

Maximum Distance Separable Codes: Recent advances and applications

Simeon Ball
Universitat Politècnica Catalunya

June 2019

1. MDS codes
2. Arcs in projective spaces.
3. Arcs and tensors.
4. Arcs and interpolation.
5. Arcs and quadrics.
6. Linear MDS codes which are not Reed-Solomon codes.
7. Quantum MDS codes.

MDS codes

Let A be a set of size q (the **alphabet**).

A **code** $C \subseteq A^n$ has minimum distance d if the minimum number of coordinates in which any two elements of C differ is d .

Example 1 Let $A = \{0, 1\}$ and $n = 3$. The set

$$C = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$$

is a code with minimum distance $d = 2$.

Example 2 Let $A = \{0, 1\}$ and $n = 5$. The set

$$C = \{(0, 0, 0, 0, 0), (0, 0, 1, 1, 1), (1, 1, 0, 0, 1), (1, 1, 1, 1, 0)\}$$

is a code with minimum distance $d = 3$.

Let C be a code over an alphabet with q elements of length n and minimum distance d .

(Singleton) $|C| \leq q^{n-d+1}$.

Proof. Choose any $n - d + 1$ coordinates.

If $|C| > q^{n-d+1}$ then pigeon-hole implies there are two codewords (elements of C) which agree on these coordinates.

$$(a_1, \dots, a_{n-d+1}, b_1, \dots, b_{d-1})$$

$$(a_1, \dots, a_{n-d+1}, c_1, \dots, c_{d-1})$$

If $|C| = q^{n-d+1}$ then it is **maximum distance separable** (MDS).

Example 1

$$C = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}.$$

is an MDS code with $q = 2$, $n = 3$ and $d = 2$.

Observe that MDS codes have the **MDS property**.

For any $k = n - d + 1$ coordinates, each of the possible k -tuples in these coordinates appears in a unique codeword.

$$(a_1, \dots, a_k, b_1, \dots, b_{d-1})$$

Some applications of MDS codes: quantum mechanics, distributed storage systems, error-correction codes, representation of matroids, threshold sharing schemes.

Distributed storage systems

Suppose we have n servers and tolerate r failures.

Simple solution: copy data a onto $r + 1$ of the servers.

This occupies $r + 1$ times the size of the data.

MDS solution: Split data into $k = n - r$ equally sized chunks.

Store $a = (a_1, \dots, a_k)$ on n servers as (a_1, a_2, \dots, a_n) .

This occupies n/k times the size of the data.

This storage tolerates $r = n - k$ server failures, since we can recover the file (a_1, \dots, a_k) from any k servers. (MDS property).

Imagine $a = (a_1, a_2)$ is an element of $\{0, 1\}^2$ and we have $n = 3$ servers and tolerate $r = 1$ failure.

We could store this using 4 bits as

Server 1	Server 2	Server 3
(a_1, a_2)	(a_1, a_2)	.

or

Server 1	Server 2	Server 3
(a_1, a_2)	a_1	a_2

The code in Example 1 gives the MDS solution using 3 bits

Server 1	Server 2	Server 3
a_1	a_2	$a_1 + a_2$

where we perform the addition modulo 2.

Communicating over a noisy channel (error-correction)

For each k bits (a_1, \dots, a_k) of data, we send a codeword

$$a = (a_1, \dots, a_n)$$

and receive an n -tuple

$$y = (y_1, \dots, y_n).$$

If $e \leq \frac{1}{2}(d - 1)$ errors occur in the transmission then there is a unique codeword a which differs in e coordinates from y .

This must have been the sent codeword.

Fixing k and the size of the alphabet, we want to maximise d (equivalently maximise $n = k + d - 1$.)

The Reed-Solomon code (1960)

Let $A = \mathbb{F}_q = \{a_1, \dots, a_q\}$ and let

$$C = \{(f(a_1), \dots, f(a_q), c_f) \mid f \in \mathbb{F}_q[X], \deg f \leq k - 1\},$$

where c_f is coefficient of X^{k-1} in f .

