Non-linear Goppa codes

Azniv Kasparian, Tatjana Todorova, Ivan Marinov *

The absolute Galois group

$$\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \{\varphi \in \mathrm{Aut}(\overline{\mathbb{F}_q}) \mid \varphi|_{\mathbb{F}_q} = \mathrm{Id}_{\mathbb{F}_q}\}$$

of a finite field $\mathbb{F}_q$ is the Galois group of the algebraic closure $\overline{\mathbb{F}_q} = \cup_{m=1}^{\infty} \mathbb{F}_{q^m}$ of $\mathbb{F}_q$ over $\mathbb{F}_q$. The group $\mathfrak{G}$ is isomorphic to the pro-finite closure $\widehat{\mathbb{Z}} := \lim\limits_{\leftarrow} (\mathbb{Z}, +)/(n\mathbb{Z}, +)$ of the infinite cyclic group $(\mathbb{Z}, +)$, i.e., to the projective limit of the finite quotient groups $(\mathbb{Z}, +)/(n\mathbb{Z}, +)$ of $(\mathbb{Z}, +)$. If a group $\mathfrak{G}$ acts on a set M, we say that M is a $\mathfrak{G}$-module. The $\mathfrak{G}$-action on M is locally finite if all the $\mathfrak{G}$-orbits on M are finite and for any $n \in \mathbb{N}$ there are finitely many $\mathfrak{G}$-orbits on M. The cardinality of an orbit $\mathrm{Orb}_{\mathfrak{G}}(x)$, $x \in M$ is called the degree of $\mathrm{Orb}_{\mathfrak{G}}(x)$ and denoted by $\deg \mathrm{Orb}_{\mathfrak{G}}(x)$ or by $|\mathrm{Orb}_{\mathfrak{G}}(x)|$. The non-trivial $\mathfrak{G}$-modules M under consideration have $\mathfrak{G}$-orbits of arbitrary degree $n \in \mathbb{N}$ and, therefore, infinitely many $\mathfrak{G}$-orbits.

Let us denote by $\mathcal{P}$ the set of the $\mathfrak{G}$-orbits on M. If X is a smooth irreducible projective curve, defined over $\mathbb{F}_q$, then $\mathcal{P}$ is naturally isomorphic to the set of the places (i.e., the equivalence classes of the discrete valuations) of the function field $F = \mathbb{F}_q(X)$ of X over $\mathbb{F}_q$. The elements of the free $\mathbb{Z}$-module $\mathrm{Div}(M)$, generated by $\mathcal{P}$ are called divisors on M. The degree

$$\deg : (\mathrm{Div}(M), +) \longrightarrow (\mathbb{Z}, +),$$

$$\deg \left(\sum_{j=1}^{s} a_j \nu_j \right) := \sum_{j=1}^{s} a_j \deg(\nu_j) \quad \text{for} \quad a_j \in \mathbb{Z},\ \nu_j \in \mathcal{P}.$$

is easily seen to be a homomorphism of $\mathbb{Z}$-modules or abelian groups. For an arbitrary $m \in \mathbb{Z}^{\geq 0}$, we denote by $\mathrm{Div}^m(M)$ the set of the divisors of degree m. Note that $(\mathrm{Div}^0(M), +)$ is a subgroup of $(\mathrm{Div}(M), +)$ and fix a subgroup $(\mathcal{F}, +)$ of $\mathrm{Div}^0(M), +)$ of index $h \in \mathbb{N}$. If $M = X$ is a smooth irreducible curve, defined over $\mathbb{F}_q$ with function field $F = \mathbb{F}_q(X)$ over $\mathbb{F}_q$ and $\mathcal{F} = \{(f) = (f)_0 - (f)_\infty \mid f \in F^*\}$ is the group of the principal divisors on X then h is the class number of X. That motivates us to say that h is the class number of M with respect to $\mathcal{F}$. Note that for an arbitrary $m \in \mathbb{N}$ with $\mathrm{Div}^m(M) \neq \emptyset$ there are h linear equivalence classes of divisors of M of degree m. Namely, for an arbitrary $G_o \in \mathrm{Div}^m(M)$, there is a bijective map

$$\varphi : \mathrm{Div}^m(M) \longrightarrow \mathrm{Div}^0(M),$$

$$\varphi(G) = G - G_o.$$

*Research partially supported by Contract 144/2015 with the Scientific Foundation of Kliment Ohridski University of Sofia.

A divisor $G = a_1\nu_1 + \ldots + a_s\nu_s$ with $a_j \in \mathbb{Z}$, $\nu_j \in \mathcal{P}$ is effective if $a_j \geq 0$ for $\forall 1 \leq j \leq s$. Let $\mathrm{Div}_{\geq 0}(M)$ be the set of the effective divisors of M. The ζ-function of M is the formal power series

$$\zeta_M(t) = \prod_{\nu \in \mathcal{P}} \left(\frac{1}{1 - t^{\deg \nu}} \right).$$

Note that $\deg(n\nu) = n\deg(\nu)$ for $\forall n \in \mathbb{Z}^{\geq 0}$, $\nu \in \mathcal{P}$ and expand

$$\frac{1}{1 - t^{\deg \nu}} = \sum_{n=0}^{\infty} t^{\deg(n\nu)}$$

as a sum of a geometric progression. Then

$$\zeta_M(t) = \prod_{\nu \in \mathcal{P}} \left(\sum_{n=0}^{\infty} t^{\deg(n\nu)} \right) = \sum_{D \in \mathrm{Div}_{\geq 0}(M)} t^{\deg(D)} = \sum_{i=0}^{\infty} \mathcal{A}_i t^i$$

for the numbers $\mathcal{A}_i$ of the effective divisors of M of degree $i \in \mathbb{Z}^{\geq 0}$.

