New constructions of CSS codes obtained by moving to higher alphabets

Iryna Andriyanova *, Denise Maurice[†], Jean-Pierre Tillich[†]

* ETIS group, ENSEA/UCP/CNRS-UMR8051, France
[†] INRIA, Equipe Secret, Domaine de Voluceau BP 105, F-78153 Le Chesnay cedex, France.

Abstract—We generalize a construction of non-binary quantum LDPC codes over $\mathbb{F}_{2^m}$ due to [KHIK11] and apply it in particular to toric codes. We obtain in this way not only codes with better rates than toric codes but also improve dramatically the performance of standard iterative decoding. Moreover, the new codes obtained in this fashion inherit the distance properties of the underlying toric codes and have therefore a minimum distance which grows as the square root of the length of the code for fixed m.

I. INTRODUCTION

LDPC codes [Gal63] and their variants are one of the most satisfying answers to the problem of devising codes guaranteed by Shannon's theorem. They display outstanding performance for a large class of error models with a fast decoding algorithm. Generalizing these codes to the quantum setting seems a promising way to devise powerful quantum error correcting codes for protecting, for instance, the very fragile superpositions manipulated in a quantum computer. It should be emphasized that a fast decoding algorithm could be even more crucial in the quantum setting than in the classical one. In the classical case, when error correction codes are used for communication over a noisy channel, the decoding time translates directly into communication delays. This has been the driving motivation to devise decoding schemes of low complexity, and is likely to be important in the quantum setting as well. However, there is an important additional motivation for efficient decoding in the quantum setting. Quantum computation is likely to require active stabilization. The decoding time thus translates into computation delays, and most importantly in error suppression delays. If errors accumulate faster than they can be identified, quantum computation may well become infeasible: fast decoding is an essential ingredient to fault-tolerant computation.

Quantum generalizations of LDPC codes have indeed been proposed in [MMM04]. However, it has turned out that the design of high performance quantum LDPC codes is much more complicated than in the classical setting. This is due to several reasons, the most obvious of which being that the parity-check matrix of quantum LDPC codes must satisfy certain orthogonality constraints. This complicates significantly the construction of such codes. In particular, the plain random constructions that work so well in the classical setting are pointless here. There have been a number of attempts at overcoming this difficulty and a variety of methods for constructing quantum LDPC codes have been proposed [Pos01], [Kit03],

[MMM04], [COT05], [COT07], [LGF06], [GFL08], [HI07], [IM07], [Djo08], [SMK08], [Aly07], [Aly08], [HBD08], [TZ09], [TL10], [KHIK11]. However, with the exception of [TZ09] which gives a construction of LDPC codes with minimum distance of the order of the square root of the block-length, all of these constructions suffer from disappointingly small minimum distances, namely whenever they have non-vanishing rate and parity-check matrices with bounded row-weight, their minimum distance is either proved to be *bounded*, or unknown and with little hope for unboundedness.

The point has been made several times that minimum distance is not everything, because there are complex decoding issues involved, whose behavior depends only in part on the minimum distance, and also because a poor asymptotic behavior may be acceptable when one limits oneself to practical lengths. This is illustrated for instance in our case by the codes constructed in [KHIK11] whose performance under iterative decoding is quite good even if their minimum distance might be bounded. Their construction can be summarized as follows. There are three ingredients:

(i) The starting point is a CSS quantum code associated to a couple $(\mathscr{C}_X, \mathscr{C}_Z)$ of binary LDPC codes satisfying $\mathscr{C}_Z^{\perp} \subset \mathscr{C}_X$ (see Section II) obtained from a construction due to [HI07]. These LDPC codes have parity check matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ which are $(2, L)$-regular, meaning that each column contains exactly 2 "1"'s and each row contains exactly L-ones.

(ii) From this construction, a pair of q-ary LDPC codes $(\mathscr{C}_X^{(q)}, \mathscr{C}_Z^{(q)})$ is deduced which satisfies $\mathscr{C}_Z^{(q)\perp} \subset \mathscr{C}_X^{(q)}$, where q is some power of two, $q = 2^m$. These codes have parity-check matrices $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ of the same size as $\mathbf{H}_X$ and $\mathbf{H}_X$ respectively and which have nonzero entries whenever the corresponding entry of $\mathbf{H}_X$ (respectively $\mathbf{H}_Z$) is equal to 1, that is

$$x_{i,j}^{(q)} \neq 0 \Leftrightarrow x_{i,j} = 1, \ z_{i,j}^{(q)} \neq 0 \Leftrightarrow z_{i,j} = 1, \quad (1)$$

where $x_{i,j,}^{(q)}, x_{i,j}, z_{i,j}^{(q)}, z_{i,j}$ denote the entry corresponding to the i-th row and the j-th column of $\mathbf{H}_X^{(q)}, \mathbf{H}_X, \mathbf{H}_Z^{(q)}, \mathbf{H}_Z$ respectively.

(iii) By denoting the length of $\mathscr{C}_X, \mathscr{C}_Z, \mathscr{C}_X^{(q)}, \mathscr{C}_Z^{(q)}$ by n, and by replacing each entry of $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ in the finite field $\mathbb{F}_q$ over q elements by a binary matrix of size $2^m \times 2^m$, through a ring isomorphism $A : \mathbb{F}_{2^m} \to \mathcal{M}_{2^m}$ where $\mathcal{M}_{2^m}$ is a certain subring of binary $2^m \times 2^m$ matrices (i.e.

a one-to-one mapping preserving field addition and multiplication), a pair of two parity-check matrices $(\hat{\mathbf{H}}_X, \hat{\mathbf{H}}_Z)$ is obtained. They define a pair of binary codes $(\hat{\mathscr{C}}_X, \hat{\mathscr{C}}_Z)$ of length $n \times m$ satisfying the CSS condition $\hat{\mathscr{C}}_Z^{\perp} \subset \hat{\mathscr{C}}_X$.

The point of this construction is that the new quantum code associated to the pair $(\hat{\mathscr{C}}_X, \hat{\mathscr{C}}_Z)$ can now be decoded on the extension field $\mathbb{F}_q$ and this improves dramatically the performance in the same way as the performance of classical binary $(2, L)$ regular LDPC codes is improved by moving to a larger extension field $\mathbb{F}_{2^m}$ as shown in [Hu02], [HEA05].

Our purpose in this article is here to generalize the construction of [KHIK11] and to show that it can be applied to any pair of binary codes $(\mathscr{C}_X, \mathscr{C}_Z)$ satisfying $\mathscr{C}_Z^{\perp} \subset \mathscr{C}_X$ which are LDPC codes which have parity check matrices which have exactly 2 "1"'s per column[1], not only the particular family of quasi-cyclic codes of this type which are constructed in [HI07]. We apply this generalized construction to the toric codes of [Kit03] which are a particular instance of the CSS construction corresponding to a pair of LDPC codes $(\mathscr{C}_X, \mathscr{C}_Z)$ which are $(2, 4)$-regular. It presents the advantage of having a minimum distance which grows like the square root of the length but has also the drawback to be able to encode only 2 qubits. We obtain in this way a new code family which displays several attractive features compared to the toric code family:

(i) it has the same two dimensional structure as toric codes, this might turn out to very helpful for its implementation. It represents for instance a quite attractive code choice for performing quantum fault-tolerant computation [Kit03].

