Non binary quantum LDPC codes

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

Journées C2

October 9, 2012
1 Introduction
   - Quantum error-correction
   - LDPC quantum codes

2 Codes in $\mathbb{F}_q$
   - Construction
   - Application to the toric code

3 Conclusion
Why do we need quantum error correction?

- Quantum state:
  \[ |\psi\rangle = \alpha |\text{\large \ding{100}}\rangle + \beta |\text{\large \ding{110}}\rangle \]

  where \( \{|\text{\large \ding{100}}, |\text{\large \ding{110}}\rangle \} \) is an orthonormal basis of \( \mathbb{C}^2 \), \( \alpha, \beta \in \mathbb{C} \)

- Measurement:
  \[ \Rightarrow \] either

  \[ \begin{align*}
  |\text{\large \ding{100}}\rangle & \quad \text{w.p. } \alpha^2 \\
  |\text{\large \ding{110}}\rangle & \quad \text{w.p. } \beta^2
  \end{align*} \]

Observe = Measure = Modify!
If our system is not perfectly isolated, there will be "unexpected measurements", and errors.
⇒ If our system is not perfectly isolated, there will be "unexpected measurements", and errors

⇒ In a quantum computer, there would be errors during the computation...

⇒ 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 $H_X$ and $H_Z$ (of sizes $r_X \times n$ and $r_Z \times n$) that verify

$$H_X H_Z^T = 0$$
CSS codes

- Length: $n$
- Dimension: $n - \text{rank}(H_X) - \text{rank}(H_Z)$
- Minimum distance: $\min(d_X, d_Z)$, where
  \[ d_X = \min |w|, w \in C_X \setminus C_Z, \quad d_Z = \min |w|, w \in C_Z \setminus C_X, \]
  where $C_X = \{ w, H_X w^T = 0 \}$, $C_Z = \{ w, H_Z w^T = 0 \}$
  and $C_X^\perp = \text{Vect}(\text{rows of } H_X)$, $C_Z^\perp = \text{Vect}(\text{rows of } H_Z)$
  Note: $C_X \in C_Z^\perp$ and $C_Z \in C_X^\perp$
- Decoding: decoding of $C_X$ and $C_Z$
LDPC codes

LDPC = Low Density Parity Check (matrix)

= Matrices $H_X$ and $H_Z$ are *sparse*
LDPC codes

\[
\begin{align*}
\text{LDPC} & = \text{Low Density Parity Check (matrix)} \\
& = \text{Matrices } H_X \text{ and } H_Z \text{ are sparse}
\end{align*}
\]

Why?

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

But...

- Not fully adapted to the quantum case: the rows of $H_Z$ give small codewords for $C_X$ (since $H_X H_Z^T = 0$) on which the decoder fails (even if not in $C_X \setminus C_Z^\perp$).
Kasai’s construction


- Construct a \((2, L)\) pair of quasi-cyclic codes that verify the condition \(H_X H_Z^\top = 0\),

- Replace each "1" in both matrices with a non-zero element of \(\mathbb{F}_q\), and make sure that we still have \(H_X^{(q)} H_Z^{(q)^\top} = 0\) 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 \(\hat{H}_X \hat{H}_Z^\top = 0\).

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 $H_{Z_i}^{(q)}$ be a row of $H_Z^{(q)}$. We want:

$$H_X^{(q)} H_{Z_i}^{(q)T} = 0$$

We remove from $H_X^{(q)}$ all columns that have no common entry with $H_{Z_i}^{(q)}$, and all the empty rows. Ex:

$$\begin{pmatrix} 0 & 0 & \ast & \bullet \\ \diamond & 0 & 0 & \triangle \\ \ast & \Box & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \spadesuit \\ \heartsuit \end{pmatrix} \rightarrow \begin{pmatrix} 0 & \ast \\ \Box & 0 \end{pmatrix} \begin{pmatrix} \spadesuit \\ \heartsuit \end{pmatrix}$$
From $\mathbb{F}_2$ to $\mathbb{F}_q$

Let $H_Z^{(q)}_i$, be a row of $H_Z^{(q)}$. We want:

$$H_X^{(q)} H_Z^{(q)^T} = 0$$

We remove from $H_X^{(q)}$ all columns that have no common entry with $H_Z^{(q)}_i$, and all the empty rows. Ex:

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

We want to make sure that all these systems have non-trivial solutions.
Non binary quantum LDPC codes

Codes in $\mathbb{F}_q$

Construction

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* $V = \{1, \ldots n\}$
- The second set, called *check nodes* $C = \{1, \ldots r\}$
- 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:**

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

![Tanner graph example](image-url)
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

⇒ The associated reduced Tanner graph has even degrees for all nodes (variable & checks).
⇒ It can be decomposed into a set of *disjoint cycles*.
Non binary quantum LDPC codes

Codes in $\mathbb{F}_q$

Construction

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

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

$$\det C_i = 0 \iff a_1^{-1} a_2 a_3^{-1} \cdots a_{2l} = 1$$
Non-binary quantum LDPC codes

Codes in $\mathbb{F}_q$

Construction

\[ \mathbf{H}_X^{(q)}_\text{red} = \begin{pmatrix} C_1 & \cdots & \vdots & \cdots & \cdots \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ C_k & \cdots & C_1 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \vdots & \ddots & \vdots & \ddots & \vdots \end{pmatrix}, \quad C_i = \begin{pmatrix} a_1 \\ a_2 \\ \cdots \\ a_{2l} \\ \cdots \\ a_2 \\ a_1 \end{pmatrix} \]

\[ \det C_i = a_1 \ldots a_{2l-1} - a_2 \ldots a_{2l} \]

\[ \det C_i = 0 \iff a_1^{-1} a_2 a_3^{-1} \ldots a_{2l} = 1 \]

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

**Product over a cycle**

The product over a cycle $v_1, c_1, v_2, \ldots, c_k, v_1$ 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 $C$ of the Tanner graph associated to $H^{(q)}_X$, product over $C = 1$.

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

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

Non binary quantum LDPC codes

- Codes in $\mathbb{F}_q$
- Application to the toric code

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

Bad:
- Small dimension
- Bad performances with BP (small codewords)
The toric code

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

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

Length: $2n^2$
Dimension: 2
Non binary quantum LDPC codes

Codes in $\mathbb{F}_q$

Application to the toric code

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 $n$


**Performances:**

![Graph showing the performances of the extended toric code with different error probabilities and field sizes.](image-url)
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