If $k \leq q$ then C is an MDS code of length $n = q + 1$.

The codewords given by f and g agree on at most $k - 1$ coordinates (indexed by the zeros of $f - g$), so differ in at least $n - k + 1$ coordinates.

The **MDS conjecture** claims that for $4 \leq k \leq q - 2$ there is no MDS code longer than the Reed-Solomon code.

The geometry of Reed-Solomon codes

The Reed-Solomon code is the row span of the **generator matrix**

$$G = \begin{pmatrix} 1 & \dots & \dots & 1 & 0 \\ a_1 & \dots & \dots & a_q & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1^{k-2} & \dots & \dots & a_q^{k-2} & 0 \\ a_1^{k-1} & \dots & \dots & a_q^{k-1} & 1 \end{pmatrix}.$$

The set of columns of G is a set \mathcal{A} of points of $\text{PG}(k-1, q)$.

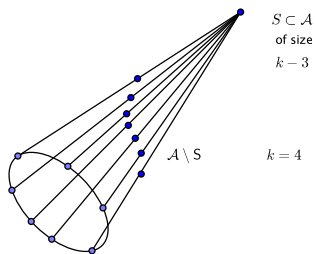
For $k=3$ these points are $(1, a_i, a_i^2)$ which are points of the conic

$$X_2^2 = X_1 X_3.$$

The set \mathcal{A} from the Reed-Solomon code is a **normal rational curve**.

It has the following properties:

1. It is contained in $\binom{k-1}{2}$ linearly independent quadrics.
2. The projection of \mathcal{A} from any $k-3$ points of \mathcal{A} is onto a conic.



Arcs in projective spaces

Suppose that C is a k -dimensional subspace of \mathbb{F}_q^n .

Let \mathcal{A} be the set of points obtained from the columns of a $k \times n$ generator matrix of a linear MDS code.

If the code is a Reed-Solomon code then \mathcal{A} is a **normal rational curve**.

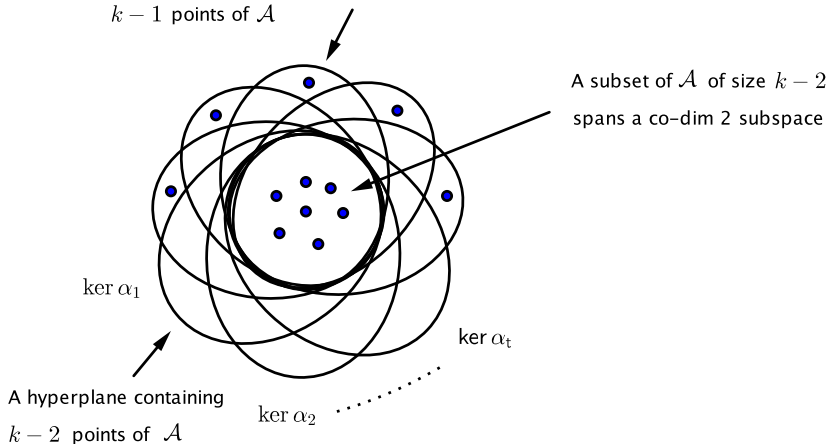
The MDS property implies that any k points of \mathcal{A} span the whole space.

A set of points of $PG(k-1, q)$ with this property is called an **arc**.

The MDS conjecture claims that an arc \mathcal{A} cannot be larger than a normal rational curve.

A hyperplane (co-dim 1 subspace) containing

$k - 1$ points of \mathcal{A}



A subset of \mathcal{A} of size $k - 2$
spans a co-dim 2 subspace

A hyperplane containing
 $k - 2$ points of \mathcal{A}

Let S be a subset of \mathcal{A} of size $k - 2$.

The parameter t counts the number of hyperplanes containing S and no other points of \mathcal{A} .

