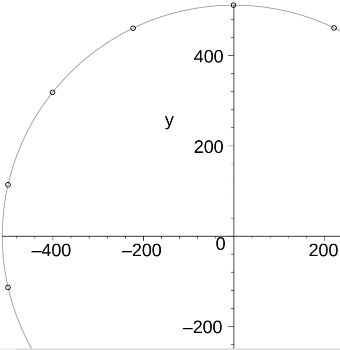
Fundamental Operations on Rank Metric Codes

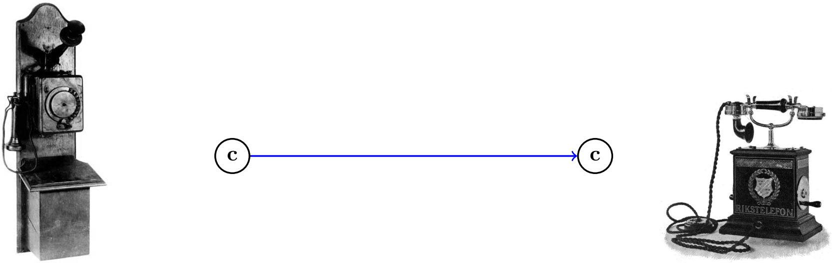
Eimear Byrne
University College Dublin

MEGA
Nice, 2017



What is Coding Theory About?

Coding Theory was introduced after Shannon's noisy channel theorem (1948) for efficient communication across noisy channels.



sender transmits **c**, receiver gets **c**

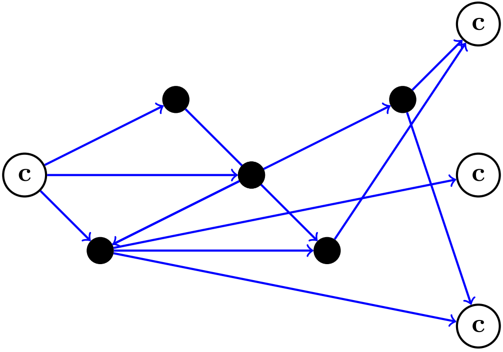
What is Coding Theory About?

Coding Theory was introduced after Shannon's noisy channel theorem (1948) for efficient communication across noisy channels.

sender transmits $\mathbf{c}$, receiver gets $\mathbf{c}+\mathbf{e}=\mathbf{v}$

What is Coding Theory About?

Coding Theory was introduced after Shannon's noisy channel theorem (1948) for efficient communication across noisy channels.



sender transmits **c**, receivers want **c**

Encoding

- $m \in \mathbb{F}_q^k$ is a message
- encode m by multiplication with a full-rank $k \times n$ matrix

$$G : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n : m \mapsto c = mG$$

$$C = \{mG : m \in \mathbb{F}_q^k\}$$

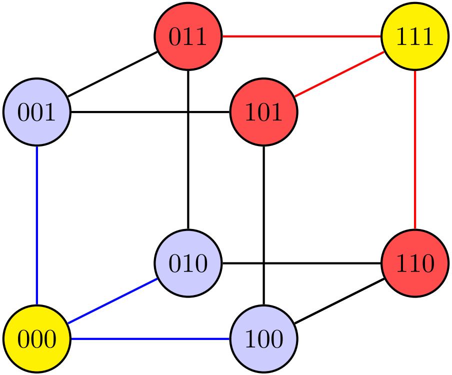
is an $\mathbb{F}_q$-$[n, k, d]$ code.

What is d?

d is the minimum distance between a pair of distinct codewords.

Want low n, high k, high d.
The higher d is, the more robust the code is to noise (packing problem).

Sphere-Packing



Fundamentals in Coding Theory

- Operations on codes - making new codes from old:
  - puncturing,
  - shortening,
  - extending,
  - concatenating,
  - products,
- Parameters of codes
  - length,
  - dimension,
  - minimum distance,
  - packing radius,
  - covering radius,
  - weight enumerators.
- Weight enumerators
  - MacWilliams duality theorem,
  - the zeta function.

q-Analogues

subsets $\{s_1, \ldots, s_k\}$ of $[n]$	subspaces $\langle s_1, \ldots, s_k \rangle$ of $\mathbb{F}_q^n$
set cardinality	vector space dimension
binomial coefficients $\binom{n}{k}$	Gaussian coefficients $\begin{bmatrix} n \\ k \end{bmatrix}_q$
Hamming weight of $(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$	$\mathbb{F}_q$-dimension of $\langle v_1, \ldots, v_n \rangle \subset \mathbb{F}_{q^m}^n$
Hamming weight of $(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$	$\mathbb{F}_q$-rank of $\begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix} \in \mathbb{F}_q^{m \times n}$

Rank Metric Codes

- Introduced by Delsarte (1978) as a q-analogue of coding theory.
- Independently introduced by Gabidulin (1986) and Roth (1991) for array error correction.
- Studied more after 2000 in the context of code-based-cryptosystems.
- Since 2008, generated interest among algebraic coding theorists due to their applicability in network error correction.
- Many open problems in coding theory: only since 2015 have we seen new optimal families of rank metric codes.

