The spectrum of linear pure quantum $[[n, n-10, 4]]$-codes

Stefano Marcugini

joint work with

Daniele Bartoli and Fernanda Pambianco

ACCT 2010

SUMMARY

1. Historical introduction

SUMMARY

1. Historical introduction
2. Basic definitions

SUMMARY

1. Historical introduction
2. Basic definitions
3. Geometrical point of view

SUMMARY

1. Historical introduction
2. Basic definitions
3. Geometrical point of view
4. Search and classification of quantum caps in $PG(4,4)$

SUMMARY

1. Historical introduction
2. Basic definitions
3. Geometrical point of view
4. Search and classification of quantum caps in $PG(4,4)$
5. Results

Heisenberg uncertainty principle

$\Downarrow$

Quantum mechanics

$\Downarrow$

quantum information

The fundamental unit of quantum information is the **quantum bit** (qubit), which is like a two states physical system (0 and 1) on which the superposition principle acts.

The fundamental unit of quantum information is the **quantum bit** (qubit), which is like a two states physical system (0 and 1) on which the superposition principle acts.

This principle states that more than one state is present in the system at the same time. Physically a qubit is a two state quantum system, like the electron spin (up and down).

The idea of using quantum mechanical effects to perform computations was first introduced by **Feyman** in the 1980s, when he discovered that classical computers could not simulate all the aspects of quantum physics efficiently.

The idea of using quantum mechanical effects to perform computations was first introduced by **Feyman** in the 1980s, when he discovered that classical computers could not simulate all the aspects of quantum physics efficiently.

In 1985 **Deutsch** showed that it is possible to implement any function which is computable by classical computers using registers of entangled qubits and array of quantum gates.

The idea of using quantum mechanical effects to perform computations was first introduced by **Feyman** in the 1980s, when he discovered that classical computers could not simulate all the aspects of quantum physics efficiently.

In 1985 **Deutsch** showed that it is possible to implement any function which is computable by classical computers using registers of entangled qubits and array of quantum gates.

In 1994 **Shor** presented an algorithm which can factor an integer in polynomial time.

DECOHERENCE

One of the most important problems in constructing quantum computer is decoherence.

DECOHERENCE

One of the most important problems in constructing quantum computer is decoherence.

In the process of decoherence some qubits become entangled with the environment and this makes the state of the quantum computer *collapse*.

DECOHERENCE

One of the most important problems in constructing quantum computer is decoherence.

In the process of decoherence some qubits become entangled with the environment and this makes the state of the quantum computer *collapse*.

The conventional assumption was that once one qubit has decohered, the entire computation of the quantum computer is corrupted and the result of the computation will not be correct.

In 1995 **Shor** analyzed the problem of reducing the effects of decoherence for information stored in quantum memory, using the quantum analog of error correcting codes, and presented a procedure to encode a single qubit in nine qubits which can restore the original state if no more than one qubit of a nine-tuple decoheres.

It is an example of $[[9,1,3]]$-code.

Definition

Quantum Code

set of configurations of a certain number of qubits.

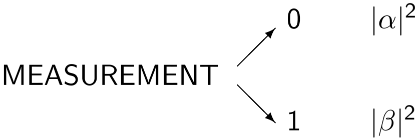
Qubit

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

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

PROBLEMS

1. Measurement destroys information:
   it is not possible to know the phases α and β of a single qubit.



PROBLEMS

1. Measurement destroys information:
   it is not possible to know the phases α and β of a single qubit.

   MEASUREMENT → 0 $\quad |\alpha|^2$
   MEASUREMENT → 1 $\quad |\beta|^2$

2. *No cloning theorem*

PROBLEMS

1. Measurement destroys information:
   it is not possible to know the phases α and β of a single qubit.

$$\text{MEASUREMENT} \begin{cases} \nearrow \; 0 & |\alpha|^2 \\ \searrow \; 1 & |\beta|^2 \end{cases}$$

2. *No cloning theorem*
3. Qubit errors are a *continuum*.

