Stabiliser codes over fields of even order

Robin Simoens

Ghent University & Universitat Politècnica de Catalunya

June 3, 2024

Joint work with Simeon Ball and Edgar Moreno arXiv : 2401.06618

Parity check matrix:

$$H = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & & \vdots \\ h_{r1} & h_{r2} & \cdots & h_{rn} \end{pmatrix}$$

Parity check matrix:

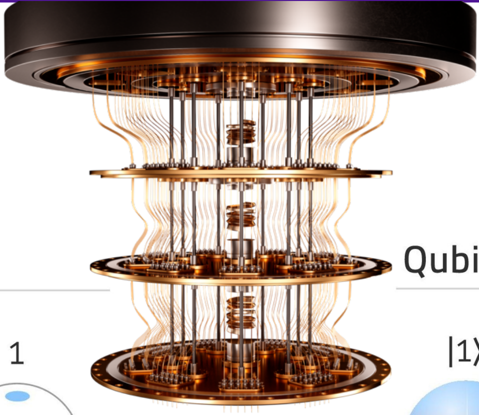
$$H = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & & \vdots \\ h_{r1} & h_{r2} & \cdots & h_{rn} \end{pmatrix}$$

Theorem.

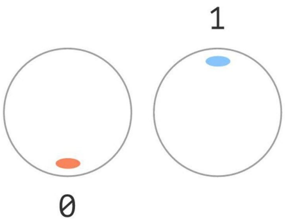
The following are equivalent:

- *A linear $[n, k, d]_q$ code.*
- *A set of n points in PG$(k-1, q)$ such that d is the smallest size of a subset of dependent points.*

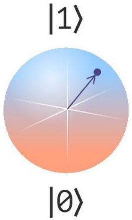
Quantum computers



Bit



Qubit



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Qubits:

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

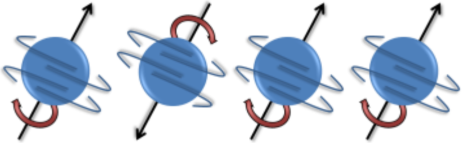
$$\psi = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

Three axioms

Axiom 1.

n particles are described by a unit vector $\psi \in (\mathbb{C}^q)^{\otimes n}$.

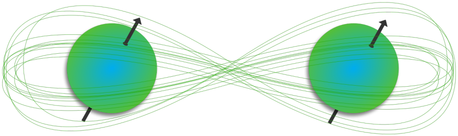


$$|1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle$$

Three axioms

Axiom 1.

n particles are described by a unit vector $\psi \in (\mathbb{C}^q)^{\otimes n}$.



$$\frac{1}{\sqrt{2}} |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \otimes |1\rangle$$

Three axioms

Axiom 1.

n particles are described by a unit vector $\psi \in (\mathbb{C}^q)^{\otimes n}$.

Axiom 2.

A measurement causes ψ to collapse onto a basis vector.

$$\frac{1}{\sqrt{2}} |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \otimes |1\rangle \mapsto \begin{cases} |0\rangle \otimes |0\rangle & \text{with 50\% chance} \\ |1\rangle \otimes |1\rangle & \text{with 50\% chance} \end{cases}$$

Three axioms

Axiom 1.

n particles are described by a unit vector $\psi \in (\mathbb{C}^q)^{\otimes n}$.

Axiom 2.

A measurement causes ψ to collapse onto a basis vector.

Axiom 3.

An error corresponds to multiplying ψ with a unitary operator.

Quantum coding theory

Definition.

An $((n, k, d))_q$ **quantum code** is a k-dimensional subspace of $\mathcal{H} := (\mathbb{C}^q)^{\otimes n}$ that can detect all errors of weight at most $d - 1$.

Theorem (Discretisation of errors).

Suppose $q = 2$. It suffices to correct the following errors:

- *Bit flips:*

$$|0\rangle \mapsto |1\rangle \text{ and } |1\rangle \mapsto |0\rangle\,, \text{ i.e. } \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

Theorem (Discretisation of errors).