Hamming Metric Codes

Definition 1

A linear $\mathbb{F}_q$-$[n,k,d]$ code C is a k-dimensional subspace of $\mathbb{F}_q^n$ of minimum Hamming distance

$$d = \min\{d_H(c,c') : c,c' \in \mathbb{C}\}.$$

- $d_H((u_1,...,u_n),(v_1,...,v_n)) := |\{i \in [n] : u_i \neq v_i\}|$.
- C is optimal if k attains the max. possible dimension for fixed n,d.

Theorem 2 (Singleton Bound, 1964)

If C is an $[n,k,d]$ code then $k \leq n-d+1$.

- Codes that meet the Singleton bound are called **maximum distance separable** (MDS).
- MDS code exist for $n \leq q+1$ (via Reed-Solomon codes).
- Segre (1955) conjectured that if $k \leq q$, q odd then $n \leq q+1$.

Rank-Metric Codes

Definition 3

A linear $\mathbb{F}_q$-$[m \times n, k, d]$ rank-metric code C is a k-dimensional subspace of $\mathbb{F}_q^{m \times n}$ of minimum rank distance

$$d = \min\{\mathrm{rk}(A - B) : A, B \in C\}.$$

- rk is a distance function on $\mathbb{F}_q$-$[m \times n, k, d]$.
- C is optimal if k attains the max. possible dimension for fixed m, n, d.

Theorem 4 (Rank Singleton Bound, Delsarte 1978)

If C is an $[m \times n, k, d]$ code with $n \leq m$ then $k \leq m(n - d + 1)$.

- Codes that meet the rank Singleton bound are called **maximum rank distance** codes (MRD).
- MRD codes exist for all m, n, d.

A Construction of MDS Codes

The Reed-Solomon Codes form a class of MDS codes.
Choose $\alpha_1, ..., \alpha_n$ distinct in $\mathbb{F}_q^\times$.

$$\mathrm{RS}(n,k) := \{c_f = (f(\alpha_1), ..., f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) \leq k-1\}$$

Any pair of distinct polynomials $f, g \in \mathbb{F}_q[x]$ of degree $\leq k-1$ have at most $k-2$ common roots so

$$d_H(c_f, c_g) \geq n-k+1.$$

From the Singleton bound its minimum distance is $\leq n-k+1$, so $\mathrm{RS}(n,k)$ is MDS.
Remark: For a basis-free approach, identify $\mathrm{RS}(n,k)$ with

$$\{f \in \mathbb{F}_q[x], \deg(f) \leq k-1\}.$$

A Construction of MRD Codes

The Delsarte-Gabidulin Codes form a class of MRD codes (1978, 1984).

- $L_m := \{f_0x + f_1x^q + \cdots + f_kx^{q^{m-1}} : f_i \in \mathbb{F}_{q^m}\}$ (linearized polynomials in $\mathbb{F}_{q^m}[x]$)
- Choose $\alpha_1, ..., \alpha_n \subset \mathbb{F}_{q^m}$, linearly independent over $\mathbb{F}_q$

$$\mathscr{G}(m,n,k) := \{c_f = (f(\alpha_1), ..., f(\alpha_n)) : f \in L_m, \deg(f) \leq q^{k-1}\}$$

$$f, g \in L_m, \deg f, \deg g \leq q^{k-1} \implies \dim(\ker f \cap \ker g) \leq k-1 \implies$$
$$d_{\mathrm{rk}}(c_f, c_g) \geq n-k+1.$$

- $\mathscr{G}(n,k)$ is MRD by rank Singleton bound.
- $M_{n\times n}(\mathbb{F}_q) \cong L_n$ as rings (multiplication modulo $x^{q^n} - 1$).

For a basis-free approach, define

$$\mathscr{G}(m,k) := \{f_0x + f_1x^q + \cdots + f_kx^{q^{k-1}} : f_i \in \mathbb{F}_{q^m}\}.$$

MRD Codes

- Delsarte-Gabidulin codes admit fast decoding.
- Until 2015 they were the only known family of MRD codes.

The twisted Delsarte-Gabidulin codes were discovered by Sheekey in 2015.

$$\mathscr{H}(n,k) := \{f_0 x + f_1 x^q + \cdots + f_k x^{q^{k-1}} + f_0 \theta^{q^h} x^{q^k} : f_i \in \mathbb{F}_{q^n}\}.$$

Theorem 5

If $\theta^{\frac{q^n-1}{q-1}} \neq (-1)^{nk}$ then $\mathscr{H}(n,k)$ is MRD with parameters $[n \times n, kn, n-k+1]$

- The converse is false.
- The Delsarte-Gabidulin codes are $\mathbb{F}_{q^n}$-linear.
- The twisted Delsarte-Gabidulin codes are not always $\mathbb{F}_{q^n}$-linear.
- Few other families of rank-metric codes are known.
- Most MRD codes are not twisted Delsarte-Gabidulin codes.

The Hamming Weight Enumerator

The weight of a codeword is its distance to zero, wrt a given distance function. Given a linear code $C \subset \mathbb{F}_q^n$, its Hamming weight enumerator is

$$W(x,y) = \sum_{i=0}^{n} W_i x^{n-i} y^i,$$

where $W_t := |\{c \in C : d_H(c,0) = t\}|$ for $0 \leq t \leq n$.

