

Description of a quantum convolutional code

Harold Ollivier* and Jean-Pierre Tillich†

INRIA, Projet CODES, BP 105, F-78153 Le Chesnay, France

(Dated: February 1, 2009)

We describe a quantum error correction scheme aimed at protecting a flow of quantum information over long distance communication. It is largely inspired by the theory of classical convolutional codes which are used in similar circumstances in classical communication. The particular example shown here uses the stabilizer formalism, which provides an explicit encoding circuit. An associated error estimation algorithm is given explicitly and shown to maximize the likelihood over *any* memoryless quantum channel, while its complexity grows only linearly with the number of encoded qubits.

In recent years, the discovery and development of quantum computation and communication has shed new light on quantum physics. The potential applications of these new fields encompass a wide variety of subjects, ranging from unconditionally secure secret key generation protocols [1] to efficient integer factoring algorithms [2] or enhancement of communication complexity [3]. However, the practical realization of such protocols and algorithms remains a very involved task mainly because of the inherent instability of quantum superpositions [4] as well as intrinsic imprecisions of the physical devices that process quantum information. These errors wipe out the quantum superpositions together with entanglement, which are usually seen as key resources of the power of quantum algorithms and protocols [5]. Hence, protecting the quantum nature of information became one of the most important challenges to prove the feasibility of quantum computers. The discovery of quantum error correction schemes [6, 7] opened the future of large scale quantum information processing: a certain, but unfortunately very small, degree of imprecision can be tolerated at each step of a quantum transformation and still allow a speed-up over classical information processing [8, 9]. However, building a fault-tolerant quantum computer remains largely out of reach of the present day practical realizations, principally because of the large number of physical qubits required to account for the error correction.

On the other hand, quantum cryptography and more generally the field of quantum communication seems more promising in a near future. Some quantum key distribution protocols have been implemented and the associated devices seem to be close to commercialization [10]. Within this context, we construct a new family of codes — quantum convolutional codes — aimed at protecting a stream of quantum information in a long distance communication. They are the correct generalization to the quantum domain of their classical analogues, and hence inherit their most important properties. First, they have a *maximum likelihood* error estimation algorithm for *all* memoryless channels with a complexity growing *linearly* with the number of encoded qubits. Note that the estimation of the most likely error is the recovery strategy which minimizes the probability of guessing a wrong

codeword. In contrast, under the same circumstances, a generic block code with the same rate has a maximum likelihood error estimation algorithm with a complexity growing *exponentially* with the number of encoded qubits. Hence, generic block codes rapidly require to employ suboptimal error estimation procedures which, as a consequence, do not exploit the whole error correcting capabilities of the code. Moreover, our algorithm can easily handle variations in the properties of the communication channel (i.e. a change in the single qubit error probabilities). The second advantage of quantum convolutional codes is their ability to perform the encoding of the qubits *online* (i.e. as they arrive in the encoder). Thus, it is not necessary to wait for all the qubits to be ready to start sending the encoded state through the communication channel: it reduces the overall processing time of the qubits which is an additional source of decoherence. Note that an attempt at defining quantum convolutional codes has been made some time ago [11, 12], but missed some crucial points in the error estimation algorithm as well as in the study of the decoding algorithm and error propagation properties.

In this letter, we deal with a specific example drawn from our general theory. We construct a quantum convolutional code achieving a rate equal to 1/5: we explain how to encode and decode a stream of qubits efficiently, and we expose the maximum likelihood error estimation algorithm. This will give all the necessary intuition to understand how to generalize the present results to a wider framework [14].

Description of the code — The particular code we wish to present is best described by using the stabilizer formalism [13]. This provides a simple way to understand the encoding and decoding operations. Moreover, the error syndromes can be easily identified, which considerably simplifies the description of the error estimation algorithm. We use the following standard notations for the Pauli operators acting on a single qubit:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1)$$

The identity matrix will be denoted by I . Since convolutional codes are designed to deal with a stream of

information qubits, the number of generators of the stabilizer group will possibly be infinite. However in practice, transmission starts and ends at a given time, which means that we only consider generators made of a finite number of Pauli operators.

