New Constructions of Quantum MDS codes

Oisin Campion

University College Dublin

26 May 2025

Joint work with Gary McGuire (UCD) and Fernando Hernando (UJI)
https://arxiv.org/abs/2501.17010

Quantum Information

The State Vector

- The object at the centre of attention is the **state vector**:

$$|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}, \quad \||\psi\rangle\| = 1$$

- It gives a full description of the system.
- e.g. the state of a quantum computer as it processes some computation.
- e.g the contents of Alice's "quantum message" to Bob.

The State Vector

- The object at the centre of attention is the **state vector**:

$$|\psi\rangle \in (\mathbb{C}^q)^{\otimes n}, \quad \||\psi\rangle\| = 1$$

- It gives a full description of the system.
- e.g. the state of a quantum computer as it processes some computation.
- e.g the contents of Alice's "quantum message" to Bob.
- Aim: protect the state vector from "noise".
- Noise is complicated, but we can get away with a simple model.
- I will follow the notations of Ketkar et. al.

Pauli Operators

- Let $q = p^m$ be a prime power.

Definition 1

The **Pauli operators**, denoted $X(\alpha)$ and $Z(\beta)$ for $\alpha, \beta \in \mathbb{F}_q$, are defined on an orthonormal basis $\mathcal{B} = \{|x\rangle : x \in \mathbb{F}_q\}$ for $\mathbb{C}^q$ by

- $X(\alpha)|x\rangle = |x + \alpha\rangle$.
- $Z(\beta)|x\rangle = \omega^{\mathrm{Tr}(\beta x)}|x\rangle$

where Tr() is the absolute trace, and $\omega = e^{2\pi i/p}$ is a primitive p-th root of unity.

- e.g the Binary Pauli Matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Pauli Strings and Errors

Definition 2

Given $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, a **Pauli String** is an operator of the form

$$\omega^c X(a)Z(b) = \omega^c \bigotimes_{i=1}^{n} X(a_i)Z(b_i).$$

where $\omega = e^{2\pi i/p}$ and $c \in \mathbb{F}_p$. The set of all Pauli-strings forms a group under multiplication, which we denote by $\mathcal{P}$.

- Our model for the noise channel is as follows:

$$|\psi\rangle \longrightarrow E\,|\psi\rangle\,, \quad E \in \mathcal{P}.$$

- Goal of error-correction: determine E.

Stabilizer Codes and Finite Fields

Mapping to Finite Fields

Lemma 3

The multiplication in $\mathcal{P}$ satisfies:

- $X(a)X(a') = X(a+a'), \quad Z(b)Z(b') = Z(b+b').$
- $Z(b)X(a) = \omega^{\mathrm{Tr}(a\cdot b)}X(a)Z(b).$

Lemma 4

$\omega^c X(a)Z(b)$ and $\omega^{c'}X(a')Z(b')$ commute $\iff$ $\mathrm{Tr}(b\cdot a' - b'\cdot a) = 0.$

Proposition 5

The map

$$r : \mathcal{P} \to \mathbb{F}_q^{2n}$$

$$\omega^c X(a)Z(b) \mapsto (a|b)$$

is a surjective group homomorphism with kernel $\langle \omega^c I \rangle$.

Stabilizer Codes

Definition 6

A **stabilizer group** is an abelian subgroup $\langle g_1, \ldots, g_t \rangle = \mathcal{S} \leq \mathcal{P}$ such that $-I \notin \mathcal{S}$. We denote by $V_{\mathcal{S}} \subseteq (\mathbb{C}^q)^{\otimes n}$ the common $+1$-eigenspace of $\mathcal{S}$, and $\dim V_{\mathcal{S}} = n - t$.

Stabilizer Codes

Definition 6

A **stabilizer group** is an abelian subgroup $\langle g_1, \ldots, g_t \rangle = \mathcal{S} \leq \mathcal{P}$ such that $-I \notin \mathcal{S}$. We denote by $V_{\mathcal{S}} \subseteq (\mathbb{C}^q)^{\otimes n}$ the common $+1$-eigenspace of $\mathcal{S}$, and $\dim V_{\mathcal{S}} = n - t$.

Proposition 7

Let $E \in \mathcal{P}$. If $|\psi\rangle$

Stabilizer Codes

Definition 6

A **stabilizer group** is an abelian subgroup $\langle g_1, \ldots, g_t \rangle = \mathcal{S} \leq \mathcal{P}$ such that $-I \notin \mathcal{S}$. We denote by $V_{\mathcal{S}} \subseteq (\mathbb{C}^q)^{\otimes n}$ the common $+1$-eigenspace of $\mathcal{S}$, and $\dim V_{\mathcal{S}} = n - t$.

