



**HAL**  
open science

## A decoding algorithm for CSS codes using the X/Z correlations

Nicolas Delfosse, Jean-Pierre Tillich

► **To cite this version:**

Nicolas Delfosse, Jean-Pierre Tillich. A decoding algorithm for CSS codes using the X/Z correlations. IEEE International Symposium on Information Theory - ISIT 2014, Jun 2014, Honolulu, United States. pp.1071-1075. hal-01081586

**HAL Id: hal-01081586**

**<https://hal.science/hal-01081586>**

Submitted on 10 Nov 2014

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# A decoding algorithm for CSS codes using the $X/Z$ correlations

Nicolas Delfosse\*, Jean-Pierre Tillich†

\*Département de Physique, Université de Sherbrooke, Sherbrooke, Québec, J1K 2R1, Canada

nicolas.delfosse@usherbrooke.ca

†INRIA, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cédex, France

jean-pierre.tillich@inria.fr

**Abstract**—We propose a simple decoding algorithm for CSS codes taking into account the correlations between the  $X$  part and the  $Z$  part of the error. Applying this idea to surface codes, we derive an improved version of the perfect matching decoding algorithm which uses these  $X/Z$  correlations.

## I. INTRODUCTION

Low Density Parity–Check (LDPC) codes are linear codes defined by low weight parity-check equations. It is one of the most satisfying construction of error-correcting codes since they are both capacity approaching and endowed with an efficient decoding algorithm. It is therefore natural to investigate their quantum generalization.

Besides their use for quantum communication, quantum LDPC codes could play a central role in quantum computing. A striking difference between classical and quantum information is the fact that every manipulation of quantum bits (qubits) is very noisy. Quantum gates must therefore be implemented in a fault-tolerant way. This is realized by applying operations on qubits encoded by a quantum error-correcting code. These qubits can then be regularly corrected. Some recent work of Gottesman [18] has shown that quantum LDPC codes are well-suited for fault-tolerance. These codes, which are defined by low weight constraints on qubits, naturally limit the propagation of errors.

The first difficulty in the generalization of LDPC codes is that most of the constructions have bounded distance (see [26] and references therein). The rare families of quantum LDPC codes equipped with a growing distance are derived from Kitaev’s construction. Kitaev’s toric code is defined by local interactions between qubits placed on a square tiling of the torus. Similar constructions were proposed, based on tilings of surfaces [5], [28], 3-colored tilings [4], [9], Cayley graphs [8] or other geometrical objects [26], [22], [15], [2].

The belief propagation decoding algorithm is an essential ingredient of the success of LDPC codes. Unfortunately, it is much less effective in the quantum setting due to two facts (i) the unavoidable presence of 4-cycles in the Tanner graph [7] and (ii) the low weight generators can be considered as low-weight errors which are not detected by the belief propagation decoder but which are harmful for its convergence [23]. To circumvent this obstacle, some techniques originating from classical coding theory were imported in quantum information recently [19], [1]. Another direction to avoid the 4-cycles, is

to consider the error, which is a quaternary vector, as a pair of binary vectors. These two binary vectors can then be decoded separately. The main problem of this point of view is that it does not consider the correlations between the two binary components of the error. In this work, we present a simple and general strategy to take into account these correlations. To illustrate this idea, we focus on surface codes equipped with the perfect matching decoding algorithm. This algorithm is usually unable to consider the correlations. Applying our method to a family of surface codes constructed from triangular tilings of a torus, we observe a clear improvement of the performance of the decoding algorithm. The depolarizing error threshold of these triangular codes is approximately 13.3% while it is close to 9.9% without considering the correlations.

This article is organised as follows. The definition of surface codes and the geometrical description of errors and syndrome over these codes are recalled in Section II. Section III explains how decoding can be performed by using the aforementioned correlations. Section IV is devoted to the description of the perfect matching decoding algorithm and its improvement to take into account the correlations.

