NEW QUANTUM CAPS IN PG(4,4)

Daniele Bartoli

joint work with

Stefano Marcugini and Fernanda Pambianco

Summer Doctoral School 2009
Groebner bases, Geometric codes and Order Domains

Trento 8-14 June 2009
SUMMARY

1. Physical introduction to Quantum Codes
SUMMARY

1. Physical introduction to Quantum Codes
2. Mathematical description of Quantum Codes
SUMMARY

1. Physical introduction to Quantum Codes
2. Mathematical description of Quantum Codes
3. Search and classification of Quantum Caps in $PG(4, 4)$
SUMMARY

1. Physical introduction to Quantum Codes
2. Mathematical description of Quantum Codes
3. Search and classification of Quantum Caps in $PG(4, 4)$
4. Results
Definition

**Quantum Code**

set of configurations of a certain number of qubits.

\[ \alpha |0\rangle + \beta |1\rangle \in \mathcal{H}_2(\mathbb{C}), \]

where \( \alpha \) and \( \beta \) are complex numbers such that \( |\alpha|^2 + |\beta|^2 = 1 \).
1. Measurement destroys informations:
   it is not possible to know the phases $\alpha$ and $\beta$ of a single qubit.

   \[ \text{MEASUREMENT} \]

   \[
   \begin{align*}
   0 & \quad |\alpha|^2 \\
   1 & \quad |\beta|^2
   \end{align*}
   \]
1. Measurement destroys informations:
it is not possible to know the phases $\alpha$ and $\beta$ of a single qubit.

\[ \begin{align*}
0 & \quad |\alpha|^2 \\
1 & \quad |\beta|^2
\end{align*} \]

2. No cloning theorem
1. Measurement destroys informations:
   it is not possible to know the phases $\alpha$ and $\beta$ of a single qubit.

\[
\begin{array}{cc}
0 & |\alpha|^2 \\
1 & |\beta|^2 \\
\end{array}
\]

MEASUREMENT

2. No cloning theorem

3. Qubit errors are a continuum.
PAULI MATRICES

$$\begin{align*}
\mathbb{I} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\
\sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\end{align*}$$

| Identity     | $\mathbb{I}$ | $\mathbb{I}|a\rangle = |a\rangle$ |
|--------------|--------------|----------------------------------|
| Bit Flip     | $\sigma_x$   | $\sigma_x|a\rangle = |a \oplus 1\rangle$ |
| Phase Flip   | $\sigma_z$   | $\sigma_z|a\rangle = (-1)^a|a\rangle$ |
| Bit and Phase Flip | $\sigma_y$ | $\sigma_y|a\rangle = i(-1)^a|a \oplus 1\rangle$ |
**ERROR OPERATORS**

\[ E = (A_1 \otimes \ldots \otimes A_n), \quad A_i = \langle B_i^1, \ldots, B_i^{j_i} \rangle \]

\[ B_i^{j_i} \in \{I, \sigma_x, \sigma_y, \sigma_z\} . \]

**BASE ERROR OPERATORS**

\[ E \in \langle B_{1}^{l_1} \otimes \ldots \otimes B_{n}^{l_n} \rangle, \quad \text{where } l_i = 1, \ldots, j_i . \]

**PRODUCT OF TWO ERRORS**

\[ E \times F = (A_1 \otimes \ldots \otimes A_n) \times (B_1 \otimes \ldots \otimes B_n) \]

\[ = (A_1 \times B_1) \otimes \ldots \otimes (A_n \times B_n) \]
QUANTUM STABILIZER CODES

Let $C$ be a set of possible quantic configurations of $n$ qubits. Let $\mathcal{G}$ be the set of all error-operators.

$$S = \{ E \in \mathcal{G} \mid E|\psi\rangle = |\psi\rangle \ \forall \psi \in C \}$$

is the set of the operators which fix all the codewords.

$$ME + EM = 0 \implies ME|\psi_i\rangle = -EM|\psi_i\rangle = -E|\psi_i\rangle$$

$$ME = EM \implies ME|\psi_i\rangle = EM|\psi_i\rangle = E|\psi_i\rangle$$

The stabilizer quantum code can correct all the errors of the set $\mathcal{E}$, s.t.

$$E_a^H E_b \in S \cup (\mathcal{G} \setminus N(S)) \ \forall E_a, E_b \in \mathcal{E}$$

$N(S)$ : the set of the operators which commute with the elements of $S$. 
Physical introduction to Quantum Codes
Mathematical description of Quantum Codes
Search and classification of Quantum Caps in $PG(4,4)$

Results

TRANSLATION:

\[ T(\sigma_x) = 10 \quad T(\sigma_y) = 11 \]
\[ T(\sigma_z) = 01 \quad T(\mathbb{I}) = 00 \]

SYMPLECTIC FORM

Let $F = GF(2)$ and $V = F^{2n}$. $\Phi : V \times V \to F$

\[ \omega_1 = (x_{1,1}y_{1,1}, x_{1,2}y_{1,2}, \ldots, x_{1,n}y_{1,n}) \]
\[ \omega_2 = (x_{2,1}y_{2,1}, x_{2,2}y_{2,2}, \ldots, x_{2,n}y_{2,n}) \]
\[ \Phi(\omega_1, \omega_2) = \sum_{i=1}^{n} (x_{1,i}y_{2,i} - y_{1,i}x_{2,i}) \]

