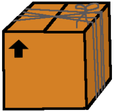
Non binary quantum LDPC codes

Denise Maurice (INRIA)
Iryna Andriyanova (ENSEA), Jean-Pierre Tillich (INRIA)

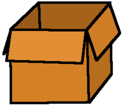
Journées C2

October 9, 2012

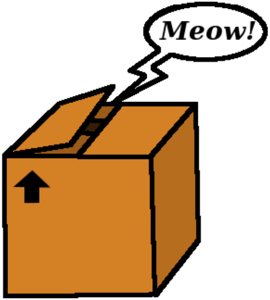
Why do we need quantum error correction?

- Quantum state:  $\Rightarrow$ $|\psi\rangle = \alpha|$$> +\beta|$$>$

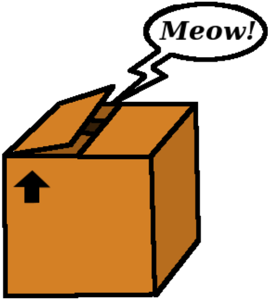
  where $\{|$$, |$$\}$ is an orthonormal basis of $\mathbb{C}^2, \alpha, \beta \in \mathbb{C}$

- Measurement:  $\Rightarrow$ either $\begin{cases} |$$>$ w.p. α^2 \\ $|$$>$ w.p. β^2 \end{cases}$

Observe = Measure = Modify!

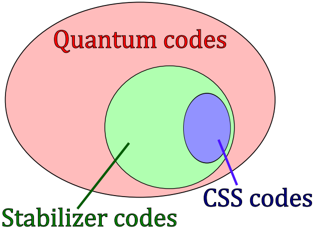


- $\Rightarrow$ If our system is not perfectly isolated, there will be "unexpected measurements", and errors



- $\Rightarrow$ If our system is not perfectly isolated, there will be "unexpected measurements", and errors
- $\Rightarrow$ In a quantum computer, there would be errors during the computation...
- $\Rightarrow$ We need *efficient* error-correcting codes!

CSS codes



- Quantum codes: continuous space, complicated
- Stabilizer codes: classical codes over $\mathbb{F}_4$
- CSS codes: binary codes

CSS code

A *CSS code* is given by a pair of matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ (of sizes $r_X \times n$ and $r_Z \times n$) that verify

$$\mathbf{H}_X {\mathbf{H}_Z}^{\intercal} = 0$$

CSS codes

- Length: n
- Dimension: $n - \text{rank}(\mathbf{H}_X) - \text{rank}(\mathbf{H}_Z)$
- Minimum distance: $\min(d_X, d_Z)$, where
  $d_X = \min|w|, w \in \mathcal{C}_X \backslash \mathcal{C}_Z^\perp, \quad d_Z = \min|w|, w \in \mathcal{C}_Z \backslash \mathcal{C}_X^\perp,$
  where $\mathcal{C}_X = \{w, \mathbf{H}_X w^\intercal = 0\}, \quad \mathcal{C}_Z = \{w, \mathbf{H}_Z w^\intercal = 0\}$
  and $\mathcal{C}_X^\perp = \text{Vect}(\text{rows of } \mathbf{H}_X), \quad \mathcal{C}_Z^\perp = \text{Vect}(\text{rows of } \mathbf{H}_Z)$
  Note: $\mathcal{C}_X \in \mathcal{C}_Z^\perp$ *and* $\mathcal{C}_Z \in \mathcal{C}_X^\perp$
- Decoding: decoding of $\mathcal{C}_X$ and $\mathcal{C}_Z$

LDPC codes

$$\begin{aligned} \text{LDPC} &= \text{Low Density Parity Check (matrix)} \\ &= \text{Matrices } \mathbf{H}_X \text{ and } \mathbf{H}_Z \text{ are } \textit{sparse} \end{aligned}$$

LDPC codes

$$
\begin{aligned}
\text{LDPC} &= \text{Low Density Parity Check (matrix)} \\
&= \text{Matrices } \mathbf{H}_X \text{ and } \mathbf{H}_Z \text{ are } \textit{sparse}
\end{aligned}
$$

Why?