For an arbitrary divisor $G = a_1\nu_1 + \ldots + a_s\nu_s$ on M with $a_j \in \mathbb{Z} \setminus \{0\}$, introduce the sero

$$G^+ := \sum_{a_j > 0} a_i \nu_j \in \mathrm{Div}_{\geq 0}(M)$$

of G and the pole

$$G^- := \sum_{a_j < 0} (-a_j)\nu_j \in \mathrm{Div}_{\geq 0}(M)$$

of G, in order to represent

$$G = G^+ - G^-.$$

For any divisor $G = a_1\nu_1 + \ldots + a_s\nu_s \in \mathrm{Div}(M)$, introduce the support

$$\mathrm{Supp} G := \{\nu_j \mid a_j \neq 0\} \subset \mathcal{P}$$

of G as the set of the $\mathfrak{G}$-orbits on M with non-zero coefficients in G. By the very definition of a $\mathbb{Z}$-module, all divisors G have finite support. Let us fix a sum $D = P_1 + \ldots + P_n$ of $\mathfrak{G}$-fixed points $P_j \in M$, viewed as orbits of degree 1. A divisor $G \in \mathrm{Div}(M)$ is regular at D if $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. If any linear equivalence class $[G_j]$, $1 \leq j \leq h$ of divisors of M of degree $m \in \mathbb{N}$ has an effective representative G_j, regular at D, we say that D is m-saturated. Let $(G_j + \mathcal{F})_{\geq 0} := (G_j + \mathcal{F}) \cap \mathrm{Div}_{\geq 0}(M)$ and represent

$$\mathrm{Div}^m_{\geq 0}(M) = (G_1 + \mathcal{F})_{\geq 0} \coprod \ldots \coprod (G_h + \mathcal{F})_{\geq}$$

as a disjoint union. For an arbitrary finite set S, we denote by $|S|$ the cardinality of S. Note that if G_j is regular at D then for any $\varphi \in \mathcal{F}$ with $G_j + \varphi = G_j + \varphi^+ - \varphi^- \geq 0$ one has $G_j \geq \varphi^-$, due to $\mathrm{Supp}(\varphi^+ \cap \mathrm{Supp}(\varphi^- = \emptyset$. The effectiveness of G_j and φ^- implies $\mathrm{Supp}(\varphi^-) \subset \mathrm{Supp}(G_j)$, whereas $\mathrm{Supp}(\varphi^-) \cap \mathrm{Supp}(D) = \emptyset$. Thus, for an arbitrary m-saturated divisor $D = P_1 + \ldots + P_n$ with $P_j \in \mathcal{P}$ of degree $\deg(P_j) = 1$, there is an weight function

$$\mathrm{wt}_D : \mathrm{Div}^m_{\geq 0}(M) = \coprod_{j=1}^{h} (G_j + \mathcal{F})_{\geq 0} \longrightarrow \{0, 1, \ldots, n\}$$

$$\mathrm{wt}_D(G_j+\varphi) := n - |\mathrm{Supp}(\varphi)\cap \mathrm{Supp}(D)| = n - |\mathrm{Supp}(\varphi^+)\cap \mathrm{Supp}(D)|$$

of $\mathrm{Div}^m_{\geq}(M)$ with respect to D. Note that $\varphi = \varphi^+ - \varphi^- \in \mathcal{F} \subset \mathrm{Div}^0(M)$ and $\varphi^- \leq G_j$ imply $\deg(\varphi^+) = \deg(\varphi^-) \leq \deg G_j = m$, whereas $|\mathrm{Supp}(\varphi^+)| \leq \deg(\varphi^+) \leq m$. As a result, $|\mathrm{Supp}(\varphi^+)\cap \mathrm{Supp}(D)| \leq |\mathrm{Supp}(\varphi^+)| \leq m$ and $\mathrm{wt}_D(G_j+\varphi) \geq n-m$ for $\forall G_j+\varphi \in \mathrm{Div}^m_{\geq 0}(M)$. From now on, we consider only $m<n$ and refer to $n-m$ as to the designed minimum weight of $\mathrm{Div}^m_{\geq 0}(M)$ with respect to D.

Note that the set $\mathrm{Div}^m_{\geq 0}(M)$ is finite, as far as there are finitely many effective divisors $\varphi^+, \varphi^- \in \mathrm{Div}^{\geq 0}(M)$ of degree $\leq m$. We treat $\mathrm{Div}^m_{\geq 0}(M)$ as a non-linear code and denote by $\mathcal{Q}^{(s)}_m$ the number of the words $G_j+\varphi \in \mathrm{Div}^m_{\geq 0}(M)$ of D-weight $\mathrm{wt}_D(G_j+\varphi) = s$. The homogeneous polynomial

$$\mathcal{W}_m(x,y) := \sum_{i=0}^{m} \mathcal{W}^{(n-m+i)}_m x^{m-i} y^{n-m+i} \in \mathbb{Z}[x,y]^{(n)}$$

of degree n is referred to as the weight enumerator of $\mathrm{Div}^m_{\geq 0}(M)$ with respect to D.

In order to represent $\mathcal{W}_m(x,y)$ by the homogeneous weight enumerators of MDS-codes, let $C \subset \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear subspace of $\dim_{\mathbb{F}_q} C = k < n$. The weight of $c = (c_1, \ldots, c_n) \in C$ is the number of the non-zero components $c_j \neq 0$ of c. The minimum weight w of C is the minimum weight of a non-zero word of C. Singleton Bound asserts that $n+1-k-w \geq 0$. The linear codes $C_{n,w}$, attaining the equality $n+1-k-w=0$ are called Maximum Distance Separable or, briefly, MDS-ones. An arbitrary MDS-code $C \subset \mathbb{F}_q^n$ of minimum weight w has

$$\mathcal{M}^{(s)}_{n,w} = \binom{n}{s} \sum_{j=0}^{s-w} (-1)^j \binom{s}{j} (q^{s+1-w-j} - 1)$$

words of weight $w \leq s \leq n$. The homogeneous polynomial

$$\mathcal{M}_{n,w}(x,y) := x^n + \sum_{s=w}^{n} \mathcal{M}^{(s)}_{n,w} x^{n-s} y^s$$

of degree n is called the homogeneous weight enumerator of $C_{n,w}$.