(ii) it inherits the distance properties from the underlying toric code and has therefore a minimum distance which grows like the square root of the length,

(iii) the number of encoded qubits is not constant anymore as for toric codes but grows as $2m$ where m is the degree of the extension field,

(iv) whereas iterative decoding displays very bad performances when applied to toric codes, plain iterative decoding behaves much better for this new family of codes and when $m = 9$ for instance, we obtain codes for which iterative decoding performs quite well (see Section V).

Apart from the practical relevance of the codes constructed, there is also a theoretical aspect. This shows for instance that it is possible to obtain families of CSS codes with a prescribed degree distribution on the check nodes with an unbounded minimum distance with the construction strategy of [KHIK11]. It is questionable whether or not the codes constructed in [KHIK11] meet this property (one of the drawback of the codes constructed there is that they start with a certain construction of quasi-cyclic CSS codes which can be easily proved to have bounded minimum distance).

II. CSS CODES AND TANNER GRAPHS

a) **CSS codes***:* The codes constructed in this paper fall into the category of Calderbank-Shor-Steane (CSS) codes [CS96], [Ste96] which belong to a more general class of

[1]In other words they are cycle codes of a graph [HB68].

quantum codes called stabilizer codes [Got97], [CRSS98]. The first class is described with the help of a pair of mutually orthogonal binary codes, whereas the second class is given by an additive self-orthogonal code over $\mathbb{F}_4$ with respect to the trace hermitian product. Quantum codes on n qubits are linear subspaces of a Hilbert space of dimension 2^n and do not necessarily have a compact representation in general. The nice feature of stabilizer codes is that they allow to define such a space with the help of a very short representation, which is given here by a set of generators of the aforementioned additive code. Each generator is viewed as an element of the Pauli group on n qubits and the quantum code is then nothing but the space stabilized by these Pauli group elements. Moreover, the set of errors that such a quantum code can correct can also be deduced directly from this discrete representation. For the subclass of CSS codes, this representation in terms of additive self-orthogonal codes is equivalent to a representation in terms of a pair $(\mathscr{C}_X, \mathscr{C}_Z)$ of binary linear codes satisfying the condition $\mathscr{C}_Z^{\perp} \subset \mathscr{C}_X$. The *quantum minimum distance* of such a CSS code is given by

$$
\begin{aligned}
d_Q &\overset{\text{def}}{=} \min\{d_X, d_Z\}, \quad \text{where} \quad &(2)\\
d_X &\overset{\text{def}}{=} \min\{|x|, x \in \mathscr{C}_X \setminus \mathscr{C}_Z^{\perp}\},\\
d_Z &\overset{\text{def}}{=} \min\{|x|, x \in \mathscr{C}_Z \setminus \mathscr{C}_X^{\perp}\}.
\end{aligned}
$$

Such a code allows to protect a subspace of k_Q qubits against errors where

$$
k_Q \overset{\text{def}}{=} \dim \mathscr{C}_X - \dim \mathscr{C}_Z^{\perp}. \quad (3)
$$

k_Q is called the *quantum dimension* of the CSS code.

b) **LDPC codes***:* LDPC codes are linear codes which have a sparse parity-check matrix. They can be decoded by using the *Tanner graph* associated to such a parity-check matrix $\mathbf{H}$. This graph is defined as follows. Assume that $\mathbf{H} = (H_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}}$ is an $r \times n$ matrix (where n is the length of the code). The associated Tanner graph is bipartite and has:

(i) vertex set $V \cup C$, where the first set V is in bijection with the indices of the columns of $\mathbf{H}$, say $V = \{1, \ldots, n\}$ and is called the set of *variable nodes*, whereas the second set C is called the set of *check nodes* and is in bijection with the indices of the rows of $\mathbf{H}$: $C = \{\oplus_1, \ldots, \oplus_r\}$.

(ii) edge set E; there is an edge between $\oplus_i$ and j if and only if $H_{ij} \neq 0$ and the edge receives label H_{ij} in this case.

A CSS code defined by a couple of binary code $(\mathscr{C}_X, \mathscr{C}_Z)$ is said to be a *quantum LDPC code* if and only if $\mathscr{C}_X$ and $\mathscr{C}_Z$ are LDPC codes.

III. A GENERALIZATION OF THE CONSTRUCTION OF [KHIK11]

We show in this section how to derive for any integer $m > 1$ from a pair of binary LDPC codes $(\mathscr{C}_X, \mathscr{C}_Z)$ with parity-check matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ satisfying

(1) $\mathbf{H}_X \mathbf{H}_Z{}^T = 0$,

(2) all the columns of $\mathbf{H}_X$ and $\mathbf{H}_Z$ have exactly 2 "1"'s in it, a pair of 2^m-ary LDPC codes $(\mathscr{C}_X^{(q)}, \mathscr{C}_Z^{(q)})$ with parity-check matrices $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ satisfying

(1) $\mathbf{H}_X^{(q)} \mathbf{H}_Z^{(q)}{}^T = 0$,

(2) all the columns of $\mathbf{H}_X$ and $\mathbf{H}_Z$ have exactly 2 non zero elements in it.

This generalizes the construction of [KHIK11] to other codes than the ones obtained from [HI07] by using the ring isomorphism A from the finite field $\mathbb{F}_{2^m}$ to $\mathcal{M}_{2^m}$ which is described in Subsection II.C of [KHIK11].

We show the existence of the couple $(\mathscr{C}_X^{(q)}, \mathscr{C}_Z^{(q)})$ by providing an efficient algorithm which outputs a couple of matrices $(\mathbf{H}_X^{(q)}, \mathbf{H}_Z^{(q)})$ meeting (1) and (2). To explain how the algorithm works let us bring in the following definition

Definition 1: To each row k of $\mathbf{H}_Z$ we associate a parity-check matrix $\mathbf{H}_X(k)$ consisting of the submatrix of $\mathbf{H}_X$ formed by the columns j of $\mathbf{H}_X$ such that $z_{k,j} \neq 0$ and by keeping only the non zero rows in it. Let $\mathcal{G}_X(k)$ be the Tanner graph associated to this parity-check matrix.

The crucial point is the following lemma

Lemma 1: The degree of every variable node of $\mathcal{G}_X(k)$ is two, whereas the degree of every check node is an even positive number.