PAULI MATRICES

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

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

ERROR OPERATORS

$$E = (A_1 \otimes \ldots \otimes A_n), \quad A_i = \langle B_i^1, \ldots, B_i^{j_1} \rangle$$

$$B_i^j \in \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}.$$

BASE ERROR OPERATORS

$$E \in \langle B_1^{l_1} \otimes \ldots \otimes B_n^{l_n} \rangle, \quad \text{where } l_i = 1, \ldots, j_i.$$

QUANTUM STABILIZER CODES

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

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

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

QUANTUM STABILIZER CODES

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

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

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

$$\begin{aligned} ME = EM \quad &\Longrightarrow \quad ME|\psi_i\rangle = EM|\psi_i\rangle = E|\psi_i\rangle \\ ME + EM = 0 \quad &\Longrightarrow \quad ME|\psi_i\rangle = -EM|\psi_i\rangle = -E|\psi_i\rangle \end{aligned}$$

QUANTUM STABILIZER CODES

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

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

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

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

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

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

$N(\mathcal{S})$: the set of the operators which commute with the elements of $\mathcal{S}$.

TRANSLATION :

$$T(\sigma_x) = 10 \qquad T(\sigma_y) = 11$$

$$T(\sigma_z) = 01 \qquad T(\mathbb{I}) = 00$$

TRANSLATION :

$$T(\sigma_x) = 10 \qquad T(\sigma_y) = 11$$
$$T(\sigma_z) = 01 \qquad T(\mathbb{I}) = 00$$

SYMPLECTIC FORM

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

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

TRANSLATION :

$$T(\sigma_x) = 10 \qquad T(\sigma_y) = 11$$
$$T(\sigma_z) = 01 \qquad T(\mathbb{I}) = 00$$

SYMPLECTIC FORM

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

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

$$B_i \times B_j = B_j \times B_i \iff \Phi(T(B_i), T(B_j)) = 0$$
$$B_i \times B_j = -B_j \times B_i \iff \Phi(T(B_i), T(B_j)) = 1$$

MATRIX OF QUANTUM STABILIZER CODE

$$\begin{pmatrix} P_{1,1}Q_{1,1} & P_{1,2}Q_{1,2} & \dots & P_{1,n}Q_{1,n} \\ P_{2,1}Q_{2,1} & P_{2,2}Q_{2,2} & \dots & P_{2,n}Q_{2,n} \\ \vdots & \vdots & & \vdots \\ P_{n-k,1}Q_{n-k,1} & P_{n-k,2}Q_{n-k,2} & \dots & P_{n-k,n}Q_{n-k,n} \end{pmatrix}$$

$$P_{i,j}, Q_{i,j} \in \mathbb{Z}_2 \quad \forall i = 1, \dots, n-k \quad j = 1, \dots, n.$$

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 $\mathcal{C}$ 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:

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

Definition

A quantum code $\mathcal{C}$ 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 $\mathcal{C}^{\perp}$ having weight $\leq d - 1$ is in $\mathcal{C}$.

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

Definition

A quantum code $\mathcal{C}$ 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 $\mathcal{C}^{\perp}$ having weight $\leq d - 1$ is in $\mathcal{C}$.

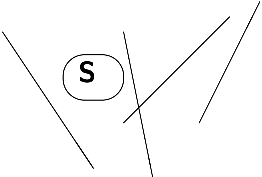
The code is **pure** if $\mathcal{C}^{\perp}$ does not contain codewords of weight $< d$, equivalently if $\mathcal{C}$ has **strength** $t \geq d - 1$.

An $[[n, 0, d]]$-code $\mathcal{C}$ is a **self-dual** quaternary quantum stabilizer code of **strength** $t = d - 1$.

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.*

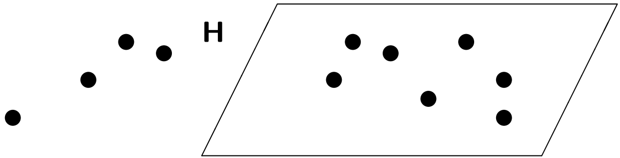


The geometry of quantum codes, J. Bierbrauer, G. Faina, M. Giulietti, S. M., F. Pambianco. *Innovation in Incidence Geometry* **6-7** (2007-2008) 53-71.