Let $C \subset \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear code of $\dim_{\mathbb{F}_q} C = k$ and minimum weight $w \leq n+1-k$ with dual

$$C^{\perp} := \left\{ x \in \mathbb{F}_q^n \mid \langle x, c \rangle = \sum_{i=1}^{n} x_i c_i = 0 \quad \text{for} \quad \forall c \in C \right\}$$

of minimum weight $w^{\perp} \leq k+1$. Let $\mathcal{W}^{(s)}_C$ be the number of the words $c \in C \subset \mathbb{F}_q^n$ with s non-zero components and

$$\mathcal{W}_C(x,y) := x^n + \sum_{s=w}^{n} \mathcal{W}^{(s)}_C x^{n-s} y^s \in \mathbb{Z}[x,y]^{(n)}$$

be the weight enumerator of C. In [3] Duursma shows the existence of a unique polynomial

$$P_C(t) = \sum_{i=0}^{r(C)} a_i t^i \in \mathbb{Q}[t]$$

of degree $\deg P_C = r(C) := n + 2 - w - w^{\perp}$, such that

$$\frac{\mathcal{W}_C(x,y) - x^n}{q-1} = \sum_{i=0}^{r(C)} a_i \frac{\mathcal{M}_{n,w+i}(x,y) - x^n}{q-1}.$$

After showing

$$\frac{\mathcal{M}_{n,n-m+i}(x,y) - x^n}{q-1} = \mathrm{Coeff}_{t^{m-i}} \left(\frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right) \tag{1}$$

in Proposition 1 from [3], he observes that $P_C(t)$ is uniquely determined by the equality

$$\frac{\mathcal{W}_C(x,y) - x^n}{q-1} = \mathrm{Coeff}_{t^{n-w}} \left(P_C(x,y) \frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right)$$

and calls $P_C(t)$ the ζ-polynomial of C. Suppose that $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ is a smooth irreducible curve of genus g, defined over $\mathbb{F}_q$ and $D = P_1 + \ldots + P_n$ is an m-saturated divisor on X, which consists of $\mathbb{F}_q$-rational points P_i. Choose effective representatives $G_1, \ldots, G_h$ of the linear equivalence classes of the divisors of $F = \mathbb{F}_q(X)$ of degree $2g-2 < m < n$, which are regular at D and consider the Riemann-Roch spaces

$$\mathcal{L}(G_j) = H^0(X, \mathcal{O}_X([G_j])) := \{ f \in \mathbb{F}_q(X)^* \,|\, (f) + G_j \geq 0 \} \cup \{0\}.$$

Let

$$\mathcal{E}_D : \mathcal{L}(G_j) \longrightarrow \mathbb{F}_q^n,$$
$$\mathcal{E}_D(f) = (f(P_1), \ldots, f(P_n))$$

be the evaluation map at D and $C_j := \mathcal{E}_D \mathcal{L}(G_j) \subset \mathbb{F}_q^n$ be the images of $\mathcal{L}(G_j)$ under $\mathcal{E}_D$, viewed as linear codes of length n. Note that the poles of $f \in \mathcal{L}(G_j)$ are contained in G_j and form an effective divisor of degree $\leq m$. Therefore $f \in \mathcal{L}(G_j)$ has at most m zeros, counted with their multiplicities and the word $\mathcal{E}_D(f) \in C_j$ has at least $n - m$ non-zero components. In other words, the non-zero words of C_j are of weight $\geq n - m$. The ζ-function of X is

$$\zeta_X(t) = \frac{L_X(t)}{(1-t)(1-qt)}$$

for a polynomial $L_X(t) \in \prod_{i=1}^{2g} (1 - \omega_i t) \in \mathbb{Z}[t]$ with $L_X(0) = 1$, $L_X(1) = h$ and $\omega_i \in \mathbb{C}$, $|\omega_i| = \sqrt{q}$ for $\forall 1 \leq i \leq g$. We call $L_X(t)$ the ζ-polynomial of X. Duursma's considerations from [2] imply that

$$\begin{gathered} \mathrm{Coeff}_{t^m} \left(L_X(t) \frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right) = \sum_{i=1}^{h} \frac{\mathcal{W}_{C_i}(x,y) - x^n}{q-1} = \\ \mathrm{Coeff}_{t^m} \left(\sum_{i=1}^{h} t^{m-n+w_i} P_{C_i}(t) \frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right) \end{gathered} \tag{2}$$

for the minimal weights w_i of $C_i = \mathcal{E}_D \mathcal{L}(G_i)$. Note that $\sum_{i=1}^{h} \frac{\mathcal{W}_{C_i}(x,y) - x^n}{q-1}$ is the weight enumerator of $\mathrm{Div}_{\geq 0}^m(X)$ with respect to D and the ζ-polynomials $P_{C_i}(t)$ of algebro-geometric

Goppa codes $C_i = \mathcal{E}_D\mathcal{L}(G_i)$, $1 \leq i \leq h$ are related with the ζ-polynomial $L_X(t)$ of X by the equality

$$L_X(t) = \sum_{i=1}^{h} t^{m-n+w_i} P_{C_i}(t).$$

That motivates Duursma to call the polynomial $P_C(t)$ of an abstract linear code $C' subset \mathbb{F}_Q^n$ the ζ-polynomial of C.