Since there are $q + 1$ hyperplanes containing a fixed co-dimension 2 subspace,

$$|\mathcal{A}| = k - 2 + q + 1 - t.$$

Then $t \geq 0$ implies

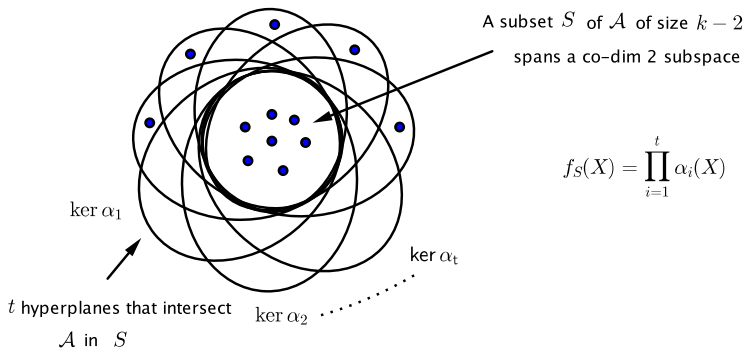
$$|\mathcal{A}| \leq q + k - 1.$$

For the Reed-Solomon code, a normal rational curve has $|\mathcal{A}| = q + 1$.

In terms of the minimum distance of the code this implies $d \leq q$, where for the Reed-Solomon code $d = q + 2 - k$.

(Ball - J. European Math. Soc. 2012) If q is prime then there is no better linear MDS code than the Reed-Solomon code.

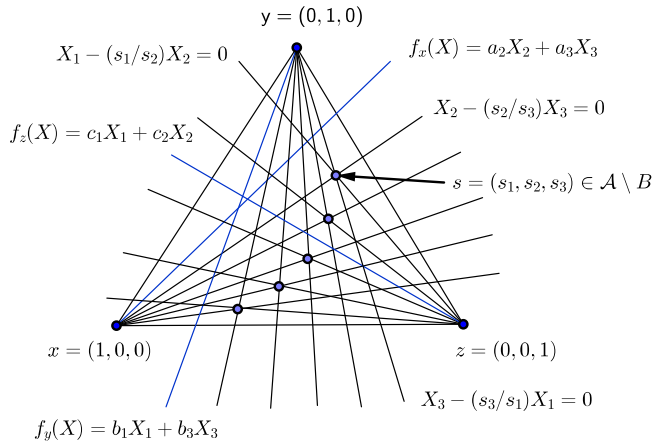
If, furthermore, $k \neq \frac{1}{2}(q + 1)$ then the longest MDS codes are the Reed-Solomon codes.



$$f_S(X) = \prod_{i=1}^t \alpha_i(X)$$

Suppose $k = 3$ and $t = 1$ and let $B = \{x, y, z\} \subset \mathcal{A}$.

Coordinates with respect to the basis B , we have



Since

$$\frac{s_3}{s_1} \frac{s_2}{s_3} \frac{s_1}{s_2} = 1$$

this implies

$$\frac{a_3}{a_2} \frac{b_1}{b_3} \frac{c_2}{c_1} = 1$$

Therefore,

$$a_2 b_3 c_1 = a_3 b_1 c_2$$

where $f_x(X) = a_2 X_2 + a_3 X_3$, etc.

But $a_2 = f_x(y)$, etc, so we get

$$f_x(y) f_y(z) f_z(x) = f_y(x) f_z(y) f_x(z).$$

For general t the same proof gives

$$f_x(y) f_y(z) f_z(x) = (-1)^{t+1} f_y(x) f_z(y) f_x(z).$$

For any subset D of \mathcal{A} of size $k - 3$,

$$f_{D \cup \{x\}}(y) f_{D \cup \{y\}}(z) f_{D \cup \{z\}}(x) = (-1)^{t+1} f_{D \cup \{y\}}(x) f_{D \cup \{z\}}(y) f_{D \cup \{x\}}(z).$$

Let \mathcal{A} be an arc of size $q + k - 1 - t$.

