Simple scheme for encoding and decoding a qubit in unknown state for various topological codes

Justyna Łodyga[1], Paweł Mazurek[2,3], Andrzej Grudka[1], Michał Horodecki[2,3]
[1]*Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland*
[2]*Institute for Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[3]*National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland*

— *Full version: arXiv:1404.2495* —

Protecting a qubit in unknown state against decoherence is one of crucial concerns when one regards practical implementations of quantum communication and computation; it also constitutes a problem of reliable quantum memory on its own. The so called threshold theorem [1] states that every quantum computation can be realized with arbitrary precision provided the error probability is below some threshold value, with polylogarithmic overhead in space and time. Stabilizer formalism [2], analogical to construction of classical binary linear codes, offers a framework for description of many codes granting protection in the sense of threshold theorem. In topological stabilizer codes, stabilizer group can be generated by local operators, which implies that logical subspace is protected from the local noise. We present a simple, general procedure of encoding and decoding a qubit in unknown state for broad class of CSS topological codes [3–5]. We briefly describe the fault-tolerant version of the protocol and note that the fidelity of quantum memory based on its application to some CSS codes scales as $1-\mathcal{O}(p)$ in a large code size limit, where p is a probability of error on a single qubit per time step.

Before presenting the decoding/encoding protocol, it is necessary to introduce the notation and concept of stabilizer codes. The logical codespace $\mathcal{H}_{log}$ of a stabilizer code, i.e. the subspace of the Hilbert space $\mathcal{H}_{system} = \otimes_i \mathcal{H}_i$ of N qubits, with i-th qubit defined on Hilbert space $\mathcal{H}_i$ ($\dim\mathcal{H}_i = 2$), is spanned by eigenvectors with eigenvalue 1 of the stabilizer group elements $\mathcal{S}$: $\{|\Psi\rangle : s|\Psi\rangle = |\Psi\rangle, \forall s \in \mathcal{S}\}$. Here S is an abelian subgroup of Pauli group P_N such that $-\mathcal{I} \notin \mathcal{S}$, where $\mathcal{I}$ is an identity operator on $\mathcal{H}_{system}$, and P_N is generated by $\{\sigma_i^A\}$, where bottom index indicates particular qubit $i = \{1,\ldots,N\}$, upper index $A = \{X,Y,Z\}$ describes one of the Pauli matrices given by $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and $\sigma_i^A = \mathcal{I}_1 \otimes \cdots \otimes \mathcal{I}_{i-1} \otimes A_i \otimes \mathcal{I}_{i+1} \cdots \otimes \mathcal{I}_N$. $G(S)$, generator of S, can always be found to be the set of hermitian mutually commuting operators from the Pauli group P_N. Logical operators of the code are those operators from P_N which commute with all operators from $G(S)$, but are not generated by them. Because S is abelian, logical operators are defined *modulo* $G(S)$. If we denote by $N - |G(S)| = D$, where $|G(S)|$ is the number of elements of G(S), then we can write $\dim\mathcal{H}_{log} = 2^D$ and $\mathcal{H}_{log} = \mathcal{H}_{L,1} \otimes \cdots \otimes \mathcal{H}_{L,D}$. The set of operators commuting with S is $\{Z_{L,1}, X_{L,1}, \ldots, Z_{L,D}, X_{L,D}, S\}$. $Z_{L,i}, X_{L,i}$ create a pair of complementary observables (logical operators) acting on $\mathcal{H}_{L,i}$, i.e. i-th logical qubit subsystem of $\mathcal{H}_{log}$ ($\dim\mathcal{H}_{L,i}$=2). They obey the following commutation and anti-commutation relations: $Z_{L,i}X_{L,i} = -X_{L,i}Z_{L,i}$ and $[X_{L,i}, Z_{L,j}] = 0$ for $i \neq j$ as well as $[X_{L,i}, X_{L,j}] = 0$ and $[Z_{L,i}, Z_{L,j}] = 0$ for arbitrary i and j. We now consider one of N physical qubits which is labeled by index $i \in [1,\ldots,N]$. Without loss of generality we assume that it is in a $\alpha_i|0\rangle_i + \beta_i|1\rangle_i$ state (where $\{|0\rangle_i, |1\rangle_i\}$ is the set of eigenvectors of Z_i), i.e. it is non entangled with other qubits. We define encoding i-th qubit into the i-th logical qubit described on system $\mathcal{H}_{L,i}$ as a process after which the i-th logical qubit is in the state $|\Psi_{L_i}\rangle = \alpha_i|0\rangle_{L,i} + \beta_i|1\rangle_{L,i}$, where $\{|0\rangle_{L,i}, |1\rangle_{L,i}\}$ is the set of eigenvectors of a logical operator $Z_{L,i}$ on subsystem $\mathcal{H}_{L,i}$. We define decoding as reversed process.