The next proposition shows the existence of a unique ζ-polynomial $P_m^D(t) = \sum\limits_{i=0}^{m} a_i t^i \in \mathbb{Q}[t]$ of $\deg P_m^D(t) \leq m$ of the effective divisors $\mathrm{Div}_{\geq 0}^m(M)$ of a ζ-module M of degree m with respect to an m-saturated sum D of $\mathfrak{G}$-fixed points on M.

Proposition 1. *Let M be a locally finite $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-module and $D = P_1 + \ldots + P_n \in \mathrm{Div}(M)$ be an m-saturated sum of $\mathfrak{G}$-fixed points P_i on M for some $m < n$. Denote by $\mathcal{W}_m(x,y)$ the weight enumerator of $\mathrm{Div}_{\geq 0}^m(M)$ with respect to D and put $\mathcal{M}_{n,w}(x,y)$ for the weight enumerator of an MDS-code $C_{n,w} \subset \mathbb{F}_q^n$ of minimal weight w. Then there is a unique polynomial $P_m^D(t) = \sum\limits_{i=0}^{m} a_i t^i \in \mathbb{Q}[t]$ of degree $\deg P_m^D \leq m$ with*

$$\mathcal{W}_m(x,y) = \sum_{i=0}^{m} a_i \frac{\mathcal{M}_{n,n-m+i}(x,y) - x^n}{q-1}. \tag{3}$$

The polynomial $P_m^D(t)$ is uniquely determined by the equality

$$\mathcal{W}_m(x,y) = \mathrm{Coeff}_{t^m}\left(P_m^D(t) \frac{[y(1-t)+xt]^n}{(1-t)(1-qt)} \right), \tag{4}$$

where $\mathrm{Coeff}_{t^m}(f(t))$ stands for the coefficient of t^m in a formal power series $f(t) \in \mathbb{Q}[[t]]$. We call $P_m^D(t) = \sum\limits_{i=0}^{m} a_i t^i \in \mathbb{Q}[t]$ the ζ-polynomial of $\mathrm{Div}_{\geq 0}^m(M)$ with respect to D.

Proof. Note that

$$\mathcal{W}_m(x,y) := \sum_{i=0}^{m} \mathcal{W}_m^{(n-m+i)} x^{m-i} y^{n-m+i} \in \mathbb{Z}[x,y]^{(n)}$$

belongs to the $\mathbb{Q}$-span of the homogeneous monomials $x6m - iy^{n-m+i}$ of total degree n, which are of degree $\geq n-m$ with respect to y. For any $0 \leq i \leq m$ one has

$$\frac{\mathcal{M}_{n,n-m+i}(x,y) - x^n}{q-1} = \frac{1}{q-1}\left(\sum_{s=n-m+i}^{n} \mathcal{M}_{n,n-m+i}^{(s)} x^{n-s} y^s \right)$$

from $\mathrm{Span}_{\mathbb{Q}}\{x^{n-s}y^s \,|\, n-m+i \leq s \leq n\}$ with non-zero coefficient

$$\frac{1}{q-1}\mathcal{M}_{n,n-m+i}^{(n-m+i)} = \binom{n}{n-m+i} = \binom{n}{m-i}$$

of $x^{m-i}y^{n-m+i}$. Therefore $\frac{\mathcal{M}_{n,n-m+i}(x,y)-x^n}{q-1}$ with $0 \leq i \leq m$ are $\mathbb{Q}$-linearly independent and form a $\mathbb{Q}$-basis of $\mathrm{Span}_{\mathbb{Q}}\{x^{n-s}y^s \,|\, n-m \leq s \leq n\}$. Now, $\mathcal{W}_m(x,y) \in \mathrm{Span}_{\mathbb{Q}}\{x^{n-s}y^s \,|\, n-m \leq s \leq n\}$ has uniquely determined coordinates a_i with respect to the basis $\frac{\mathcal{M}_{n,n-m+i}(x,y)-x^n}{q-1}$, which satisfy (**??**). Making use of (1), we note that

$$\frac{\mathcal{M}_{n,n-m+i}(x,y)-x^n}{q-1} = \mathrm{Coeff}_{t^m}\left(t^i \frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) \quad \text{for} \quad \forall 0 \leq i \leq m.$$

Thus, there exist uniquely determined $a_i \in \mathbb{Q}$ with

$$\mathcal{W}_m(x,y) = \sum_{i=0}^{m} a_i \mathrm{Coeff}_{t^m}\left(t^i \frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right) = \mathrm{Coeff}_{t^m}\left(\sum_{i=0}^{m} a_i t^i \frac{[y(1-t)+xt]^n}{(1-t)(1-qt)}\right),$$

so that the polynomial $P_m^D(t) := \sum_{i=0}^{m} a_i t^i$ can be defined by (4).

□

Combining (4) with (2), one observes that for any smooth irreducible curve $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ of genus $g \geq 1$, any natural number $2g-2 < m < n$ and any m-saturated sum $D = P_1 + \ldots + P_n$ of $\mathbb{F}_q$-rational points $P_i \in X(\mathbb{F}_q)$, the ζ-function

$$\zeta_{X,m}^D(t) := \frac{P_m^D(t)}{(1-t)(1-qt)} \in \mathbb{Q}[[t]]$$

of $\mathrm{Div}_{\geq 0}^m(X)$ with respect to D coincides with the ζ-function

$$\zeta_X(t) = \frac{L_X(t)}{(1-t)(1-qt)} \in \mathbb{Z}[[t]]$$

of X. That leads to the next

Definition 2. *A locally finite module M over $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is (m,D)-balanced if the ζ-function*

$$\zeta_m^D(t) := \frac{P_m^D(t)}{(1-t)(1-qt)} = \zeta_M(t)$$

of $\mathrm{Div}_{\geq 0}^m(M)$ with respect to the m-saturated sum $D = P_1 + \ldots + P_n$ of $\mathfrak{G}$-fixed points $P_i \in M$ coincides with the ζ-function of M.

