An Overview of the MDS Conjecture

Dongchun Han

School of Mathematics, Southwest Jiaotong University

Coding theory, finite geometry, and subset sums

Roadmap

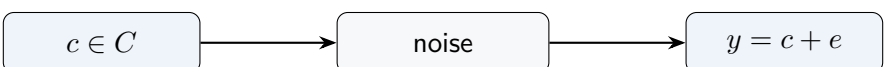
1. Codes and linear codes.
2. Hamming distance and error correction.
3. Singleton bound and MDS codes.
4. The MDS conjecture.
5. Zero-sum constructions of MDS/NMDS codes.

Finite fields: the alphabet

- A finite field is denoted by $\mathbb{F}_q$.
- Here q is a prime power.
- If this is new, think of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- Example in $\mathbb{F}_5$: $3 + 4 = 2$, and $3 \cdot 4 = 2$.

Words and codewords

- A word of length n is a vector in $\mathbb{F}_q^n$.
- A code is a set $C \subseteq \mathbb{F}_q^n$.
- We send a codeword through a noisy channel.
- The receiver tries to recover the original word.



Linear codes

Definition

A linear $[n, k]$ code over $\mathbb{F}_q$ is a k-dimensional linear subspace

$$C \leq \mathbb{F}_q^n.$$

- n is the length.
- k is the amount of information.
- The number of codewords is $|C| = q^k$.

Generator matrix

- A generator matrix is a $k \times n$ matrix G.
- Its rows form a basis of C.
- A message $u \in \mathbb{F}_q^k$ is encoded as $uG \in \mathbb{F}_q^n$.

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} = (v_1\ v_2\ \cdots\ v_n).$$

Hamming weight and distance

For $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$,

$$w(x) = |\{i : x_i \neq 0\}|, \qquad d(x, y) = w(x - y).$$

Example in $\mathbb{F}_2^9$

$$\begin{aligned} x &= (0, 0, 1, 1, 0, 1, 1, 1, 1), \\ y &= (1, 1, 1, 1, 1, 1, 1, 1, 0), \\ x - y &= (1, 1, 0, 0, 1, 0, 0, 0, 1), \\ d(x, y) &= 4. \end{aligned}$$

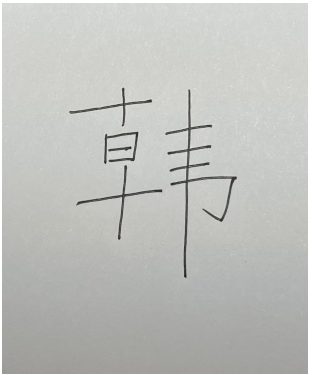
One wrong letter can still be readable

Correct word	Received word	Errors
UNIVERSITY	UNIVXRSITY	1
MATHEMATICS	MATHEMATXCS	1
PROFESSOR	PROFESXOR	1
TRANSLATION	TRANSXATION	1
INFORMATION	INFORMATXON	1

A good code makes different messages far apart.

A Chinese one-stroke example

- The character has one extra stroke.
- Chinese readers still recognize it immediately.
- Minimum distance formalizes this intuition.



Minimum distance

Definition

For a code C, its minimum distance is

$$d(C) = \min\{d(x, y) : x, y \in C,\ x \neq y\}.$$

- A code with distance d detects up to $d - 1$ errors.
- It corrects up to $\lfloor (d-1)/2 \rfloor$ errors.

The three parameters

A linear code with length n, dimension k, and minimum distance d is written as

$$[n, k, d]_q.$$

length n | dimension k | distance d

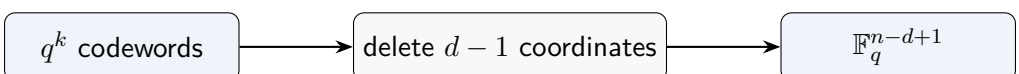
We want large k and large d, but they constrain each other.

Singleton bound

Singleton bound

Every $[n, k, d]_q$ linear code satisfies

$$d \leq n - k + 1.$$



No two codewords can collide after the deletion.

MDS codes

Definition

A code is MDS if it meets the Singleton bound:

$$d = n - k + 1.$$

- MDS means "maximum distance separable."
- For fixed n and k, it has the largest possible distance.

MDS codes in linear algebra

Let $G = (v_1\ v_2\ \cdots\ v_n)$ be a generator matrix.

MDS criterion

A linear $[n, k]_q$ code is MDS if and only if every k columns of G are linearly independent.

So every k selected columns form a basis of $\mathbb{F}_q^k$.

The basic example: Reed–Solomon codes

Choose distinct finite points $a_1, \ldots, a_n \in \mathbb{F}_q$ and also ∞.

$$C = \{(f(a_1), \ldots, f(a_n), f(\infty)) : \deg f < k\}.$$

Here $f(\infty)$ means the coefficient of x^{k-1}.

$$G_{\mathrm{RS}} = \begin{pmatrix} a_1^{k-1} & a_2^{k-1} & \cdots & a_n^{k-1} & 1 \\ a_1^{k-2} & a_2^{k-2} & \cdots & a_n^{k-2} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_1 & a_2 & \cdots & a_n & 0 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix}.$$

Why ask for maximal length?