Proof: The fact that the degree of every variable node is exactly two is a direct consequence of the fact that the columns of $\mathbf{H}_X(k)$ are all of weight 2 since the columns of $\mathbf{H}_X$ have exactly this property. The second claim about the degree of the check nodes is a consequence of $\mathbf{H}_X \mathbf{H}_Z{}^T = 0$. This can be verified as follows. Each check node corresponds to a row of $\mathbf{H}_X(k)$ which corresponds itself to some row of $\mathbf{H}_X$. We denote such a row by i. The degree of the check node corresponding to i is nothing but the weight of row i of $\mathbf{H}_X(k)$. It is equal to the number of j's such that we both have $x_{i,j} = z_{k,j} = 1$. Notice that $\mathbf{H}_X \mathbf{H}_Z{}^T = 0$ implies in particular that

$$\sum_j x_{i,j} z_{k,j} = 0 \qquad (4)$$

This implies the aforementioned claim about the degree of the check node, since the aforementioned number of j's is necessarily even in order to meet (4). ∎

Since the degrees of all the vertices of $\mathcal{G}_X(k)$ is even, $\mathcal{G}_X(k)$ can be decomposed in an edge-disjoint subset of cycles $\text{Cyc}_X(k)$. Each variable node vertex j belongs to a unique cycle of this kind whereas a check node $\oplus_i$ may belong to several cycles of $\text{Cyc}_X(k)$. Our strategy to ensure that there is a choice of $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ meeting Condition (1) and $\mathbf{H}_X^{(q)} \mathbf{H}_Z^{(q)}{}^T = 0$ is to look for solutions which satisfy for all rows k of $\mathbf{H}_Z^{(q)}$, all cycles $\mathcal{C}$ of $\text{Cyc}_X(k)$, and all check nodes $\oplus_i$ belonging to $\mathcal{C}$

$$\sum_{j:\oplus_i, j \in \mathcal{E}} x_{i,j}^{(q)} z_{k,j}^{(q)} = 0 \qquad (5)$$

where we denote by $\mathcal{E}$ the set of edges of $\mathcal{C}$. Notice that there are exactly two variable nodes which are adjacent to $\oplus_i$ in $\mathcal{C}$.

The first point is that the sum $\sum_j x_{i,j}^{(q)} z_{k,j}^{(q)}$ can be decomposed as a sum $\sum_{\mathcal{C}:\mathcal{C} \in \text{Cyc}_X(k), \oplus_i \in \mathcal{C}} \sum_{j:\oplus_i j \text{ edge of } \mathcal{C}} x_{i,j}^{(q)} z_{k,j}^{(q)}$ which implies that ensuring (5) implies (4) and therefore $\mathbf{H}_X^{(q)} \mathbf{H}_Z^{(q)}{}^T = 0$. Moreover the code associated to the cyclic Tanner graph $\mathcal{C}$ is non trivial if and only if the product of its labels on its cycle is equal to 1. We define here for a Tanner graph the product over a cycle by

*Definition 1 (***product over a cycle of a Tanner graph**): Let $\mathcal{C} = v_1, c_1, v_2, \ldots, c_k, v_1$ be a cycle in the Tanner graph code. Then the product over this cycle is the product of all the coefficients of the edges over this cycle, with a power 1 if it is a check-to-node edge, and -1 if it is node-to-check. We denote this product by $\Pi(\mathcal{C})$.

It is namely well known that

Proposition 1: The code associated to Tanner graph which is a unique cycle is not reduced to the zero codeword if and only if the product of the labels over the cycle is equal to 1. In such a case, all the non-zero codewords have only non-zero positions.

The proof of this proposition is given in the appendix.

The algorithm for choosing the entries of $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ is described below as Algorithm 1. The fact that the $z_{k,j}^{(q)}$'s can

---

Algorithm 1 Choosing the entries of $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$

Choose the entries $x_{i,j}^{(q)}$ of $\mathbf{H}_X^{(q)}$ such that for all rows k of $\mathbf{H}_Z^{(q)}$ and all cycles of $\text{Cyc}_X(k)$ the product of the labels $x_{i,j}^{(q)}$ along these cycles is equal to 1.

for all rows k of $\mathbf{H}_Z^{(q)}$ **do**
  for all cycles $\mathcal{C}$ of $\text{Cyc}_X(k)$ **do**
    Choose non-zero entries $z_{k,j}^{(q)}$ for all variable nodes j of $\mathcal{C}$ such that (5) holds for all edges of $\mathcal{C}$.
  end for
end for

---

be chosen to be different from zero comes from the fact that the product of the labels $x_{i,j}$ along $\mathcal{C}$ is equal to 1 and from Proposition 1. It just amounts to choose a non-zero codeword in the code whose Tanner graph is given by $\mathcal{C}$ and the labels of the edges are given by the $x_{i,j}^{(q)}$'s. This leads to two matrices $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ which satisfy Condition (1) and $\mathbf{H}_X^{(q)} \mathbf{H}_Z^{(q)}{}^T = 0$. Finally, it remains to explain how we choose the entries $x_{i,j}^{(q)}$ of $\mathbf{H}_X^{(q)}$. We will actually provide an algorithm which provides a stronger condition on the $x_{i,j}^{(q)}$'s, namely that

$$\text{for all cycles } \mathcal{C} \text{ of } \mathcal{G}_X, \Pi(\mathcal{C}) = 1. \qquad (6)$$

The fact that the product over all cycles of $\mathcal{G}_X$ will be equal to 1 (and not only the cycles of the subgraphs $\mathcal{G}_X(k)$) will be quite useful when applied to the toric code and this stronger condition can be met with Algorithm 2 which gives a very large choice for the coefficients.

Proof: (of correctness of Algorithm 2) Let $\mathcal{C}$ be a cycle of $\mathcal{G}_X$. Let us prove that $\Pi(\mathcal{C}) = 1$. This product can be written

Algorithm 2 Algorithm to ensure (6)

    for all check nodes $\oplus_k$ of the Tanner graph $\mathcal{G}_X$ associated to $\mathbf{H}_X$ **do**

        Choose arbitrarily a non zero element a_k and non-zero elements a_{jk} for all variable nodes j adjacent to $\oplus_k$.

    end for

    for all variable nodes j of $\mathcal{G}_X$ **do**

        $x_{i,j}^{(q)} \leftarrow a_i b_{ij} b_{kj}$

        $x_{k,j}^{(q)} \leftarrow a_k b_{kj} b_{ij}$ {Here $\oplus_i$ and $\oplus_k$ denote the two check nodes adjacent to j.}

    end for

as

$$\Pi(\mathcal{C}) = \Pi_{\text{check nodes } \oplus_k \text{ in } \mathcal{C}} f(k),$$

where $f(k)$ counts the contribution to the product which involves terms which depend on k. By denoting by j and l the two variable nodes adjacent to $\oplus_k$ in the cycle and by $\oplus_i$ and $\oplus_m$ the two other check nodes which are adjacent in the cycle to j and l respectively we can decompose $f(k)$ as

$$f(k) = g(ij)g(jk)g(kl)g(lm)$$

where $g(ab)$ gives the part of the contribution to $\Pi(\mathcal{C})$ stemming from edge ab by keeping only elements of the product which depend on k. We observe now that $g(ij) = b_{kj}$, $g(jk) = a_k^{-1}b_{kj}^{-1}$, $g(kl) = a_k b_{kl}$ and $g(lm) = b_{kl}^{-1}$. This implies $f(k) = 1$, which in turn implies that $\Pi(\mathcal{C}) = 1$. ∎