Theorem

[*BFGMP 07-08*] *The following are equivalent:*

1. *A pure quantum* $[[n,k,d]]$*-code which is linear over* $GF(4)$.
2. *A set of n points in* $PG(\frac{n-k}{2}-1,4)$ *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.*

The geometry of quantum codes, J. Bierbrauer, G. Faina, M. Giulietti, S. M., F. Pambianco. *Innovation in Incidence Geometry* **6-7** (2007-2008) 53-71.

In 1999 **Bierbrauer and Edel** showed that 41 is the maximum size of complete caps in $PG(4,4)$ and this cap is quantic.

In 2003 the same authors presented a complete 40-cap in $AG(4,4)$ which is also quantic.

In 1999 **Bierbrauer and Edel** showed that 41 is the maximum size of complete caps in $PG(4,4)$ and this cap is quantic.

In 2003 the same authors presented a complete 40-cap in $AG(4,4)$ which is also quantic.

In 2008 **Tonchev** constructed quantum caps of sizes $10, 12, 14-27, 29, 31, 33, 35$, starting from the complete 41-quantum cap in $PG(4,4)$.

It is not difficult to see that this method cannot produce quantum caps of sizes between 36 and 40 in $PG(4,4)$.

In 2010 **Bartoli, Bierbrauer, M. and Pambianco** showed examples of quantum caps of sizes $13, 28, 30, 32, 34, 36, 38$.

In 2010 **Bartoli, Bierbrauer, M. and Pambianco** showed examples of quantum caps of sizes $13, 28, 30, 32, 34, 36, 38$.

In 2010 **Bartoli, M. and Pambianco** showed that there exist no examples of quantum caps of sizes 11, 37 and 39.

In 2010 **Bartoli, Bierbrauer, M. and Pambianco** showed examples of quantum caps of sizes $13, 28, 30, 32, 34, 36, 38$.

In 2010 **Bartoli, M. and Pambianco** showed that there exist no examples of quantum caps of sizes 11, 37 and 39.

Theorem

If $\mathcal{K} \subset PG(4,4)$ is a quantum cap, then $10 \leq |\mathcal{K}| \leq 41$, with $|\mathcal{K}| \neq 11, 37, 39$.

SEARCH FOR 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 caps obtained correspond to quantum stabilizer codes, using the weights distribution condition.

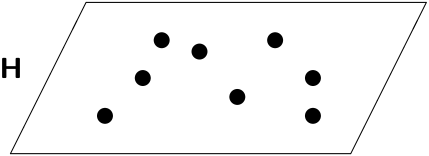
REMARK

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).

The smallest size of a complete cap in $PG(3, 7)$, J. Bierbrauer, S. M.,F. Pambianco. *Discrete Mathematics* **306** (2006), 1257-1263.

$$\begin{cases} [n,k,d]_4 \\ k = 5 \\ n \geq 19 \quad \Longrightarrow \quad d \leq n-8 \end{cases}$$

$\exists$ **H** 

Non-equivalent caps $\mathcal{K}$ in $PG(3,4)$

$\|\mathcal{K}\|$	# COMPLETE CAPS	# INCOMPLETE CAPS	CORRESPONDING SIZES IN $PG(4,4)$
7	0	8	≤ 17
8	0	16	≤ 24
9	0	19	≤ 25
10	1	22	≤ 30
11	0	15	≤ 35
12	5	8	≤ 40
13	1	3	≤ 41
14	1	1	≤ 41
15	0	1	≤ 41
16	0	1	≤ 41
17	1	0	≤ 41

SEARCH FOR 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 $PG(4,4)$;

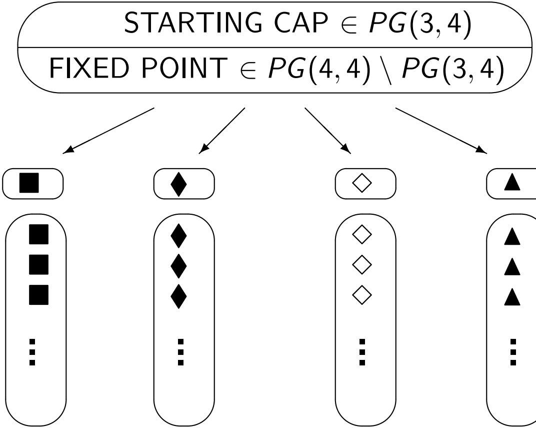
3. The searching algorithm organizes the caps in a tree and the extension process ends when the obtained caps are complete;