The code subspace is described by the generators of its stabilizer group, S . These generators are given by:

$$\begin{aligned} M_0 &= X Z I I I I I I \dots, \\ M_1 &= Z X X Z I I I I \dots, \\ M_2 &= I Z X X Z I I I \dots, \\ M_3 &= I I Z X X Z I I \dots, \\ M_4 &= I I I Z X X Z I \dots, \\ M_{4i+j} &= I^{\otimes 5i} \otimes M_j, \quad 0 < i, \quad 1 \leq j \leq 4, \\ M_\infty &= \dots I I I I Z X. \end{aligned} \quad (2)$$

It is easy to check that all the generators commute and are independent.

An important point to address when considering stabilizer codes is the ability to manipulate encoded information. Namely, we want to find the encoded Pauli operators \bar{X}_i, \bar{Z}_i corresponding to logical qubit i . These operators must satisfy the following relations:

$$\bar{X}_i, \bar{Z}_i \in N(S) - S, \quad (3)$$

$$[\bar{X}_i, \bar{X}_j] = 0, \quad (4)$$

$$[\bar{Z}_i, \bar{Z}_j] = 0, \quad (5)$$

$$[\bar{X}_i, \bar{Z}_j] = 0, \quad i \neq j, \quad (6)$$

where $N(S)$ denotes the normalizer of S . Equation (3) states that the encoded Pauli operators leave the code subspace globally invariant, but have a non-trivial action on its elements, while the Equations (4-6) ensure that manipulating qubit i does not affect other qubits. There exists a great choice of different sets of such operators but, because we often need to manipulate encoded information directly, we further impose that each encoded Pauli operator has only a finite number of terms different from the identity. Moreover, for our particular example, it is possible to require that the whole set of those operators has a structure invariant by a shift of five qubits. This set is given by:

$$\begin{aligned} \bar{X}_1 &= I Z I X I Z I I \dots, \\ \bar{Z}_1 &= I Z Z Z Z I I \dots, \\ \bar{X}_n &= I^{\otimes 5n} \otimes \bar{X}_1, \quad n > 1, \\ \bar{Z}_n &= I^{\otimes 5n} \otimes \bar{Z}_1, \quad n > 1. \end{aligned} \quad (7)$$

At this point, one can wonder what in this code differs from a generic block code. The answer to this question comes from the particular structure of the stabilizer generators: beside M_0 and M_∞ , the generators of the stabilizer group can be casted into sets of constant size (e.g. four), each set acting on a fixed number (e.g. seven) of consecutive qubits. In addition, each set has a fixed overlap (e.g. of two qubits) with the set immediately before and immediately after. This very peculiar structure defines quantum convolutional codes and we can

prove [14] that this implies the possibility of online encoding and the existence of an efficient error estimation algorithm.

Encoding and decoding circuits — As explained in section 4 of D. Gottesman's Ph.D. thesis [13], there are various ways to realize the encoding into the code subspace given the \bar{X}_i and \bar{Z}_i operators. For quantum convolutional codes, the properties of the generators of the stabilizer group give the

Here, we will first identify a set of orthonormal eigenstates of the \bar{Z}_i operators in the total Hilbert space. Then, we will project these states onto the code subspace and show that it gives the computational basis of the logical qubits. From there, we will derive an encoding circuit which implements the appropriate transformation in a unitary way.

More specifically, for $c_j \in \{0, 1\}$ we have:

$$\begin{aligned} \bar{Z}_i |0, 0, 0, 0, 0, c_1, 0, 0, 0, 0, c_2, 0, 0, 0, 0, c_3, \dots\rangle = \\ (-1)^{c_i} |0, 0, 0, 0, 0, c_1, 0, 0, 0, 0, c_2, 0, 0, 0, 0, c_3, \dots\rangle. \end{aligned} \quad (8)$$

Because \bar{Z}_i commutes with the projection operator onto the code subspace, $P = \prod_i (I + M_i) / \sqrt{2}$, we obtain that the set

$$\{|P|0, 0, 0, 0, 0, c_1, 0, 0, 0, 0, c_2, 0, 0, 0, 0, c_3, \dots\rangle\}_{c_i \in \{0, 1\}} \quad (9)$$

is indeed the computational basis for the logical qubits of the code.