Proposition 7

Let $E \in \mathcal{P}$. If $|\psi\rangle \in V_{\mathcal{S}}$, then each g_i defines a measurement of the state $E|\psi\rangle$ which records whether E and g_i commute. Moreover, these measurements leave the state $E|\psi\rangle$ unchanged.

Definition 8

An $[[n, k, d]]_q$ quantum stabilizer code is a code $V_{\mathcal{S}} \subseteq \mathbb{C}_q^{\otimes n}$, where $q^k = dim_{\mathbb{C}}(V_{\mathcal{S}})$,

Stabilizer Codes

Definition 6

A **stabilizer group** is an abelian subgroup $\langle g_1, \ldots, g_t \rangle = \mathcal{S} \leq \mathcal{P}$ such that $-I \notin \mathcal{S}$. We denote by $V_{\mathcal{S}} \subseteq (\mathbb{C}^q)^{\otimes n}$ the common $+1$-eigenspace of $\mathcal{S}$, and $\dim V_{\mathcal{S}} = n - t$.

Proposition 7

Let $E \in \mathcal{P}$. If $|\psi\rangle \in V_{\mathcal{S}}$, then each g_i defines a measurement of the state $E|\psi\rangle$ which records whether E and g_i commute. Moreover, these measurements leave the state $E|\psi\rangle$ unchanged.

Definition 8

An $[[n, k, d]]_q$ quantum stabilizer code is a code $V_{\mathcal{S}} \subseteq \mathbb{C}_q^{\otimes n}$, where $q^k = dim_{\mathbb{C}}(V_{\mathcal{S}})$, and $d := \min\{w(E) : E \in \overline{N(\mathcal{S})} \setminus \overline{S}\}$. We refer to n as the **length**, k as the **dimension**, and d as the **(minimum) distance**.

Symplectic Spaces

- Define a form on $\mathbb{F}_q^{2n}$: $\langle (a|b), (a'|b') \rangle_s = Tr(b \cdot a' - b' \cdot a)$.

Ketkar et. al)

An $[[n, k, d]]_q$ quantum code exists if and only if there exists an additive code $C \subseteq \mathbb{F}_q^{2n}$, with $C \subseteq C^{\perp_s}, |C| = q^{n-k}$, $d = \min\{w_s(x) : x \in C^{\perp_s} \setminus C\}$.

Symplectic Spaces

- Define a form on $\mathbb{F}_q^{2n}$: $\langle (a|b), (a'|b') \rangle_s = Tr(b \cdot a' - b' \cdot a)$.

Ketkar et. al)

An $[[n, k, d]]_q$ quantum code exists if and only if there exists an additive code $C \subseteq \mathbb{F}_q^{2n}$, with $C \subseteq C^{\perp_s}, |C| = q^{n-k}$, $d = \min\{w_s(x) : x \in C^{\perp_s} \setminus C\}$.

- Consider the map: $\phi : \mathbb{F}_q^{2n} \longrightarrow \mathbb{F}_{q^2}^n, \quad (a|b) \mapsto a + \gamma \cdot b, \quad \gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.
- The **Hermitian inner product** on $\mathbb{F}_{q^2}^n$ is defined as

$$x \cdot_h y = \sum_{i=0}^{n-1} x_i y_i^q.$$

Lemma 10 (Ketkar et. al)

For $x, y \in \mathbb{F}_{q^2}^n$, $x \cdot_h y = 0 \implies \langle \phi^{-1}(x), \phi^{-1}(y) \rangle_s = 0$.

The Black Box

Theorem 11 (Hermitian Construction)(Ketkar et. al)

Let C be a linear $[n, k, d]$ error-correcting code over the field $\mathbb{F}_{q^2}$ such that $C \subseteq C^{\perp_h}$. Then, there exists an $[[n, n-2k, \geq d^{\perp_h}]]_q$ stabilizer quantum code, where $d^{\perp_h}$ stands for the minimum distance of $C^{\perp_h}$.

New Quantum MDS codes

Quantum MDS Codes

Proposition 12 (Quantum Singleton Bound)

If a $[[n, k, d]]_q$ stabilizer quantum code exists, then the parameters satisfy $k + 2d \leq n + 2$.

