Improved Quantum Hypergraph-Product LDPC Codes

arXiv:1202.0928v2

- Alexey A. Kovalev

Collaborators:

- Leonid Pryadko (University of California, Riverside)

OUTLINE

- Why *LDPC codes* are useful.

- LDPC code construction from two binary matrices.
  - Relation to *toric codes* and *hypergraph product codes*.
  - Example of quantum LDPC (generalized toric) code with *finite rate*.

- Improvements of quantum LDPC codes by permutations corresponding to *toric code rotation* (checker board codes).
  - *Bipartite* and *non-bipartite* constructions result from permutations, improve the code rate up to four times (important at small blocklength).

CONSTRUCTING FAMILIES OF LDPC CODES

1. Easy error correction for such codes: simple quantum measurements, easy classical processing, and parallelism.

2. We hope that some of such codes will allow fault tolerant error correction and computation via local deformations, in analogy to toric codes.

3. To this end, we construct binary quantum stabilizer codes with low weight stabilizer generators. We consider Pauli group

$$\mathscr{P}_n = i^m \{I, X, Y, Z\}^{\otimes n},\ m = 0, \ldots, 3$$

An $[[n, k, d]]$ stabilizer code $\mathcal{Q}$ is a 2^k-dimensional subspace of the Hilbert space $\mathcal{H}_2^{\otimes n}$ stabilized by an Abelian stabilizer group $\mathscr{S} = \langle G_1, \ldots, G_{n-k} \rangle$, $-\mathbb{1} \notin \mathscr{S}$; $\mathcal{Q} = \{|\psi\rangle : S\,|\psi\rangle = |\psi\rangle\,, \forall S \in \mathscr{S}\}$.

BINARY REPRESENTATION

Pauli operators are mapped to two binary strings, $\mathbf{v}, \mathbf{u} \in \{0,1\}^n$,
$U \equiv i^{m'} X^{\mathbf{v}} Z^{\mathbf{u}} \;\rightarrow (\mathbf{v}, \mathbf{u})$, where $X^{\mathbf{v}} = X_1^{v_1} X_2^{v_2} ... X_n^{v_n}$ and $Z^{\mathbf{u}} = Z_1^{u_1} Z_2^{u_2} ... Z_n^{u_n}$.
A product of two quantum operators corresponds to a sum $(\mathrm{mod}\, 2)$ of the corresponding pairs $(\mathbf{v}_i, \mathbf{u}_i)$.

In this representation, a stabilizer code is represented by parity check matrix written in binary form for X and Z Pauli operators so that,
e.g. XIYZYI=-(XIXIXI)x(IIZZZI) -> (101010)|(001110).

$$
\begin{array}{cc}
\text{Ax} & \text{Az}
\end{array}
$$

$$
H=\left(\begin{array}{cccccccccccccccccc|cccccccccccccccccc}
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0 & 1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0 & 0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0 & 0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0 & 0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0 & 0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0 & 0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0 & 1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1 & 0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1 & 0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0
\end{array}\right)
$$

Example of a parity check matrix *H* of a toric code written in X-Z form.

$$\boxed{A_X A_Z^T + A_Z A_X^T = 0}$$

Necessary and sufficient condition for existence of stabilizer code with stabilizer commuting operators corresponding to A.

QUANTUM CODE FROM TWO CLASSICAL

We construct a stabilizer code from two classical codes with parity check matrices (may have linearly dependent rows/columns):

$$\overset{n_1}{r_1\,\mathcal{H}_1} \qquad \overset{n_2}{r_2\,\mathcal{H}_2}$$

Such ansatz ensures commutativity!

$$\boldsymbol{H=}\left(\begin{array}{cc|cc} \mathrm{E}_2\times\mathcal{H}_1 & 0 & 0 & \mathcal{H}_2\times\mathrm{E}_1 \\ 0 & \tilde{\mathrm{E}}_2\times\mathcal{H}_1^{\mathrm{T}} & \mathcal{H}_2^{\mathrm{T}}\times\tilde{\mathrm{E}}_1 & 0 \end{array}\right)$$

E – unit matrix and (x) – Kronecker product.