Thus, to encode a stream of qubits q_i , we first add to it ancillary qubits in the $|0\rangle$ state such that the 'to-be-protected' qubit i is now at the position $5i + 1$. Then, we need to implement P for these specific input states as a unitary transformation onto the whole Hilbert space. This can be done in full generality as explained in [13], and gives the encoding circuit of FIG. 1. Note that alternative encoding methods can be found and can be relevant when considering some specific applications, but these questions are beyond the scope of this letter.

Due to their very specific nature, convolutional codes propagate information contained in a given qubit to its successors (see again FIG. 1). During the decoding process (i.e. the inverse of encoding) this can actually become a problem: an error affecting a *finite* number of qubits before decoding can propagate through the decoding circuit and finally affect an *infinite* number of qubits. Such error is called *catastrophic*. In practice, only non-catastrophic encoders are useful (i.e. without catastrophic errors). We can show [14] that this condition is equivalent to a requirement on the encoding circuit: its gates form a finite number of layers and commute with each other inside a layer. The idea behind this theorem is simple. In general, an error affecting some qubits will propagate to all the other qubits involved in a gate with the erroneous ones. When those qubits are further used in other gates the error continues to propagate until no more gates are applied. The

commutation relation together with the finiteness of the number of layers ensures that, for any finite size error, only a finite number of gates will enter in the propagation process. Thus all errors are non-catastrophic. FIG. 2 illustrates this ‘pearl-necklace’ structure for our example, and thus proves that our rate $1/5$ quantum convolutional code is non-catastrophic. Moreover, it can be shown that this condition implies the existence of a *forward* decoding scheme: there is no need to wait for the last qubit to start decoding. For non-catastrophic codes, both encoding and decoding can be done online [14].

Maximum likelihood error estimation — An error correcting code aims at protecting information sent over a noisy communication channel by letting the receiver infer which error possibly affected the information. This is the role of the error estimation algorithm. On average, the correct information is most often retrieved when the estimated error coincides with the most likely error. Hence, it is both of theoretical and practical relevance to have an efficient maximum likelihood error estimation algorithm for our quantum convolutional codes. In this section, we exhibit such algorithm. It is indeed the quantum analogue of the well-known Viterbi algorithm for classical convolutional codes. The Viterbi algorithm realizes a maximum likelihood error estimation on all memoryless channels with a complexity linear in the number of encoded qubits. In contrast, for a generic family of block codes with fixed rate, the complexity of such algorithm grows exponentially. This explains why classical convolutional codes are so widely used for reducing the noise on communication channels.

Our algorithm for quantum convolutional codes processes the information obtained through the syndrome in order to infer the most likely error. The circuit for obtaining the syndromes follows the usual phase estimation scheme: an ancillary qubit is prepared in the $|0\rangle$ state; undergoes a Hadamard transform; controls the application of one of the generator M_i of the stabilizer group; again undergoes a Hadamard transform; and is finally measured in the $\{|0\rangle, |1\rangle\}$ basis. Then, the algorithm constructs and updates a list of maximum likelihood error candidates by looking at a small number of syndromes at a time, and by taking local decisions. It is preceded and followed by appropriate initialization and termination steps.