Suppose $q = 2$. *It suffices to correct the following errors:*

- *Bit flips:*

$$|0\rangle \mapsto |1\rangle \text{ and } |1\rangle \mapsto |0\rangle \,, \text{ i.e. } \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

- *Phase flips:*

$$|0\rangle \mapsto |0\rangle \text{ and } |1\rangle \mapsto -|1\rangle \,, \text{ i.e. } \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\alpha\\ -\beta\end{bmatrix}$$

Theorem (Discretisation of errors).

Suppose $q = 2$. It suffices to correct the following errors:

- *Bit flips:*

$$|0\rangle \mapsto |1\rangle \text{ and } |1\rangle \mapsto |0\rangle, \text{ i.e. } \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

- *Phase flips:*

$$|0\rangle \mapsto |0\rangle \text{ and } |1\rangle \mapsto -|1\rangle, \text{ i.e. } \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \mapsto \begin{bmatrix}\alpha\\ -\beta\end{bmatrix}$$

- *Both a bit flip and a phase flip.*

These errors are elements of the **Pauli group**.

$\boxed{q=2}$

Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Pauli group

$$\begin{aligned} \mathcal{P} =& \langle X, Y, Z \rangle \\ =& \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \end{aligned}$$

Pauli group.

$$\mathcal{P}_n := \{cX(a_1)Z(b_1) \otimes \cdots \otimes X(a_n)Z(b_n) \mid a_i, b_i \in \mathbb{F}_q\}$$

where

$$X(a)\,|x\rangle = |x + a\rangle$$

$$Z(b)\,|x\rangle = (-1)^{\mathrm{tr}(bx)}\,|x\rangle$$

for an orthonormal basis $\{|x\rangle \mid x \in \mathbb{F}_q\}$ of $\mathbb{C}^q$.

Stabiliser code.

$C = \{\psi \in \mathcal{H} \mid E\psi = \psi \text{ for all } E \in S\} \quad \text{where } S \leqslant \mathcal{P}_n$

Stabiliser code.

$C = \{\psi \in \mathcal{H} \mid E\psi = \psi \text{ for all } E \in S\} \quad \text{where } S \leqslant \mathcal{P}_n$

Stabiliser group.

$S = \{E \in \mathcal{P}_n \mid E\psi = \psi \text{ for all } \psi \in \mathcal{C}\}$

Stabiliser code.

$C = \{\psi \in \mathcal{H} \mid E\psi = \psi \text{ for all } E \in S\}$ where $S \leqslant \mathcal{P}_n$

Stabiliser group.

$S = \{E \in \mathcal{P}_n \mid E\psi = \psi \text{ for all } \psi \in \mathcal{C}\}$

Theorem.

S is abelian.

Stabiliser codes

Stabiliser code.

$C = \{\psi \in \mathcal{H} \mid E\psi = \psi \text{ for all } E \in S\}$ where $S \leqslant \mathcal{P}_n$

Stabiliser group.

$S = \{E \in \mathcal{P}_n \mid E\psi = \psi \text{ for all } \psi \in \mathcal{C}\}$

Theorem.

S is abelian.

Theorem.

$d(C) =$ minimum weight of $\mathrm{Centraliser}(S) \setminus S$.

Stabiliser code.

$C = \{\psi \in \mathcal{H} \mid E\psi = \psi \text{ for all } E \in S\}$ where $S \leqslant \mathcal{P}_n$

Stabiliser group.

$S = \{E \in \mathcal{P}_n \mid E\psi = \psi \text{ for all } \psi \in \mathcal{C}\}$

Theorem.

S is abelian.

Theorem.