$B_i \times B_j = B_j \times B_i \iff \Phi(T(B_i), T(B_j)) = 0$

$B_i \times B_j = -B_j \times B_i \iff \Phi(T(B_i), T(B_j)) = 1$
**Matrix of Quantum Stabilizer Code**

\[
\begin{pmatrix}
P_{1,1}Q_{1,1} & P_{1,2}Q_{1,2} & \cdots & P_{1,n}Q_{1,n} \\
P_{2,1}Q_{2,1} & P_{2,2}Q_{2,2} & \cdots & P_{2,n}Q_{2,n} \\
& \vdots & \ddots & \vdots \\
P_{n-k,1}Q_{n-k,1} & P_{n-k,2}Q_{n-k,2} & \cdots & P_{n-k,n}Q_{n-k,n}
\end{pmatrix}
\]

\[P_{i,j}, Q_{i,j} \in \mathbb{Z}_2 \quad \forall i = 1, \ldots, n-k \quad j = 1, \ldots, n.\]
Definition
An additive quaternary code $\mathcal{C}$ is a quaternary quantum stabilizer code if

$$\mathcal{C} \subset \mathcal{C}^\perp$$

The duality is with respect to the symplectic form.
Definition
A quantum code $C$ with parameters

$$n, k, d \quad (\text{[[}n, k, d\text{]]-code}), \quad k > 0,$$

is a quaternary quantum stabilizer code of binary dimension $n - k$ satisfying the following:

any codeword of $C^\perp$ having weight $\leq d - 1$ is in $C$.  

Definition

A quantum code $C$ with parameters

$$n, k, d \quad (\text{[[}n, k, d\text{]]-code}), \quad k > 0,$$

is a quaternary quantum stabilizer code of binary dimension $n - k$ satisfying the following:

any codeword of $C^\perp$ having weight $\leq d - 1$ is in $C$.

The code is **pure** if $C^\perp$ does not contain codewords of weight $< d$, equivalently if $C$ has **strength** $t \geq d - 1$. 
Definition
A quantum code $C$ with parameters

$$n, k, d \quad ([n, k, d]\text{-code}), \quad k > 0,$$

is a quaternary quantum stabilizer code of binary dimension $n - k$ satisfying the following:

any codeword of $C^\perp$ having weight $\leq d - 1$ is in $C$.

The code is **pure** if $C^\perp$ does not contain codewords of weight $< d$, equivalently if $C$ has **strength** $t \geq d - 1$.

An $[[n, 0, d]]$-code $C$ is a **self-dual** quaternary quantum stabilizer code of **strength** $t = d - 1$. 
### Matrix of Quantum Stabilizer Code

\[
\begin{pmatrix}
    P_{1,1}Q_{1,1} & P_{1,2}Q_{1,2} & \cdots & P_{1,n}Q_{1,n} \\
    P_{2,1}Q_{2,1} & P_{2,2}Q_{2,2} & \cdots & P_{2,n}Q_{2,n} \\
    \vdots & \vdots & \ddots & \vdots \\
    P_{n-k,1}Q_{n-k,1} & P_{n-k,2}Q_{n-k,2} & \cdots & P_{n-k,n}Q_{n-k,n}
\end{pmatrix}
\]

\(P_{i,j}, Q_{i,j} \in \mathbb{Z}_2\) \(\forall i = 1, \ldots, n - k \quad j = 1, \ldots, n.\)
Theorem

[BFGMP 07-08] The following are equivalent:

► a [[n, k, t + 1]4 pure quantum code;
► a set of n lines in PG(n − k − 1, 2):
  ► any t of which are in general position
  ► for each secundum S (subspace of codimension 2) the number of lines which are skew to S is even.

Definition

A code is **linear over \( GF(4) \)** if it is closed under multiplication by \( \omega \) \((\omega^2 + \omega + 1 = 0)\).

A \([[n, k, d]]\)-quantum code **linear over \( GF(4) \)** can be described by a generator matrix of dimension \( \frac{n-k}{2} \times n \):

\[
\bar{G} = \begin{pmatrix}
W_{1,1} & W_{1,2} & \ldots & W_{1,n} \\
W_{2,1} & W_{2,2} & \ldots & W_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
W_{\frac{n-k}{2},1} & W_{\frac{n-k}{2},2} & \ldots & W_{\frac{n-k}{2},n}
\end{pmatrix}
\]
Theorem

[BFGMP 07-08] The following are equivalent:

1. A pure quantum $[[n, k, d]]$-code which is linear over $\text{GF}(4)$.

2. A set of $n$ points in $\text{PG}(\frac{n-k}{2} - 1, 4)$ of strength $t = d - 1$, s.t. the intersection size with any hyperplane has the same parity as $n$.

