Quantum turbo codes with unbounded minimum distance and excellent error-reducing performance

Mamdouh Abbara*, Jean-Pierre Tillich*
* INRIA, Equipe Secret, Domaine de Voluceau BP 105, F-78153 Le Chesnay cedex, France.

***Abstract*— We construct here a new family of quantum codes related to serial turbo-codes which are excellent error-reducing codes under iterative decoding for very large channel noise values. Moreover we also show that this family of codes has unbounded minimum distance.**

I. INTRODUCTION

Quantum codes suitable for iterative decoding. Turbo-codes [1], LDPC codes [2] and their variants are one of the most satisfying answer to the problem of devising codes promised by Shannon's theorem. They display outstanding performances for a large class of error models with a decoding algorithm of reasonable complexity. Generalizing these codes to the quantum setting seems a promising way to efficiently approach the quantum capacity, and quantum generalizations of LDPC codes have indeed been proposed in [3].

However, it has turned out that the design of high performance quantum LDPC codes is much more complicated than in the classical setting. In particular, most constructions suggested in the literature [4], [3], [5], [6], [7], [8], [10], [11], [12] suffer from having a bounded minimum distance. There are a few exceptions, namely [9] or quantum LDPC codes based on tessellations of surfaces which have been proposed in [13], [14], [15]. The latter family provides for instance quantum LDPC codes with non vanishing rate and logarithmic minimum distance. More recently, quantum LDPC codes with non vanishing rate and minimum distance growing like the square root of the block length have been proposed [16]. However in all these constructions, unlike in the classical setting, there are issues with the decoder. The Tanner graph associated to a quantum LDPC code necessarily contains many 4-cycles which are well known for their negative effect on the performances of iterative decoding. Moreover, quantum LDPC codes are by definition highly degenerate but their decoder does not exploit this property, rather it is impaired by it, see [17].

On the other hand, generalizing turbo-codes to the quantum setting first requires a quantum analogue of convolutional codes. These have been introduced in [18], [19], [20] and followed by further investigations [21], [22]. Quantum turbo-codes can be obtained from the interleaved serial concatenation of convolutional codes. This idea was first introduced in [23]. There, it was shown that, on memoryless Pauli channels, quantum turbo-codes can be decoded similarly to classical serial turbo-codes. The construction given in [23] had rather poor performance under iterative decoding. In [24] it was shown that it was possible to come up with quantum turbo-codes with good performance under iterative decoding. However, the families of codes constructed in this article have bounded minimum distance and the performance of these codes degrades for large blocklength. It was even proved there that it is not possible to obtain quantum serial turbo-codes with unbounded minimum distance and with an iterative decoding algorithm which converges. For this, we should have quantum convolutional encoders which are at the same time non-catastrophic (to ensure convergence of iterative decoding) and recursive (to avoid having bounded minimum distance). Unfortunately such codes do not exist [24].

A new approach. Our purpose is to present here a modification of the construction presented in [24] to meet both requirements, namely good performance under iterative decoding and unbounded minimum distance. Our strategy for achieving this goal can be described as follows. In order to obtain families of codes with unbounded minimum distance we first choose in the quantum serial turbo-construction a recursive inner encoder. Because of the non existence result of [24], such an encoder will necessarily be catastrophic and the standard iterative decoding algorithm will be helpless in this case : due to its catastrophicity, in the first iteration the inner code is unable to pass useful information to the outer code, which in turn is not able to pass a better information to the inner code and so on and so forth.

We circumvent this problem by changing a little bit the structure. First, we do not feed all qubits of the outer code into the inner encoder. A small fraction of these qubits will be sent directly to the channel. We also choose in an appropriate way the outer code in such a way that the first decoding iteration of the outer code is able to pass useful information to the inner code. It turns out that the structure which is needed at the outer code in order to decrease the noise level at the first iteration also prevents the iterative decoding to converge to zero. Actually, the codes we obtain from our approach will be excellent error-reducing codes : they are able to reduce the noise level of the channel up to a tiny fraction of noise and this even under very bad channel conditions. They are able to operate at noise levels for which the only known quantum codes of reasonable decoding complexity operating successfully at this regime are families of codes with vanishing rate, such as for instance the toric codes [25], [26]. This is not the case in our construction, since we have a fixed rate of $\frac{1}{8}$.