$d(C) =$ *minimum weight of* Centraliser(S) *if C is pure.*

Assumption: C is pure.

$$S = \left\langle \pm X^{\vec{a}_i} Z^{\vec{b}_i} \right\rangle_{1 \le i \le r}$$

Stabiliser codes

$$S = \left\langle \pm X^{\vec{a}_i} Z^{\vec{b}_i} \right\rangle_{1 \leq i \leq r} \implies \dim C = 2^{n-r} =: 2^k \implies [\![n, k, d]\!]_q$$

$$S = \left\langle \pm X^{\vec{a}_i} Z^{\vec{b}_i} \right\rangle_{1 \le i \le r} \quad \Longrightarrow \dim C = 2^{n-r} =: 2^k \Longrightarrow [\![n, k, d]\!]_q$$

$$\mathcal{G} = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r1} & \cdots & a_{rn} & b_{r1} & \cdots & b_{rn} \end{array}\right)$$

Stabiliser codes

$$S = \left\langle \pm X^{\vec{a}_i} Z^{\vec{b}_i} \right\rangle_{1 \le i \le r} \quad \Longrightarrow \dim C = 2^{n-r} =: 2^k \Longrightarrow [\![n, k, d]\!]_q$$

$$\mathcal{G} = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r1} & \cdots & a_{rn} & b_{r1} & \cdots & b_{rn} \end{array} \right)$$

Trace-symplectic inner product.

$$\langle (\vec{a}|\vec{b}), (\vec{a}'|\vec{b}') \rangle_s := \operatorname{tr}\left(\vec{a} \cdot \vec{b}' + \vec{a}' \cdot \vec{b} \right).$$

$$S = \left\langle \pm X^{\vec{a}_i} Z^{\vec{b}_i} \right\rangle_{1 \leq i \leq r} \quad \Longrightarrow \dim C = 2^{n-r} =: 2^k \Longrightarrow [\![n,k,d]\!]_q$$

$$\mathcal{G} = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r1} & \cdots & a_{rn} & b_{r1} & \cdots & b_{rn} \end{array} \right)$$

Ketkar, Klappenecker, Kumar and Sarvepalli (2006).

The following are equivalent:

- *An $[\![n,k,d]\!]_q$ stabiliser code.*
- *An additive code C over $\mathbb{F}_q$ contained in its symplectic dual $C^{\perp_s}$, such that d is the minimum symplectic weight of $C^{\perp_s}$.*

CSS construction:

$$\mathcal{G} = \left(\begin{array}{c|c} G & O \\ \hline O & H \end{array} \right)$$

where G and H are the generator matrix and parity check matrix of a classical linear code.

Graph state:

$$\mathcal{G} = \left(\begin{array}{c|c} I_n & A \end{array} \right)$$

where A is the adjacency matrix of a graph.

Equivalent stabiliser codes:

$$\begin{pmatrix} & & \\ & L & \\ & & \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \overset{\circlearrowleft}{\cdots} & a_{1,hn} & b_{11} & \overset{\circlearrowleft}{\cdots} & b_{1,hn} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r1} & \cdots & a_{r,hn} & b_{r1} & \cdots & b_{r,hn} \end{pmatrix} \cdot \begin{pmatrix} R_1 & & & S_1 & & \\ & \ddots & & & \ddots & \\ & & R_n & & & S_n \\ T_1 & & & U_1 & & \\ & \ddots & & & \ddots & \\ & & T_n & & & U_n \end{pmatrix}$$

Quantum sets of lines

$\boxed{q = 2}$

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & b_{11} & b_{12} & \cdots & b_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} & b_{r1} & b_{r2} & \cdots & b_{rn} \end{array}\right)$$

Quantum sets of lines

$\boxed{q = 2}$

$$\left(\begin{array}{cccc|cccc} a_{11} & \boxed{a_{12}} & \cdots & a_{1n} & b_{11} & \boxed{b_{12}} & \cdots & b_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} & b_{r1} & b_{r2} & \cdots & b_{rn} \end{array}\right)$$

Glynn, Gulliver, Maks and Gupta (2014).