Remark: One might wonder whether or not it is possible to obtain q-ary versions of $\mathbf{H}_X$ and $\mathbf{H}_Z$ which satisfy the orthogonality condition $\mathbf{H}_X^{(q)}\mathbf{H}_Z^{(q)T} = 0$ when the columns of $\mathbf{H}_X$ and $\mathbf{H}_Z$ have weight greater than 2. While this can be easily done for certain structured constructions such as the one proposed in [TZ09], it is not clear how to achieve this in all generality. The difficulty is the following. Consider the code defined by a Tanner graph which is a subgraph of $\mathcal{G}_X$ labelled by a certain choice of the $x_{i,j}^{(q)}$ and which consists in codewords of the form $(z_{k,j}^{(q)})_{j:z_{k,j}=1}$ satisfying (4). All these codes (for k ranging over all rows of $\mathbf{H}_Z^{(q)}$) should be not reduced to the zero codeword. While this is easily achieved in the case of column weight 2 essentially by the fact that the number of check nodes of the Tanner graphs $\mathcal{G}_X(k)$ is always less than or equal to the number of variable nodes (since by Lemma 1 the degree of the check nodes is greater than or equal to 2 and the degree of the variable nodes is constant and equal to 2), this is not the case anymore when the column weight is higher.

IV. AN APPLICATION: THE EXTENDED TORIC CODE

A. Definition of the toric code and its extended version

The toric code (see [BK98] for more details) is a CSS code of length $2n^2$ which encodes 2 qubits. It is convenient to define the Tanner graphs $\mathcal{G}_X$ and $\mathcal{G}_Z$ of the couple $(\mathscr{C}_X, \mathscr{C}_Z)$ of binary codes of the CSS code simultaneously. Let C_X and C_Z be the set of variable nodes of $\mathcal{G}_X$ and $\mathcal{G}_Z$ respectively and

we identify the variable node sets V_X and V_Z of both codes, say $V_X = V_Z = V$. These graphs are defined as follows:

$$
\begin{aligned}
V &= \{(i,j) \in [0..2n-1] \times [0..2n-1] : i+j \text{ even}\} \\
C_X &= \{(i,j) \in [0..2n-1] \times [0..2n-1] : i \text{ odd}, j \text{ even}\} \\
C_Z &= \{(i,j) \in [0..2n-1] \times [0..2n-1] : i \text{ even}, j \text{ odd}\}
\end{aligned}
$$

A check node (i,j) is connected to 4 variable nodes $(i\pm 1, j\pm 1)$ in both graphs (where addition is performed modulo $2n$). The degree of the variable nodes is of course 2.

The construction, summarized on Fig 1, has the shape of a torus of length and width $2n$.
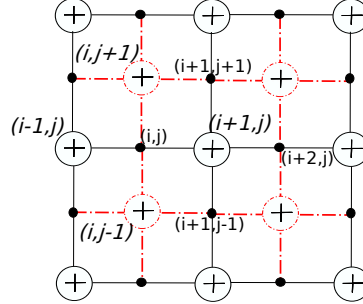

Fig. 1. The Tanner graph of the toric code, with both X and Z parts together. The black dots represent the qubits, the dotted crosses the checks of the Z part, and the black crosses the checks of the X part. The left part is identified to the right part, and the upper part to the lower part, so that the global shape of the graph is a torus.

Even if this code has as many checks as qubits, its dimension is positive: the rank of $\mathbf{H}_X$ and $\mathbf{H}_Z$ associated to $\mathcal{G}_X$ and $\mathcal{G}_Z$ is $n^2 - 1$ instead of n^2, thus the dimension is $\dim(\mathscr{C}_X) - \dim(\mathscr{C}_Z^\perp) = n^2 + 1 - (n^2 - 1) = 2$ (from (3)). The code has a rather large minimum distance [Kit03], however its performances when decoded with standard belief propagation is quite bad, because of the presence of many small cycles and also because the (classical) minimum distance of $\mathscr{C}_X$ and $\mathscr{C}_Z$ is only 4.

Now we construct a q-ary version of this code, in the same way as in Section III. In other terms, we just put some non-zero labels on the edges of the graph. For simplicity of notation we will further use $x_{i,j}$ to design $x_{i,j}^{(q)}$, the label in $\mathbb{F}_q \setminus \{0\}$ on the edge between check i and node j. Labeling is performed through Algorithm 1 by choosing the coefficients a_i and b_{jk} at random in Algorithm 2. We obtain a couple $(\mathscr{C}_X^{(q)}, \mathscr{C}_Z^{(q)})$ of q-ary codes satisfying

$$\mathscr{C}_Z^{(q)\perp} \subset \mathscr{C}_X^{(q)}.$$

We obtain the *extended toric code* by applying the aforementioned ring isomorphism to the entries of the parity-check matrices $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ of $\mathscr{C}_X^{(q)}$ and $\mathscr{C}_Z^{(q)}$: the resulting code has length $2mn^2$. We denote the couple of binary codes defining this toric code by $(\hat{\mathscr{C}}_X, \hat{\mathscr{C}}_Z)$.

B. Dimension

Strictly speaking, by applying Algorithm 1, the dimension of $\mathscr{C}_X^{(q)}$ minus the dimension of $\mathscr{C}_Z^{(q)\perp}$ could be smaller than

$\dim \mathscr{C}_X - \dim \mathscr{C}_Z$. Indeed $\mathbf{H}_X^{(q)}$ and $\mathbf{H}_Z^{(q)}$ might now be of full rank and we might have $\dim \mathscr{C}_X^{(q)} = \dim \mathscr{C}_Z^{(q)\perp} = n^2$. This would imply that $\dim \hat{\mathscr{C}}_X = \dim \hat{\mathscr{C}}_Z^{\perp}$ and the quantum dimension of the extended toric code would be 0. However, when we apply Algorithm 2 to choose the labels (so that the product of the labels $x_{i,j}$ over *all* cycles of $\mathcal{G}_X$ is equal to 1), then it will turn out that

$$\dim \mathscr{C}_X^{(q)} - \dim \mathscr{C}_Z^{(q)\perp} = \dim \mathscr{C}_X - \dim \mathscr{C}_Z^{\perp} = 2,$$

so that $\dim \hat{\mathscr{C}}_X - \dim \hat{\mathscr{C}}_Z = 2m$. This means that

Theorem 1 (Dimension of the extended toric code): If $\mathscr{C}_X^{(q)}$ and $\mathscr{C}_Z^{(q)}$ are constructed such that $\mathscr{C}_X^{(q)}$ verifies (6) and $\mathscr{C}_Z^{(q)\perp} \subset \mathscr{C}_X^{(q)}$, then the extended toric code has dimension $2m$.