However, our codes are not error-correcting codes when decoded by standard iterative decoding: when the block size tends to infinity, the block error goes to one. On the other hand, the minimum distance of this family is unbounded. We prove that most of these codes have minimum distance at least $\Omega\left(\frac{\log n}{\log\log n}\right)$, where n stands for the code length. It would be interesting to study whether or not the few remaining qubits which are still in error after iterative decoding could be corrected by changing the decoding procedure.

II. Stabilizer codes

Quantum LDPC codes were constructed by using the stabilizer code construction [27], [28]. We also use this construction for the variant of quantum turbo-codes we suggest here. We recall in this section a few facts about this construction. We depart slightly from the classical way of presenting these codes since we need to address for turbo-codes encoding issues. The style of presentation we adopt here is to suit a readership familiar with classical codes but not with quantum information theory.

Let us recall that the trace hermitian inner product between $E = (E_i)_{1\leq i\leq n}$ and $F = (F_i)_{1\leq i \leq n}$ in $\mathbb{F}_4^n$ is given by:

$$E \star F \triangleq \sum \operatorname{Tr} E_i \bar{F}_i, \quad (1)$$

where $\bar{u} = u^2$ and $\operatorname{Tr} u = u + \bar{u}$ for u in $\mathbb{F}_4$. For a set $C \subset \mathbb{F}_4^n$ we denote by $C^\perp$ the set $\{E \in \mathbb{F}_4^n | E \star F = 0,\ \forall F \in C\}$. A stabilizer code is defined by

Definition 1 (stabilizer code): Any $(n-k)\times n$ matrix over $\mathbb{F}_4$ whose rows are independent over $\mathbb{F}_2$ and orthogonal with respect to the trace hermitian inner product defines a stabilizer code of length n and rate $\frac{k}{n}$. It is called a parity-check matrix for the stabilizer code. Such a code is said to be of type $[[n,k]]$. The associated stabilizer group is the group generated by the rows of the parity-check matrix.

An important property which allows to speak about the stabilizer group of a stabilizer code is that

Property 1: Two parity-check matrices with the same stabilizer group define the same stabilizer code.

We refer to [24] for further explanations about how such a discrete object defines a continuous space encoding k qubits by embedding it into a larger n-qubit system. We call this space the *continuous stabilizer code*. Such codes are tailored to correct errors belonging to $\mathbb{F}_4^n$. An important error model is here

Definition 2 (Depolarizing channel): The depolarizing channel on n qubits of error probability p picks up an element $E \in \mathbb{F}_4^n$ by choosing randomly the coordinates E_i of E independently of each other according to $\mathbf{P}(E_i = 0) = 1-p, \mathbf{P}(E_i = 1) = \mathbf{P}(E_i = \omega) = \mathbf{P}(E_i = \bar{\omega}) = \frac{p}{3}$.

Moreover, there is a quantum measure associated to any parity-check matrix for the stabilizer code which enables to gain information on the error which has affected the quantum system. Its outcome belongs to $\mathbb{F}_2^{n-k}$ and is defined by

Definition 3 (error syndrome): The error syndrome associated to an error $E = (E_i)_{1\leq i\leq n} \in \mathbb{F}_4^n$ with respect to a parity-check matrix H with rows $H_1, \dots, H_{n-k}$ is the binary vector

$$s(E) \triangleq (E \star H_i)_{1\leq i\leq n-k}.$$

Apart from the fact that the rows of the parity-check matrix have to satisfy the aforementioned orthogonality conditions there is another fundamental difference with the classical setting. It can be checked that not all errors change the quantum state belonging to a stabilizer code. More precisely

Fact 1: The set of errors which leaves the continuous stabilizer code invariant is given by its stabilizer group.

This fact has an important consequence, namely that maximum-likelihood decoding of a stabilizer code does not mean we look for the most likely error satisfying the syndrome which was measured, but we look for the *most likely coset* of the stabilizer group (see [24] for further information about this).