The dual $C^\perp := \{v \in \mathbb{F}_q^n : c \cdot v = 0 \, \forall c \in C\}$ has weight enumerator $W^\perp(x,y)$ st:

Theorem 6 (MacWilliams Duality Theorem)

$$W^\perp(x,y) = \frac{1}{|C|} W(x+(q-1)y, x-y)$$

The Rank Weight Enumerator

Given a linear code $C \subset \mathbb{F}_q^{m \times n}$, its rank weight enumerator is

$$W(x,y) = \sum_{i=0}^{n} W_i x^{n-i} y^i,$$

where $W_t := |\{X \in C : \operatorname{rk} X = t\}|$ for $0 \leq t \leq n$.

In 2008 Gadouleau and Yan derived the q-analogue of the MacWilliams duality theorem. (Also Delsarte 1970s via association schemes)

$C^\perp := \{Y \in \mathbb{F}_q^{m \times n} : \operatorname{tr}(XY^T) = 0 \; \forall X \in C\}$ has weight enumerator $W^\perp(x,y)$ st:

Theorem 7 (Rank metric duality theorem)

$$W^\perp(x,y) = \frac{1}{|C|} \tilde{W}(x + (q^m - 1)y, x - y)$$

where $\tilde{W}(x,y)$ is a q-transform of $W(x,y)$.

Weight Enumerators

The weight enumerator is an important invariant of a code.

For example, weight enumerators relate codes to designs, strongly regular graphs and association schemes.

It also tells us precisely how effective the code is for transmitting information.

- For some extremal codes, the weight enumerator is determined.
- In the Hamming metric, this occurs for MDS codes.
- In the rank metric, this occurs for MRD codes.
- The MDS/MRD property of a weight enumerator is invariant under puncturing and shortening.
- The MDS/MRD weight enumerators are $\mathbb{Q}$-bases for the spaces of Hamming/rank metric weight enumerators.

Puncturing Hamming Metric Codes

Puncture an $[n,k,d]$ code in $\mathbb{F}_q^n$ by deleting the same coord. from each codeword. If $d>1$ this results in an $[n-1,k,\geq d-1]$ code.

Example 8

Puncture an $\mathbb{F}_2$-$[8,4,4]$ code on the last coordinate to get an $\mathbb{F}_2$-$[7,4,3]$ code.

$$\begin{array}{cc} 00000000 & 11111111 \\ 11100001 & 00011110 \\ 10011001 & 01100110 \\ 10000111 & 01111000 \\ 01010101 & 10101010 \\ 01001011 & 10110100 \\ 00110011 & 11001100 \\ 00101101 & 11010010 \end{array} \rightarrow \begin{array}{cc} 0000000 & 1111111 \\ 1110000 & 0001111 \\ 1001100 & 0110011 \\ 1000011 & 0111100 \\ 0101010 & 1010101 \\ 0100101 & 1011010 \\ 0011001 & 1100110 \\ 0010110 & 1101001 \end{array}$$

The punctured code has a better rate, but worse minimum distance.

Shortening Hamming Metric Codes

Shorten an $[n,k,d]$ code by choosing the subcode with zero entries in a given coordinate and then deleting that same coordinate from each selected codeword. If $d>1$ this results in an $[n-1,k-1,\geq d]$ code.

Example 9

Shorten an $\mathbb{F}_2$-$[8,4,4]$ code on the last coordinate to get an $\mathbb{F}_2$-$[7,3,4]$ code.

$$\begin{array}{cc} 00000000 & 11111111 \\ 11100001 & 00011110 \\ 10011001 & 01100110 \\ 10000111 & 01111000 \\ 01010101 & 10101010 \\ 01001011 & 10110100 \\ 00110011 & 11001100 \\ 00101101 & 11010010 \end{array} \rightarrow \begin{array}{cc} 0000000 & \\ & 0001111 \\ & 0110011 \\ & 0111100 \\ & 1010101 \\ & 1011010 \\ & 1100110 \\ & 1101001 \end{array}$$

The shortened code has a worse rate, but may have a higher minimum distance.

Shortening and Puncturing Rank-Metric Codes

We define shortening/puncturing as projections to $\mathbb{F}_q^{m\times(n-1)}$.

Definition 10

Let $H \in \mathbb{F}_q^{n\times(n-1)}$ have rank $n-1$. Let $h \in \mathbb{F}_q^n \backslash \mathrm{col}(H)$.
The punctured and shortened codes of C wrt H are:

$$\begin{aligned} \Pi_H(C) &:= \{XH : X \in C\} \subset \mathbb{F}_q^{m\times(n-1)} \text{ (punctured code)}, \\ \Sigma_{h,H}(C) &:= \{XH : X \in C, Xh^T = 0\} \subset \mathbb{F}_q^{m\times(n-1)} \text{ (shortened code)}. \end{aligned}$$

Example 11

Let $E_i = [e_j^T : j \neq i]$, $e_j = [0,\dots,1,\dots,0]$.

- $\Pi_{E_i}(C)$: delete the ith col of each elt of C.
- $\Sigma_{e_i,E_i}(C)$: delete the ith col of each elt of C whose ith col is zero.

