Zeta Polynomials of Rank-Metric Codes

Eimear Byrne
University College Dublin
Open Problems in Rank-Metric Codes

Caserta, Feb 14-16, 2024

The Zeta Function of a Curve

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

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

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

Theorem 1

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

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

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

Hartshorne, Algebraic Geometry. Springer, New York (1977). Graduate Texts in Math, No. 52.

Zeta Functions for Hamming-Metric Codes

Definition 2 (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 $n - d$ 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.

- Gives proofs of the Mallows-Sloane bounds.
- Obtains a classification of extremal self-dual codes.
- Versions of Greene's theorem.
- Raises conjectures on the 'Riemann hypothesis' for linear codes.

I. Duursma, 'Weight distributions of geometric Goppa codes,'Trans. Amer. Math. Soc., 351(9):3609–3639, 1999.

Rank-Metric Codes

- These are linear spaces of matrices, endowed with the rank metric.
- Introduced by Delsarte (1978), Gabidulin (1986) and Roth (1991).
- Studied more after 2000 in the context of code-based-cryptosystems (Gabidulin, Loidreau, Gaborit, Couvreur, most of France).
- Since 2008, generated interest among algebraic coding theorists due to their applicability in network error correction.

P. Delsarte, ‘Bilinear forms over a finite field, with applications to coding theory,’ J. Combin. Theory Ser. A, 25(3):226–241, 1978.

Bartz; Holzbaur; Liu; Puchinger; Renner; Wachter-Zeh, ‘Rank-Metric Codes and Their Applications,’ 2022 http://ieeexplore.ieee.org/document/9767796

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-metric Singleton bound)

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

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

Shortened Subcodes and Binomial Moments

Definition 5 (The shortened subcode of C)

The **shortened subcode** of C wrt $U \subseteq \mathbb{F}_q^n$ is:

$$C(U) := \{X \in C : \mathrm{colspace}(X) \leq U\}.$$

Definition 6 (The Binomial Moments of C)

$$B_u := \sum_{\mathrm{dim} U = u} (|C(U)| - 1) \text{ and } b_u := \begin{bmatrix} n \\ u+d \end{bmatrix}^{-1} B_{u+d}$$

$$B_u = \begin{cases} 0 & \textit{if } u < d, \\ \begin{bmatrix} n \\ u \end{bmatrix} \begin{bmatrix} k - m(n-u) \\ i \end{bmatrix} & \textit{if } u > n - d^{\perp}. \end{cases}$$

The B_u are determined if C is MRD ($n - d^{\perp} = d - 2$).

The Rank-Weight Enumerator

Definition 7

The rank-weight enumerator an $\mathbb{F}_q$-$[n \times m, k]$ code C is:

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

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

By Möbius inversion, we have the following relations:

Theorem 8 (Ravagnani, 2015)

- $b_u = \begin{bmatrix} n \\ u+d \end{bmatrix}^{-1} \sum_{i=1}^{u+d} W_i \begin{bmatrix} n-i \\ n-u-d \end{bmatrix}$
- $W_u = \begin{bmatrix} n \\ t \end{bmatrix} \sum_{i=d}^{u} (-1)^{u-i} q^{\binom{u-i}{2}} \begin{bmatrix} t \\ i \end{bmatrix} b_{i-d}$

A. Ravagnani, 'Rank-metric codes and their duality theory,' Designs, Codes Cryptogr., 2015.

q-Bernstein Polynomials

Definition 9

$\mathscr{B}_i^n(x,y) := \begin{bmatrix} n \\ i \end{bmatrix} y^i \prod_{j=0}^{n-i-1} (x - q^j y)$ is called a q-Bernstein polynomial.

We have the following inversion formulae:

$$
\begin{aligned}
x^{n-i} y^i &= \begin{bmatrix} n \\ i \end{bmatrix}^{-1} \sum_{t=i}^{n} \begin{bmatrix} t \\ i \end{bmatrix} \mathscr{B}_t^n(x,y) \\
\mathscr{B}_i^n(x,y) &= \begin{bmatrix} n \\ i \end{bmatrix} \sum_{t=0}^{n-i} (-1)^t q^{\binom{t}{2}} \begin{bmatrix} n-i \\ t \end{bmatrix} x^t y^{n-t}.
\end{aligned}
$$

We thus get:

$$
W(x,y) = \sum_{i=0}^{n} W_i x^{n-i} y^i = \sum_{i=d}^{n} b_{i-d} \mathscr{B}_i^n(x,y) + x^n.
$$

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

Example 10

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 $\dim U \leq 1$.
- If $\dim U = 2$ then $|C(U)| = 2, 2, 2, 2, 4, 4, 4$.