For each $(k - 2)$ -subset S of \mathcal{A} , there are precisely t hyperplanes which contain S and no other points of \mathcal{A} .

These hyperplanes are called the **tangent hyperplanes**.

We defined the **tangent polynomial** at S as

$$f_S(X) = \prod_{i=1}^t \alpha_i(X)$$

where $\alpha_i(X)$ is a linear form in k variables whose kernel is one of the t tangent hyperplanes containing S .

This defines f_S up to a scalar factor.

(Ball-Lavrauw 2019) Scaling the tangent functions appropriately, for any subset C of \mathcal{A} of size $k - 1$

$$f_{C \setminus \{a\}}(a),$$

is the same for all $a \in C$ (up to a possible sign change).

For example, with $k = 3$ and t odd

$$f_x(y) = f_y(x)$$

for all pairs of points $x, y \in \mathcal{A}$.

In particular, if $t = 1$, i.e. $|\mathcal{A}| = q + 1$.

Segre's theorem (1955) states that if q is odd then \mathcal{A} is a conic.

For $x \in \mathcal{A}$, the unique tangent is defined by a linear form $f_x(X)$.

Segre's theorem using interpolation, knowing $f_x(y) = f_y(x)$.

$$f_x(X) = f_x(e_1)X_1 + f_x(e_2)X_2 + f_x(e_3)X_3$$

and so

$$f_x(X) = f_{e_1}(x)X_1 + f_{e_2}(x)X_2 + f_{e_3}(x)X_3.$$

Substituting $X = x$ gives

$$0 = f_{e_1}(x)x_1 + f_{e_2}(x)x_2 + f_{e_3}(x)x_3.$$

This implies that for all $x \in \mathcal{A}$,

$$0 = 2(f_{e_1}(e_2)x_1x_2 + f_{e_2}(e_3)x_2x_3 + f_{e_3}(e_1)x_1x_3).$$

Arcs and interpolation

Using interpolation one obtains a system of equations in which the values of $f_{C \setminus \{a\}}(a)$ are the variables.

If $|\mathcal{A}| = q + 1$ then this system of equations implies

$$(k - 1)!(c_1 x_i x_j + c_i x_1 x_j + c_j x_1 x_i) = 0$$

for all $x \in \mathcal{A}$.

Let p be the prime such that $q = p^h$.

If $k \leq p$ then \mathcal{A} is contained in the intersection of $\binom{k-1}{2}$ conical cone quadrics which implies \mathcal{A} is a normal rational curve.

Arcs and tensors

Segre's theorem using the tensor, knowing $f_x(y) = f_y(x)$.

Let $b(X, Y)$ be the symmetric bilinear form such that

$$b(X, e_i) = f_{e_i}(X)$$

for $i \in \{1, 2, 3\}$.

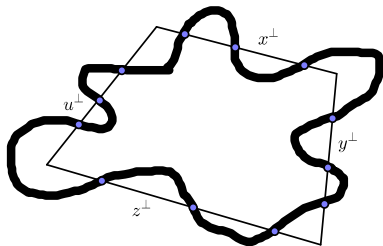
Then for $y \in \mathcal{A} \setminus \{e_1, e_2, e_3\}$, the form $b(X, y)$ and $f_y(X)$ agree at the basis points so they are the same.

Thus, $b(x, x) = 0$ for all $x \in \mathcal{A}$, which is Segre's theorem.

Using Segre's lemma of tangents one can prove the following.