Shortening and Puncturing Rank-Metric Codes

Example 12

Here's an $\mathbb{F}_2$-$[4 \times 4, 3, 4]$ code, C.

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

Then $\Sigma_{e_1,E_1}(C) = \{0\}$ as C has weight enumerator $x^4 + 7xy^3$.

$Xh^T \neq 0$ for any $h \neq 0$, so all shortened codes of C are trivial.

Shortening and Puncturing Rank-Metric Codes

Example 13

Here's an $\mathbb{F}_2$-$[3 \times 3, 4, 2]$ code with $W(x,y) = x^3 + 13xy^2 + 2y^3$.

$$C = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right\rangle.$$

H	h	$W_{\Sigma_{h,H}}(x,y)$	H	h	$W_{\Sigma_{h,H}}(x,y)$
E_2	110	$x^2 + y^2$	E_3	001	$x^2 + 3y^2$
	010	$x^2 + y^2$		111	$x^2 + y^2$
	111	$x^2 + y^2$		011	$x^2 + y^2$
	011	$x^2 + y^2$		101	$x^2 + 3y^2$

Duality of Puncturing and Shortening in the Hamming Metric

- The MDS property $(k = n - d + 1)$ is invariant under shortening and puncturing.
- Puncturing is really a projection to $\mathbb{F}_q^{n-1}$.
- Shortening is projection of a subcode to $\mathbb{F}_q^{n-1}$.
- We can puncture/shorten on several coords.

Recall $C^\perp := \{x \in \mathbb{F}_q^n : c \cdot x = 0 \, \forall c \in C\}$.

Theorem 14 (Duality of Puncturing and Shortening)

Let $\mathbf{P}_i(C)$ and $\mathbf{S}_i(C)$ be the punctured and shortened codes of C at the ith coordinate, respectively. Then

$$\mathbf{P}_i(C)^\perp = \mathbf{S}_i(C^\perp).$$

Pf: (Easy) $\mathbf{S}_i(C^\perp) \subset \mathbf{P}_i(C)^\perp$. Show equality by comparing dimensions.

Duality of Puncturing and Shortening in the Rank Metric

Recall for an $\mathbb{F}_q$-$[m \times n, k, d]$ code C,

$$C^\perp := \{N \in \mathbb{F}_q^{m\times n} : \mathrm{Tr}(MN^t) = 0 \text{ for all } M \in C\} \subseteq \mathbb{F}_q^{m\times n}.$$

Theorem 15 (B., Ravagnani 2016)

Duality of puncturing and shortening also holds for rank metric codes. In particular,

$$\Pi_{E_i}(C)^\perp = \Sigma_{e_i,E_i}(C^\perp).$$

- $k^\perp := \dim(C^\perp) = mn - k$
- $C^{\perp\perp} = C$
- If C is not $\mathbb{F}_{q^m}$-linear, its duals under the trace inner product and the scalar inner product are different.

Parameters of Punctured and Shortened Codes

Lemma 16 (Hamming Metric)

Let C be an $\mathbb{F}_q$-$[n,k,d]$ code.

1. $\mathbf{P}_i(C)$ *is* $[n-1, k, \geq d-1]$
2. $\mathbf{S}_i(C)$ *is* $[n-1, k-1, \geq d]$.
3. *If C is MDS then so is* $\mathbf{P}_i(C)$.
4. *If C is MDS then so is* $\mathbf{S}_i(C)$.

Lemma 17 (Rank Metric)

Let C be an $\mathbb{F}_q$-$[m \times n, k, d]$ code. Let $H \in \mathbb{F}_q^{n\times(n-1)}$ have rank $n-1$ with $h \notin \mathrm{col}(H)$.

1. $\Pi_H(C)$ *is* $[m \times (n-1), k, \geq d-1]$
2. $\Sigma_{h,H}(C)$ *is* $[m \times (n-1), \geq k-m, \geq d]$.
3. *If C is MRD then so is* $\Pi_H(C)$.
4. *If C is MRD then so is* $\Sigma_{h,H}(C)$.

The Zeta Function of a Curve

- $\mathscr{C}$ non-singular projective curve over $\mathbb{F}_q$,
- N_k the number of $\mathbb{F}_{q^k}$-rational points of $\mathscr{C}$,

The zeta-function of $\mathscr{C}$ is

$$Z(\mathscr{C}, T) = exp\left(\sum_{k\geq 1} \frac{N_k}{k} T^k\right).$$

Theorem 18 (Weil, Dwork)

The zeta function of any non-singular projective curve of genus g can be expressed as

$$Z(\mathscr{C}, T) = \frac{P(T)}{(1-T)(1-qT)},$$

some $P(T) \in \mathbb{Q}[T]$ $\deg P(T) \leq 2g$. $|\omega| = q^{-1/2}$ for each root ω of $P(T)$.

Zeta Functions for Hamming-Metric Codes

Definition 19 (Duursma 1999)

The **zeta polynomial** of a (Hamming metric) $\mathbb{F}_q$-$[n,k,d]$ code C is the unique polynomial $P(T)$ of degree at most $n-d+1$ such that

$$\frac{P(T)}{(1-T)(1-qT)}(Tx+(1-T)y)^n = \cdots + \frac{W(x,y)-x^n}{q-1}T^{n-d} + \cdots .$$

The quotient

$$Z(T) := \frac{P(T)}{(1-T)(1-qT)}$$

is called the **zeta function** of C.