## II. DEFINITIONS AND BASIC PROPERTIES

*Error model.* We deal here with the *depolarizing channel* model which is one of the most natural quantum error model and the quantum analog of the binary symmetric channel. Over the depolarizing channel of probability  $p$ , each qubit is subjected, independently, to an error  $X, Y$  or  $Z$  with probability  $p/3$  or is left unchanged with probability  $1 - p$  where  $X, Y$  and  $Z$  denote the usual Pauli matrices. An error  $E$  over  $n$  qubits is therefore a tensor product  $\otimes_{i=1}^n E_i$  where  $E_i \in \{I, X, Y, Z\}$ . Errors are considered up to the phase  $\{\pm 1, \pm i\}$ , since quantum states are defined up to a phase.

*Stabilizer and CSS codes.* A quantum code is a subspace of dimension  $2^k$  of  $(\mathbb{C}^2)^{\otimes n}$ . This code encodes  $k$  qubits into  $n$  qubits. A very useful way of constructing such codes is through the stabilizer code construction [17] where the code is described by the set of fixed states of a family of commuting Pauli operators  $\{S_1, \dots, S_r\}$ . In other words, the  $S_i$ ’s are generators of the stabilizer group of the quantum code. A particular case of this construction is the *CSS construction* due to Calderbank, Shor [6] and Steane [25]. It consists in choosing some of these Pauli operators in  $\{I, X\}^{\otimes n}$  and the

rest of them in  $\{I, Z\}^{\otimes n}$ . This brings several benefits, first it simplifies the commutation relations and helps in constructing such codes and second decoding of such codes can be achieved by decoding two binary codes as will be explained in the next paragraph.

*Syndrome measurement and decoding of CSS codes.* For a stabilizer code with stabilizer generators  $\{S_1, \dots, S_r\}$  subjected to a Pauli error  $E$ , it is possible to perform a measurement which reveals the vector  $s(E) \stackrel{\text{def}}{=} (E \star S_i)_{1 \leq i \leq r}$  where  $E \star S_i$  is equal to 0 if  $E$  commutes with  $S_i$  and is equal to 1 otherwise. In the case of a CSS code, the syndrome splits into two parts, one corresponding to the commutation with the generators belonging to  $\{I, X\}^{\otimes n}$  and the other one corresponding to the commutation relations with the generators in  $\{I, Z\}^{\otimes n}$ . Moreover, if we decompose the error  $E$  as  $E = E_X E_Z$  where  $E_X \in \{I, X\}^{\otimes n}$  and  $E_Z \in \{I, Z\}^{\otimes n}$  and if we let  $S_1, \dots, S_{r_X}$  be the generators which are in  $\{I, X\}^{\otimes n}$  and  $S_{r_X+1}, \dots, S_r$  be the generators which are in  $\{I, Z\}^{\otimes n}$ , then the syndrome part  $s_X$  which corresponds to the generators in  $\{I, X\}^{\otimes n}$  verifies  $s_X \stackrel{\text{def}}{=} (E \star S_i)_{1 \leq i \leq r_X} = (E_Z \star S_i)_{1 \leq i \leq r_X}$  whereas the syndrome part  $s_Z$  which corresponds to the generators in  $\{I, Z\}^{\otimes n}$  verifies  $s_Z \stackrel{\text{def}}{=} (E \star S_i)_{r_X+1 \leq i \leq r} = (E_X \star S_i)_{r_X+1 \leq i \leq r}$ .

Notice that if we bring in the binary matrices  $\mathbf{H}_X$  and  $\mathbf{H}_Z$  whose rows are formed for  $\mathbf{H}_X$ , respectively  $\mathbf{H}_Z$ , by the generating elements belonging to  $\{I, X\}^{\otimes n}$ , respectively  $\{I, Z\}^{\otimes n}$  (and replacing  $I$  by 0 and  $X$  by 1, respectively replacing  $I$  with 0 and  $Z$  with 1), then  $s_X$  is nothing but the syndrome  $\mathbf{H}_X e_Z^T$  of the binary error  $e_Z$  (obtained from  $E_Z$  by replacing  $I$  by 0 and  $Z$  by 1), whereas  $s_Z$  is nothing but the syndrome  $\mathbf{H}_X e_Z^T$  of the binary error  $e_Z$  (obtained from  $E_Z$  by replacing  $I$  by 0 and  $Z$  by 1). In other words decoding a CSS code amounts to decode two binary codes. This is how decoding a CSS code is usually performed. We call this decoding technique the *standard CSS decoder*.