It is well known that the series

$$\sum_{i=0}^{\infty} \mathcal{A}_i t^i = \frac{P_m^D(t)}{(1-t)(1-qt)}$$

is a rational function with polynomial denominator

$$qt^2 - (q+1)t + 1$$

if and only if the sequence $\{\mathcal{A}_i\}_{i=0}^{\infty}$ satisfies the recurrence relation

$$\mathcal{A}_n - (q+1)\mathcal{A}_{n-1} + q\mathcal{A}_{n-2} = 0$$

for sufficiently large $n \geq n_0$. This, in turn, is equivalent to

$$\mathcal{A}_n = C_1 q^n + C_2 \quad \text{for} \quad \forall n \geq n_0$$

and some constants $C_1, C_2 \in \mathbb{C}$. In fact, C_1, C_2 are rational numbers, due to

$$C_1 = \frac{\mathcal{A}_{n+1} - \mathcal{A}_n}{q^n(q-1)}, \quad C_2 = \frac{q\mathcal{A}_n - \mathcal{A}_{n+1}}{q-1}$$

with $\mathcal{A}_n, \mathcal{A}_{n+1} \in \mathbb{Z}^{\geq 0}$. Note also that

$$1 = \zeta_M(0) = \mathcal{A}_0 = a_0,$$

so that $P_m^D(t)$ can be represented in the form

$$P_m^D(t) = \prod_{i=1}^{\deg P_m^D} (1 - \omega_i t)$$

for some complex numbers $\omega_i \in \mathbb{C}$.

Recall that the connected sum of two smooth irreducible curves $X_1/\mathbb{C} \subset \mathbb{P}^{N_1}(\mathbb{C})$, $X_2/\mathbb{C} \subset \mathbb{P}^{N_2}(\mathbb{C})$, defined over the field $\mathbb{C}$ of complex numbers is obtained from the disjoint union $X_1 \coprod X_2$ by removing small discs from X_1, X_2 and gluing along their boundaries. The boundary of a disc is a circle and has vanishing Euler number. That is why, the Euler number of $X_1 \sharp X_2$ equals

$$e(X_1 \sharp X_2) = e(X_1) + e(X_2) - 2.$$

Note that one of the removed small discs from X_1 and X_2 is homotopic to a point, so that up to a homotopy, the connected sum can be obtained from $X_1 \coprod X_2$ by removing a projective line $\mathbb{P}^1(\mathbb{C})$ and gluing along subsets of X_1 and X_2 with vanishing Euler numbers.

Now, suppose that M_1 and M_2 are locally finite modules over $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_1)$. Then the disjoint union $M_1 \coprod M_2$ is a $\mathfrak{G}$-module with ζ-function

$$\zeta_{M_1 \coprod M_2}(t) = \zeta_{M_1}(t)\zeta_{M_2}(t),$$

as far as the union of the $\mathfrak{G}$-orbits on M_j of degree d is the set of the $\mathfrak{G}$-orbits on $M_1 \coprod M_2$ of degree d. In particular, if M_1 is (m_1, D_1)-balanced and M_2 is (m_2, D_2)-balanced then

$$\zeta_{M_1 \coprod M_2}(t) = \frac{P_{m_1}^{D_1}(t) P_{m_2}^{D_2}(t)}{(1-t)^2(1-qt)^2}$$

reveals that $M_1 \coprod M_2$ cannot be balanced. We form the connected sum $M_1 \sharp_{\mathbb{F}_q} M_2$ of M_1 and M_2 over $\mathbb{F}_q$ by removing a projective line $\mathbb{P}^1(\overline{\mathbb{F}_q})$ form the disjoint union $M_1 \coprod M_2$. The ζ-function

$$\zeta_{M_1 \sharp_{\mathbb{F}_q} M_2}(t) = \zeta_{M_1 \coprod M_2}(t) : \zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \frac{\zeta_{M_1}(t)\zeta_{M_2}(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = (1-t)(1-qt)\zeta_{M_1}(t)\zeta_{M_2}(t).$$

It is clear that if M_1 is (m_1, D_1)-balanced and M_2 is (m_2, D_2)-balanced then $M_1 \sharp_{\mathbb{F}_q} M_2$ is $(m_1 + m_2, D_1 + D_2)$-balanced and the ζ-function

$$\zeta_{M_1 \sharp_{\mathbb{F}_q} M_2}(t) = \frac{P_{m_1}^{D_1}(t) P_{m_2}^{D_2}(t)}{(1-q)(1-qt)}.$$

Lemma 3. *(i) Let M be a locally finite $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-module with ζ-function*

$$\zeta_M(t) = \frac{P_M(t)}{(1-t)(1-qt)}$$

for some polynomial

$$P_M(t) = \prod_{i=1}^{d}(1-\omega_i t) \in \mathbb{Q}[t]$$

of $\deg P_M(t) = d$ *with* $P_m(0) = 1$ *and*

$$\check{P_M}(t) := \prod_{i=1}^{d}\left(1 - \frac{q}{\omega_i}t\right).$$

Then the product $P_M^*(t) := P_M(t)\check{P_M}(t)$ *satisfies the functional equation*

$$P_M^*(t) = P_M^*\left(\frac{1}{qt}\right) q^d t^{2d}$$

and has leading coefficient $\mathrm{LC}(P_M^*(t)) = q^d$.

(ii) If a polynomial $P^*(t) \in \mathbb{R}[t]$ *of degree* $\deg P^*(t) = \delta$ *with* $P^*(0) = 1$ *and leading coefficient* $\mathrm{LC}(P^*(t)) = q^{\frac{\delta}{2}}$ *satisfies the functional equation*

$$P^*(t) = P^*\left(\frac{1}{qt}\right) q^{\frac{\delta}{2}} t^{\delta},$$

then $\frac{1}{\omega_i} \in \mathbb{C}$ *is a root of* $P^*(t)$ *exactly when* $\frac{\omega_i}{q} \in \mathbb{C}$ *is a root of* $P^*(t)$.