- The weight enumerator $M_{n,d}$ of an $\mathbb{F}_q$-$[n,d]$ MDS code is determined.
- $P(T) = \sum_{i=0}^{n-d+1} p_i T^i \implies W(x,y) = \sum_{i=0}^{n-d} p_i M_{n,d+i}(x,y) + p_{n-d+1}x^n$.
- If C is MDS then $P(T) = 1$.

MRD Weight Enumerators

- If C is MRD, then its weight enumerator is determined (Delsarte, 1978).

$$M_{m\times n,d}(x,y) \quad = \quad x^n + \sum_{i=d}^{n}(q^{m(i-d+1)}-1)\begin{bmatrix} n \\ i \end{bmatrix} y^i \prod_{t=0}^{n-i-1}(x-q^t y).$$

- The MRD weight enumerators

$$\left\{M_{m\times n,d}(x,y) : 0 \leq d \leq n\right\} \cup \{x^n\}$$

  are a $\mathbb{Q}$-**basis** for the space of all $m \times n$ 'weight enumerators' (homog. polys of degree n).
- Given any $[m\times n, k, d]$ code C, there exist unique coefficients $p_i \in \mathbb{Q}$ s.t. for some r,

$$W(x,y) = p_0 M_{m\times n,d}(x,y) + \cdots + p_r M_{m\times n,d+r}(x,y).$$

- The $p_0, \ldots, p_r$ turn out to coincide with the coefficients of the **zeta polynomial** of C.

Zeta Functions, Zeta Polynomials, Weight Enumerators

Theorem 20 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

$$Z(T)\phi_n(T) = \frac{P(T)\phi_n(T)}{(1-T)(1-q^m T)} = \cdots + \frac{W(x,y)-x^n}{q^m-1} T^{n-d} + \cdots .$$

$P(T)$ is the unique polynomial of degree at most $n-d+1$ such that

$$W(x,y) = \sum_{i=0}^{n-d} p_i M_{m\times n, d+i}(x,y) + p_{n-d+1} x^n.$$

- $\phi_{n,r} = \begin{bmatrix} n \\ r \end{bmatrix} \prod_{j=0}^{r-1} (x - q^j y) y^{n-r}$,
- $\phi_n(T) := \sum_{r=0}^{n} \phi_{n,r}(x,y) T^r$,
- if C is MRD then $P(T) = 1$.

Zeta Functions

- $Z(\mathscr{C}, T)$ is the generating function for the number of points on a curve.
- $Z(T)$ is the generating function of **binomial moments** of a code.
- The binomial moments measure the average size of the **shortened subcodes**.
- The property $|\omega| = q^{-1/2}$ for every root ω of the zeta polynomial is called the Riemann hypothesis (RH).
- Many infinite families of codes with extremal Hamming weight enumerators sat. RH.
- It is conjectured that a sufficient condition for RH of a formally self-dual Hamming metric code is that it has weight distribution close to a random code.

Question 1

Which families of rank-metric codes satisfy the Riemann hypothesis?

$$(|\omega| = q^{-m/2}?)$$

The Riemann Hypothesis for Rank Metric Codes

Example 21

Any MRD code satisfies RH - it has $P(T) = 1$!

Example 22

- Take a (Hamming metric) extended binary QR code in $\mathbb{F}_2^{18}$.
- Puncture and shorten this code to get a code in $\mathbb{F}_2^{16}$.
- Express each resulting word in $\mathbb{F}_2^{16}$ as a 4×4 matrix.

The binomial moments are

$$b_0 = 0, b_1 = 0, b_2 = 3/5, b_3 = 15, b_4 = 255$$

$$P(T) = (1 + 8T + 16T^2)/25 = (1 + 4T)^2/25.$$

The zeroes $T = -1/4$ have absolute value $(2^4)^{-1/2} = 1/\sqrt{16}$ and so satisfy RH.

The zeta polynomial is that of a maximal elliptic curve over $\mathbb{F}_{16}$.

The Riemann Hypothesis for Rank Metric Codes

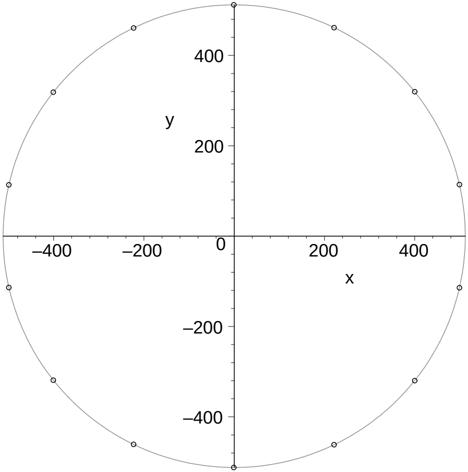


Figure: Complex zeroes for $P(T)$ of $\mathbb{F}_4^{9\times 9}$ in $\mathbb{F}_4^{18\times 18}$.