Proof: This is shown with the help of two lemmas:

Lemma 2: If $\mathscr{C}_X^{(q)}$ verifies (6) and $\mathscr{C}_Z^{(q)\perp} \subset \mathscr{C}_X^{(q)}$, then $\mathscr{C}_Z^{(q)}$ verifies also (6).

Lemma 3: If $\mathscr{C}_X^{(q)}$ verifies (6), then it has q-ary dimension $n^2 + 1$.

From these two lemmas, we obtain that the dimension of $\mathscr{C}_X^{(q)}$ and $\mathscr{C}_Z^{(q)}$ is $n^2 + 1$, which gives

$$\dim \mathscr{C}_X^{(q)} - \dim \mathscr{C}_Z^{(q)\perp} = 2$$

This implies that the quantum dimension of the extended toric code is

$$\dim(\hat{\mathscr{C}}_X) - \dim(\hat{\mathscr{C}}_Z^{\perp}) = m(\dim \mathscr{C}_X^{(q)} - \dim \mathscr{C}_Z^{(q)\perp}) = 2m$$

$\blacksquare$

The proof of the two lemmas is given in the appendix.

C. Minimum distance

Choosing the product of the labels to be equal to 1 on all cycles of $\mathcal{G}_X$ brings another benefit : it allows to control the minimum distance, since we have in this case

Lemma 4: $\min\{|x| \in \mathscr{C}_X^{(q)} \setminus \mathscr{C}_Z^{(q)\perp}\} = \min\{|x| \in \mathscr{C}_Z^{(q)} \setminus \mathscr{C}_X^{(q)\perp}\} = n$.

The proof is given in the appendix. This implies that

Theorem 2 (minimum distance of the extended toric code): The minimum distance of the extended toric code is $\geq n$.

Proof: The minimum distance of the extended toric code is the minimal weight of a word from $\hat{\mathscr{C}}_X \setminus \hat{\mathscr{C}}_Z^{\perp}$ or $\hat{\mathscr{C}}_Z \setminus \hat{\mathscr{C}}_X^{\perp}$. The Hamming weight of such a word is greater than or equal to the Hamming weight of the word in $\mathscr{C}_X^{(q)} \setminus \mathscr{C}_Z^{(q)\perp}$ or $\mathscr{C}_Z^{(q)} \setminus \mathscr{C}_X^{(q)\perp}$ it corresponds to after taking the aforementioned ring isomorphism A. $\blacksquare$

Remark 1: There is also an upper bound on the minimum distance: it is at most nm, since a word of weight n in $\mathbb{F}_q$ has minimal weight n and maximal weight mn in $\mathbb{F}_2$.

V. RESULTS

We have implemented standard belief propagation over $\mathbb{F}_{2^m}$ to decode extended toric codes for several values of n and m (see Section III of [KHIK11]) but which correspond to the same final length $2mn^2$, which is 1152 here. We have chosen
(i) $m = 1$, $n = 24$,
(ii) $m = 4$, $n = 12$
(iii) $m = 9$, $n = 8$.
The channel error model is the depolarizing channel model with depolarizing probability p, meaning that the probability of an X, Y or Z error is $p/3$ which implies that the codes $\hat{\mathscr{C}}_X$ and $\hat{\mathscr{C}}_Z$ see a binary symmetric channel of probability $\frac{2p}{3}$.

The performance of belief propagation is quite bad in the binary case (that is for standard toric code), even if the qubit error rate is rather low, the whole error is typically badly estimated. On the other hand the performances get better by moving from $\mathbb{F}_2$ to $\mathbb{F}_{16}$ and become quite good over $\mathbb{F}_{512}$. This is remarkable since the length of these CSS codes is constant but the rate increases with m. For instance, the rate of the toric code is $\frac{1}{576}$ whereas the rate of the extended toric code over $\mathbb{F}_{512}$ is equal to $\frac{1}{64}$. It would be interesting to carry over the renormalizing approach of [DCP10] which improves dramatically belief propagation over standard toric codes and study how much it is able to improve the performance of standard belief propagation over these larger alphabets.
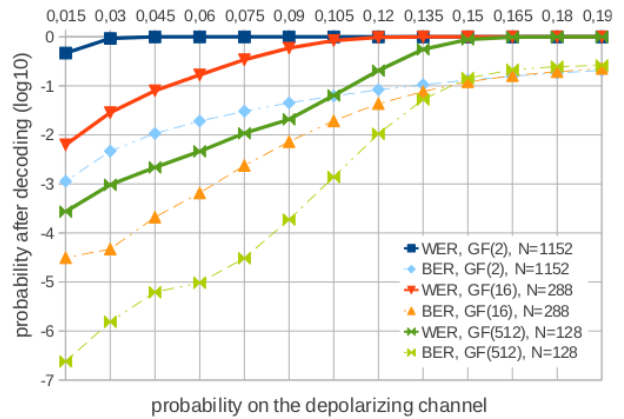

Fig. 2. Word and qubit error rates for several extended toric codes.

APPENDIX

Proof of Proposition 1: Let us consider a Tanner graph composed of a cycle $v_0, C_0, v_1, C_1, \ldots v_{k-1}, C_{k-1}$, and let $x_{i,j}$ be the label on the edge between check i and node j. A codeword $w_0 w_1, \ldots w_{k-1}$ of the code associated to this Tanner graph is such that:

$$
\begin{aligned}
x_{0,0} w_0 &+ x_{0,1} w_1 = 0 \\
x_{1,1} w_1 &+ x_{1,2} w_2 = 0 \\
&\cdots \\
x_{k-1,k-1} w_{k-1} &+ x_{k-1,0} w_0 = 0
\end{aligned}
$$

This system has non-trivial solutions if and only if the determinant of this system is 0, ie if:

$$x_{0,0} \ldots x_{k-1,k-1} + x_{0,1} \ldots x_{k-1,0} = 0$$
$$\iff \quad x_{0,0} x_{0,1}^{-1} \ldots x_{k-1,k-1} x_{k-1,0}^{-1} = 1$$

which means that the product over the cycle is 1.

If this condition is verified, and one of the w_i's is zero, for example w_0, we can see from the system that $w_1, \ldots w_{k-1}$ have to be equal to zero too. So the non-zero codewords have only non-zero positions. ∎

Proof of Lemma 2:

We consider here two basic types of cycles in the Tanner graphs of $\mathscr{C}_X^{(q)}$ and $\mathscr{C}_Z^{(q)}$: the minimal cycles of length 8, and cycles of length $2n$ that go through the length or the width of the torus, we call the last ones "big cycles". An example is shown on Fig 3.
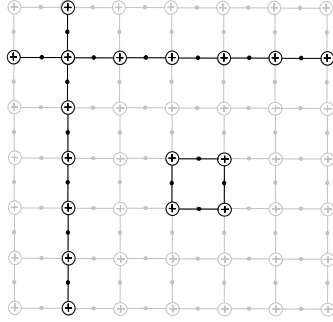
Fig. 3. Two big cycles (horizontal, vertical) and a minimal cycle.