Because the fidelity of quantum process depends only on the outcomes of measurements on two complementary sets of input states [6], to prove the correctness of encoding/decoding procedure it is enough to show that it performs a mapping between the eigenstates of X_i, Z_i (acting on $\mathcal{H}_i$) and $X_{L,i}$, $Z_{L,i}$ (acting on $\mathcal{H}_{L,i}$), respectively.

Encoding/decoding of an unknown qubit state into/from CSS stabilizer code with $Z_{L,i}$ and $X_{L,i}$ crossing at a single point. We select $\mathcal{H}_i$ arbitrarily and identify the corresponding vertex of the lattice with an intersection point of logical operators (Fig.1(a)). Using the fact that in CSS codes $Z_{L,i}$ ($X_{L,i}$) is a tensor product of Z (X) single qubit operators and identities, we make the parity of operators $Z_{L,i}$ ($X_{L,i}$) dependent only on the state of the i-th physical qubit. To this end we prepare all other qubits on which $Z_{L,i}$ ($X_{L,i}$) acts non-trivially (labeled here by k (l)) in eigenstates associated with $+1$ eigenvalues of Z_k (X_l). Since we assumed that $Z_{L,i}$ and $X_{L,i}$ operators cross at a single point, preparing procedures are independent. We will use the convention: $Z_i|0\rangle_i = +|0\rangle_i$, $Z_i|1\rangle_i = -|1\rangle_i$, $X_i|+\rangle_i = +|+\rangle_i$, $X_i|-\rangle_i = -|-\rangle_i$. Remaining qubits (i.e. those on which logical operators $Z_{L,i}$ and $X_{L,i}$ act trivially) are prepared in such a way that qubits on which $Z_{L,i}$ ($X_{L,i}$) acts non-trivially are surrounded by qubits in $|0\rangle$ ($|+\rangle$) states.

In order to drive a system state into a subspace $\mathcal{H}_{log}$, we measure stabilizer generators and join those of Z-type

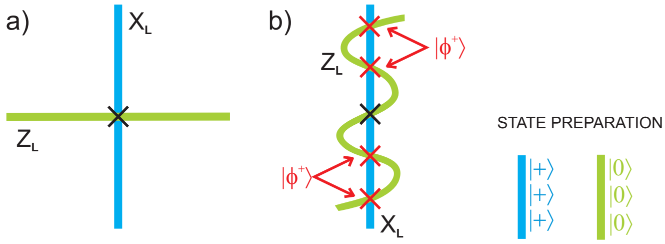

FIG. 1: (a) Logical operators crossing at one physical qubit. (b) Logical operators crossing at many physical quits. Note that this is schematic picture. In reality the logical operators need not be the strings, and codes need not be planar. We put a qubit which we want to encode at one of crossing points (black cross). We prepare other qubits on which only one of logical operators Z_L and X_L acts non-trivially in states $|0\rangle$ and $|+\rangle$, respectively. In case of many crossing points we divide qubits on which both logical operators act non-trivially (red crosses) into pairs and prepare each pair in the maximally entangled state $\frac{1}{\sqrt{2}}(|0\rangle_{i,k}|0\rangle_{i,j} + |1\rangle_{i,k}|1\rangle_{i,j})$ where (i,k) and (i,j) label qubits composing each pair.

(X-type) that gave outcome -1 by chains of X (Z) operators. Chains of X (Z) that cross logical operators $Z_{L,i}$ ($X_{L,i}$) change their parity. However, as we can track the number of times it happens, we can revert this parity change by performing additional $X_{L,i}$ ($Z_{L,i}$) operation whenever this number is odd. Moreover, in many specific cases of CSS codes [7–10] it happens that the matching can always be performed in a way that does not affect the parity of logical operators and no additional corrections are needed at all. Therefore, desired mapping $|0\rangle_i \to |0\rangle_{L,i}$, $|1\rangle_i \to |1\rangle_{L,i}$, $|+\rangle_i \to |+\rangle_{L,i}$, $|-\rangle_i \to |-\rangle_{L,i}$ is realized, where $|0\rangle_{L,i}$, $|1\rangle_{L,i}$, $|+\rangle_{L,i}$, $|-\rangle_{L,i}$ are eigenvectors of logical operators $Z_{L,i}$, $X_{L,i}$.