Proof. (i) Straightforwardly,

$$P_M^*\left(\frac{1}{qt}\right) q^d t^{2d} = P_M\left(\frac{1}{qt}\right)\check{P_M}\left(\frac{1}{qt}\right) q^d t^{2d} = \left[\prod_{i=1}^{d}\left(1-\frac{\omega_i}{qt}\right)\left(1-\frac{1}{\omega_i t}\right)\right] q^d t^{2d} =$$

$$\prod_{i=1}^{d}(1-\omega_i t)\left(1-\frac{q}{\omega_i}t\right) = P_M(t)\check{P_M}(t) = P_M^*(t)$$

by

$$\left(1-\frac{\omega_i}{qt}\right)\left(1-\frac{1}{\omega_i t}\right) = \frac{qt^2}{(}1-\omega_i t)\left(1-\frac{q}{\omega_i}t\right).$$

(ii) Due to $P^*(0) = 1$, one has $P^*(t) = \prod_{i=1}^{\delta}(1-\omega_i t)$ for the reciprocals $\omega_i \in \mathbb{C}$ of the complex roots of $P^*(t)$. Making use of

$$1 - \frac{\omega_i}{qt} = \frac{(-\omega_i)}{qt}\left(1-\frac{q}{\omega_i}t\right),$$

one observes that

$$P^*\left(\frac{1}{qt}\right) q^{\frac{\delta}{2}} t^{\delta} = \left[\prod_{i=1}^{\delta}\left(1 - \frac{\omega_i}{qt}\right)\right] q^{\frac{\delta}{2}} t^{\delta} = \frac{\prod_{i=1}^{\delta}(-\omega_i)}{q^{\delta} t^{\delta}} \left[\prod_{i=1}^{\delta}\left(1 - \frac{q}{\omega_i} t\right)\right] q^{\frac{\delta}{2}} t^{\delta} =$$

$$\frac{\mathrm{LC}(P^*)}{q^{\frac{\delta}{2}}} \left[\prod_{i=1}^{\delta}\left(1 - \frac{q}{\omega_i}\right)\right] = \prod_{i=1}^{\delta}\left(1 - \frac{q}{\omega_i} t\right)$$

coincides with $P^*(t) = \prod_{i=1}^{\delta}(1-\omega_i t)$ if and only if for any root $\frac{1}{\omega_i} \in \mathbb{C}$ of $P^*(t) = 0$ the complex number $\frac{\omega_i}{q} \in \mathbb{C}$ is also a root of $P^*(t) = 1$.

□

Let M be a $\mathfrak{G}$-module with ζ-polynomial

$$P_M(t) = \prod_{i=1}^{d}(1 - \omega_i t)$$

for some $\omega_i \in \mathbb{C}^*$. If there is a $\mathfrak{G}$-module $\check{M}$ with ζ-polynomial

$$\check{P_M}(t) := \prod_{i=1}^{d}\left(1 - \frac{q}{\omega_i} t\right)$$

then

$$P_M^*(t) := P_M(t)\check{P_M}(t) = P_{M \sharp_{\mathbb{F}_q} \check{M}}(t)$$

is the ζ-polynomial of the connected sum of M and $\check{M}$ over $\mathbb{F}_q$.

Let $C \subset \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear code of dimension $\dim_{\mathbb{F}_q} C = k$ and minimum weight w with dual $C^{\perp}$ of minimum weight $w^{\perp}$. The deviation $g := n + 1 - k - w$, respectively, $g^{\perp} := n + 1 - (n - k) - w^{\perp} = k + 1 - w^{\perp}$ from the equality in the Singleton Bound $g \geq 0$, respectively, $g^{\perp} \geq 0$ is called the genus of C, respectively, $C^{\perp}$. The ζ-polynomials $P_C(t), P_{C^{\perp}}(t) \in \mathbb{Q}[t]$ of C and $C^{\perp}$ are of degree $g + g^{\perp}$. Mac Williams identities for the weight distribution of C and $C^{\perp}$ are equivalent to the equality

$$P_{C^{\perp}}(t) = P_C\left(\frac{1}{qt}\right) q^g t^{g+g^{\perp}}$$

for their ζ-polynomials. An $\mathbb{F}_q$-linear code $C \subset \mathbb{F}_q^n$ is formally self-dual if C and $C^{\perp}$ have one and a same number of words od weight s for all $0 \leq s \leq n$. The formal self-duality of C is equivalent to the functional equation

$$P_C(t) = P_C\left(\frac{1}{qt}\right) q^g t^{2g}$$

for its ζ-polynomial $P_C(t)$. That motivates the next

Lemma-Definition 4. *Let M be a locally finite module over $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ with ζ-function*

$$\zeta_M(t) = \frac{P_M(t)}{(1-t)(1-qt)}$$

for some polynomial $P_M(t) \in \mathbb{Q}[t]$ of even degree $\deg P_M(t) = 2d$ and $R(t) \in \mathbb{Q}[[t]]$ be the formal power series, defined by the equality

$$R(t) := (q-1)t^{1-d}\zeta_M(t) + h\left[\frac{t^{1-d}}{1-t} - \frac{q^d t^d}{1-qt}\right] \in \mathbb{Q}[[t]]. \tag{5}$$

Then the following conditions are equivalent:

(i) $P_M(t)$ satisfies the functional equation

$$P_M(t) = P_M\left(\frac{1}{qt}\right) q^d t^{2d}; \tag{6}$$

(ii) the rational function

$$t^{1-d}\zeta_M(t) = \left(\frac{1}{qt}\right)^{1-d} \zeta_M\left(\frac{1}{qt}\right) \tag{7}$$

is invariant under the substitution $t \mapsto \frac{1}{qt}$;

(iii) $R(t)$ is a Laurent polynomial of the form

$$R(t) = R_0 + \sum_{i=1}^{d-1} R_i\left(t^i + \frac{1}{q^i t^i}\right) \in \mathrm{Span}_{\mathbb{Q}}\left\{ t^i + \frac{1}{q^i t^i} \,\Big|\, 0 \leq i \leq d-1 \right\}. \tag{8}$$

If there holds one and, therefore, any one of the aforementioned conditions, we say that the $\mathfrak{G}$-module M is formally self-dual.