Constructed code has parameters [[N,K,D]]!

Commutativity follows from:

$$(A\times B)(C\times D) = AC\times BD$$

$$N = n_1 r_2 + n_2 r_1$$

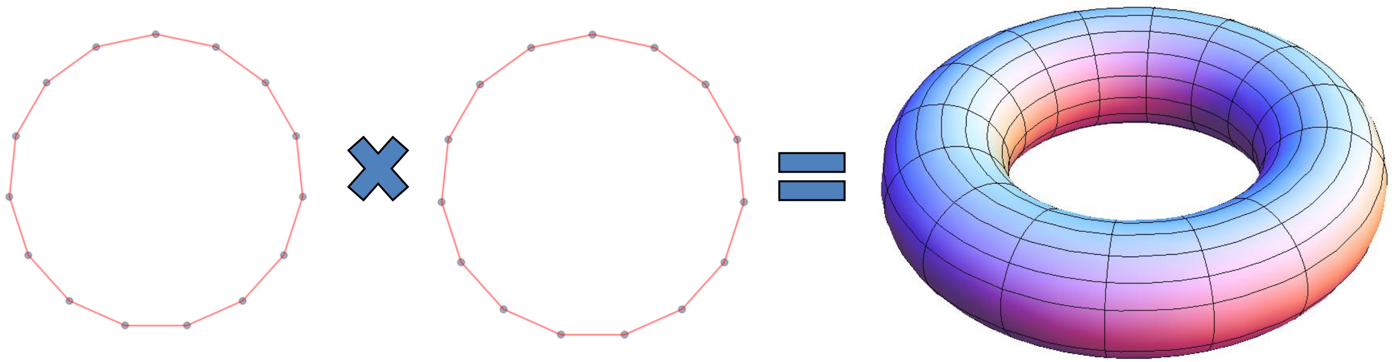
$$K = 2\dim(C_{\mathcal{H}_1})\dim(C_{\mathcal{H}_2}) - \dim(C_{\mathcal{H}_1})(n_2 - r_2) - \dim(C_{\mathcal{H}_2})(n_1 - r_1)$$

$$D \geq \mathrm{Min}[\mathrm{dist}(\mathcal{H}_1), \mathrm{dist}(\mathcal{H}_2), \mathrm{dist}(\mathcal{H}_1^T), \mathrm{dist}(\mathcal{H}_2^T)]$$

CONNECTION WITH GRAPHS AND HYPERGRAPHS

Example: Toric code is obtained when binary code $\mathcal{H}_1$ is a repetition code given by nxn circulant matrix! The parameters are [[2n^2, 2, n]], $\mathcal{H}_2^T = \mathcal{H}_1$

A. Y. Kitaev, Ann. Phys., vol. 303, p. 2, 2003



$$H = \left(\begin{array}{c|c} G_X & 0 \\ 0 & G_Z \end{array} \right), \quad \begin{array}{c} G_X = (E_2 \otimes \mathcal{H}_1 \;\; \mathcal{H}_2 \otimes E_1), \\ G_Z = (\mathcal{H}_2^T \otimes \widetilde{E}_1 \;\; \widetilde{E}_2 \otimes \mathcal{H}_1^T). \end{array}$$

In CSS form, Gx and Gz correspond to two dual hypergraphs.

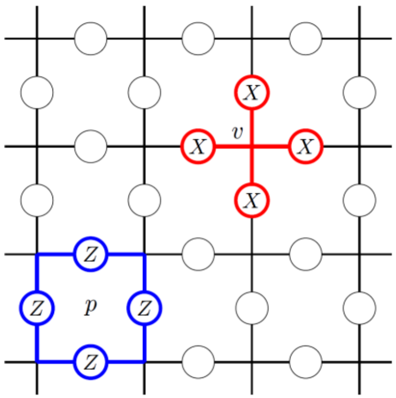
Tilich & Zemor, in Information Theory, (2009), arxiv:0903.0566.