- Small size
- Efficient algorithm (O(non-zero entries)) for decoding: Belief Propagation

But...

- Not fully adaptated to the quantum case: the rows of $\mathbf{H}_Z$ give small codewords for $\mathcal{C}_X$ (since $\mathbf{H}_X {\mathbf{H}_Z}^\intercal = 0$) on which the decoder fails (even if not in $\mathcal{C}_X \backslash \mathcal{C}_Z^\perp$).

Kasai's construction

Kasai et al, *IEEE transactions on Information Theory*, Sep 2011.

- Construct a $(2, L)$ pair of quasi-cyclic codes that verify the condition $\mathbf{H}_X {\mathbf{H}_Z}^\intercal = 0$,
- Replace each "1" in both matrices with a non-zero element of $\mathbb{F}_q$, and make sure that we still have $\mathbf{H}_X^{(q)} {\mathbf{H}_Z^{(q)}}^\intercal = 0$ in $\mathbb{F}_q$ $(q = 2^m)$,
- Replace each element by a $m \times m$ matrix of $\mathbb{F}_2$, with a ring isomorphism, such that the final matrices verify $\hat{\mathbf{H}}_X \hat{\mathbf{H}}_Z^\intercal = 0$

Decoding is performed in $\mathbb{F}_q$.

Our contribution

- Generalized construction: works with *any* pair of code that verifies the condition and has variable node degree 2,
- Applied to the family of toric code, we can ensure a non-bounded minimum distance and an increasing dimension,
- Performances under BP decoding are significantly improved

From $\mathbb{F}_2$ to $\mathbb{F}_q$

Let ${\mathbf{H}_Z^{(q)}}_i$ be a row of $\mathbf{H}_Z^{(q)}$. We want:

$$\mathbf{H}_X^{(q)} {\mathbf{H}_Z^{(q)}}_i^{\mathsf{T}} = 0$$

We remove from $\mathbf{H}_X^{(q)}$ all columns that have no common entry with ${\mathbf{H}_Z^{(q)}}_i$, and all the empty rows. Ex:

$$\begin{pmatrix} 0 & 0 & * & \bullet \\ \diamond & 0 & 0 & \triangle \\ \star & \square & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \spadesuit \\ \clubsuit \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & * \\ \square & 0 \end{pmatrix} \begin{pmatrix} \spadesuit \\ \clubsuit \end{pmatrix}$$

From $\mathbb{F}_2$ to $\mathbb{F}_q$

Let ${\mathbf{H}_Z^{(q)}}_i$ be a row of $\mathbf{H}_Z^{(q)}$. We want:

$$\mathbf{H}_X^{(q)} {\mathbf{H}_Z^{(q)}}_i^{\mathsf{T}} = 0$$

We remove from $\mathbf{H}_X^{(q)}$ all columns that have no common entry with ${\mathbf{H}_Z^{(q)}}_i$, and all the empty rows. Ex:

$$\begin{pmatrix} 0 & 0 & * & \bullet \\ \diamond & 0 & 0 & \triangle \\ \star & \square & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \spadesuit \\ \clubsuit \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & * \\ \square & 0 \end{pmatrix} \begin{pmatrix} \spadesuit \\ \clubsuit \end{pmatrix}$$

We want to make sure that all these systems have non-trivial solutions.

Tanner graph

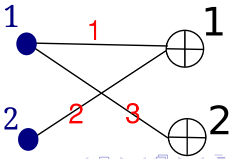
Tanner graph

The associated Tanner graph of a $r \times n$ matrix H is the bipartite graph defined by:

- The first set of nodes, called *variable nodes* $V = \{1, \dots n\}$
- The second set, called *check nodes* $C = \{1, \dots r\}$
- There is an edge between node i and check j iff $H_{ij} \neq 0$. In this case the edge is labeled by H_{ij}.

Ex:

$$H = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$$



In our reduced matrix:

- Each row has an even number of non-zero entries

In our reduced matrix:

- Each row has an even number of non-zero entries
- Each column has 2 non-zero entries

In our reduced matrix:

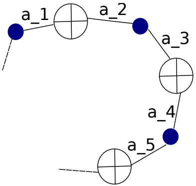
- Each row has an even number of non-zero entries
- Each column has 2 non-zero entries

$\Rightarrow$ The associated reduced Tanner graph has even degrees for all nodes (variable & checks).