*Tiling of a surface.* A surface code is a CSS code associated with a tiling of surface. Let us recall the definition of a tiling of surface. A *tiling of surface* is defined to be a cellular embedding of a graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  in a 2-manifold, that is, a surface. Without loss of generality, we can assume that the surface is smooth. We assume that the graph  $\mathcal{G}$  contains neither loops nor multiple edges. This embedding defines a set of faces  $\mathcal{F}$ . Each face is described by the set of edges on its boundary. This tiling of surface is denoted  $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{F})$ . The *dual graph* of  $\mathcal{G}$  is the graph  $\mathcal{G}^* = (\mathcal{V}^*, \mathcal{E}^*)$  of vertex set  $\mathcal{V}^* = \mathcal{F}$  such that two vertices are linked by an edge if and only if the two corresponding faces of  $\mathcal{G}$  share an edge. There is a clear bijection between the edges of  $\mathcal{G}$  and the edges of  $\mathcal{G}^*$ . This graph  $\mathcal{G}^*$  is endowed with a structure of tiling of surface and its faces correspond to the vertices of  $\mathcal{G}$ : these faces are induced by the set of edges of  $\mathcal{G}$  incident to a vertex  $v \in \mathcal{V}$ .

*Surface Codes.* Surface codes are a special case of CSS codes. They have been introduced by Kitaev [20]. Assume that qubits are placed on the edges of a tiling of surface  $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{F})$ . The space of the system is  $\bigotimes_{e \in \mathcal{E}} \mathcal{H}_e$ , with

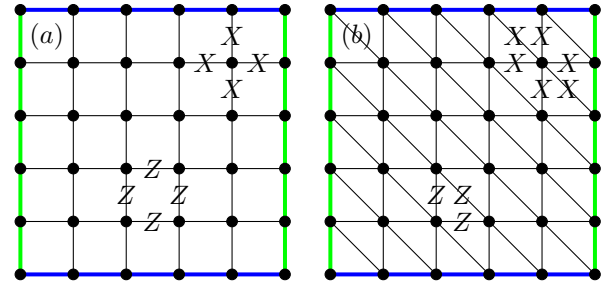


Figure 1. A plaquette operator and a site operator acting on a square tiling of the torus in Fig. (a) and on a triangular tiling of the torus in Fig. (b). The opposite boundaries are identified.

$\mathcal{H}_e = \mathbb{C}^2$  for every edge  $e \in \mathcal{E}$ . The Pauli operators acting on this space are the tensor products  $\bigotimes_{e \in \mathcal{E}} P_e$  such that  $P_e \in \{I, X, Y, Z\}$ . For every edge  $i \in \mathcal{E}$ , denote by  $X_i = \bigotimes_e P_e$  the Pauli operator which is the identity on every edge except on edge  $i$ , where  $P_i = X$ . The operators  $Z_i$  are defined similarly for all  $i \in \mathcal{E}$ . The site operators  $X_v$  and the plaquette operators  $Z_f$  are the Pauli operators defined by

$$X_v = \prod_{e \in \mathcal{E}} X_e \quad \text{and} \quad Z_f = \prod_{e \in \mathcal{E}} Z_e,$$

for every vertex  $v \in \mathcal{V}$  and for every face  $f \in \mathcal{F}$ . Then, the *surface code* associated with the tiling of surface  $\mathcal{G}$  is the CSS code fixed by the site operators and the plaquette operators. The commutation between these operators follows from the structure of the tiling. Note that  $\mathbf{H}_X$  is in this case the incidence matrix of the graph  $\mathcal{G}$  and  $\mathbf{H}_Z$  the incidence matrix of its dual  $\mathcal{G}^*$ . The site operators and the plaquette operators of Kitaev's toric codes are represented in Figure 1 (a).

*Syndrome of a surface code.* In the case of a surface code, the syndrome has a graphical interpretation that we recall now. Consider the surface code associated with a tiling of surface  $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{F})$ . Assume that an error  $E_Z$  acts on a path  $\gamma \subset \mathcal{E}$  of  $\mathcal{G}$ . In other words, we have  $E_Z = \prod_{e \in \gamma} Z_e$ . Then, the syndrome  $s_X = (E_Z \star X_v)_{v \in \mathcal{V}}$  of this error is indexed by the vertices of the graph and is non-trivial if and only if the vertex  $v$  is an end-point of the path  $\gamma$ . This follows from the fact that  $E_Z$  commutes with all the operators  $X_v$ , except the two operators centered on the end-points of  $\gamma$ . More generally, the support of the error  $E_Z$  can be decomposed as a union of disjoint paths and its syndrome indicates the end-points of the support of  $E_Z$ . In what follows, we denote  $\partial(U) \subset \mathcal{V}$  the set of end-points of a set  $U \subset \mathcal{E}$ .