Decoding procedure of a logical qubit stored within $\mathcal{H}_{L,i}$ logical subspace of CSS code, with $Z_{L,i}$, $X_{L,i}$ logical operators crossing at a single physical qubit i, consists of performing single qubit measurement in Z_k (X_l) basis on all the qubits where $Z_{L,i}$ ($X_{L,i}$) is non-trivially defined, except for the i-th physical qubit (Fig.1(a)). From those measurements the parity of *truncated* operator $Z_{T,i}$ ($X_{T,i}$) is calculated, where truncated operators are analogous to logical operators $Z_{L,i}$ and $X_{L,i}$, with the only difference that they act on i-th qubit trivially. If computed parity is odd, an operator X_i (Z_i) is applied to the qubit defined on $\mathcal{H}_i$. This performs a demanded mapping $|0\rangle_{L,i} \to |0\rangle_i$, $|1\rangle_{L,i} \to |1\rangle_i$, $|+\rangle_{L,i} \to |+\rangle_i$, $|-\rangle_{L,i} \to |-\rangle_i$.

Encoding/decoding of an unknown qubit state into/from a CSS stabilizer code with $Z_{L,i}$ and $X_{L,i}$ crossing at more than one qubit. This case is illustrated schematically in Fig.1(b), where $Z_{L,i}$, $X_{L,i}$ operators act non-trivially on line of qubits. However, the following schemes are applicable to codes with arbitrary structure of logical operators. In addition, if logical operators $Z_{L,i}$ and $X_{L,i}$ cross at neighboring qubits, then our encoding will be local. This is the case for Haah code [11], where $Z_{L,i}$, $X_{L,i}$ are nontrivially defined on surfaces of 3-dimensional rectangular lattice, with every vertex occupied by two qubits. To our best knowledge, no encoding scheme applicable to important class of Haah codes was proposed so far.

By (i,k) we denote qubits on which at least one of logical operators $Z_{L,i}$, $X_{L,i}$ acts non-trivially. We choose a qubit to be encoded (i,l) as one of the qubits at intersection points. As before, we prepare all physical qubits on which *only one* logical operator acts nontrivially in the appropriate eigenstate of single qubit Pauli operators $Z_{i,k}$ (for $Z_{L,i}$) and $X_{i,k}$ (for $X_{L,i}$). Even number of qubits on which *both* logical operators act non-trivially (not taking here into account the (i,l) qubit) can always be divided into pairs consisting of qubits (i,j_1) and (i,j_2) that are prepared in eigenstates of $Z_{i,j_1} \otimes Z_{i,j_2}$ and $X_{i,j_1} \otimes X_{i,j_2}$ corresponding to eigenvalues 1, i.e. maximally entangled states $\frac{1}{\sqrt{2}}(|0\rangle_{i,j_1}|0\rangle_{i,j_2} + |1\rangle_{i,j_1}|1\rangle_{i,j_2})$. Note that these operators commute. Such preparation scheme makes the parity of $Z_{L,i}$ ($X_{L,i}$) dependent only on the eigenvalue of $Z_{i,l}$ ($X_{i,l}$), as required. We drive the state of the system into $\mathcal{H}_{log}$ by performing a sequence of measurements and applying appropriate corrections (bit-flips and phase-flips operations) that either do not change the parity of logical operators (due to obeyed commutation relations) or change the parity (which can be fixed by applying additional logical operator to the code, as explained before). As an example, we present a preparation scheme for the encoding procedure for Haah code in Fig. 2.

Decoding procedure relies on measuring the parity of truncated operators $Z_{T,i}$ and $X_{T,i}$. In case of codes with logical operators crossing at one qubit i, the parity of truncated operators can be calculated from the measurements of single qubit Pauli operators, as there is no qubit k enforcing anti-commutation relation of Z_k and X_k measurements. Decoding procedure for codes with logical operators crossing at larger number of qubits relies on the same idea for solving the non-commutativity problem as the encoding one: we divide an even number of qubits on which both truncated operators act non-trivially, and perform commuting measurements of $Z_{i,j_1} \otimes Z_{i,j_2}$ and $X_{i,j_1} \otimes X_{i,j_2}$. After the parity of truncated logical operators is calculated, the (i,l) qubit is flipped by $X_{i,l}$ ($Z_{i,l}$) if the parity of $Z_{T,i}$