(Segre 1967, Blokhuis-Bruen-Thas 1990) (q even)

There is an algebraic hypersurface of degree t which contains all the points dual to the tangent hyperplanes.



q even

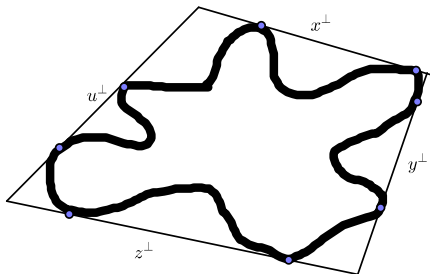
$k = 3$

$t = 3$

• point dual to a tangent hyperplane

(Segre 1967, Blokhuis-Bruen-Thas 1990) (q odd)

There is an algebraic hypersurface of degree $2t$ which contains all the points dual to the tangent hyperplanes, with intersection multiplicity 2 with the lines dual to a subspace spanned by a subset of \mathcal{A} of size $k - 2$.



q odd

$k = 3$

$t = 2$

• point dual to a tangent hyperplane

(Blokhuis 1995)

“Segre’s lemma of tangents is not enough to prove the MDS conjecture”.

For q odd, one uses the fact that

$$f_{C \setminus \{a\}}(a)^2$$

is the same for all $a \in C$, which is weaker.

(Blokhuis-Bruen-Thas 1990) (q odd) implies

There is a $(2t, 2t, \dots, 2t)$ -form $F(X_1, \dots, X_{k-1})$, homogeneous of degree $2t$ in each vector variable X_j , such that

$$F(X, y_1, \dots, y_{k-2}) = f_{y_1, \dots, y_{k-2}}(X)^2$$

for all $y_1, \dots, y_{k-2} \in \mathcal{A}$.

(Ball-Lavrauw 2019)

Let $\phi(X)$ be the subspace of homogeneous polynomials of degree t in k variables which are zero on \mathcal{A} .

There is a (t, t, \dots, t) -form $F(X_1, \dots, X_{k-1})$, homogeneous of degree t in each variable X_j , such that

$$F(X, y_1, \dots, y_{k-2}) = f_{y_1, \dots, y_{k-2}}(X) \pmod{\phi(X)}$$

for all $y_1, \dots, y_{k-2} \in \mathcal{A}$.

For $k = 3$ and most t this holds without the modulo $\phi(X)$.

Then the coefficients of X^j in

$$F(X + Y, Y) - F(X, Y)$$

are low degree curves which are zero on \mathcal{A} .

This leads to the following theorem.

(Ball-Lavrauw 2017)

If q is odd and $k = 3$ and \mathcal{A} is an arc not contained in a conic then \mathcal{A} is contained in the intersection of two curves of degree at most $t + p^{\lfloor \log_p t \rfloor}$ which do not share a common component.

Extending this to higher dimensions is complicated.

We could prove the following.

(Ball-Lavrauw 2019)

If q is odd and $k = 4$ then an arc of size $q + 1$ is contained in the intersection of two quadrics.

But we already know that

(Segre 1955)

If q is odd and $k = 4$ then an arc of size $q + 1$ is a normal rational curve.

Arcs and quadrics

The space of quadrics on $\text{PG}(k-1, q)$ has dimension $\binom{k+1}{2}$.

Let U be a subspace of the space of quadrics containing no reducible quadric.

Let $V(U)$ denote the set of common zeros of the quadrics in U .

(Glynn 1994)

If U has dimension $\binom{k-1}{2}$ and $V(U)$ spans the space then $V(U)$ is an arc of $\text{PG}(k-1, q)$.

Let \mathcal{A} be an arc and $U(\mathcal{A})$ be the space of quadrics which are zero on \mathcal{A} .

In his 1994 article Glynn conjectures the following.

(Conjecture) If $U(\mathcal{A})$ has dimension $\binom{k-1}{2}$ and $2k \leq q + 2$ and $|\mathcal{A}| = q + 1$ then \mathcal{A} is a normal rational curve.

(Ball-Pepe 2019) This conjecture is true assuming $2k \leq q$.

(Castelnuovo 1889) If $U(\mathcal{A})$ has dimension $\binom{k-1}{2}$ and $|\mathcal{A}| \geq 2k + 1$ then \mathcal{A} is contained in a normal rational curve.