For a classical linear code the minimum distance of the code is equal to the minimum weight of an nonzero error of zero syndrome. The minimum distance of stabilizer codes is defined by

Definition 4 (minimum distance): The minimum distance of a stabilizer code is the minimum Hamming weight of an error with zero syndrome which does not belong to the stabilizer group.

With this definition of the minimum distance it is readily seen that a stabilizer code of minimum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors by choosing the error of minimum Hamming weight satisfying the syndrome.

Turbo-codes are defined in the classical setting with the help of convolutional codes and their properties are strongly related to the way the constituent convolutional codes are encoded. To generalize these notions properly to the quantum setting we need a notion of encoding matrix and a suitable definition of a quantum convolutional code. An encoding matrix is given by

Definition 5 (encoding matrix): An encoding matrix with syndrome positions set $S \subset \{1,\dots,n\}$ (where $|S| = n-k$) for a stabilizer code of type $[[n,k]]$ and stabilizer group C_0 is any $2n\times n$ matrix over $\mathbb{F}_4$ with rows $\overline{X}_1, \overline{Z}_1, \dots, \overline{X}_n, \overline{Z}_n$ satisfying

(i) $\overline{X}_i \star \overline{Z}_j = \delta_{ij},\ \overline{X}_i \star \overline{X}_j = \overline{Z}_i \star \overline{Z}_j = 0$, where δ_{ij} stands for the Kronecker symbol,

(ii) $C_0 = <\overline{Z}_s, s \in S>$.

Convention 1: When the stabilizer positions set S is not specified we assume that $S = \{k+1,\dots,n\}$.

Notice that such an encoding matrix contains as a sub-matrix a parity-check of the stabilizer code, namely the matrix formed by the rows $\{\overline{Z}_s, s \in S\}$. If we define

$$X_i \triangleq (0\dots0 \underbrace{\omega}_{i\text{th position}} 0\dots0)$$

$$Z_i \triangleq (0\dots0 \underbrace{1}_{i\text{th position}} 0\dots0)$$

then

Definition 6 (Encoding transformation): The *encoding transformation* associated to an encoding matrix with rows $\{\overline{X}_1, \overline{Z}_1, \dots, \overline{X}_n, \overline{Z}_n\}$ is given by the $\mathbb{F}_2$-linear transformation which maps X_i to $\overline{X}_i$ and Z_i to $\overline{Z}_i$ for any $i \in \{1,\dots,n\}$.

Notice that this transformation preserves by definition the trace-hermitian inner product (since the X_i's and the Z_i's share the same orthogonality relations as the $\overline{X}_i$'s and the $\overline{Z}'_i s$). It allows to define the serial concatenation of two stabilizer codes, which is defined similarly as in the classical setting through the encoding procedure. More precisely the serial concatenation of two stabilizer codes is defined as follows.

Definition 7 (serial concatenation of two stabilizer codes): Consider two stabilizer codes of type $[[n^{\text{out}}, k^{\text{out}}]]$ and $[[n^{\text{in}}, k^{\text{in}}]]$ respectively which are such that $n^{\text{out}} = k^{\text{in}}$. The first one is called the outer code, whereas the second one is called the inner code. Choose for the inner code an encoding transformation U^{out} and for the outer code U^{in}. We assume that the set S^{in} of syndrome positions for U^{in} are the $n^{\text{in}} - k^{\text{in}}$ last positions. We denote the set of syndrome positions of the outer code by S^{out} and we extend U^{out} to $\widetilde{U^{\text{out}}}$ to act on $(\mathbb{F}_4)^{n^{\text{in}}}$ as follows. We view $(\mathbb{F}_4)^{n^{\text{in}}}$ as $(\mathbb{F}_4)^{n^{\text{out}}} \times (\mathbb{F}_4)^{n^{\text{in}}-n^{\text{out}}}$ and for $(E, F) \in (\mathbb{F}_4)^{n^{\text{out}}} \times (\mathbb{F}_4)^{n^{\text{in}}-n^{\text{out}}}$ we let

$$\widetilde{U^{\text{out}}}.(E, F) = (U^{\text{out}}.E, F).$$

Then the serial concatenation of the outer code and the inner code is the stabilizer code defined by the encoding transformation $U^{\text{in}}\widetilde{U^{\text{out}}}$ with syndrome positions set $S^{\text{in}} \cup S^{\text{out}}$.