The initialization step lists all error candidates, $\{E_j^0\}_j$, for the first two qubits (which are assumed to be at position 1 and 2) which are compatible with the syndrome M_0 . There are exactly $8 = 4^2/2$ of them (there are 4^2 different operators with support on the first two qubits, but the constraint associated with M_0 divides this set into two equal parts). This list constitutes the input of the main loop of the algorithm. We could compute recursively all error candidates compatible with the first i syndromes, however the number of these candidates is exponential in i . Fortunately, we can avoid this exponen-

tial blow-up by keeping only the most likely candidates among this list in the following way. Index all 16 possible couples of 2 errors by 1 to 16, and denote by E_j^i the most likely error candidate for the the first $5i + 2$ qubits (or one of them in the case of ties) which agrees at positions $5i + 1$ and $5i + 2$ with the couple of errors of index j and which is compatible with syndromes M_0 to M_{4i} . Then the crucial point is the fact that $\{E_j^{i+1}\}_{1 \leq j \leq 16}$ can be computed recursively from $\{E_j^i\}_{1 \leq j \leq 16}$. Indeed, consider for $i \geq 0$ and a candidate E_j^{i+1} , its restriction E' to the first $5i + 2$ positions and assume that the couple of errors of this restriction at positions $5i + 1$ and $5i + 2$ has index k . Then it is straightforward to see that E' is either E_k^i or that E_j^{i+1} can be modified so as to agree with E_k^i on positions 1 to $5i + 2$ and with the old candidate E_j^{i+1} at positions $5i + 3$ to $5i + 7$, to yield a new candidate which is still compatible with syndromes M_0 to $M_{4(i+1)}$ and which is as likely as the old candidate E_j^{i+1} . Obviously the new candidate is at least as likely as the old one, and the only point to check is that the new candidate is compatible with syndromes M_0 to M_{4i+4} . This is a simple consequence of the fact that E_k^i satisfies by definition syndromes M_0 to M_{4i} , and that the only positions of errors which are involved in the computation of syndromes M_{4i+1} to M_{4i+4} are at position $5i + 2$ to $5i + 7$ (note that the new candidate agrees with the old candidate at these positions). In other words, any E_j^{i+1} can be computed from the set of 16 candidates $\{E_k^i\}_{1 \leq k \leq 16}$ by looking for each candidate E_k^i the most likely way to extend it at positions $5i + 3$ to $5i + 7$ so as to satisfy also syndromes M_{4i+1} to M_{4i+4} , and then choosing among these 16 extended candidates the most likely one. We compute in this way the list $\{E_j^1\}_j$ of 16 candidates from $\{E_j^0\}_j$, then $\{E_j^2\}_j$ is computed from $\{E_j^1\}_j$ and so on and so forth until reaching M_∞ . This last syndrome again selects half of the candidates. The termination of the algorithm consists in choosing the most likely error among the remaining candidates.

It is easy to prove that the complexity of the algorithm is linear with respect to the number of encoded qubits: the same task of constant complexity is repeated for each block of four syndromes, whose number equals the number of logical qubits. In other words, the specific structure of the generators of convolutional codes allows to take local decisions while constructing the maximum likelihood error. These decisions manage to keep a finite list of candidates at each step, and thus leads to linear complexity. Note that, the error maximizing the likelihood is known when the last syndrome is measured. Hence, it is in principle necessary to wait till the end of the transmission to actually correct the estimated error. However, as for the classical Viterbi algorithm, numerical simulations show that the different candidates at a given step coincide with the most likely error except on their last few positions. Thus, in practice it is possible to

estimate the error online. In addition, we want to stress, that without increasing its complexity, this algorithm can take into account all memoryless quantum channels even if the single qubit error probabilities are not constant in time. For example, one could imagine that the qubits are photons sent through an optical fiber, and that the probabilities are evaluated by sending probe photons containing no useful information. Finally, as the codes described here are the exact translation to the quantum setting of the classical convolutional codes, one can also derive suboptimal error estimation algorithms (for their classical analogues see [15, 16]). Most importantly, quantum convolutional codes can be decoded iteratively and allow quantum turbo decoding [14].

Conclusion — In this article, we presented an example of quantum convolutional code based on the stabilizer formalism. We showed specific ways for encoding and decoding this code as well as a low complexity maximum likelihood error estimation algorithm. This specific example can be encompassed in a broader theory of quantum convolutional codes. We believe that such codes could be used to reduce errors for long distance quantum communications provided that we are able to perform a small and fixed number quantum gates with good fidelity.