To obtain an analogous description of the error  $E_X$  and its syndrome, replace the graph by its dual. Indeed, this transformation exchanges the roles of  $X$  and  $Z$  in the definition of the code.

The following well known lemma summarizes the graphical description of the error.

**Lemma 1.** *Let  $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{F})$  be a tiling of surface and let  $\mathcal{G}^* = (\mathcal{V}^*, \mathcal{E}^*, \mathcal{F}^*)$  be its dual. An error acting on the surface code associated with  $\mathcal{G}$  corresponds to a pair  $(E_X, E_Z)$  such that  $E_X \subset \mathcal{E}^*$  and  $E_Z \subset \mathcal{E}$ , and its syndrome is the pair*

$(s_X, s_Z)$  such that  $s_X \subset \mathcal{V}$  is the set  $\partial(E_Z)$  of end-points of  $E_Z$  and  $s_Z \subset \mathcal{V}^*$  is the set  $\partial(E_X)$  of end-points of  $E_X$ .

### III. DECODING BY USING CORRELATIONS BETWEEN ERRORS IN $X$ AND $Z$

Virtually all decoders of CSS codes try to recover the  $E_X$  and  $E_Z$  part of the error independently by decoding two binary codes as explained in Section II. There is however some correlation between the  $X$  part of the error and the  $Z$  part as shown by the following conditional probabilities computed for a single error  $E = E_X E_Z$  generated by the depolarizing channel of depolarizing probability  $p$ :

$$\mathbb{P}(E_Z = I | E_X = X) = 1/2 \quad (1)$$

$$\mathbb{P}(E_Z = Z | E_X = X) = 1/2 \quad (2)$$

whereas

$$\mathbb{P}(E_Z = I | E_X = I) = \frac{1-p}{1-2p/3} \quad (3)$$

$$\mathbb{P}(E_Z = Z | E_X = I) = \frac{p/3}{1-2p/3}. \quad (4)$$

When  $E_X = X$ , we recognize an erasure channel and in the second case this corresponds to a binary symmetric channel of probability  $p'' \stackrel{\text{def}}{=} \frac{p/3}{1-2p/3}$ . This can be exploited by the following strategy for decoding. First, decode the  $X$  component of the error. Then, erase the coefficients of  $E_Z$  corresponding to the  $X$  errors. Finally, decode the  $Z$  component of the error, which is subjected to a combination of errors and erasures. We call such a decoder a *CSS decoder using  $X/Z$  correlations*.

It is insightful to calculate the capacity of the two classical channels that both decoders face. The  $X$  decoder has to work for a binary symmetric channel of crossover probability  $p' \stackrel{\text{def}}{=} 2p/3$  whereas the  $Z$  decoder has to work for a binary error and erasure channel, where a bit gets erased with probability  $p'$  and corrupted with probability  $(1-p')p''$ . The capacity of the first channel is equal to  $1-h(p')$  whereas the capacity of the second channel is equal to  $(1-p')(1-h(p''))$ . It can be readily observed that the second capacity is always larger than the first one.

This suggests two things

- (i) if the two binary codes have the same rate (that is if the number of  $X$  generators is the same as the number of  $Z$  generators), then we may expect that the second decoder behaves much better than the first decoder and that the probability of the whole decoding is essentially the probability that the first decoder fails instead of being essentially twice this probability as is usually the case for the standard CSS decoder described in the previous section.
- (ii) In order to fully use this decoder, the best strategy for choosing the CSS code (without using the possible degeneracy of the code) is to choose an asymmetric CSS code where the number of  $Z$  generators of the CSS code is chosen such that the binary code associated to  $\mathbf{H}_Z$  has rate slightly below  $1-h(p')$  whereas the  $X$  generators are chosen such that the rate of the binary code associated

to  $\mathbf{H}_X$  has rate slightly below  $(1-p')(1-h(p''))$ . This strategy of decoding is able to reach the hashing bound, which is equal to  $1+p \log \frac{p}{3} + (1-p) \log(1-p)$  for a depolarizing channel as explained by the following theorem.