- A code that attains the above bound is called **quantum MDS**.
- All MDS codes with $n \leq q + 1$ are known (Grassl, Beth, Rotteler), and it is conjectured that the length of an MDS code must be $n \leq q^2 + 2$ (Ketkar & Klappenecker).
- If $d \leq q/2$, then many codes are constructed in (Jin et. al.).
- For $d \geq q/2$, most lengths are multiples of $(q - 1)$ or $(q + 1)$.
- There are extensive (but incomplete) tables in (Wan, Zheng, Zhu).

GRS Codes

- To create a Generalized Reed-Solomon Code, you need three things:
  - A set of functions: $\mathbb{F}_{q^2}[X]_{<k}$.
  - Evaluation Set: $\boldsymbol{A} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_{q^2}^n$.
  - Twist vector: $\boldsymbol{v} = (v_0, \ldots v_{n-1}) \in (\mathbb{F}_{q^2}^*)^n$.
- Our code C is obtained as the image of the linear evaluation map:

$$ev_{\boldsymbol{v},\boldsymbol{A}} : \mathbb{F}_{q^2}[X]_{<k} \longrightarrow \mathbb{F}_{q^2}^n, \ \ f \mapsto (v_0 f(a_0), \ldots, v_{n-1} f(a_{n-1}))$$

GRS Codes

- To create a Generalized Reed-Solomon Code, you need three things:
  - A set of functions: $\mathbb{F}_{q^2}[X]_{<k}$.
  - Evaluation Set: $\boldsymbol{A} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_{q^2}^n$.
  - Twist vector: $\boldsymbol{v} = (v_0, \ldots v_{n-1}) \in (\mathbb{F}_{q^2}^*)^n$.
- Our code C is obtained as the image of the linear evaluation map:

$$ev_{\boldsymbol{v},\boldsymbol{A}} : \mathbb{F}_{q^2}[X]_{<k} \longrightarrow \mathbb{F}_{q^2}^n, \ f \mapsto (v_0 f(a_0), \ldots, v_{n-1} f(a_{n-1}))$$

- It is important that $x \cdot_h y = 0$ for every $x, y \in C$.
  For two monomials:

$$ev_{\boldsymbol{v},\boldsymbol{A}}(X^{e_1}) \cdot_h ev_{\boldsymbol{v},\boldsymbol{A}}(X^{e_2}) = \sum_i \boldsymbol{v}(i)^{q+1} \boldsymbol{A}(i)^{e_1+qe_2}$$

- We choose $\boldsymbol{A}$ and $\boldsymbol{v}$ carefully to ensure orthogonality.

Our Construction

- Let $\lambda, \tau, \rho, \sigma, L$ be positive integers.
- Let ζ_λ denote a primitive λ root of unity.
- The evaluation set for our code is:

$$\boldsymbol{A} := \{\zeta_\lambda^i \zeta_\tau^j \zeta_\rho^k : 0 \leq i, j, k < \lambda, \tau, \sigma\}$$

Our Construction

- Let $\lambda, \tau, \rho, \sigma, L$ be positive integers.
- Let ζ_λ denote a primitive λ root of unity.
- The evaluation set for our code is:

$$\boldsymbol{A} := \{\zeta_\lambda^i \zeta_\tau^j \zeta_\rho^k : 0 \leq i, j, k < \lambda, \tau, \sigma\}$$

- Choose $s_0 \ldots s_{\sigma-1} \in \mathbb{F}_q^*$ such that

$$\sum_{k=0}^{\sigma-1} s_k = 0$$

- We select the twist vector $\boldsymbol{v}$ so that the $(q+1)$-power of $\boldsymbol{v}$ has $\zeta_\lambda^{-iL} \cdot s_k$ in the coordinate labelled (i, j, k).

Orthogonality Conditions

Theorem 13 (C.-Hernando-McGuire)

Let X^{e_1}, X^{e_2} be two monomials. Then the evaluation vectors for these two monomials are orthogonal under the Hermitian inner product if any one of the following conditions holds:

1. $e_1 + e_2 \not\equiv L \pmod{\lambda}$.
2. $e_1 \not\equiv e_2 \pmod{\tau}$.
3. $e_1 \equiv e_2 \pmod{\rho}$.