A quantum convolutional code corresponds to the serial concatenation of a same encoding transformation shifted in time. More precisely

Definition 8 (Quantum convolutional code): A quantum convolutional code of type $((n, k, m))$ composed of N blocks and associated to a seed encoding transformation U acting on $\mathbb{F}_4^{n+m}$ with syndrome positions set S is a stabilizer code of type $[[Nn + m, Nk + m]]$ and
(i) encoding transformation given by $U_N U_{N-1} \dots U_1$ where the U_i's act on $\mathbb{F}_4^{Nn+m}$ as follows
we view elements of $\mathbb{F}_4^{Nn+m}$ as triples (E, F, G) in $\mathbb{F}_4^{n(i-1)} \times \mathbb{F}_4^{n+m} \times \mathbb{F}_4^{n(N-i)}$ and we let $U_i.(E, F, G) \triangleq (E, U.F, G)$,
(ii) stabilizer positions set $S_0 \cup \dots \cup S_{N-1}$ where $S_i = \{s + ni, s \in S\}$.

Finally we will also need the notion of quantum interleaver

Definition 9 (quantum interleaver): A quantum interleaver of size n is an encoding transformation U of the form

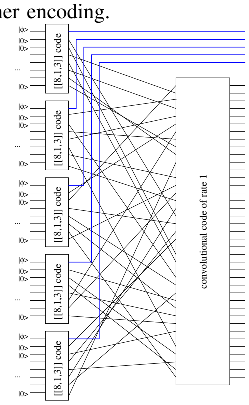
$$U.(E_1, \dots, E_n) = (f_1(E_{\pi(1)}), \dots, f_n(E_{\pi(n)}))$$

where π is a permutation of $\{1, \dots, n\}$ and the f_i's are permutations of $\mathbb{F}_4$ which leave 0 invariant.

III. The construction

Our construction is obtained from a particular form of interleaved concatenation of quantum stabilizer codes. It consists in taking in the serial concatenation:
(i) an outer quantum code of type $[[8K, K]]$ consisting in the juxtaposition of K identical stabilizer codes of type $[[8, 1]]$ and minimum distance 3. There is a position in this code of type $[[8, 1]]$ which has a special status.
(ii) an intermediate quantum interleaver of size $8K$ acting trivially on K positions which are precisely the union of the positions of each code of type $[[8, 7]]$ which have a special status.
(iii) an inner code which is a quantum convolutional code of type $((2, 2, 1))$ consisting of N blocks with N satisfying $2N + 1 = 7K$. The encoding transformation for this convolutional code acts only on the $7K$ positions corresponding to the $7K$ positions over which the quantum interleaver has (potentially) some non trivial action.

Fig. 1. The lines on the left-hand side carrying a $|0\rangle$ correspond to syndrome positions of the $[[8, 1]]$ code whereas the blue lines correspond to positions which have a special status and which do not participate in the quantum interleaver or in the inner encoding.



The concatenated code obtained in this way is therefore of type $[[8K, K]]$. Figure 1 illustrates the construction.

The $[[8, 1]]$ stabilizer code we use is given by the following parity-check matrix

$$\begin{pmatrix} \omega & \omega & 0 & 0 & 0 & 0 & 0 & 0 \\ \omega & 0 & \omega & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ \omega & 0 & 0 & \omega & 1 & 1 & \omega & 0 \\ 0 & 0 & 0 & 0 & \omega & 1 & 1 & \omega \\ 0 & 0 & 0 & \omega & 0 & \omega & 1 & 1 \\ 0 & 0 & 0 & 1 & \omega & 0 & \omega & 1 \end{pmatrix} \tag{2}$$

The first position is the distinguished position which participates neither in the subsequent interleaving nor in the inner encoding process. The crucial property which explains the choice of this code is the following fact

Proposition 1: Let $\mathscr{C}$ be the stabilizer code over 8 qubits defined by the parity-check matrix specified in (2) Let C_0 be its stabilizer group. The code is of minimum distance 3 and

$$P_1 \dots P_8 \in C_0^{\perp} \setminus C_0 \Rightarrow |\{i : P_i \neq 0, i \geq 2| \geq 3.$$

The reason of this choice will be given in what follows.