A Bound on the Minimum Distance

Theorem 23 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

Let $P(T)$ be the zeta polynomial of an $\mathbb{F}_q$-$[m \times n, k, d]$ rank metric code and let θ be the negative of the sum of its reciprocal roots. Then

$$d \leq \log_q [(\theta + q^m + 1)(q-1) + 1] - 1.$$

- Follows due to MacWilliam's duality theorem for rank metric codes.

Shortened Subcodes, Binomial Moments and $W(x,y)$

Definition 24 (The shortened subcode of C)

We define the **shortened subcode** of C wrt $U \subseteq \mathbb{F}_q^n$ as:

$$C_U := \left\{ X \in C : Xu^T = 0 \ \ \forall u \in U \right\}.$$

Definition 25 (The Binomial Moments of C)

$$b_r = \begin{cases} \begin{bmatrix} n \\ \dim U \end{bmatrix}^{-1} \displaystyle\sum_{\dim U = n-d-r} (|C_U| - 1) & \text{if } 0 \leq r \leq n-d \\ 0 & \text{if } r < 0 \\ q^{k-mu} - 1, u = n-d-r & \text{if } r > n - d^{\perp} - d \end{cases}$$

Theorem 26 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

$W(x,y)$ is completely determined by the b_i.

Shortened Subcodes, Binomial Moments and $W(x,y)$

Example 27

Here's an $\mathbb{F}_2$-$[3\times 3,4,2]$ code with $W(x,y)=x^3+13xy^2+2y^3$ and $d^\perp=1$.

$$C=\left\langle \begin{bmatrix}1&0&0\\0&0&0\\0&1&0\end{bmatrix},\begin{bmatrix}0&0&1\\1&0&0\\0&0&0\end{bmatrix},\begin{bmatrix}0&1&0\\0&0&1\\0&0&0\end{bmatrix},\begin{bmatrix}0&0&1\\0&1&0\\0&1&0\end{bmatrix}\right\rangle .$$

- $C_U=\{0\}$ if $\dim U\geq 2$ and $C_U=C$ if $U=\{0\}$.
- If $\dim U=1$ then $|C_U|=2,2,2,2,4,4,4$.

$$b_0=\tfrac{13}{7}, b_1=2^4-1, b_2=2^7-1, b_3=2^{10}-1,\ldots, b_r=2^{4+3(r-1)}-1,\ldots$$

$$\begin{aligned} W(x,y) &= x^3+\begin{bmatrix}3\\2\end{bmatrix}(x-y)b_0+\begin{bmatrix}3\\3\end{bmatrix}b_1=x^3+7(x-y)y^2\frac{13}{7}+15y^3\\ &= x^3+13xy^2+2y^3. \end{aligned}$$

Zeta Functions for Rank Metric Codes

Definition 28 (The Zeta Function of C)

$$Z(T) := (q^m - 1)^{-1} \sum_{r \geq 0} b_r T^r.$$

$$b_r - (q^m + 1) b_{r-1} + q^m b_{r-2} = 0, r \notin \{0, ..., n - d^{\perp} - d + 2\}. \tag{1}$$

Definition 29 (The Zeta Polynomial of C)

$$P(T) := \sum_{r=0}^{n-d+1} p_r T^r,$$

$$p_r := (q^m - 1)^{-1} (b_r - (q^m + 1) b_{r-1} + q^m b_{r-2}).$$

The recurrence relation (1) yields

$$Z(T) = \frac{P(T)}{(1 - T)(1 - q^m T)}.$$

Zeta Functions, Zeta Polynomials, Weight Enumerators

$$\phi_{n,n-i}(x,y) := (q^m-1)^{-1}\left(M_{m\times n,i} - (q^m+1)M_{m\times n,i+1} + q^m M_{m\times n,i+2}\right).$$

$$\phi_n(T) := \sum_{r=0}^{n} \phi_{n,r}(x,y)T^r.$$

Theorem 30 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

$$Z(T)\phi_n(T) = \frac{P(T)\phi_n(T)}{(1-T)(1-q^mT)} = \cdots + \frac{W(x,y)-x^n}{q^m-1}T^{n-d} + \cdots.$$

$P(T)$ is the unique polynomial of degree at most $n-d+1$ such that

$$W(x,y) = \sum_{i=0}^{n-d} p_i M_{m\times n,d+i}(x,y) + p_{n-d+1}x^n.$$

Example 31

For the $\mathbb{F}_q$-$[3\times 3,4,2]$ code C with $W(x,y)=x^3+13xy^2+2y^3$,

$$\begin{aligned}\phi_3(T) &= y^3+7(x-y)y^2T+\cdots\\ Z(T) &= \frac{13}{49}+\frac{15}{7}T+\frac{127}{7}T^2+\frac{1023}{7}T^3+\cdots,\\ P(T) &= \frac{13}{49}-\frac{12}{49}T+\frac{48}{49}T^2.\end{aligned}$$

Then

$$\begin{aligned}\frac{P(T)\phi_3(T)}{(1-T)(1-2^3T)} &= \frac{(13-12T+48T^2)(y^3+7(x-y)y^2T+\cdots)}{49(1-T)(1-8T)}\\ &= \cdots+\frac{1}{7}(13xy^2+2y^3)+\cdots\end{aligned}$$

and

$$\begin{aligned}p_0M_{3\times 3,2}+p_1M_{3\times 3,3}+p_2x^3 &= \frac{13}{49}(x^3+49xy^2+14y^3)-\frac{12}{49}(x^3+7y^3)+\frac{48}{49}x^3\\ &= x^3+13xy^2+2y^3.\end{aligned}$$