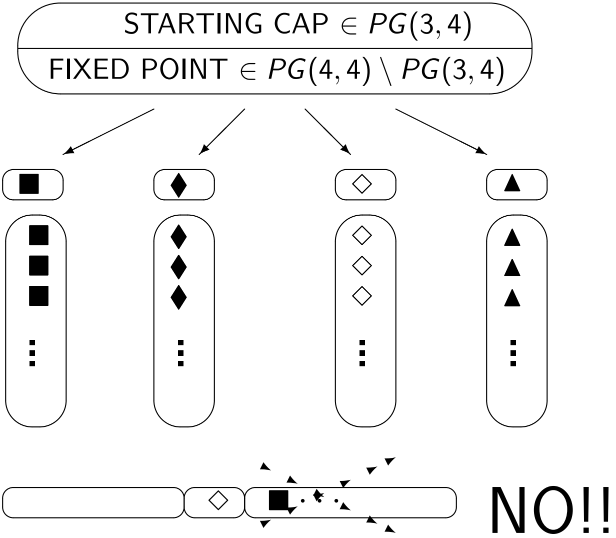
4. Some considerations about equivalence of caps allow us not to consider, during the process, the caps that will produce caps already found or equivalent to one of these;

5. We control if the caps obtained correspond to quantum stabilizer codes, using the weights distribution condition.

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

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


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


STARTING CAP $\in PG(3,4)$
FIXED POINT $\in PG(4,4) \setminus PG(3,4)$
NO!!

SEARCH FOR 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 caps obtained correspond to quantum stabilizer codes, using the weights distribution condition.

RESULTS

SPECTRUM OF QUANTUM CAPS IN $PG(4,4)$

Theorem

If $\mathcal{K} \subset PG(4,4)$ is a quantum cap, then $10 \leq |\mathcal{K}| \leq 41$, with $|\mathcal{K}| \neq 11, 37, 39$.

RESULTS

SPECTRUM OF QUANTUM CAPS IN $PG(4,4)$

- $|\mathcal{K}| = 11$ exhaustive search.
- $|\mathcal{K}| = 37, 39$ extending the four 13 caps, the 15 cap and the 17 cap of $PG(3,4)$.

RESULTS

SPECTRUM OF QUANTUM CAPS IN $PG(4,4)$

- $|\mathcal{K}| = 11$ exhaustive search.
- $|\mathcal{K}| = 37, 39$ extending the four 13 caps, the 15 cap and the 17 cap of $PG(3,4)$.

Execution time about 15 days.

RESULTS

MINIMUM SIZE OF COMPLETE CAPS IN $PG(4,4)$

RESULTS

MINIMUM SIZE OF COMPLETE CAPS IN $PG(4,4)$

Theorem

$\mathcal{K} \subset PG(4,4)$ *complete cap,*

$$\boxed{|\mathcal{K}| \geq 20.}$$

Average execution time extending $\mathcal{K}$, $10 \leq |\mathcal{K}| \leq 17$

$\lvert\mathcal{K}\rvert$	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 $\mathcal{K}$, $|\mathcal{K}| = 8, 9$

$\lvert\mathcal{K}\rvert$	AVERAGE EXECUTION TIME
9	29 h
8	6 d

Non-equivalent complete quantum-caps $\mathcal{K}$ in $PG(4,4)$

Sizes of obtained Caps	Numbers of obtained Caps	Sizes and Types of starting Caps
20	1	12 complete
29	**1**	17 complete
29	1	13 incomplete
30	**1**	16 incomplete
32	**1**	16 incomplete
33	3	13 incomplete
34	$>$130	16 incomplete
36	2	16 incomplete
38	1	16 incomplete

Non-equivalent complete quantum-caps $\mathcal{K}$
in $PG(4,4)$

Sizes of obtained Caps	Numbers of obtained Caps	Sizes and Types of starting Caps
20	1	12 complete
29	**1**	17 complete
29	1	13 incomplete
30	**1**	16 incomplete
32	**1**	16 incomplete
33	3	13 incomplete
34	>130	16 incomplete
36	2	16 incomplete
38	1	16 incomplete

Classified quantum caps of size ≤ 12

THANKS FOR THE ATTENTION!