings of the 26th Symposium on Information Theory in the Benelux*, Brussels, Belgium,, 2005.
[11] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In S. Goldwasser, editor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124–134, Los Alamitos, CA, 1994. IEEE Computer Society.
[12] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:2493, 1995.
[13] P. W. Shor and J. A. Smolin. Quantum error-correcting codes need not completly reveal the error syndrome, 1996.
[14] G. Smith and J.A. Smolin. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space, 2006.
[15] J. S. Yedidia, W. T. Freeman, and Y. Weiss. Constructing free energy approximations and generalized belief propagation algorithms. Technical Report TR2004-40, Mitsubishi Electric Research Laboratories, 2004.