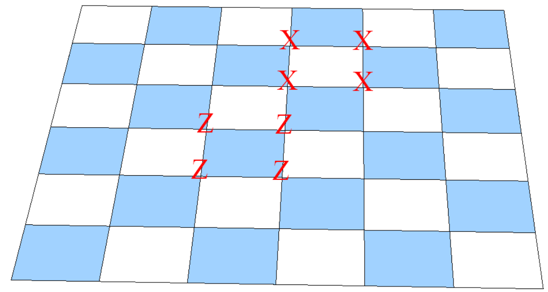
Example: Suppose we take LDPC code [n,k,d] with full rank matrix $\mathcal{H}_1$; $\mathcal{H}_2^T = \mathcal{H}_1$ $n-k$
then parameters of the quantum code are: n

$$[[(n-k)^2 + n^2, k^2, d]]$$

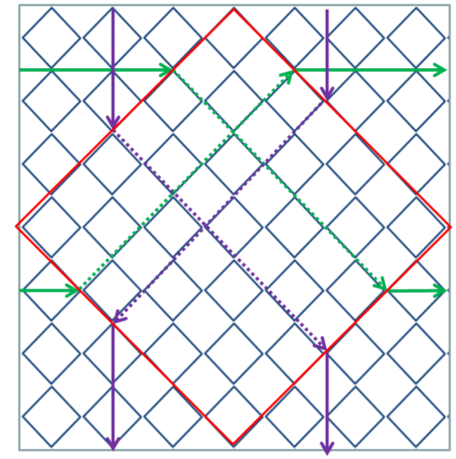
Example: If $\mathcal{H}_1$ is a circulant matrix of a cyclic code ([n,k,d]) given by nxn matrix, then parameters of the corresponding quantum codes are [[2n^2, 2k^2, d]], $\mathcal{H}_2^T = \mathcal{H}_1$

OPTIMIZING TORIC CODE BY ROTATION

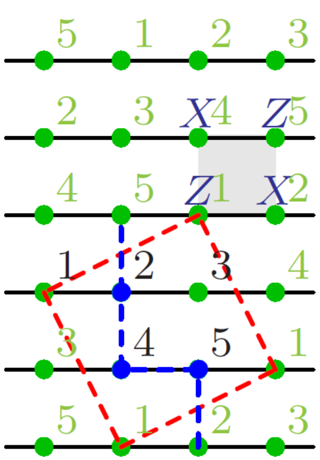




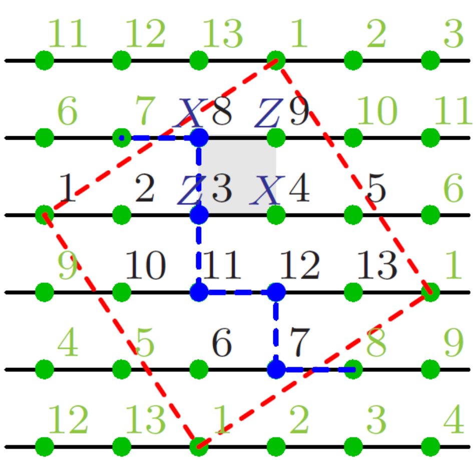
Even case!



Toric code can be broken into two rotated toric codes by the procedure on the right; rotated by 45 degrees codes have the same distance but twice smaller blocklength.
Examples: [[9,1,3]], [[25,1,5]], [[16,2,4]] and [[36,2,6]].



[[5,1,3]] Toric code



[[13,1,5]] Toric code

H. Bombin and M. A. Martin-Delgado, Phys. Rev. A, vol. 76, no. 1, p.012305, 2007

When the translation vectors are (a,b) and (b,-a) (orthogonal), then n=a^2+b^2, d=|a|+|b|, and k=1 if d is odd or 2 if d is even.
The example is for a=t+1, b=t, with t=1,2.

A. A. Kovalev, I. Dumer, and L. P. Pryadko, Phys. Rev. A, vol. 84, p. 062319, 2011

ROTATED HYPERGRAPH CODES

Similar to toric code, the hypergraph code can be "rotated" by
45 degrees which can lead to improved parameters (e.g. halved blocklength).