**Theorem 2.** *For any  $\epsilon > 0$ , there exists a family of CSS codes of quantum rate  $\leq 1+p \log \frac{p}{3} + (1-p) \log(1-p) - \epsilon$  for which the error probability after decoding with the CSS decoder using  $X/Z$  correlations goes to 0 as the length goes to infinity.*

This theorem is proved by random coding techniques and will be given in the full version of this paper. Notice that the hashing bound is significantly bigger than  $1-2h(p')$  which is the biggest quantum rate that random CSS codes may have in order to be decoded successfully by the standard CSS decoder.

### IV. IMPROVEMENT OF THE PERFECT MATCHING DECODING

In this section, we recall the perfect matching decoding algorithm [11] for surface codes, we discuss about its two main weakness and improve its performance by using the strategy outlined in Section III.

#### A. The Perfect Matching Decoding Algorithm

We consider that a surface code is subjected to a random error  $(E_X, E_Z)$  generated by a depolarizing channel of probability  $p$ . The goal of this algorithm is to determine a most likely error  $E_Z$  which corresponds here to an error of minimum weight (since in general we are in a situation where  $p' \leq 1/2$ ) which has syndrome  $s_X$ . The component  $E_X$  is decoded similarly in the dual graph.

To determine an error  $E_Z \subset \mathcal{E}$  of minimum weight, given its end-points  $s_X = \partial(E_Z) \subset \mathcal{V}$ , we are looking for a set of paths whose end-points are exactly  $s_X$  and whose size is minimum. Algorithm 1 computes such a set using Edmonds' minimum weight perfect matching algorithm [13], [14], [21]. This decoding algorithm first computes the distance graph associated with a syndrome  $s \subset \mathcal{V}$ . It is the weighted complete graph  $\mathcal{K}(s)$ , with vertex set  $s = \{s_1, s_2, \dots, s_m\}$ , such that the weight of the edge  $\{s_i, s_j\}$  is the distance  $d(s_i, s_j)$  in  $\mathcal{G}$ . The second step of the algorithm is the determination of a minimum weight perfect matching  $M$  in  $\mathcal{K}(s)$ . Recall that a perfect matching in a graph  $\mathcal{H}$  is a set of edges of  $\mathcal{H}$  meeting all the vertices of  $\mathcal{H}$  exactly once. With each edge  $\{v_i, v_j\} \in M$ , we associate a geodesic of  $\mathcal{G}$  joining the vertices  $v_i$  and  $v_j$ . Denote by  $\mathcal{G}(v_i, v_j)$  this geodesic. The algorithm returns the symmetric difference of all the geodesics corresponding to the edges of  $M$ . It is the support of a most likely error of syndrome  $s$ .

#### B. Degeneracy and Correlations

We now discuss of two cases of failure of the perfect matching decoding algorithm and their effect on the performance.

First, by definition, surface codes are fixed by the plaquette operators of the tiling. Thus two errors which differ in a sum

---

**Algorithm 1** Perfect Matching Decoding

---

**Require:** A graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ , a subset  $s \subset \mathcal{V}$  of odd size.

**Ensure:** A subset  $x \subset \mathcal{E}$  of minimum size with end-points  $\partial(x) = s$ .

- 1: Construct the distance graph  $\mathcal{K}(s)$  associated with  $s$ .
  - 2: Determine a minimum weight perfect matching  $M$
  - 3: return the symmetric difference of all the geodesics  $\mathcal{G}(v_i, v_j)$  for  $\{v_i, v_j\} \in M$ .
- 

of plaquettes (or faces) have exactly the same effect on the quantum code. We should thus look for the most likely error coset up the sums of faces instead of the most likely error. This phenomenon is called *degeneracy*. The threshold of the toric code obtained by taking account optimally of the degeneracy has been estimated using an Ising model interpretation of the decoding problem [11]. This threshold is close to  $p = 0.163$  whereas the perfect matching algorithm reaches its threshold at approximately  $p = 0.155$ . Note that the renormalization group approach of [12] is one of the rare decoding algorithm of the toric code which is able to make use of the degeneracy of the code.