$$b_0 = \tfrac{13}{7}, b_1 = 2^4 - 1,$$

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

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.

$$\begin{aligned} M_{m\times n,d}(x,y) &= x^n + \sum_{i=d}^{n} \underbrace{(q^{m(i-d+1)}-1)}_{b_{i-d}} \underbrace{\begin{bmatrix} n \\ i \end{bmatrix} y^i \prod_{t=0}^{n-i-1} (x-q^t y)}_{\mathscr{B}_i^n(x,y)}. \\ &= x^n + \sum_{i=d}^{n} b_{i-d}\mathscr{B}_i^n(x,y) \end{aligned}$$

MRD Weight Enumerators

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

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

- The MRD weight enumerators

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

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

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

Equivalent Expressions of the Weight Enumerator

$$
\begin{aligned}
W(x,y) &= x^n + \sum_{i=d}^{n} W_i x^{n-i} y^i \\
&= x^n + \sum_{i=d}^{n} b_{i-d} \mathscr{B}_i^n(x,y) \\
&= \sum_{i=0}^{n-d} p_i M_{n\times m, d+i}(x,y)
\end{aligned}
$$

Definition 11

- The **zeta polynomial** of C is $P(T) = \sum_{j=0}^{n-d} p_j T^j$.
- The **zeta function** of C is defined to be $Z(T) := \sum_{j\geq 0} b_j T^j$,

where $b_j = q^{k-m(n-j-d)} - 1$, $j > n-d-d^{\perp}$.

Recurrence Relations

From the different expressions of the weight enumerator we obtain:

$$p_j = b_j - (q^m + 1)b_{j-1} + q^m b_{j-2}.$$

Therefore:

$$Z(T) = (q^m + 1)T\, Z(T) - q^m T^2 Z(T) + P(T),$$

The recurrence relation gives us:

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

Zeta Functions, Zeta Polynomials, Weight Enumerators

Theorem 12 (B., Blanco-Chacón, Duursma, Sheekey, 2018)

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

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

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

- $\mathscr{B}_{n,r}(x,y) = \begin{bmatrix} n \\ r \end{bmatrix} \prod_{j=0}^{r-1}(x-q^jy)y^{n-r}$.
- $\mathscr{B}_n(T) := \sum_{r=0}^{n} \mathscr{B}_{n,r}(x,y)T^r$.
- If C is MRD then $P(T)=1$.

Duality for the Zeta Polynomial

Theorem 13 (B., Blanco-Chacón, Duursma, Sheekey, 2018)

$$P^{\perp}(T) = T^{n-d-d^{\perp}+2} q^{m(n-d+1)-k} P\left(\frac{1}{q^m T}\right).$$

If C is formally self-dual then

$$P(T) = T^{n-2d+2} q^{m(n-d+1)-k} P\left(\frac{1}{q^m T}\right).$$

and the roots of $P(T)$ occur in pairs $(\alpha, (q^m \alpha)^{-1})$.

Then

$$|\alpha| = |(q^m \alpha)^{-1}| \Leftrightarrow |\alpha| = q^{-m/2}.$$

Riemann Hypothesis for Hamming Weight Enumerators

Definition 14

We say that a Hamming weight enumerator $W(x, y)$ satisfies the Riemann hypothesis (RH) if all the roots of its zeta polynomial $P(T)$ have modulus $q^{-1/2}$.

- $Z(T)$ is the generating function of binomial moments of a code.
- Codes whose zeta functions behave like those of curves will satisfy RH.
- It has been conjectured that all codes whose parameters meet the Mallows-Sloane bound satisfy RH.
- It has been 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.
- The Riemann hypothesis has been studied in the more general setting of a self-dual weight enumerator (Chinen & Imamura, 2021).

The Riemann Hypothesis for Rank Metric Codes

Example 15

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

Example 16

- Take an extended binary quadratic residue 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 to get a self-dual code with rank-weight distribution

$$[1, 0, 21, 162, 72].$$

The binomial moments are

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

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

The zeroes $\omega = -1/4$ have $|\omega| = 2^{-4/2}$ and so satisfy RH.

RH for Codes from a QR Code

We get inequivalent $\mathbb{F}_2$-$[4 \times 4, 8, 2]$ rank-metric codes from a QR code.