3. An $[n, k]_4$ linear code of strength $t = d - 1$, all of whose weights are even.

4. An $[n, k]_4$ linear code of strength $t = d - 1$ which is self-orthogonal with respect to the Hermitian form.
SEARCH FOR COMPLETE QUANTUM CAPS

1. We start computing non-equivalent complete and incomplete caps in $PG(3, 4)$;

2. We try to extend every starting cap joining new points in $PG(4, 4)$;

3. The searching algorithm organizes the caps in a tree and the extension process ends when the obtained caps are complete;

4. Some considerations about equivalence of caps allow us not to consider, during the process, the caps that will produce caps already found or equivalent to one of these;

5. We control if the non-equivalent complete caps obtained are quantum stabilizer codes, using the hyperplane condition and weights distribution.
REMARK

The following are equivalent:

1. An \([n, k, d']_q\)-code with \(d' \geq d\).
2. A multiset \(\mathcal{M} \subset PG(k - 1, q)\):
   - \(|\mathcal{M}| = n\)
   - for every hyperplane \(H \subset PG(k - 1, q)\) there are at least \(d\) points of \(\mathcal{M}\) outside \(H\) (in the multiset sense).

NEW QUANTUM CAPS IN PG(4, 4)

\[
\begin{cases}
[n, k, d]_4 \\
n \geq 19 \implies d \leq n - 8 \\
k = 5
\end{cases}
\]
SEARCH FOR COMPLETE QUANTUM CAPS

1. We start computing non-equivalent complete and incomplete caps in $PG(3,4)$;
2. We try to extend every starting cap joining new points in $PG(4,4)$;
3. The searching algorithm organizes the caps in a tree and the extension process ends when the obtained caps are complete;
4. Some considerations about equivalence of caps allow us not to consider, during the process, the caps that will produce caps already found or equivalent to one of these;
5. We control if the non-equivalent complete caps obtained are quantum stabilizer codes, using the hyperplane condition and weights distribution.
Physical introduction to Quantum Codes
Mathematical description of Quantum Codes
Search and classification of Quantum Caps in $PG(4,4)$
Results

STARTING CAP $\in PG(3,4)$

FIXED POINT $\in PG(4,4) \setminus PG(3,4)$

NO!!
SEARCH FOR COMPLETE QUANTUM CAPS

1. We start computing non-equivalent complete and incomplete caps in $PG(3,4)$;
2. We try to extend every starting cap joining new points in $PG(4,4)$;
3. The searching algorithm organizes the caps in a tree and the extension process ends when the obtained caps are complete;
4. Some considerations about equivalence of caps allow us not to consider, during the process, the caps that will produce caps already found or equivalent to one of these;
5. We control if the non-equivalent complete caps obtained are quantum stabilizer codes, using the hyperplane condition and weights distribution.
RESULTS

- CLASSIFICATION
RESULTS

- CLASSIFICATION
- EXAMPLES

NEW QUANTUM CAPS IN PG(4,4)
RESULTS

- CLASSIFICATION
- EXAMPLES
- MINIMUM ORDER OF COMPLETE CAPS IN $PG(4, 4)$
Non-equivalent caps $\mathcal{K}$ in $PG(3, 4)$

| $|\mathcal{K}|$ | # COMPLETE CAPS | # INCOMPLETE CAPS |
|---|---|---|
| 8 | 0 | 15 |
| 9 | 0 | 19 |
| 10 | 1 | 22 |
| 11 | 0 | 15 |
| 12 | 5 | 8 |
| 13 | 1 | 3 |
| 14 | 1 | 1 |
| 15 | 0 | 1 |
| 16 | 0 | 1 |
| 17 | 1 | 0 |
Non-equivalent complete quantum-caps $\mathcal{K}$ in $PG(4,4)$

<table>
<thead>
<tr>
<th>Sizes of obtained Caps</th>
<th>Numbers of obtained Caps</th>
<th>Sizes and Types of starting Caps</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>1</td>
<td>12 complete</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>17 complete</td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>13 incomplete</td>
</tr>
<tr>
<td>30</td>
<td>1</td>
<td>16 incomplete</td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td>16 incomplete</td>
</tr>
<tr>
<td>33</td>
<td>3</td>
<td>13 incomplete</td>
</tr>
<tr>
<td>34</td>
<td>$&gt;130$</td>
<td>16 incomplete</td>
</tr>
</tbody>
</table>
Average execution time extending $\mathcal{K}$, $10 \leq |\mathcal{K}| \leq 17$

| $|\mathcal{K}|$ | AVERAGE EXECUTION TIME |
|---|---|
| 17 | <20'' |
| 16 | 1' |
| 15 | 2' |
| 14 | 20' |
| 13 | 40' |
| 12 | 1 h 20' |
| 11 | 4 h |
| 10 | 8 h |

Average execution time extending $\mathcal{K}$, $|\mathcal{K}| = 8, 9$

| $|\mathcal{K}|$ | AVERAGE EXECUTION TIME |
|---|---|
| 9 | 29 h |
| 8 | 6 d |
MINIMUM SIZE

Theorem

\[ \mathcal{K} \subset PG(4, 4) \text{ complete cap}, \]

\[ |\mathcal{K}| \geq 20. \]
THANKS FOR THE ATTENTION!