The second possibility of improvement of the decoding algorithm is the most important potential gain in the performance. It is the correlation between the 2 components,  $E_X$  and  $E_Z$ , of the error and consists in using the decoding strategy explained in Section III. The threshold of the toric code using the  $X/Z$  correlations has been estimated close to 0.189 with the Ising model correspondence [3] and is approximately 0.185 with the non-efficient Metropolis decoding algorithm [27].

These two remarks are generally true for all surface codes.

### C. A Correlated Perfect Matching Algorithm

To implement the decoding strategy of Section III we need to be able to correct errors and erasures when decoding the  $E_Z$  part. The correction of combinations of errors and erasures for topological codes has been considered by Stace, Barrett, and Doherty [24]. We choose here to adapt Algorithm 1 to find a most likely error for this error model.

Denote by  $E_Z^e$  the restriction of  $E_Z$  to the erased positions, that is the positions (or edges) such that  $E_X = X$ , and denote by  $E_Z^{\bar{e}}$  its restriction to the non-erased positions. To find the error  $E_Z$  of syndrome  $s_X$  such that the weight of  $E_X E_Z$  is minimum, we just have to modify the distance function in Algorithm 1. We introduce the  $e$ -distance  $d_e$ , associated with an erasure  $e$ . The usual distance between two vertices of a graph  $\mathcal{G}$  is the length of a shortest path joining these two vertices. The distance  $d_e$  is defined similarly but the length of a path is its number of non-erased edges. An  $e$ -geodesic between two vertices  $u$  and  $v$  of  $\mathcal{G}$  is a path of  $\mathcal{G}$  of length  $d_e(u, v)$  joining these two vertices. This provides us a version of the perfect matching algorithm to correct combinations of errors and erasures. It is presented in Algorithm 2. The distance graph based on the  $e$ -distance  $d_e$  is denoted  $\mathcal{K}^e(s)$ . The notation  $\mathcal{G}^e(u, v)$  represents a  $e$ -geodesic between  $u$  and  $v$ .

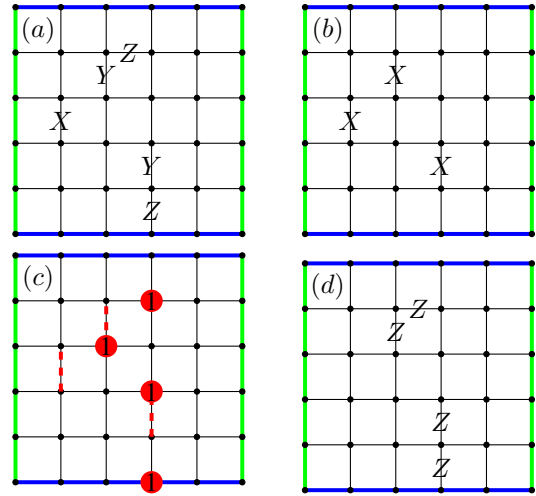


Figure 2. An example of error correction using Algorithm 3. (a) An error for Kitaev's toric code. (b) The component  $E_X$  computed at Step 1. of Algorithm 3. (c) The syndrome  $s_X$  of  $E_Z$  is given by the vertices marked with '1'. The dashed edges form the erasure defined from  $E_X$ . (d) The  $Z$  component estimated in Step 2. of Algorithm 3. It is the error of syndrome  $s_X$  which has minimum weight on the non-erased qubits.

---

**Algorithm 2** Perfect Matching Decoding for errors and erasures

---

**Require:** A graph  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ , a subset  $s \subset \mathcal{V}$  of odd size, a set of erased edges  $e \subset \mathcal{E}$ .

**Ensure:** A subset  $x \subset \mathcal{E}$  with end-points  $\partial(x) = s$  such that the cardinality of  $x \setminus e$  is minimum.

- 1: Construct the  $e$ -distance graph  $\mathcal{K}^e(s)$  associated with  $s$ .
  - 2: Determine a minimum weight perfect matching  $M \subset \mathcal{E}(\mathcal{K}^e(s))$ .
  - 3: return the symmetric difference of all the  $e$ -geodesics  $\mathcal{G}^e(v_i, v_j)$  for  $\{v_i, v_j\} \in M$ .
- 

Combining Algorithm 1 and Algorithm 2, we obtain Algorithm 3, which is an improved version of the Perfect Matching Decoding algorithm taking partially account of the  $X/Z$  correlations.