Invariance of the Zeta Polynomial

The weight enumerator of punctured/shortened MRD code is determined (it is MRD), so:

Theorem 32 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

The zeta polynomial $P_C(T)$ is invariant under shortening and puncturing.

$$W(x,y) = \sum_{i=0}^{n-d} p_i M_{m\times n, d+i}(x,y) + p_{n-d+1}x^n.$$

$$\downarrow$$

puncturing

$$\downarrow$$

$$\sum_{i=0}^{n-d} p_i M_{m\times(n-1), d-1+i}(x,y) + p_{n-d+1}x^{n-1}.$$

Invariance of the Zeta Polynomial

The weight enumerator of punctured/shortened MRD code is determined (it is MRD), so:

Theorem 33 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

The zeta polynomial $P(T)$ is invariant under shortening and puncturing.

$$W(x,y) = \sum_{i=0}^{n-d} p_i M_{m\times n, d+i}(x,y) + p_{n-d+1}x^n.$$

$$\downarrow$$

shortening

$$\downarrow$$

$$\sum_{i=0}^{n-1-d} p_i M_{m\times(n-1), d+i}(x,y) + p_{n-d}x^{n-1}.$$

Puncturing/Shortening Operations on Rank Weight Enumerators

- The weight enumerator of a punctured/shortened code depends on H.
- The **average** weight enum. after puncturing/shortening **is** determined.
- The average punctured/shortened weight enumerator can by computed by applying q-**derivatives** to $W(x,y)$.

$$\mathbf{P} := \begin{bmatrix} n \\ 1 \end{bmatrix}^{-1} (D_{q,x} + D_y) \text{ and } \mathbf{S} := \begin{bmatrix} n \\ 1 \end{bmatrix}^{-1} D_x.$$

Theorem 34 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

1. $\mathbf{P}(W(x,y)) = \begin{bmatrix} n \\ 1 \end{bmatrix}^{-1} \sum_{\dim H = n-1} W_{\Pi_{H(C)}}(x,y),$
2. $\mathbf{S}(W(x,y)) = \begin{bmatrix} n \\ 1 \end{bmatrix}^{-1} \frac{1}{q^{n-1}} \sum_{\dim H = n-1, \langle h \rangle \not\subset H} W_{\Sigma_{h,H}}(x,y).$

Normalized Weight Enumerators and the Zeta Function

Arguments based on **puncturing/shortening** show that:

Theorem 35 (Duursma, 2001)

Let C be an $\mathbb{F}_q$-$[n, k, d]$ Hamming metric code. Then

$$\frac{P(T)}{(1-T)(1-qT)}(1-T)^{d+1} \equiv \mathscr{W}\left(\frac{1}{1-T}\right) \mod T^{n-d+1},$$

where

$$\mathscr{W}(T) := \frac{1}{q-1}\sum_{i=d}^{n}\binom{n}{i}^{-1} W_i T^{i-d},$$

is the **normalized weight enumerator** *of C.*

Gives a nice classification of **random divisible** self-dual codes wrt their $P(T)$.

We do not yet have a q-analogue of this result.

Normalized Weight Enumerators and the Zeta Function

Lemma 36 (Duursma, 2001)

Let $\mathscr{W}(T)$ be a n.w.e. Let $\mathscr{W}^{\mathbf{P}}(T)$ and $\mathscr{W}^{\mathbf{S}}(T)$ be the punctured and shortened n.w.e.s.

- $\mathscr{W}^{\mathbf{S}}(T) \equiv \mathscr{W}(T) \mod T^{n-d}$,
- $\mathscr{W}^{\mathbf{P}}(T) \equiv (1+T)\mathscr{W}(T) \mod T^{n-d+1}$.

$$
\begin{array}{rcl}
W(x,y) & = & p_0 M_{n,d}(x,y) + p_1 M_{n,d+1}(x,y) \\
 & = & (p_0\mathbf{P} + p_1\mathbf{S}) M_{n+1,d+1}(x,y) \\
\downarrow & & \quad\quad\downarrow \\
\mathscr{W}(T) & = & (p_0(1+T) + p_1 T)\mathscr{M}_{n+1,d+1}(T) \mod T^{n-d+1} \\
\Longrightarrow \mathscr{W}\left(\dfrac{T}{1-T}\right) & = & (p_0 + p_1 T)\dfrac{1}{1-T}\mathscr{M}_{n+1,d+1}\left(\dfrac{T}{1-T}\right) \mod T^{n-d+1}
\end{array}
$$

Normalized Weight Enumerators and the Zeta Function

Lemma 37 (Duursma, 2001)

Let $\mathscr{W}(T)$ be the Hamming distance n.w.e. Let $\mathscr{W}^{\mathbf{P}}(T)$ and $\mathscr{W}^{\mathbf{S}}(T)$ be the punctured and shortened n.w.e.s, resp.