More formally,

Definition 2 (minimal cycle): A *minimal cycle* in the Tanner graph of $\mathscr{C}_X^{(q)}$ or $\mathscr{C}_Z^{(q)}$ is a cycle of the form: $(i,j), (i+1,j), (i+1,j-1), (i+1,j-2), (i,j-2), (i-1,j-2), (i-1,j-1), (i-1,j), (i,j)$ with $i+j$ even, so that (i,j) is a variable node.

Definition 3 (Big cycle): A *horizontal big cycle* in the Tanner graph of $\mathscr{C}_X^{(q)}$ or $\mathscr{C}_Z^{(q)}$ is a cycle of the form: $(i,j), (i+1,j), \ldots (i+2n-1,j), (i,j)$, with $i+j$ even. [2]
A *vertical big cycle* in the Tanner graph of $\mathscr{C}_X^{(q)}$ or $\mathscr{C}_Z^{(q)}$ is a cycle $(i,j), (i,j+1), \ldots (i,j+2n-1), (i,j)$, with $i+j$ even.

Our first observation is that it is enough to prove Condition (6) on the minimal cycles and the big cycles of the Tanner graph of $\mathscr{C}_Z^{(q)}$, since the product of any other cycle in this Tanner graph can be decomposed as a product of products over these basic cycles.

Let us now consider a 4-cycle which lives in the union of the two Tanner graphs of $\mathscr{C}_X^{(q)}$ and $\mathscr{C}_Z^{(q)}$. It consists in two checks (see Fig 4) A and B, that are both connected to two variable nodes 1 and 2. From the orthogonality constraint $\mathbf{H}_X^{(q)} \mathbf{H}_Z^{(q)^T} = 0$, we deduce that the labels on the edges of this cycle satisfy

$$x_{A,1} z_{B,1} + x_{A,2} z_{B,2} = 0$$

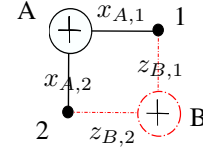[2]recall that addition on the indices is performed modulo $2n$.

Fig. 4. A 4-cycle. The black cross A is a check from $\mathscr{C}_X^{(q)}$, the dotted cross B is one from $\mathscr{C}_Z^{(q)}$, and the dots 1 and 2 are the qubits where they interact

We can reformulate this:

$$x_{A,1} z_{B,1} z_{B,2}^{-1} x_{A,2}^{-1} = 1$$

With the following definition, we obtain in this way that the product over such cycles of size 4 is equal to 1.

Definition 4 (Product over a cycle - extended version):
The notion of *product over a cycle* can be extended to the union of the Tanner graphs of $\mathscr{C}_X^{(q)}$ and $\mathscr{C}_Z^{(q)}$. If $v_1, c_1, v_2, \ldots, c_k, v_1$ is a cycle in this union, the product over this cycle is the product of all the labels of the edges over this cycle, with a power:

- 1 if the edge is check-to-variable node and belongs to the X-part,
- -1 if the edge is variable node-to-check and belongs to the X-part,
- -1 if the edge is check-to-variable node and belongs to the Z-part,
- 1 if the edge is variable node-to-check and belongs to the Z-part,

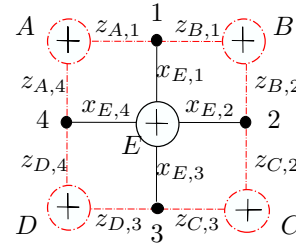Now, let us look at a combination of 4 such small cycles, as in Fig 5.

Fig. 5. A view of a X check (E) with the four related Z checks around (A, B, C, D).

The product over all small cycles is 1 :

$$z_{A,1}^{-1} x_{E,1}^{-1} x_{E,4} z_{A,4} = 1$$
$$z_{B,1} z_{B,2}^{-1} x_{E,2}^{-1} x_{E,1} = 1$$
$$x_{E,2} z_{C,2} z_{C,3}^{-1} x_{E,3}^{-1} = 1$$
$$x_{E,4}^{-1} x_{E,3} z_{D,3} z_{D,4}^{-1} = 1$$

By multiplying all these equations, we obtain:

$$z_{A,1}^{-1} z_{A,4} z_{B,1} z_{B,2}^{-1} z_{C,2} z_{C,3}^{-1} z_{D,3} z_{D,4}^{-1} = 1$$

which is exactly the product over a minimal cycle of $\mathscr{C}_Z^{(q)}$.

Now, we consider another combination of $2n$ 4-cycles such as in Fig 4, among one direction of the torus, as shown in Fig 6. It consists, in the subgraph of both Tanner graphs, in the variable and check nodes in the cartesian product $[0..2n-$

1] $\times \{0,1\}$. To simplify notation we have relabeled a variable node $(i,0)$ by $\frac{i}{2}+n$, a variable node $(i,1)$ by $\frac{i-1}{2}$, a check node $(i,1)$ corresponding to $\mathscr{C}_X^{(q)}$ by $\frac{i}{2}$ and a check node $(i,0)$ corresponding to $\mathscr{C}_Z^{(q)}$ also by $\frac{i-1}{2}$. It is summarized in Fig 6.
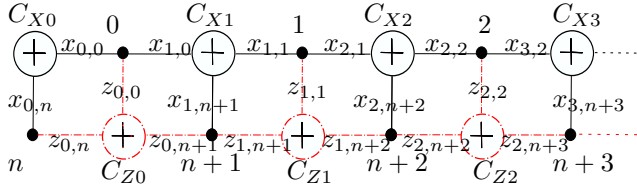

Fig. 6. An ensemble of small cycles of $\mathscr{C}_X^{(q)}$ (black) and $\mathscr{C}_Z^{(q)}$ (dotted).

The product over all such cycles is 1, ie:

$$x_{0,0}z_{0,0}z_{0,n}^{-1}x_{0,n}^{-1} = 1$$
$$x_{1,0}^{-1}x_{1,n+1}z_{0,n+1}z_{0,0}^{-1} = 1$$
$$x_{1,1}z_{1,1}z_{,1}n+1^{-1}x_{1,n+1}^{-1} = 1$$
$$\cdots$$
$$x_{n-1,n-1}z_{n-1,n-1}z_{n-1,2n-1}^{-1}x_{n-1,2n-1} = 1$$
$$x_{0,n-1}^{-1}x_{0,n}z_{n-1,n}z_{n-1,n-1} = 1$$

By multiplying all these equations, we get:

$$x_{0,0}z_{0,n}^{-1}x_{1,0}^{-1}z_{0,n+1} \cdots$$
$$x_{n-1,n-1}z_{n-1,2n-1}^{-1}x_{0,n-1}^{-1}z_{n-1,n} = 1$$
$$(x_{0,0}x_{1,0}^{-1} \cdots x_{n-1,n-1}x_{0,n-1}^{-1}) \times$$
$$(z_{0,n}^{-1}z_{0,n+1} \cdots z_{n-1,2n-1}^{-1}z_{n-1,n}) = 1$$

The first parenthesis is the product over a big cycle of $\mathscr{C}_X^{(q)}$, and the second parenthesis is the product over a big cycle of $\mathscr{C}_Z^{(q)}$.