The following are equivalent:

- *An* $[\![n, k, d]\!]_2$ *stabiliser code.*
- *A quantum set of* n *lines in PG*$(n-k-1, 2)$ *with minimum distance* d*.*

$\boxed{q = 2}$

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & b_{11} & b_{12} & \cdots & b_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} & b_{r1} & b_{r2} & \cdots & b_{rn} \end{array}\right)$$

Glynn, Gulliver, Maks and Gupta (2014).

The following are equivalent:

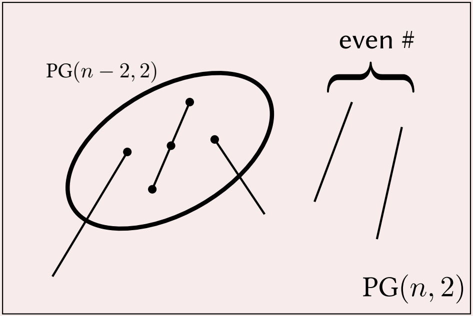
- *An* $[\![n, k, d]\!]_2$ *stabiliser code.*
- *A quantum set of* n *lines in PG*$(n-k-1, 2)$ *with minimum distance* d.

Moreover, equivalent codes correspond to projectively equivalent lines.

Quantum sets of lines

Definition.

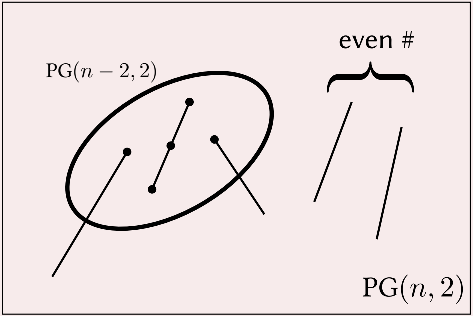
A set of lines in $\mathrm{PG}(n,2)$ is **quantum** if every codimension two space is skew to an even number of its lines.



Quantum sets of lines

Definition.

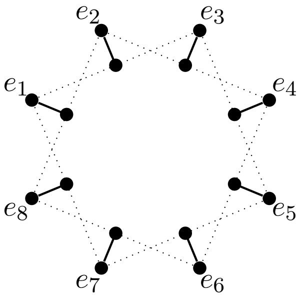
A set of lines in $\mathrm{PG}(n,2)$ is **quantum** if every codimension two space is skew to an even number of its lines.



Its **minimum distance** is the smallest size of a set of dependent points on distinct lines.

Quantum sets of lines

$$
(I_8 \,|\, C_8) = \left(\begin{array}{cccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&0
\end{array}\right)
$$



$\implies [\![8, 0, 3]\!]_2$ stabiliser code

Quantum sets of sets of lines

$q = 2^h$

Ball, Moreno and Simoens (2024+).

The isomorphism $\mathbb{F}_{2^h} \cong \mathbb{F}_2^h$ induces a bijection between $[\![n,k,d]\!]_{2^h}$ codes and $[\![hn,hk,d']\!]_2$ codes. Moreover, $d'/h \leq d \leq d'$.

Example.

Let $\alpha \in \mathbb{F}_4 \setminus \{0,1\}$, then $\{\alpha, \alpha^2\}$ is a basis of $\mathbb{F}_4$ over $\mathbb{F}_2$.

$$[\![2,1,2]\!]_4 \text{ code with matrix } \left(\begin{array}{cc|cc} 1 & 1 & \alpha & 0 \\ 0 & 1 & 1 & 1 \end{array}\right)$$

$$\implies [\![4,2,2]\!]_2 \text{ code with matrix } \left(\begin{array}{cc:cc|cc:cc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

$$\boxed{q = 2^h}$$

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & b_{11} & b_{12} & \cdots & b_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} & b_{r1} & b_{r2} & \cdots & b_{rn} \end{array}\right)$$