MacWilliams–Sloane wrote in *The Theory of Error-Correcting Codes*, Chapter 11, that MDS codes form one of the most fascinating chapters in coding theory.

- MDS codes have the strongest error-correction performance.
- Fix the information amount k.
- Since $d = n - k + 1$, maximizing d is maximizing n.

The MDS conjecture

Let $M(k,q)$ be the maximal length of a nontrivial q-ary MDS code of dimension k.

Main Conjecture for MDS codes

For $q \geq k$,

$$M(k,q) = \begin{cases} q+2, & q \text{ even and } k = 3 \text{ or } k = q-1, \\ q+1, & \text{otherwise.} \end{cases}$$

Reed–Solomon codes already give length $q+1$.

Finite geometry dictionary

Nonzero columns of G define points in projective space $\mathrm{PG}(k-1,q)$.

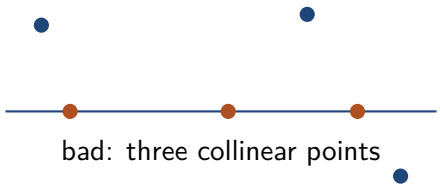
Dictionary

MDS $\iff$ no k chosen points lie in one hyperplane.

Thus the MDS conjecture is also an extremal problem in finite geometry.

Projective plane picture

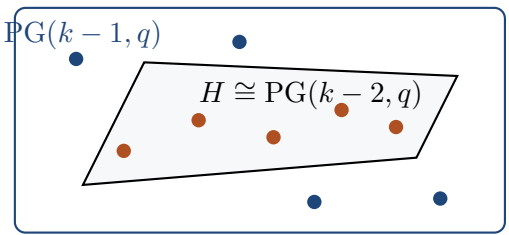
In $\mathrm{PG}(2, q)$, a hyperplane is just a line.



For $k = 3$, MDS means no three points on a line.

General projective-space picture

In $\mathrm{PG}(k-1,q)$, a hyperplane has dimension $k-2$.



Too many points must squeeze into a hyperplane.

Some major progress

- Segre: $k = 3$, q odd (Canad. J. Math., 1955).
- Blokhuis–Bruen–Thas: even q, small k (Invent. Math., 1988).
- Ball: Main Conjecture for $k \leq p$ (JEMS, 2012).
- Ball–De Beule: $k \leq 2p - 2$ (Des. Codes Cryptogr., 2012).

A proof in dimension three

Theorem

If q is odd, there is no $[q+2,3]_q$ MDS code.

- Hence $M(3,q) = q+1$ for odd q.
- The proof uses only elementary finite-field facts.

Step 1: systematic form

Assume an $[q+2, 3]_q$ MDS code.

- Any three columns are independent.
- Choose three columns and move them to the front.
- Row operations turn them into I_3.

$$G = \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & a_1 & a_2 & \cdots & a_{q-1} \\ 0 & 1 & 0 & b_1 & b_2 & \cdots & b_{q-1} \\ 0 & 0 & 1 & c_1 & c_2 & \cdots & c_{q-1} \end{array} \right).$$

Step 2: normalize the columns

Every remaining column has all coordinates nonzero.

- Otherwise it would be dependent with two basis columns.
- Scaling a column by a nonzero scalar preserves independence.
- Divide the column by its first coordinate.

So we may write every remaining column as $(1, b_i, c_i)^T$.

Step 3: three lists are all of $\mathbb{F}_q^*$

For $i \neq j$, the MDS property gives

$$b_i \neq b_j, \qquad c_i \neq c_j, \qquad c_i/b_i \neq c_j/b_j.$$

Each list has $q-1$ nonzero elements.

$$\{b_i\} = \{c_i\} = \{c_i/b_i\} = \mathbb{F}_q^*.$$

Step 4: product of nonzero elements

For odd q,

$$\prod_{x \in \mathbb{F}_q^*} x = -1.$$

Indeed,

$$x^{q-1} - 1 = \prod_{a \in \mathbb{F}_q^*} (x - a),$$

and compare constant terms.

Step 5: contradiction

Since the three lists are all $\mathbb{F}_q^*$,

$$\prod_i b_i = -1, \qquad \prod_i c_i = -1, \qquad \prod_i \frac{c_i}{b_i} = -1.$$

But also

$$\prod_i \frac{c_i}{b_i} = \frac{\prod_i c_i}{\prod_i b_i} = 1.$$

This contradiction proves the theorem.

Dual codes

For a linear code $C \leq \mathbb{F}_q^n$, its dual code is

$$C^\perp = \{x \in \mathbb{F}_q^n : x \cdot c = 0 \text{ for all } c \in C\}.$$

If C has dimension k, then $C^\perp$ has dimension $n - k$.

Duality is important in the definition of NMDS codes.

NMDS codes

Singleton defect

For an $[n, k, d]_q$ code, the defect is $n - k + 1 - d$.