---

**Algorithm 3** Correlated Perfect Matching Decoding

---

**Require:** A tiling  $G = (\mathcal{V}, \mathcal{E}, \mathcal{F})$ , a syndrome  $(s_X, s_Z) \subset V \times V^*$ .

**Ensure:** An error  $(E_X, E_Z) \subset \mathcal{E}^* \times \mathcal{E}$  of syndrome  $(s_Z, s_X)$ , such that  $|E_X|$  is minimum and  $|E_X E_Z|$  is minimum given  $E_X$ .

- 1: Compute  $E_X$  by applying Algorithm 1 to  $s_Z$  in the dual graph  $\mathcal{G}^*$ .
  - 2: Compute  $E_Z$  by applying Algorithm 2 to  $s_X$  and  $e = E_X$  in the graph  $\mathcal{G}$ .
  - 3: return  $(E_X, E_Z)$ .
- 

An example of error over the toric code that can not be corrected with the usual perfect matching decoding but that is corrected with Algorithm 3 is represented in Figure 2.

For Kitaev's toric codes, we obtain a slight improvement

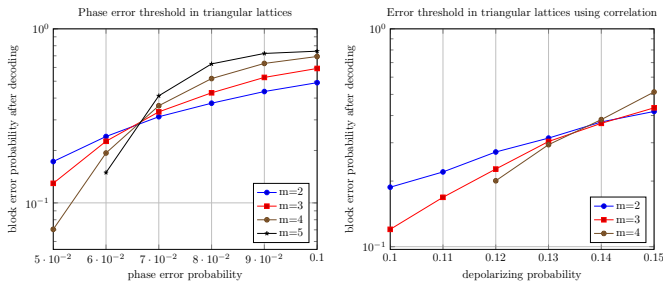


Figure 3. Phase decoding performance of Algorithm 1 and depolarizing decoding performance of Algorithm 3 for triangular toric codes of length  $3 \cdot 2^{2m}$

of the decoding performance using Algorithm 3, but we cannot overcome the usual threshold since the  $E_X$  part of the error is decoded using a standard perfect matching algorithm. Nevertheless, as explained in Section III, the use of the  $X/Z$  correlations is well appropriate to asymmetric CSS codes. To define asymmetric surface codes, it suffices to consider non-self dual tilings.

A natural construction of asymmetric surface codes is the family derived from triangular lattices of the torus. For example, the Cayley graph of the group  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  and the generating set  $\{\pm(1, 0), \pm(0, 1), \pm(1, -1)\}$ , described in Figure 1 (b), clearly defines a triangular tiling of the torus. Using Algorithm 1, we remark a threshold for the correction of phase errors at  $p' = 0.066$  in Figure 3, whereas the bit-flip error threshold, observed in the dual graph (which is a hexagonal lattice), is very high (more than  $p' = 0.14$  for this family of tiling). This implies a depolarizing error threshold at  $p = 3p'/2 = 0.099$  for the standard perfect matching algorithm, while Algorithm 3 leads to a depolarizing error threshold at approximately  $p = 0.133$ . This good performance is explained by the fact that, while the phase error threshold is low, the error correction in the dual graph exhibits a very good performance and the bit-flip error threshold is high. This allows Algorithm 3 to take into account the  $X/Z$  correlations.

## V. CONCLUDING REMARKS

We proposed a decoding algorithm for CSS codes partially taking into account the correlations between the  $X$  component and the  $Z$  component of the error for a depolarizing channel. Applied to triangular toric codes, this algorithm exhibits a good performance and clearly improves the threshold. It could be applied to other classes of codes, for instance for color codes, where the decoding algorithm by projection onto 3 surface codes can be adapted to take into account the correlations between the 3 surface codes [10].

## ACKNOWLEDGMENTS

The authors wish to thank David Poulin for useful discussions. The work of both authors was supported in part by the French PEPS ICQ2013 program (TOCQ project) and Nicolas Delfosse was supported by the Lockheed Martin Corporation.