(Conjecture) Ball-Pepe (2019)

If $U(\mathcal{A})$ has dimension $\binom{k-1}{2} - 1$ and $|\mathcal{A}| \geq 2k + 3$ then \mathcal{A} projects from any $k - 4$ points onto the intersection of two quadrics.

This is a strengthening of a theorem of Fano (1894).

From this to prove the linear MDS conjecture one only needs to prove that for an arc \mathcal{A} of size $q + 1$,

$$\dim U(\mathcal{A}) \geq \binom{k-1}{2} - 1.$$

This can possibly be done for q odd if the tensor theorem holds without the modulo $\phi(X)$.

The linear MDS conjecture is known to be true for the following k .
(bounds given only up to first order of magnitude, p is prime.)

$$k < \sqrt{q}. \quad q \text{ even (Segre) (1967)}$$

$$k < \sqrt{pq}. \quad q = p^{2h+1} \text{ (Voloch) (1991)}$$

$$k < q. \quad q = p \text{ (Ball) (2012)}$$

$$k < 2\sqrt{q}. \quad q = p^2 \text{ (Ball-De Beule) (2012)}$$

$$k < \sqrt{q}. \quad q = p^{2h} \text{ (Ball-Lavrauw) (2017)}$$

There are other bounds from Segre, Voloch and Hirschfeld-Korchmáros which are better for smaller q .

Long MDS codes which are not Reed-Solomon codes

For $k = 3$ and q even there are many known, for example

$$\mathcal{A} = \{(1, x, x^\sigma) \mid x \in \mathbb{F}_q\} \cup \{(0, 1, 0), (0, 0, 1)\},$$

for certain automorphisms σ of \mathbb{F}_q . (Segre 1957)

(Segre 1962, Glynn 1983 I/II, Payne 1985, Payne 1995, Cherowitzo 1998, Payne, Penttila and Pinneri 1995, Cherowitzo, Penttila, Pinneri, Royle 1996, Cherowitzo, O'Keefe, Penttila 2003.)

(Peter Vandendriesche 2017) There are no other examples for $q = 64$.

(Florian Caullery and Kai-Uwe Schmidt 2014) We know all examples for which the degree of the polynomial defining \mathcal{A} is less than $\frac{1}{2}q^{1/4}$.

For $k = 4$ and q even (Segre 1969)

$$\mathcal{A} = \{(1, x, x^\sigma, x^{\sigma+1}) \mid x \in \mathbb{F}_q\} \cup \{(0, 0, 0, 1)\},$$

for certain automorphisms σ of \mathbb{F}_q .

For $k = 5$ and $q = 9$ (Glynn 1986)

$$\mathcal{A} = \{(1, x, x^2 + \eta x^6, x^3, x^4) \mid x \in \mathbb{F}_9\} \cup \{(0, 0, 0, 0, 1)\},$$

where $\eta^4 = -1$.

Linear MDS codes of rate one half

Let M be a $k \times k$ matrix and $G = (I_k \mid M)$.

Theorem: G generates an MDS code where $n = 2k$ iff every $j \times j$ submatrix of M is non-singular for $j = 1, \dots, k$.

If $M^{-1} = M^\sigma$ for some automorphism σ of \mathbb{F}_q then

Theorem: G generates an MDS code where $n = 2k$ iff every $j \times j$ submatrix of M is non-singular for $j = 1, \dots, \lfloor \frac{1}{2}k \rfloor$.

If we assume M to be circulant then this restricts the first row of M to being on the intersection of certain algebraic surfaces.

$\sigma = \text{id}$ these are quadrics, $\sigma = \sqrt{q}$ these are Hermitian surfaces.

These are MDS codes which are not extendable to Reed-Solomon codes.
(e is primitive element used by GAP).

k	n	q	first row of M
5	10	9	$(1, e, e^6, e^6, e)$
5	10	11	$(1, e^2, e^8, e^8, e^2)$
7	14	17	$(1, e^3, e^5, e^{15}, e^{15}, e^5, e^3)$
7	14	19	$(1, e^3, e^7, e^8, e^8, e^7, e^3)$
9	18	25	$(1, e^9, e^{13}, e^8, e^{22}, e^{22}, e^8, e^{13}, e^9)$

Quantum MDS codes

A **quantum code** U is a subspace of $(\mathbb{C}^q)^{\otimes n}$.