- MDS means defect 0.
- Almost MDS means defect 1.
- NMDS means both C and $C^{\perp}$ are almost MDS.

Zero-sum conditions

For $A \subseteq \mathbb{F}_q$, define

$$\Sigma_k(A) = \left\{ \sum_{a \in B} a : B \subseteq A, |B| = k \right\}.$$

In many code families,

MDS or NMDS is determined by whether a special subset sum exists.

Elliptic curve codes

Let $E/\mathbb{F}_q$ be an elliptic curve and $P = \{P_1, \ldots, P_n\} \subset E(\mathbb{F}_q)$. Choose a basis $f_1, \ldots, f_k$ of $L(k\infty)$.

$$G_E = (f_i(P_j))_{1 \leq i \leq k,\, 1 \leq j \leq n}.$$

Criterion

$C(E, P, k\infty)$ is MDS iff P has no zero-sum k-subset.

Han–Ren results for elliptic codes

Han–Ren (IEEE TIT, 2023; IMRN, 2024):

- If $C(E, P, k\infty)$ is MDS and $3 \leq k \leq n-3$, then

$$n \leq \frac{|E(\mathbb{F}_q)| + 5}{2}.$$

- If $|S| > (|G| + 5)/2$, then $\Sigma_k(S) = G$.
- There are MDS elliptic codes of every length $n \leq |E(\mathbb{F}_q)|/2$ in the construction range.

Roth–Lempel codes

For $A = \{a_1, \ldots, a_n\} \subset \mathbb{F}_q$,

$$G_{\mathrm{RL}} = \begin{pmatrix} a_1^{k-1} & \cdots & a_n^{k-1} & 1 & 0 \\ a_1^{k-2} & \cdots & a_n^{k-2} & 0 & 1 \\ \vdots & & \vdots & 0 & 0 \\ a_1 & \cdots & a_n & 0 & 0 \\ 1 & \cdots & 1 & 0 & 0 \end{pmatrix}.$$

Roth–Lempel introduced these codes (IEEE TIT, 1989).

Han–Fan theorem for Roth–Lempel codes

Han–Fan proved the exact criterion (IEEE TIT, 2023).

- G_{RL} gives an MDS code iff A contains no zero-sum $(k-1)$-subset.
- G_{RL} gives an NMDS code iff A contains a zero-sum $(k-1)$-subset.

Han–Zhang codes

For $A = \{a_1, \ldots, a_n\} \subset \mathbb{F}_q$,

$$G_{\mathrm{HZ}} = \begin{pmatrix} a_1^k & a_2^k & \cdots & a_n^k \\ a_1^{k-2} & a_2^{k-2} & \cdots & a_n^{k-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_n \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Han–Zhang studied these codes (Des. Codes Cryptogr., 2024).

Han–Zhang criterion

Han–Zhang proved the following criterion (Des. Codes Cryptogr., 2024).

- G_{HZ} gives an MDS code iff A contains no zero-sum k-subset.
- G_{HZ} gives an NMDS code iff A contains a zero-sum k-subset.

(+)-twisted Reed–Solomon codes

For $A = \{a_1, \ldots, a_n\} \subset \mathbb{F}_q$ and $\eta \neq 0$,

$$G_+ = \begin{pmatrix} a_1^{k-1} + \eta a_1^k & \cdots & a_n^{k-1} + \eta a_n^k \\ a_1^{k-2} & \cdots & a_n^{k-2} \\ \vdots & & \vdots \\ a_1 & \cdots & a_n \\ 1 & \cdots & 1 \end{pmatrix}.$$

Beelen–Puchinger–Rosenkilde (IEEE TIT, 2022); Huang–Yue–Niu–Li (DCC, 2021).

$(+)$-twisted criterion

For $(+)$-twisted Reed–Solomon codes:

- MDS iff A contains no $(-\eta^{-1})$-sum k-subset.
- NMDS iff A contains a $(-\eta^{-1})$-sum k-subset.

$(*)$-twisted Reed–Solomon codes

For $A \subset \mathbb{F}_q^*$ and $\eta \neq 0$,

$$G_* = \begin{pmatrix} a_1^{k-1} & \cdots & a_n^{k-1} \\ a_1^{k-2} & \cdots & a_n^{k-2} \\ \vdots & & \vdots \\ a_1 & \cdots & a_n \\ 1+\eta a_1^k & \cdots & 1+\eta a_n^k \end{pmatrix}.$$

Beelen–Puchinger–Rosenkilde (IEEE TIT, 2022); Huang–Yue–Niu–Li (DCC, 2021).

$(*)$-twisted criterion

For $(*)$-twisted Reed–Solomon codes:

- MDS iff no k-subset has product $(-1)^k \eta^{-1}$.
- NMDS iff some k-subset has product $(-1)^k \eta^{-1}$.

Closing message

- MDS codes are optimal for error correction.
- The MDS conjecture asks for their maximal length.
- Finite geometry turns it into an extremal problem.
- Zero-sum conditions explain many MDS/NMDS constructions.

Thank you!