Proof. Making use of

$$\left(1 - \frac{1}{qt}\right)\left(1 - \frac{q}{qt}\right) = q^{-1}t^{-2}(1-t)(1-qt),$$

one observes that

$$\left(\frac{1}{qt}\right)^{1-d} \zeta_M\left(\frac{1}{qt}\right) = q^{d-1}t^{d-1} \frac{P_M\left(\frac{1}{qt}\right)}{\left(1 - \frac{1}{qt}\right)\left(1 - \frac{1}{t}\right)} = q^d t^{d+1} \frac{P_M\left(\frac{1}{qt}\right)}{(1-t)(1-qt)}$$

coincides with

$$t^{1-d}\zeta_M(t) = t^{1-d}\frac{P_M(t)}{(1-t)(1-qt)}$$

if and only if

$$t^{1-d}P_M(t) = q^d t^{d+1} P_M\left(\frac{1}{qt}\right).$$

After multiplication by t^{d-1}, this amounts to (6) and proves the equivalence of (i) and (ii).

Note that $R(t) := \sum\limits_{i=0}^{\infty} R_{i-d+1}t^{i-d+1} \in \mathbb{Q}[[t]]$ can be defined by the equalities

$$R_{i-d+1} = (q-1)\mathcal{A}_i + h(1 - q^{i-d+1}) \quad \text{for} \quad \forall i \in \mathbb{Z}^{\geq 0}. \tag{9}$$

Note that the rational function

$$Phi(t) := \frac{t^{1-d}}{1-t} - \frac{q^d t^d}{1-qt}$$

is invariant under the substitution $t \mapsto \frac{1}{qt}$, according to

$$\left(\frac{1}{qt}\right)^{1-d} . \frac{1}{1-\frac{1}{qt}} = -\frac{q^d t^d}{1-qt}$$

and

$$q^d \left(\frac{1}{qt}\right)^{d} . \frac{1}{1-\frac{q}{qt}} = -\frac{t^{1-d}}{1-t}.$$

Therefore, (7) is equivalent to the invariance

$$R(t) = R\left(\frac{1}{qt}\right) \tag{10}$$

of $R(t) := (q-1)t^{1-d}\zeta_M(t) + h\Phi(t)$ under the transformation $t \mapsto \frac{1}{qt}$. The ζ-function $\zeta_M(t) = \sum\limits_{i=0}^{\infty} \mathcal{A}_i t^i$ has no pole at $t = 0$. The power series

$$\Phi(t) = t^{1-d}\left(\sum_{s=0}^{\infty} t^s\right) - q^d t^d \left(\sum_{s=0}^{\infty} q^s t^s\right) = \sum_{s=1-d}^{\infty} \Phi_s t^s$$

has terms of degree $\geq 1-d$, as well as the power series

$$t^{1-d}\zeta_M(t) = t^{1-d}\left(\sum_{i=0}^{\infty} \mathcal{A}_i t^i\right).$$

Therefore $R(t) = \sum\limits_{i=1-d}^{\infty} R_i t^i$ has a pole of order $\leq d-1$ at $t = 0$. The functional equation (10) asserts the coincidence of the formal power series

$$R\left(\frac{1}{qt}\right) = \sum_{i=1-d}^{d-1} R_i q^{-i} t^{-i} + \sum_{i=d}^{\infty} R_i q^{--i} t^{-i} = \sum_{j=1-d}^{d-1} R_{-j} q^j t^j + \sum_{j=-\infty}^{-d} R_{-j} q^j t^j$$

with the formal power series

$$R(t) = \sum_{i=1-d}^{d-1} R_i t^i + \sum_{i=d}^{\infty} R_i t^i.$$

This is equivalent to the identical vanishing of

$$0 \equiv R(t) - R\left(\frac{1}{qt}\right) = -\sum_{i=-\infty}^{-d} R_{-i}q^i t^i + \sum_{i=1-d}^{d-1}(r_i - q^i R_{-i})t^i + \sum_{i=d}^{\infty} R_i t^i$$

and holds exactly when $R_i = 0$ for all $i \geq d$ and

$$\sum_{j=1-d}^{d-1} R_{-j}t^{-j} = \sum_{i=1-d}^{d-1} R_i t^i = \sum_{i=1-d}^{d-1} q^i R_{-i}t^i = \sum_{j=1-d}^{d-1} q^{-j}R_j t^{-j}.$$

The last equality of power series is equivalent to

$$R_{-j} = q^{-j}R_j \quad \text{for} \quad \forall 1-d \leq j \leq d-1$$

and amounts to

$$R(t) = \sum_{j=1-d}^{-1} R_j t^j + R_0 + \sum_{j=1}^{d-1} R_j t^j = \sum_{i=1}^{d-1} R_{-i}t^{-i} + R_0 + \sum_{j=1}^{d-1} R_j t^j =$$

$$R_0 + \sum_{i=1}^{d-1} R_i\left(t^i + q^{-i}t^{-i}\right).$$

That justifies $(ii) \Leftrightarrow (iii)$.