It shows that if the product over a big horizontal cycle is equal to 1 in $\mathscr{C}_X^{(q)}$, then the product over a big horizontal cycle in $\mathscr{C}_Z^{(q)}$ is also equal to 1. There is a similar proof for the vertical cycles. ∎

Proof of lemma 3:

First, we show that the dimension of $\mathscr{C}_X^{(q)}$ is at least n^2+1.

The idea is to construct a set of independent codewords associated to cycles of the Tanner graph of $\mathscr{C}_X^{(q)}$. This is obtained as follows. Since all variable nodes of this Tanner graph have degree 2, we can consider the *graph of the checks*, where the vertices are the checks, and there is an edge between two vertices if and only if there is a variable node that is adjacent to the two checks. Informally, it just consists of the same graph where an "edge-variable node-edge" is replaced by a single edge. We consider a spanning tree of this graph. An example of such spanning tree is shown in Fig 7.

This spanning tree has of course n^2 checks, and therefore $n^2 - 1$ edges between these checks. There are $n^2 + 1$ other edges: let $e_1, \ldots e_{n^2+1}$ be such edges. For all i, adding e_i to the spanning tree provides a unique cycle, c_i. Let c_i' be the corresponding cycle in the original Tanner graph. Now, the product over each such cycle is 1. From Proposition 1, each of these cycles provides a codeword of $\mathscr{C}_X^{(q)}$. These n^2+1 codewords are necessarily independent, since for all the
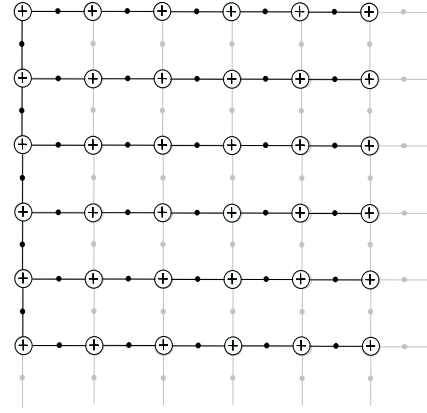

Fig. 7. A spanning tree (black) of the graph of the checks. The Tanner graph of the toric code is shown in grey.

positions which correspond to the edges $e_1, \ldots e_{n^2+1}$, exactly one of these codewords has a non zero entry (for the edge e_i it is precisely c_i' which has a non zero entry for this position).

To show that this dimension is at most $n^2 + 1$, we remove a certain check, say check c_r. We want to show that the remaining $n^2 - 1$ checks are independent. To obtain this, we prove that for any syndrome, we can construct an error that gives this syndrome. In particular, we show that for every check c_0, we can get the syndrome $(0, \ldots 0, 1, 0, \ldots 0)$ with 1 at position c_0.

Let $c_0, v_1, c_1, v_2, \ldots v_k, c_r$ be some path in the Tanner graph that links c_0 to c_r. An example of such path is shown in Fig 8.
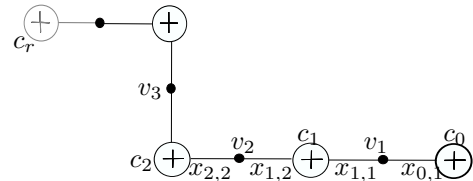

Fig. 8. A path between the removed check c_r (grey) and some check c_0 (bold).

Now we construct an error E that has 0 in every position except the v_i's:

- E_{v_1} is such that the syndrome in c_0 is 1, ie $E_{v_1} = 1/x_{0,1}$
- E_{v_2} such that c_1 has syndrome 0, ie $E_{v_2} = E_{v_1}\frac{x_{1,1}}{x_{1,2}}$, and so on and so forth.

Since c_r has been removed, all the checks except c_0 are satisfied. ∎

Proof of Lemma 4:

Consider an element E of minimal weight in the set $\mathscr{C}_Z^{(q)}/\mathscr{C}_X^{(q)\perp}$. We are going to prove that its weight is greater than or equal to n. A similar proof shows that this is also the case for the minimal weight elements of $\mathscr{C}_X^{(q)}/\mathscr{C}_Z^{(q)\perp}$ and this proves the lemma.

From Lemma 3, we know that the dimension of $\mathscr{C}_Z^{(q)}$ is n^2+1 and the dimension of $\mathscr{C}_X^{(q)\perp}$ is n^2-1. Then the quotient

$\mathscr{C}_Z^{(q)}/\mathscr{C}_X^{(q)\perp}$ has dimension 2, consequently we just need to find two independent codewords $\bar{X}_1$ and $\bar{X}_2 \in \mathscr{C}_Z^{(q)}/\mathscr{C}_X^{(q)\perp}$, and any such E can be written as $E = E_s + \alpha_1 \bar{X}_1 + \alpha_2 \bar{X}_2$, with $\alpha_1, \alpha_2 \in \mathbb{F}_q, E_s \in \mathscr{C}_X^{(q)\perp}$, and at least one of either α_1 or α_2 should be non zero.

We claim that we can choose $\bar{X}_1$ to be a codeword provided by a big vertical cycle of the Tanner graph of $\mathscr{C}_Z^{(q)}$ (obtained from Proposition 1), and $\bar{X}_2$ being defined similarly with a big horizontal cycle. We also define $\bar{Z}_1$ and $\bar{Z}_2$, provided by respectively a big horizontal cycle and a big vertical cycle of $\mathscr{C}_X^{(q)}$.

We notice that the following inner product is non zero

$$\bar{X}_1 \bar{Z}_1^T \neq 0$$

since there is only one coordinate where both $\bar{X}_1$ and $\bar{Z}_1$ are not zero.

Note that $\bar{X}_1$ belongs to $\mathscr{C}_Z^{(q)}$ by definition and $\bar{X}_1 \notin \mathscr{C}_X^{(q)\perp}$, otherwise $\bar{X}_1$ would have been orthogonal to all words of $\mathscr{C}_X^{(q)}$, including $\bar{Z}_1$. We have the same result for $\bar{X}_2$ (and $\bar{Z}_2$). We finally just need to prove that they are independent:

Assume that $\bar{X}_1 = \alpha \bar{X}_2 + E_s$, with α in $\mathbb{F}_q \setminus \{0\}$ and E_s in $\mathscr{C}_X^{(q)}$. Then we would have

$$\begin{aligned} \bar{X}_1 \bar{Z}_1^T &= \alpha \bar{X}_2 \bar{Z}_1^T + E_s \bar{Z}_1^T \\ &= \alpha \bar{X}_2 \bar{Z}_1^T \end{aligned}$$

since $E_s \bar{Z}_1^T = 0$ because $\bar{Z}_1 \in \mathscr{C}_X^{(q)}$ and $E_s \in \mathscr{C}_X^{(q)\perp}$.