Quantum sets of sets of lines

$$\boxed{q = 2^h}$$

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & b_{11} & b_{12} & \cdots & b_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} & b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} & b_{r1} & b_{r2} & \cdots & b_{rn} \end{array}\right)$$

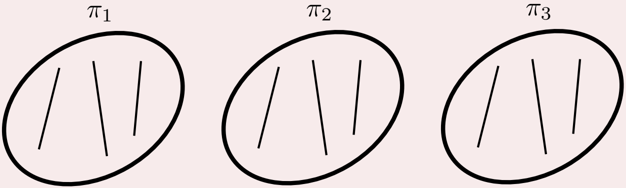
Ball, Moreno and Simoens (2024+).

The following are equivalent:

- *An* $[\![n, k, d]\!]_{2^h}$ *stabiliser code.*
- *A quantum set of* n *sets of* h *lines in PG*$(h(n-k)-1, 2)$ *with minimum distance* d.

Definition.

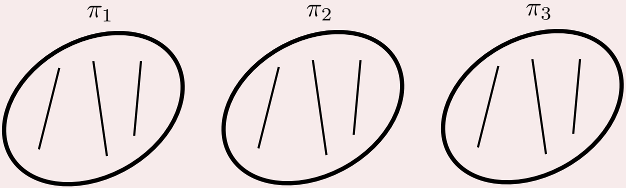
A **quantum set of sets of lines** is a partitioning of a quantum set of hn lines into n subsets of h lines, each subset spanning a projective $(2h-1)$-space $\pi_1, \pi_2, \ldots, \pi_n$ respectively.



Quantum sets of sets of lines

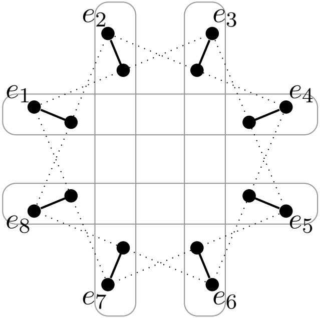
Definition.

A **quantum set of sets of lines** is a partitioning of a quantum set of hn lines into n subsets of h lines, each subset spanning a projective $(2h-1)$-space $\pi_1, \pi_2, \ldots, \pi_n$ respectively.



Its **minimum distance** is the smallest size of a set of dependent points in distinct π_i's.

$$(I_8 \mid C_8) = \left(\begin{array}{cccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&0
\end{array}\right)$$



$\Longrightarrow [\![4,0,3]\!]_4$ stabiliser code

Ball, Moreno and Simoens (2024+).

The following are equivalent:

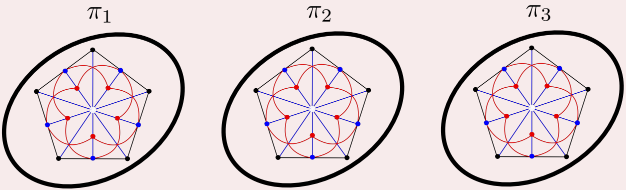
- *An* $[\![n, k, d]\!]_{2^h}$ *stabiliser code.*
- *A quantum set of* n *symplectic polar spaces of rank* h *in* $PG(h(n-k)-1, 2)$ *with minimum distance* d*.*

Moreover, equivalent codes correspond to projectively equivalent quantum sets of symplectic polar spaces.

Definition.

A **quantum set of symplectic polar spaces** is a set of projective $(2h-1)$-spaces $\pi_1, \pi_2, \ldots, \pi_n$, each equipped with a symplectic polarity with the following property:

"Every codimension two subspace intersects an even number of the π_i's in a subspace π for which $\pi^\perp$ is totally isotropic."

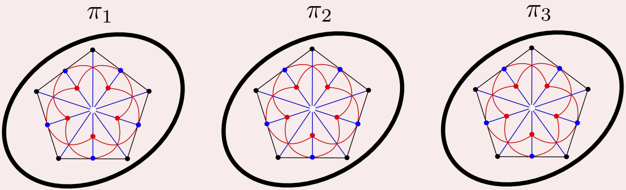


Quantum symplectic polar spaces

Definition.