It suffices to consider Pauli-errors which are unitary operators of the form

$$E = \sigma_1 \otimes \cdots \otimes \sigma_n$$

where σ_i are $q \times q$ unitary matrices.

If $\{e_i\}$ is an orthonormal basis for U then U detects an error E if

$$\langle e_i | E | e_j \rangle = \delta_{ij} c_E$$

for all i and j and where c_E is some constant.

A quantum code U has minimum distance d if one can detect Pauli-errors with up to $d - 1$ non-identity matrices.

If q is a prime power then we can index the coordinates of \mathbb{C}^q by elements of \mathbb{F}_q .

A **stabiliser code** is the intersection of the eigenspaces with eigenvalue one of a subgroup generated by a set of commuting Pauli-errors.

For example, if $q = 2$ then

$$\sigma_{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

is a basis for the subspace of $q \times q$ matrices.

The intersection of the 4 eigenspaces of the operators

$$\begin{aligned} &\sigma_x \otimes \sigma_{id} \otimes \sigma_z \otimes \sigma_y \otimes \sigma_x \\ &\sigma_z \otimes \sigma_{id} \otimes \sigma_y \otimes \sigma_x \otimes \sigma_z \\ &\sigma_{id} \otimes \sigma_z \otimes \sigma_x \otimes \sigma_y \otimes \sigma_z \\ &\sigma_{id} \otimes \sigma_x \otimes \sigma_y \otimes \sigma_z \otimes \sigma_x \end{aligned}$$

is a 2-dimensional quantum code of $(\mathbb{C}^2)^{\otimes 5}$ with minimum distance 3.

A quantum code of length n , dimension q^k and minimum distance d satisfies

$$k \leq n - 2d + 2.$$

If $k = n - 2d + 2$ then we say the code is MDS.

Define \perp_h , the Hermitian inner product over \mathbb{F}_{q^2} , as

$$u \cdot v = u_1 v_1^q + \cdots + u_n v_n^q.$$

(Ketkar et al 2005)

If there is a classical linear code C with parameters $[n, k, d]_{q^2}$ such that $C^{\perp_h} \subseteq C$ then there is a quantum code with parameters $[[n, 2k - n, d]]_q$.

Therefore, a linear MDS code of length n over \mathbb{F}_{q^2} which is Hermitian self-orthogonal, gives a quantum MDS code of $(\mathbb{C}^q)^{\otimes n}$.

Glynn's arc gives a $[[10, 0, 6]]$ quantum MDS code in $(\mathbb{C}^3)^{\otimes 10}$.

The method mentioned before gives ...

a $[[14, 0, 8]]$ quantum MDS code in $(\mathbb{C}^5)^{\otimes 14}$.

a $[[18, 0, 10]]$ quantum MDS code in $(\mathbb{C}^7)^{\otimes 18}$.

a $[[18, 0, 10]]$ quantum MDS code in $(\mathbb{C}^5)^{\otimes 18}$.

Huber and Grassl (2019) obtain bounds on quantum MDS codes.

These bounds bound the size of an arc for small q^2 which give Hermitian orthogonal MDS codes.

The MDS conjecture (1955) claims that for $q - 1 \geq d \geq 5$ an MDS code of length n and minimum distance d over an alphabet of size q satisfies

$$n \leq q + 1.$$

The Quantum MDS conjecture (2015) claims that for $d \geq 5$ a quantum MDS code of $(\mathbb{C}^q)^{\otimes n}$ with minimum distance d satisfies

$$n \leq q^2 + 1.$$

Grassl and Rötteler (2015) construct quantum MDS codes of length $q^2 + 1$ for most $1 \leq d \leq q + 1$.