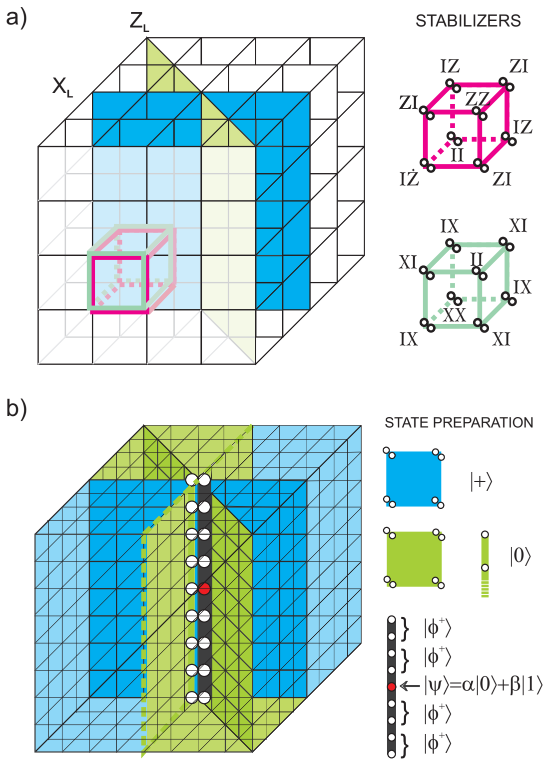

FIG. 2: Preparation for encoding procedure for Haah code [11]. (a) Code structure. Each vertex is associated with two code qubits. Stabilizer generators of types X and Z form cubes. Exemplary logical operators X_L and Z_L associated with blue and green planes cross on a line. (b) Preparation of a lattice. Logical operators X_L and Z_L (blue and green plane) cross at a line. Due to the structure of the code, there are two code qubits placed on each vertex in that line. First qubit of each pair is initialized in state $|0\rangle$. In the centre of a thick black line composed of second qubits of every pair, red qubit is inserted. Remaining qubits lying on that line are combined in pairs and every such pair is prepared in maximally entangled state $|\phi^+\rangle$. Qubits in green and blue regions are initialized in states $|0\rangle$ and $|+\rangle$, respectively.

$(X_{T,i})$ is odd.

Fault-tolerant scenario. We briefly describe a noisy scenario, where qubits are subjected to bit-flip and phase-flip errors (while being stored and prepared) and where measurements can be faulty. Such noisy syndrome measurement is modeled by flipping the ideal measurement outcome with some probability. We assume that probabilities of a bit-flip, phase-flip and syndrome measurement errors are equal to p. The general idea is to prepare all qubits as demanded by non fault-tolerant procedure, measure X_s and Z_p stabilizers many times in the area confined by the whole lattice (except for the last time step where X and Z operators are measured), store all error syndromes and use them to apply error correcting procedure. It can be shown that the fidelity of quantum memory based on Bavyi subsystem code [10] and our fault-tolerant encoding/decoding algorithm is lower bounded by $1-\mathcal{O}(p)$ for $p < 0.0039$. In a similar way one can obtain fidelity bounds for Kitaev code on a torus [7], and planar code with holes [8, 9].

In conclusions, we introduced a simple, single shot procedure for encoding/decoding an unknown state into/from logical subspace of CSS codes. The encoding procedure relies on preparing a system in a way that makes the parity of logical operators dependent only on the state of a selected qubit of the system, and on driving the state of the system into a logical subspace by sequence of operations that commute with logical operators.

Proposed general encoding/decoding processes require entanglement preparation/measurement, hence it may be, in principle, nonlocal for some codes. However, when the qubits at which logical operators cross are situated on the adjacent vertices of the code structure, this can be achieved locally, as in the Haah code.

[1] D. Aharonov and M. Ben-Or, SIAM Journal on Computing **28**, 1207 (1998).
[2] D. Gottesman, Ph.D. thesis, California Institute of Technology (1997).
[3] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[4] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[5] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[6] H. Hofmann, Phys. Rev. Lett. **94**, 160504 (2005), quant-ph/0411011.
[7] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002), quant-ph/0110143.
[8] R. Raussendorf, J. Harrington, and K. Goyal, New Journal of Physics **9**, 199 (2007).
[9] H. Bombin and M. A. Martin-Delgado, Journal of Physics A: Mathematical and Theoretical **42**, 095302 (2009).
[10] S. Bravyi, G. Duclos-Cianci, D. Poulin, and M. Suchara, ArXiv e-prints (2012), 1207.1443.
[11] J. Haah, Phys. Rev. A **83**, 042330 (2011), 1101.1962.