"Rotation" corresponds to application of a permutation $\prod$:

$$H=\left(\begin{array}{cc|cc} E_2\times\mathcal{H}_1 & 0 & 0 & \Pi\left(\mathcal{H}_2\times E_1\right)\Pi \\ 0 & \tilde{E}_2\times\mathcal{H}_1^T & \Pi\left(\mathcal{H}_2^T\times\tilde{E}_1\right)\Pi & 0 \end{array}\right)$$

Even case!

$$\prod = \frac{1}{2}\sum_{i=0}^{3}(\sigma_i \times E_{1/2}) \times (\sigma_i \times E_{1/2})$$

$$\mathcal{H} = \sigma_0 \times K + \sigma_x \times M$$

When the classical code has block structure the corresponding stabilizer generators commute.

We have two possibilities for permutations, just like when we construct checker board codes [[25,1,5]] (non-bipartite) and [[16,2,4]] (bipartite) from toric codes depending on parity of blocklength.

NON-BIPARTITE CASE

Such codes can be constructed from two symmetric matrices:

$$H = (E_2 \otimes \mathcal{H}_1 | \mathcal{H}_2 \otimes E_1), \quad \mathcal{H}_i^T = \mathcal{H}_i, \quad i = 1, 2.$$

Any classical code in a standard form $\mathcal{H}_1 = (\mathbb{1}, P)$ can be symmetrized:

$$\mathcal{H}_1^{\text{symmetrized}} = \begin{pmatrix} \mathbb{1} & P \\ P^T & P^T P \end{pmatrix},$$

The procedure allows us to make codes with smaller blocklength, same distance:

$$\mathcal{Q}^{\text{symm}} = [[n_1 n_2, k_1 k_2, \min(d_1, d_2)]],$$

e.g. [[225,100,4,weight(7)]] and [[225,49,5,weight(4)]].

Non CSS construction!

BIPARTITE CASE

We can also construct CSS codes from two block matrices corresponding to classical codes:

$$\mathcal{H}_1 = \sigma_0 \otimes a_1 + \sigma_x \otimes b_1, \quad \mathcal{H}_2^p = a_2 \otimes \sigma_0 + b_2 \otimes \sigma_x,$$

$$\boxed{\begin{array}{l} G_X = (E_2^{(1/2)} \otimes \mathcal{H}_1, \mathcal{H}_2^p \otimes E_1^{(1/2)}), \\ G_Z = (\mathcal{H}_2^{pT} \otimes \widetilde{E}_1^{(1/2)}, \widetilde{E}_2^{(1/2)} \otimes \mathcal{H}_1^T), \end{array} \qquad H = \left(\begin{array}{c|c} G_X & 0 \\ 0 & G_Z \end{array} \right),}$$

In such construction the unit matrices are half size compared to hypergraph product codes which improves code parameters. The commutativity of stabilizer generators can be easily checked.

Example. Suppose we have a classical cyclic code given by a generator polynomial $g(x)$ with parameters $[n, k, d]$. If $\mathcal{H}_1$ is the square parity matrix corresponding to the polynomial $h(x) = (1 - x^n)/g(x)$ $((1 - x^{n/2}) = h(x)\alpha(x))$ and $\mathcal{H}_2^T = \mathcal{H}_1$ then the corresponding quantum code has parameters $[[n^2, 2k^2, d]]$, e.g. [[900,200,8,weight(14)]], [[900,50,14, weight(8)]], [[900,98,10, weight(8)]], [[36,8,4,weight(6)]] and [[24,4,4,weight(5)]].

CONCLUSIONS

- We construct new families (generalized toric codes) of LDPC codes with finite rate and distance growing as the square root of blocklength.
- We improve the hypergraph construction, increasing the rates up to four times, which is especially useful for small-blocklength versions of such codes.
- We identify two situations corresponding to a bipartite and a non-bipartite geometry.

- Questions:

  1) Fault tolerant operations with such codes.

  2) Non-45 degree rotations of generalized toric codes.