A **quantum set of symplectic polar spaces** is a set of projective $(2h-1)$-spaces $\pi_1, \pi_2, \ldots, \pi_n$, each equipped with a symplectic polarity with the following property:

"Every codimension two subspace intersects an even number of the π_i's in a subspace π for which $\pi^\perp$ is totally isotropic."



Its **minimum distance** is the smallest size of a set of dependent points in distinct π_i's.

Ball, Moreno and Simoens (2024+).

A $[\![7, 1, 4]\!]_4$ *code does not exist (and neither does an* $[\![8, 0, 5]\!]_4$ *code).*

Ball, Moreno and Simoens (2024+).

A $[\![7,1,4]\!]_4$ *code does not exist (and neither does an* $[\![8,0,5]\!]_4$ *code).*

Proof (sketch). Geometrically: quantum set of 7 symplectic polar spaces of rank 2 in $\mathrm{PG}(11,2)$ with minimum distance 5.

Ball, Moreno and Simoens (2024+).

A $[\![7,1,4]\!]_4$ code does not exist (and neither does an $[\![8,0,5]\!]_4$ code).

Proof (sketch). Geometrically: quantum set of 7 symplectic polar spaces of rank 2 in $\mathrm{PG}(11,2)$ with minimum distance 5.

$$\left.\left(\begin{array}{c|c|c|c|c|c|c} I & O & O & I & I & I & I \\ \hline O & I & O & I & A_1 & B_1 & C_1 \\ \hline O & O & I & I & A_2 & B_2 & C_2 \end{array}\right)\right\}\text{341 solutions}$$

Every 3 column blocks have full rank.

Ball, Moreno and Simoens (2024+).

A $[\![7,1,4]\!]_4$ *code does not exist (and neither does an* $[\![8,0,5]\!]_4$ *code).*

Proof (sketch). Geometrically: quantum set of 7 symplectic polar spaces of rank 2 in $\mathrm{PG}(11,2)$ with minimum distance 5.

$$\left.\left(\begin{array}{c|c|c|c|c|c|c} I & O & O & I & I & I & I \\ \hline O & I & O & I & A_1 & B_1 & C_1 \\ \hline O & O & I & I & A_2 & B_2 & C_2 \end{array}\right)\right\}\text{341 solutions}$$

Every 3 column blocks have full rank.
For each line ℓ in each of the 7 solids, let

$$x_\ell = \begin{cases} 0 \text{ if } \ell \text{ is totally isotropic} \\ 1 \text{ if } \ell \text{ is hyperbolic} \end{cases}$$

$\Longrightarrow$ homogeneous equation for each codimension two subspace.

Quantum symplectic polar spaces

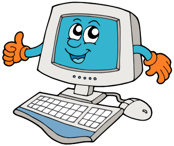
Ball, Moreno and Simoens (2024+).

A $[\![7,1,4]\!]_4$ *code does not exist (and neither does an* $[\![8,0,5]\!]_4$ *code).*

Proof (sketch). Geometrically: quantum set of 7 symplectic polar spaces of rank 2 in $\mathrm{PG}(11,2)$ with minimum distance 5.

$$\left.\left(\begin{array}{c|c|c|c|c|c|c} I & O & O & I & I & I & I \\ \hline O & I & O & I & A_1 & B_1 & C_1 \\ \hline O & O & I & I & A_2 & B_2 & C_2 \end{array}\right)\right\} \text{341 solutions}$$

Every 3 column blocks have full rank.
For each line ℓ in each of the 7 solids, let



$$x_\ell = \begin{cases} 0 \text{ if } \ell \text{ is totally isotropic} \\ 1 \text{ if } \ell \text{ is hyperbolic} \end{cases}$$

$\Longrightarrow$ homogeneous equation for each codimension two subspace.

Thank you for listening!