## REFERENCES

- [1] I. Andriyanova, D. Maurice, and J.-P. Tillich. Spatially coupled quantum ldpc codes. In *Proc. of IEEE Information Theory Workshop, ITW 2012*, pp. 327–331, 2012.
- [2] B. Audoux. An application of Khovanov homology to quantum codes. *arXiv:1307.4677*, 2013.
- [3] H. Bombin, R.S. Andrist, M. Ohzeki, H.G. Katzgraber, and M.A. Martin-Delgado. Strong resilience of topological codes to depolarization. *Phys. Rev. X*, 2(2):021004, 2012.
- [4] H. Bombin and M.A. Martin-Delgado. Topological quantum distillation. *Phys. Rev. Lett.*, 97:180501, 2006.
- [5] H. Bombin and M.A. Martin-Delgado. Homological error correction: Classical and quantum codes. *Journal of Mathematical Physics*, 48(5):052105, 2007.
- [6] A.R. Calderbank and P.W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098, 1996.
- [7] T. Camara, H. Ollivier, and J.-P. Tillich. Constructions and performance of classes of quantum LDPC codes, 2005. *arXiv:quant-ph/0502086v2*.
- [8] A. Couvreur, N. Delfosse, and G. Zémor. A construction of quantum LDPC codes from Cayley graphs. *Information Theory, IEEE Transactions on*, 59(9):6087–6098, 2013.
- [9] N. Delfosse. Tradeoffs for reliable quantum information storage in surface codes and color codes. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2013*, pp. 917–921, 2013.
- [10] N. Delfosse. Decoding color codes by projection onto surface codes. *Phys. Rev. A*, 89:012317, Jan 2014.
- [11] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43:4452, 2002.
- [12] G. Duclos-Cianci and D. Poulin. Fast decoders for topological quantum codes. *Phys. Rev. Lett.*, 104(050504), 2010.
- [13] J. Edmonds. Maximum matching and a polyhedron with 0-1 vertices. *Journal of Research at the National Bureau of Standards*, 69B:125–130, 1965.
- [14] J. Edmonds. Path, trees, and flowers. *Canadian Journal of Mathematics*, 17:449–467, 1965.
- [15] M.H. Freedman and M.B. Hastings. Quantum systems on non- $k$ -hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *arXiv:1301.1363*, 2013.
- [16] M.H. Freedman, D.A. Meyer, and F. Luo.  $Z_2$ -systolic freedom and quantum codes. *Mathematics of Quantum Computation, Chapman & Hall/CRC*, pages 287–320, 2002.
- [17] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997.
- [18] D. Gottesman. What is the overhead required for fault-tolerant quantum computation? *arXiv preprint arXiv:1310.2984*, 2013.
- [19] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa. Quantum error correction beyond the bounded distance decoding limit. *Information Theory, IEEE Transactions on*, 58(2):1223–1230, 2012.
- [20] A.Y. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):27, 2003.
- [21] V. Kolmogorov. Blossom V: a new implementation of a minimum cost perfect matching algorithm. *Mathematical Programming Computation*, 1:43–67, 2009.
- [22] A.A. Kovalev, and L.P. Pryadko. Quantum Kronecker sum-product low-density parity-check codes with finite rate. *Phys. Rev. A* 88, 1 (2013), 012311.
- [23] D. Poulin and Y. Chung. On the iterative decoding of sparse quantum codes. *Quantum Information & Computation*, 8(10):987–1000, 2008.
- [24] T.M. Stace, S.D. Barrett, and A.C. Doherty. Thresholds for topological codes in the presence of loss. *Phys. Rev. Lett.*, 102(20):200501, 2009.
- [25] A. Steane. Multiple-particle interference and quantum error correction. *Proc. of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.
- [26] J.-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to  $n^{1/2}$ . In *Proc. of IEEE International Symposium on Information Theory, ISIT 2009*, pp. 799–803, 2009.
- [27] J.R. Wootton and D. Loss. High threshold error correction for the surface code. *Phys. Rev. Lett.*, 109(16):160503, 2012.
- [28] G. Zémor. On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction. In *Proc. of the 2nd International Workshop on Coding and Cryptology, IWCC 2009*, pp. 259–273. Springer-Verlag, 2009.