The interleaver is chosen at random whereas the convolutional code of type $((2, 2, 1))$ is given by the following seed transformation

$$\begin{array}{rcl}\overline{X}_1 & = & (\omega,\omega,\omega)\\ \overline{Z}_1 & = & (1,1,1)\\ \overline{X}_2 & = & (0,\omega,\omega)\\ \overline{Z}_2 & = & (1,1,0)\\ \overline{X}_3 & = & (\omega,0,\omega)\\ \overline{Z}_3 & = & (0,1,1)\end{array}$$

This encoder is recursive but also catastrophic in the sense of [24].

Ideas underlying the construction

As explained in the introduction, the issue with the construction considered in [24] is that the constituent convolutional encoders had to be chosen to be non catastrophic to make the iterative decoding scheme which is used there to work properly. This decoding algorithm basically consists in passing information back and forth between the inner and outer code. The decoding starts with the inner code and if a catastrophic encoder is chosen for the inner code, then the outer code gets no useful information at all, and in turn it is not able to give back any useful information to the inner code. Further explanations about iterative decoding of a concatenated scheme are provided in [24].

The slight modification what we consider here, namely by allowing certain qubits encoded by the outer code not to participate to the inner encoding changes the whole picture. Indeed, we can choose now an inner catastrophic encoder. This does not change the fact that at the first iteration of the decoding algorithm no useful information is passed from the inner decoder to the outer decoder (actually this first pass of the decoding can just be skipped), but the fact that now certain qubits of the outer code get some information coming from the channel model (these are precisely the K qubits which do not participate to inner encoding), allows the outer encoder to give some useful information to the inner encoder. This enables potentially the iterative decoding algorithm to converge to the right error. In other words, it is now possible to choose in this modified scheme an inner encoder which is recursive. This is a crucial issue if the purpose is to devise an interleaved concatenated code family with unbounded minimum distance.

We make another modification in the construction of [24], instead of choosing a convolutional encoder for the outer code we choose a small stabilizer code $\mathscr{C}$ which has minimum distance 3 and which satisfies Proposition 1. This is essential to obtain an unbounded minimum distance for the whole construction if we proceed as follows. The outer code will just be a juxtaposition of copies of $\mathscr{C}$. In each copy of $\mathscr{C}$ we will leave one qubit which will not be given to the inner encoder. The point which allows an unbounded minimum distance is the following property (we assume that it is the first position of $\mathscr{C}$ which does not participate in the subsequent inner encoding, that $\mathscr{C}$ is of length n and that C_0 is the stabilizer group of $\mathscr{C}$) there is no element $(P_1 P_2 \dots P_n)$ in $C_0^{\perp} \setminus C_0$ such that the Hamming weight of $(P_2, \dots, P_n)$ is less than 3. The code we have chosen is the smallest example we could find which meets such a property.

Finally, in order that the first decoding of the outer code to be able the reduce the noise level at the first iteration it is readily checked that there should be elements in the stabilizer group C_0 of the code which have weight 2 and which involve the position which is left out the inner encoding process. In our case there are three such elements. However, it is also readily checked that if we have such codewords, then it is not possible to reduce to 0 the noise level for the positions which are involved in these weight 2 words in C_0. Therefore, the very same reason which helps the first steps of iterative decoding is also the reason which prevents iterative decoding to reduce completely the noise level. This is why we obtain with this approach an error-reducing code family and not an error-correcting code family.

IV. Minimum distance properties

It turns out that the minimum distance of the concatenated scheme which is constructed here is unbounded. More precisely we have here

Theorem 1: Let α be any constant smaller than 1. Then the probability that the concatenated coding scheme defined in Section III is of minimum distance greater than $\alpha \frac{\log K}{\log \log K}$ goes to 1 as K goes to infinity.