- Proof: With our choice of evaluation set and twist vector, the Hermitian inner product can be factorized:

$$\left(\sum_{i=0}^{\lambda-1} \zeta_\lambda^{i(e_1+qe_2-L)}\right)\left(\sum_{j=0}^{\tau-1} \zeta_\tau^{j(e_1+qe_2)}\right)\left(\sum_{k=0}^{\sigma-1} s_k \zeta_\rho^{k(e_1+qe_2)}\right).$$

Main Theorem

Theorem 14 (C.-Hernando-McGuire)

Let $q \geq 3$ be a prime power. Let $\lambda > 1$ be a divisor of $q-1$, and let $\tau > 1$ and $\rho > 1$ be divisors of $q+1$. Assume that $\gcd(\lambda, \tau) = 1$. Let $\kappa = \gcd(\lambda, \rho) \cdot \gcd(\tau, \rho)$ and assume that $\frac{\rho}{\kappa} \geq 2$. Let σ be any integer with $\frac{\rho}{\kappa} \geq \sigma \geq 2$. Let $n = \lambda\tau\sigma$. Let T be chosen according to this table:

Conditions	T
λ even	$\frac{\lambda+4\tau}{2}$
λ odd, and either $\lambda < \tau$, τ even or $\rho = 2$	$\lambda + \tau$
λ odd, $\lambda > \tau, \tau$ odd, $\rho \neq 2$	$\frac{\lambda+3\tau}{2}$

Then for any d with $2 \leq d \leq T$ there exists a $[[n, n-2d+2, d]]_q$ quantum MDS code.

New Families of MDS Codes

Corollary 15 (C.-Hernando-McGuire)

Let $q \equiv 3 \pmod 8$, $q > 3$. Then for any $2 \leq d \leq \frac{5q+1}{8}$, there exists a $[[\frac{3(q^2-1)}{8}, k, d]]_q$ quantum MDS code.

Proof.

Choose $\lambda = \frac{q-1}{2}$, $\tau = \frac{q+1}{4}$, $\rho = 4$. Then $\kappa = 1$, so we choose $\sigma = 3$. Then we are in case 3, and so $T = (\lambda + 3\tau)/2$. □

- For example, when $q = 11$ we get a $[[45, 33, 7]]_{11}$ MDS code.

New Families of MDS Codes

Corollary 16 (C.-Hernando-McGuire)

Let q be odd. Let m be a divisor of $\frac{q+1}{2}$ such that $1 \leq m < \frac{q+1}{2}$ and $\frac{q+1}{2m}$ is even. Let $2 \leq \sigma \leq 2m$. Then for any $2 \leq d \leq \frac{q-1}{2} + \frac{q+1}{2m}$, there exists a $[[\sigma\frac{(q^2-1)}{4m}, k, d]]_q$ quantum MDS code.

- For example, consider $q = 83, m = 7$. This results in a $[[492, 400, 47]]_{83}$ MDS code.

New Families of MDS Codes

Corollary 16 (C.-Hernando-McGuire)

Let q be odd. Let m be a divisor of $\frac{q+1}{2}$ such that $1 \leq m < \frac{q+1}{2}$ and $\frac{q+1}{2m}$ is even. Let $2 \leq \sigma \leq 2m$. Then for any $2 \leq d \leq \frac{q-1}{2} + \frac{q+1}{2m}$, there exists a $[[\sigma\frac{(q^2-1)}{4m}, k, d]]_q$ quantum MDS code.

- For example, consider $q = 83, m = 7$. This results in a $[[492, 400, 47]]_{83}$ MDS code.

Corollary 17 (C.-Hernando-McGuire)

Let $q \equiv 5 \pmod 8$. Let $m \mid \frac{q+1}{2}, 1 < m < \frac{q+1}{2}$. Let $2 \leq \sigma \leq m$. Then for any $2 \leq d \leq \frac{q-1}{2} + \frac{q+1}{m}$, there exists a $[[\sigma\frac{(q^2-1)}{2m}, k, d]]_q$ quantum MDS code.

- For example, we can get a $[[280, 234, 24]]_{29}$ MDS code.

Codes for q even

- We can apply our construction to $q = 8$ and get a $[[42, 42 - 2d + 2, d]]_8$ MDS code for $2 \leq d \leq 8$.
- We can use Theorem 21 from (Ball, Moreno, Simoens) and a trace-orthogonal basis to turn these into binary codes; we get a$[[3(42), 3(42 - 2d + 2), d]]_2$ code for $2 \leq d \leq 8$.
- Explicitly, we have a
  - $[[126, 114, 3]]_2$,$[[126, 108, 4]]_2$, not best known.
  - $[[126, 102, 5]]_2$, $[[126, 96, 6]]_2$, $[[126, 90, 7]]_2$, $[[126, 84, 8]]_2$ all match best known, according to codetables.de
- Our paper: "New Quantum MDS Codes with Flexible Parameters from Hermitian Self-Orthogonal GRS Codes" https://arxiv.org/abs/2501.17010