$\Rightarrow$ It can be decomposed into a set of *disjoint cycles*.

$$\mathbf{H}_{X\ red}^{(q)} = \begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_k \end{pmatrix}, C_i = \begin{pmatrix} a_1 & & & a_{2l} \\ a_2 & a_3 & & \\ & \dots & \dots & \\ & & a_{2l-2} & a_{2l-1} \end{pmatrix}$$

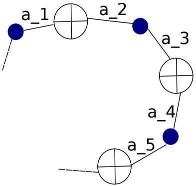
$$\det C_i = a_1 \dots a_{2l-1} - a_2 \dots a_{2l}$$



$$\det C_i = 0 \iff a_1^{-1} a_2 a_3^{-1} \dots a_{2l} = 1$$

$$\mathbf{H}_{X\ red}^{(q)} = \begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_k \end{pmatrix}, C_i = \begin{pmatrix} a_1 & & & a_{2l} \\ a_2 & a_3 & & \\ & \dots & \dots & \\ & & a_{2l-2} & a_{2l-1} \end{pmatrix}$$

$$\det C_i = a_1 \dots a_{2l-1} - a_2 \dots a_{2l}$$



$$\det C_i = 0 \iff a_1^{-1} a_2 a_3^{-1} \dots a_{2l} = 1$$

$$\det C_i = 0 \iff \text{product over the cycle} = 1$$

Product over a cycle

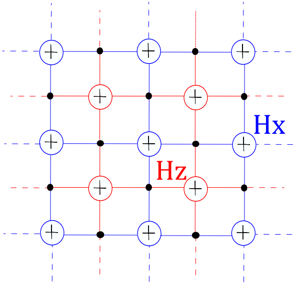
The product over a cycle $v_1, c_1, v_2, \dots, c_k, v_1$ is the product of all the coefficients of the edges over this cycle, with a power 1 if it is a check-to-node edge, and -1 if it is node-to-check.

Cycle condition

For all cycles $\mathcal{C}$ of the Tanner graph associated to $\mathbf{H}_X^{(q)}$, product over $\mathcal{C} = 1$.

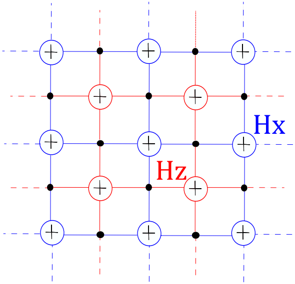
- We provide an algorithm (runs in $O(\text{edges})$) that gives entries of $\mathbf{H}_X^{(q)}$ such that this condition is verified.
- Then we can solve all the systems and find entries for $\mathbf{H}_Z^{(q)}$.

The toric code



- Length: $2n^2$
- Dimension: 2

The toric code



- Length: $2n^2$
- Dimension: 2

Good:

- Minimum distance: n
- Simple structure: (2,4)-regular

Bad:

- Small dimension
- Bad performances with BP (small codewords)

The extended toric code

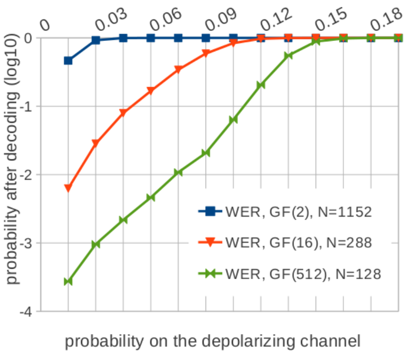
Theorem: parameters of the extended toric code

The extended toric code has:

- length $2mn^2$,
- dimension $2m$,
- minimum distance at least n

Error model: depolarizing channel with e.p. p, equivalent of a BSC with $p' = 2/3p$.

Performances:



Conclusion

- Better performances (for a simple decoding algorithm)
- Same structure (min distance & dimension in general case?)
- Hard to construct with codes that don't have degree node 2
- Application: cycle codes