To prove this result, we use the proof technique of [29] that investigates the minimum distance of classical serial turbo-codes. However, there are also new ingredients, for instance a new notion of detour and another way of counting elements in the orthogonal space $C_0^{\perp}$ to the convolutional code stabilizer group C_0. It relies on upper-bounds on the number of elements of $C_0^{\perp}$ of a certain form. The proof is too long to be included and we refer to [30] for a full proof.

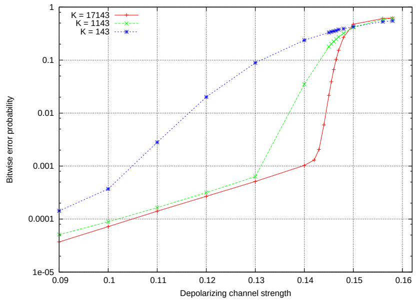
Let us just give here a few indications about what is going in our case. Let us denote the quantum convolutional inner encoding transformation by V and call the logical qubit positions all positions which are not syndrome positions. Denote by M the length of the inner convolutional code and by C_0 its stabilizer subgroup. For an element $(P_1 \dots P_M) \in \mathbb{F}_4^M$, we define its *logical weight* as the number of i's which are logical qubit positions for which P_i is different from 0. The *physical weight* of this element is just the total number of P_i's which are different from 0. An assignment of the logical positions is of type (w, d), if it is of logical weight w and if it is possible to assign the other positions such that the resulting element $P = P_1 \dots P_M$ if such that $P' = P.V$ belongs to $C_0^{\perp}$ and if P' is of physical weight d. With this definition we have

Proposition 2: For a given recursive convolutional encoder of type $((n, k, m))$ and total length M, there exists some constant η such that the number $a_{w,d}$ of assignments of logical positions of type (w, d) is upper bounded by

$$O\left(6^w \binom{M}{\lceil \frac{w}{2} \rceil} \binom{\eta n d + (2+\eta) n w}{\lfloor \frac{w}{2} \rfloor}\right).$$

Unlike in the classical setting, it turns out that we also need to prove in the quantum concatenated code scheme the dual

Fig. 2. Probability of error after decoding per qubit for various code lengths.



upper-bound

$$a_{w,d} = O\left(6^d \binom{N}{\lceil \frac{d}{2} \rceil} \binom{\eta n w + (2+\eta) n d}{\lfloor \frac{d}{2} \rfloor}\right). \qquad (3)$$

In the quantum setting, this dual upper-bound does not seem to be a consequence of the fact that the encoder is recursive. These two bounds can now be used in a similar way as in [29] to derive Theorem 1. The $\frac{\log n}{\log \log n}$ term which arises in Theorem 1 is somewhat unusual and is never encountered for classical codes. It is related to the fact that we count the number of elements of a certain weight in $C_0^\perp \setminus C_0$ and not $C_0^\perp \setminus \{0\}$.

However there are cases where this "dual" bound can be derived directly from Proposition 2. This happens for instance for the convolutional encoder of type $((2, 2, 1))$ we chose in Section III.

It is an open question to determine simple sufficient conditions which would ensure (3). This would enable to perform a computer search for such concatenated code schemes which would then have polynomial minimum distance with the hope of obtaining families of codes with record breaking performance under iterative decoding.

V. Results

We have implemented standard iterative decoding and run experiments on randomly chosen interleavers over the depolarizing channel (see Figure 2). We have fixed the number of iterations to be 30 and have observed a qubit error probability after decoding close to 10^{-3} for a depolarizing error probability of $p = 0.142$ and $K = 17143$. There is a threshold close to $p = 0.149$ below which the qubit error probability is a decreasing function of K.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near shannon limit error-correcting coding and decoding," in *ICC'93*, Genève, Switzerland, May 1993, pp. 1064–1070.

[2] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, Massachusetts: M.I.T. Press, 1963.