Weights	Binomial Moments	Zeta Polynomial
$[1, 0, 23, 156, 76]$	$[0, 23/35, 15, 255]$	$368T^2 + 134T + 23$
$[1, 0, 24, 153, 78]$	$[0, 24/35, 15, 255]$	$128T^2 + 39T + 8$
$[1, 0, 25, 150, 80]$	$[0, 5/7, 15, 255]$	$16T^2 + 4T + 1$
$[1, 0, 26, 147, 82]$	$[0, 26/35, 15, 255]$	$416T^2 + 83T + 26$
$[1, 0, 27, 144, 84]$	$[0, 27/35, 15, 255]$	$144T^2 + 22T + 9$
$[1, 0, 28, 141, 86]$	$[0, 4/5, 15, 255]$	$64T^2 + 7T + 4$
$[1, 0, 29, 138, 88]$	$[0, 29/35, 15, 255]$	$464T^2 + 32T + 29$
$[1, 0, 30, 135, 90]$	$[0, 6/7, 15, 255]$	$32T^2 + T + 2$
$[1, 0, 31, 132, 92]$	$[0, 31/35, 15, 255]$	$496T^2 - 2T + 31$

These are all formally self-dual and satisfy RH.

Riemann Hypothesis for Hamming Weight Enumerators

For self-dual MacWilliams-invariant enumerators, there are existence results.

Theorem 17 (Nishimura, 2008)

Let $W(x,y) = x^{2d} + W_d x^d y^d + \cdots$. Then $W(x,y)$ satisfies RH iff

$$\frac{\sqrt{q}-1}{\sqrt{q}+1}\binom{2d}{d} \leq W_d \leq \frac{\sqrt{q}+1}{\sqrt{q}-1}\binom{2d}{d}.$$

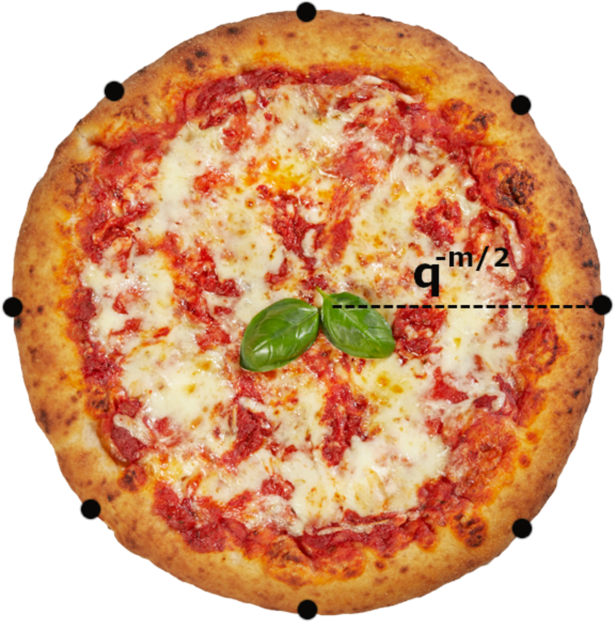
Theorem 18 (Nishimura, 2008)

Let $W(x,y) = x^{2d+2} + W_d x^{d+2} y^d + \cdots$. Then $W(x,y)$ satisfies RH iff the roots of

$$W_d z^2 - ((d-q)W_d + \frac{d+1}{d+2}W_{d+1})z + (d+1)(q+1)(W_d + \frac{W_{d+1}}{d+2}) + (q-1)\binom{2d+2}{d}$$

lie in the interval $[-2\sqrt{q}, 2\sqrt{q}]$.

K. Chinen and Y. Imamura, 'Riemann hypothesis for self-dual weight enumerators of genera three and four,' SUT J. Math, 57 (1) 2021.


$q^{-m/2}$

Open Questions and Final Remarks

- In the Hamming metric, the zeta polynomial can provide a tool for classifying codes with certain weight enumerators such as divisible codes. No analogue if this result exists for rank metric codes.
- The behaviour of zeroes of classes of codes is an interesting strand of research. There has been almost no work on the question of which rank-metric weight enumerators satisfy RH.
- It seems likely that approaches taken by Chinen & Imamura could extend to the rank-metric case.
- We can describe this theory in terms of q-polymatroids.
- This theory extends to tensor codes for the tensor-rank distance and also to generalised weights.

Thanks!

References

- I. Blanco-Chacón, E. Byrne, I. Duursma, J. Sheekey, 'Rank-Metric Codes and Zeta Functions,' Des. Codes, Cryptogr. 86, 2018.
- E. Byrne, G. Cotardo, and A. Ravagnani, 'Rank-Metric Codes, Generalized Binomial Moments and their Zeta Functions, Linear Algebra and its Applications, 2020.
- K. Chinen and Y. Imamura, 'Riemann hypothesis for self-dual weight enumerators of genera three and four,' SUT J. Math, 57 (1) 2021.
- 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.