- $\mathscr{W}^{\mathbf{S}}(T) \equiv \mathscr{W}(T) \mod T^{n-d}$,
- $\mathscr{W}^{\mathbf{P}}(T) \equiv (1+T)\mathscr{W}(T) \mod T^{n-d+1}$.

$$\begin{array}{rcl}
W(x,y) & = & p_0 M_{n,d}(x,y) + p_1 M_{n,d+1}(x,y) \\
& = & (p_0\mathbf{P} + p_1\mathbf{S}) M_{n+1,d+1}(x,y) \\
\downarrow & & \downarrow \\
\mathscr{W}(T) & = & (p_0(1+T) + p_1 T)\mathscr{M}_{n+1,d+1}(T) \mod T^{n-d+1} \\
\Longrightarrow \mathscr{W}\left(\frac{T}{1-T}\right) & = & P(T)\frac{1}{1-T}\mathscr{M}_{n+1,d+1}\left(\frac{T}{1-T}\right) \mod T^{n-d+1} \\
\Longrightarrow \mathscr{W}\left(\frac{T}{1-T}\right) & = & P(T)\frac{(1-T)^{d+1}}{(1-T)(1-qT)} \mod T^{n-d+1}
\end{array}$$

Invariance of Rank Normalized Weight Enumerators

Definition 38

The normalized weight enumerator (n.w.e.) of C is defined to be the polynomial,

$$\mathscr{W}(T) := (q^m - 1)^{-1} \sum_{i=d}^{n} \begin{bmatrix} n \\ i \end{bmatrix}^{-1} W_i T^{i-d}.$$

$\mathscr{W}^{\mathbf{P}}(T)$ and $\mathscr{W}^{\mathbf{S}}(T)$ are the n.w.e.s for $\mathbf{P}(W_C(x,y))$ and $\mathbf{S}(W_C(x,y))$.

Theorem 39 (B., Blanco-Chacón, Duursma, Sheekey, 2017)

- $\mathscr{W}^{\mathbf{S}}(T) \equiv \mathscr{W}(T) \mod T^{n-d}$,
- $\mathscr{W}^{\mathbf{P}}(T) \equiv (1 + q^d \alpha\varepsilon)\mathscr{W}(T) \mod T^{n-d+1}$.

where

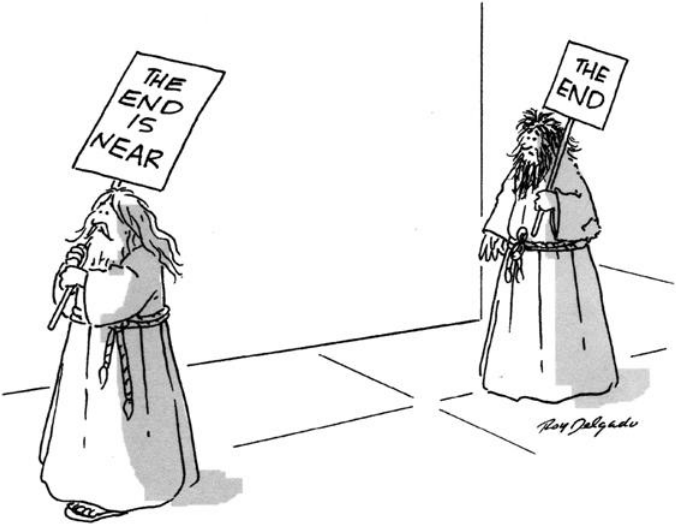
$$\alpha f(T) := Tf(T) \text{ and } \varepsilon f(T) := f(qT).$$

$$q\alpha\varepsilon = \varepsilon\alpha$$

Closing Remarks

- The theory of rank metric codes is still largely uncovered.
- The zeta polynomial can provide a tool for classifying codes with certain weight enumerators (e.g. divisible codes).
- The behaviours of zeroes of classes of codes is an interesting strand of research.
- q-commuting variables and q-derivatives feature in the theory of rank metric codes.
- Possible that many of the polynomial invariants of a rank metric code are best described in terms of q-commuting variables.

The End



References

- I. Blanco-Chacón, E. Byrne, I. Duursma, J. Sheekey, 'Rank-Metric Codes and Zeta Functions,' arXiv:1705.08397.
- E. Byrne and A. Ravagnani, 'Covering radius of matrix codes endowed with the rank metric,' SIAM Journal on Discrete Mathematics, 31(2), 927–944, 2017.
- P. Delsarte, 'Bilinear forms over a finite field, with applications to coding theory,' J. Combin. Theory Ser. A, 25(3):226–241, 1978.
- I. Duursma, 'From weight enumerators to zeta functions,'Discrete Appl. Math., 111(1- 2):55–73, 2001.
- I. Duursma, 'Weight distributions of geometric Goppa codes,'Trans. Amer. Math. Soc., 351(9):3609–3639, 1999.
- E. M. Gabidulin, 'Theory of codes with maximum rank distance,' Problemy Peredachi Informatsii, 21(1):3–16, 1985.
- M. Gadouleau and Z. Yan, 'Macwilliams identity for the rank metric,' CoRR,abs/cs/0701097, 2007.
- Ron M. Roth, 'Maximum-rank array codes and their application to crisscross error correction,' IEEE Trans. Inform. Theory, 37(2):328–336, 1991.