[3] D. J. C. MacKay, G. Mitchison, and P. L. MacFadden, "Sparse graph codes for quantum error-correction," *IEEE Trans. Info. Theor.*, vol. 50, no. 10, pp. 2315–2330, 2004.

[4] M. S. Postol, "A proposed quantum low density parity check code," 2001, available at `arXiv:quant-ph/0108131v1`. [Online]. Available: http://arxiv.org/abs/quant-ph/0108131

[5] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: construction and performances under iterative decoding," in *Proceedings of ISIT 2007*. Nice: IEEE, June 2007, pp. 811–815.

[6] J. Garcia-Frias and K. Liu, "Design of near-optimum quantum error-correcting codes based on generator and parity-check matrices of LDGM codes," in *Proceedings of CISS*, Princeton, Mar. 2008, pp. 562–567.

[7] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," in *Proc. IEEE Int. Symp. Info. Theo. (ISIT'07)*. Nice: IEEE, June 2007, pp. 806–811.

[8] I. B. Djordjevic, "Quantum LDPC codes from incomplete block designs," *IEEE Communication Letters*, vol. 12, no. 5, pp. 389–391, May 2008.

[9] S. A. Aly, "A class of quantum LDPC codes constructed from finite geometries," in *Proceedings of IEEE GLOBECOM 2008*, Dec. 2008, pp. 1–5.

[10] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Quantum quasi-cyclic low-density parity check codes," Mar. 2008, `arXiv:0803.0100v1 [quant-ph]`.

[11] P. Tan and J. Li, "Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions," *IEEE Trans. Info. Theor.*, vol. 56, no. 1, pp. 476–491, 2010.

[12] K. P. Sarvepalli, M.Rötteler, and A. Klappenecker, "Asymmetric quantum LDPC codes," in *Proceedings of ISIT 2008*, IEEE, Ed., Toronto, Canada, July 2008, pp. 305–309.

[13] M. H. Freedman, D. A. Meyer, and F. Luo, "$\mathbb{Z}_2$-systolic freedom and quantum codes," in *Mathematics of quantum computation*, ser. Chapman & Hall/CRC, Boca Raton, FL, 2002, pp. 287–320.

[14] I. H. Kim, "Quantum codes on Hurwitz surfaces," Master's thesis, MIT, 2007, available at `http://dspace.mit.edu/handle/1721.1/40917`.

[15] G. Zémor, "On Cayley graphs, surface codes and the limits of homological coding for quantum error correction," in *Coding and Cryptology, 2nd international Workshop IWCC 2009*, ser. LNCS, vol. 5557, 2009, pp. 259–273.

[16] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to $n^{\frac{1}{2}}$," in *Proceedings of ISIT 2009*, July 2009, pp. 799–803.

[17] D.Poulin and Y.Chung, "On the iterative decoding of sparse quantum codes," *Quantum Information and Computation*, vol. 8, p. 987, 2008. [Online]. Available: http://www.citebase.org/abstract?id=oai: arXiv.org:0801.1241

[18] H. F. Chau, "Quantum convolutional correcting codes," *Phys. Rev. A*, vol. 58, pp. 905–909, 1998.

[19] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, no. 17, p. 177902, 2003.

[20] ——, "Quantum convolutional codes: fundamentals," 2004.

[21] J. G. D. F. Jr., M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 865–880, 2007.

[22] M. Grassl and M. Rötteler, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proceedings of ISIT 2006*. IEEE, July 2006.

[23] 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, p. 149.

[24] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," *IEEE Trans. Info. Theor.*, vol. 55, no. 6, pp. 2776–2798, June 2009.

[25] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Ann. Phys.*, vol. 303, p. 2, 2003.

[26] G. Duclos-Cianci and D. Poulin, "Fast decoders for topological quantum codes," *Phys. Rev. Lett.*, vol. 104, no. 050504, 2010.

[27] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405–408, 1997.

[28] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, 1997.

[29] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proc. IEEE Int. Symp. Info. Theo. (ISIT'98)*, 1998, p. 31.

[30] M. Abbara and J. Tillich, "The minimum distance of classical and quantum turbo-codes," qu-phys arxiv, May 2011.