Part of this work was done when H.O. was visiting the Perimeter Institute and the Institute for Quantum Computing in Waterloo, Canada. Useful discussions with J. Kempe, R. Laflamme and D. Poulin are gratefully acknowledged.

* Electronic address: harold.ollivier@inria.fr

† Electronic address: jean-pierre.tillich@inria.fr

- [1] C. H. Bennett and G. Brassard, Proceedings of IEEE international Conference on Computers, Systems and Signal Processing p. 175 (1984).
- [2] P. W. Shor, SIAM J. Comp. **26**, 1484 (1997).
- [3] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the 30th Annual ACM Symposium on the Theory of Computation* (ACM Press, El Paso, Texas, 1998), pp. 63–68.
- [4] W. H. Zurek, Physics Today **44**, 36 (1991).
- [5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
- [6] P. W. Shor, Phys. Rev A **52**, 2493 (1995).
- [7] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
- [8] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)* (ACM Press, New York, NY, 1996), pp. 176–188.
- [9] C. Zalka, arXiv **quant-ph**, 9612028 (1996).
- [10] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and Zbinden, New J. Phys. **4**, 41 (2002).
- [11] H. Chau, Phys. Rev. A **58**, 905 (1998).
- [12] H. Chau, arXiv **quant-ph**, 9806032 (1998).

- [13] D. Gottesman, Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997).
- [14] H. Ollivier and J.-P. Tillich, in preparation.
- [15] R. Johannesson and K. Zigangirov, *Fundamentals of Convolutional Coding*, Digital and Mobile Communication (IEEE press, 1999).
- [16] L. H. C. Lee, *Convolutional coding: fundamentals and applications* (Artech House Publishers, 1997).

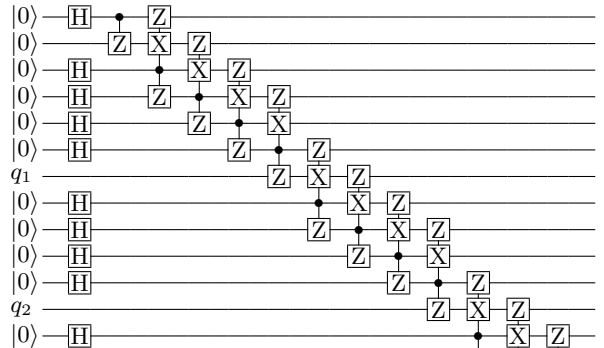


FIG. 1: Beginning of the circuit realizing the encoding once the ancillary qubits have been added to the stream containing the initial quantum information (qubits q_1, q_2, \dots). H is the Hadamard transform, and the dot represents the control qubit for a given gate. The circuit is run from left to right. When all the transformations have been performed for a given qubit, it can be sent through the communication channel.

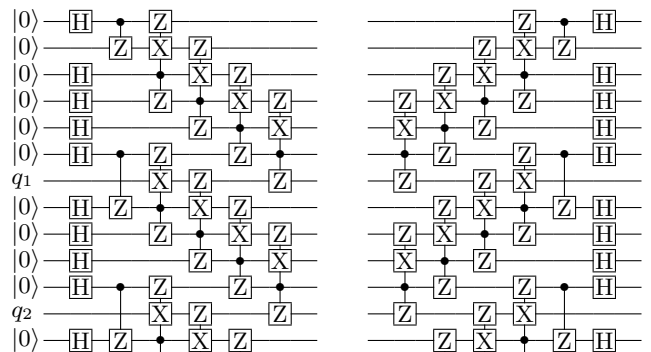


FIG. 2: *Left*: The encoding circuit of Fig. 1 where consecutive blocks of operations have been placed in different orders and the appropriate commutators introduced. There are 6 layers of gates in this circuit and in each layer all the gates commute with each other. It is what we call the ‘pearl-necklace’ structure. *Right*: Corresponding decoding circuit obtained by running the modified encoding circuit backward. In this form it is obvious that the decoding circuit has a structure allowing a forward decoding.