The left part is non zero, and the right part is zero, since the supports of $\bar{X}_2$ and $\bar{Z}_1$ are disjoint. This leads to a contradiction.

Now assume E is of the form $E = \alpha_1 \bar{X}_1 + \alpha_2 \bar{X}_2 + E_s$ with either α_1 or α_2 being different from 0. We want to show that this error is of weight at least n. Assume now that $\alpha_1 \neq 0$.

We introduce n shifts of $\bar{Z}_1$: $\bar{Z}_1^i$, for all i even, $i \in \{0, \ldots 2n-2\}$ which is the codeword provided by the cycle: $(0,i),(1,i),\ldots(2n-1,i),(0,i)$. They are just horizontal cycles, at different "heights", as shown in Fig 9.

We have

$$E_s (\bar{Z}_1^i)^T = 0$$

since $\bar{Z}_1^i \in \mathscr{C}_X^{(q)}$ and $E_s \in \mathscr{C}_X^{(q)\perp}$, and

$$\bar{X}_1 (\bar{Z}_1^i)^T \neq 0$$

Notice that we have for all i:

$$\begin{aligned} E(\bar{Z}_1^i)^T &= \alpha_1 \bar{X}_1 (\bar{Z}_1^i)^T + \alpha_2 \bar{X}_2 (\bar{Z}_1^i)^T + E_s (\bar{Z}_1^i)^T \\ &= \alpha_1 \bar{X}_1 (\bar{Z}_1^i)^T \\ &\neq 0 \end{aligned}$$

This implies that for all i, E has at least a non-zero coordinate on the support of $\bar{Z}_1^i$. Since all $\bar{Z}_1^i$'s have disjoint support, it shows that E has at least n non-zero coordinates. A similar reasoning holds in the case $\alpha_2 \neq 0$ by multiplying by $\bar{Z}_2$ this time. $\blacksquare$
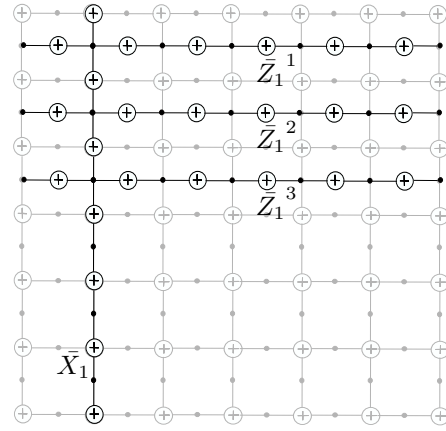

Fig. 9. The toric code (only the Z-part is displayed) of length 6 with $\bar{X}_1$ and several variants of $\bar{Z}_1$

REFERENCES

[Aly07]   S. A. Aly. A class of quantum LDPC codes derived from Latin squares and combinatorial objects. Technical report, Department of Computer Science, Texas A&M University, April 2007.

[Aly08]   S. A. Aly. A class of quantum LDPC codes constructed from finite geometries. In *Proceedings of IEEE GLOBECOM 2008*, pages 1–5, December 2008.

[BK98]   S. B. Bravyi and A. Kitaev. Quantum codes on a lattice with boundary, 1998. quant-ph/9811052.

[COT05]   T. Camara, H. Ollivier, and J.-P. Tillich. Constructions and performance of classes of quantum LDPC codes, 2005. arXiv:quant-ph/0502086v2.

[COT07]   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*, pages 811–815, Nice, June 2007. IEEE.

[CRSS98]   A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Info. Theor.*, 44:1369, 1998.

[CS96]   A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996.

[DCP10]   G. Duclos-Cianci and D. Poulin. Fast decoders for topological quantum codes. *Phys. Rev. Lett.*, 104(050504), 2010.

[Djo08]   I. B. Djordjevic. Quantum LDPC codes from incomplete block designs. *IEEE Communication Letters*, 12(5):389–391, May 2008.

[Gal63]   R. G. Gallager. *Low Density Parity Check Codes*. M.I.T. Press, Cambridge, Massachusetts, 1963.

[GFL08]   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*, pages 562–567, Princeton, March 2008.

[Got97]   D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, Pasadena, CA, 1997.

[HB68]   S. L. Hakimi and J. G. Bredeson. Graph theoretic error-correcting codes. *IEEE Trans. on Information Theory*, 14:584–591, 1968.

[HBD08]   M-H. Hsieh, T. A. Brun, and I. Devetak. Quantum quasi-cyclic low-density parity check codes, March 2008. arXiv:0803.0100v1 [quant-ph].

[HEA05]   X. Hu, E. Eleftheriou, and D.M. Arnold. Regular and irregular progressive edge-growth Tanner graphs. *IEEE Trans. on Information Theory*, 51(1):386–398, January 2005.

[HI07]   M. Hagiwara and H. Imai. Quantum quasi-cyclic LDPC codes. In *Proc. IEEE Int. Symp. Info. Theo. (ISIT'07)*, pages 806–811, Nice, June 2007. IEEE.

[Hu02]   X. Hu. *Low-delay low-complexity error-correcting codes on sparse graphs*. PhD thesis, EPFL, Lausanne, Switzerland, 2002.

[IM07]   L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. Lett. A.*, 2007.

[KHIK11] K. Kasai, M. Hagiwara, H. Imai, and Sakaniwa K. Quantum error correction beyond the bounded distance decoding limit. *IEEE Trans. Info. Theor.*, 2011. to appear, see also arXiv:1007.17782v2[cs.IT].

[Kit03]   A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *Ann. Phys.*, 303:2, 2003.

[LGF06]   H. Lou and J. Garcia-Frias. On the application of error-correcting codes with low-density generator matrix over different quantum channels. In *Proceedings of Turbo-coding 2006*, Munich, April 2006.

[MMM04]   D. J. C. MacKay, G. Mitchison, and P. L. MacFadden. Sparse graph codes for quantum error-correction. *IEEE Trans. Info. Theor.*, 50(10):2315–2330, 2004.

[Pos01]   M. S. Postol. A proposed quantum low density parity check code, 2001. available at `arXiv:quant-ph/0108131v1`.

[SMK08]   K. P. Sarvepalli, M.Rötteler, and A. Klappenecker. Asymmetric quantum LDPC codes. In IEEE, editor, *Proceedings of ISIT 2008*, pages 305–309, Toronto, Canada, July 2008.

[Ste96]   A. M. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. Lond. A*, 452:2551–2577, 1996.

[TL10]   P. Tan and J. Li. Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions. *IEEE Trans. Info. Theor.*, 56(1):476–491, 2010.

[TZ09]   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*, pages 799–803, July 2009.