□

Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ be a smooth irreducible curve of genus g, defined over $\mathbb{F}_q$. Then the ζ-polynomial of X is of degree $2g$ and Riemann-Roch Theorem implies that X has

$$\mathcal{A}_m = h\frac{q^{m-g+1}-1}{q-1}$$

effective divisors of degree $m > 2g-2$. Drawing an analogy with this example of a locally finite module over $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, we give the following

Corollary-Definition 5. *Let M be a locally finite (m, D)-balanced module over the absolute Galois group $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ with ζ-function $\zeta_M(t) = \sum_{i=0}^{\infty} \mathcal{A}_i t^i$ and $R(t)$ be the formal power series, defined by the equality*

$$R(t) := (q-1)t^{1-d}\zeta_M(t) + h\left[\frac{t^{1-d}}{1-t} - \frac{q^d t^d}{1-qt}\right] \in \mathbb{Q}[[t]].$$

Then $R(t) = \sum_{j=1-d}^{n_1} R_j t^j$ is a Laurent polynomial if and only if

$$\mathcal{A}_i = h\frac{q^{i-d+1}-1}{q-1} \quad \text{for sufficiently large} \quad i \geq n_1 + d. \qquad (11)$$

The $\mathfrak{G}$-modules M, satisfying (11) are called Riemann-Roch modules.

In particular, any formally self-dual $\mathfrak{G}$-module is a Riemann-Roch module.

Proof. If $R(t) = \sum\limits_{j=1-d}^{n_1} R_j t^j$ is a Laurent polynomial, then (9) implies that

$$R_{i-d+1} = (q-1)\mathcal{A}_i + h(1 - q^{i-d+1}) = 0 \quad \text{for all} \quad i \geq n_1 + d.$$

As a result, there holds (11) for all $i \geq n_1 + d$.

Conversely, (11) for all $i \geq n_1 + d$ and (9) imply that $R_{i-d+1} = 0$ for all $i \geq n_1 + d$, whereas $R(t) = \sum\limits_{j=1-d}^{n_1} R_j t^j$.

□

Definition 6. *Let M be a locally finite module M over $\mathfrak{G} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ with ζ-function*

$$\zeta_M(t) = \frac{P_M(t)}{(1-t)(1-qt)}$$

for some polynomial $P_M(t) \in \mathbb{Q}[t]$. Then M satisfies the Riemann Hypothesis Analogue if all the roots $\alpha \in \mathbb{C}$ of $P_M(t)$ are of $|\alpha| = \frac{1}{\sqrt{q}}$.

Proposition 7. (Това твърдение е от стария ръкопис) *Let M be a formally self-dual $\mathfrak{G}$-module with ζ-function*

$$\zeta_M(t) = \frac{P_M(t)}{(1-t)(1-qt)},$$

$$P_M(t) = \prod_{i=1}^{2d} (1 - \omega_i t) \in \mathbb{Q}[t], \quad \omega_i \in \mathbb{C} \quad \textit{and}$$

$$S_\nu := -\sum_{i=1}^{2d} \omega_i^\nu \quad \textit{for} \quad \forall \nu \in \mathbb{N}.$$

Then M satisfies the Riemann Hypothesis Analogue if and only if the sequence $\left\{ S_\nu q^{-\frac{\nu}{2}} \right\}_{\nu=1}^{\infty} \subset \mathbb{C}$ is absolutely bounded.

Proof. By Lemma 3 (ii), $1 - \omega_i t$ is a factor of $P_M(t)$ if and only if $1 - \frac{q}{\omega_i} t$ is a factor of $P_M(t)$. That is why

$$S_\nu = -\sum_{j=1}^{2d} \left(\frac{q}{\omega_i} \right)^\nu \quad \text{for} \quad \forall \nu \in \mathbb{N}. \tag{12}$$

If M satisfies the Riemann Hypothesis Analogue and $\omega_j = e^{i\varphi_j}\sqrt{q}$ for some $\varphi_j \in [0, 2\pi)$, then

$$S_\nu q^{-\frac{\nu}{2}} = -\sum_{j=1}^{2d} e^{i\nu\varphi_j}$$

by (**??**) and

$$|S_\nu q^{-\frac{\nu}{2}}| \leq \sum_{j=1}^{2d} |e^{i\nu_j \varphi_j}| \leq 2d$$

is bounded for any $\nu \in \mathbb{N}$.

Conversely, assume that

$$S_\nu q^{-\frac{\nu}{2}} = -\sum_{j=1}^{2d} \left(\frac{\omega_i}{\sqrt{q}} \right)^\nu \quad \text{for } \forall \nu \in \mathbb{N}$$

form an absolutely bounded sequence of complex numbers. Then there exist a positive real constant C and $\nu_o \in \mathbb{N}$, such that

$$|S_\nu q^{-\frac{\nu}{2}}| \leq C \quad \text{for all} \quad \nu \geq \nu_o.$$

As a result, the series

$$S(t) := \sum_{\nu=\nu_o}^{\infty} S_\nu q^{-\frac{\nu}{2}} t^\nu$$

converges absolutely for all $t \in \Delta(0,1) := \{z \in \mathbb{C} \,|\, |z| < 1\}$, according to

$$\sum_{\nu=\nu_o}^{\infty} |S_\nu q^{-\frac{\nu}{2}}||t|^\nu \leq C \left(\sum_{\nu=\nu_o}^{\infty} |t|^\nu \right) = \frac{C|t|^{\nu_o}}{1-|t|} \quad \text{for} \quad \forall |t| < 1.$$

However,

$$S(t) = \sum_{\nu=\nu_o}^{\infty} S_\nu q^{-\frac{\nu}{2}} t^\nu = -\sum_{\nu=\nu_o}^{\infty} \left[\sum_{j=1}^{2d} \left(\frac{\omega_j}{\sqrt{q}} \right)^\nu \right] t^\nu =$$

$$-\sum_{j=1}^{2d} \left[\sum_{\nu=\nu_o}^{\infty} \left(q^{-\frac{1}{2}} \omega_j t \right)^\nu \right] = -\sum_{j=1}^{2d} \frac{\left(q^{-\frac{1}{2}} \omega_j t \right)^{\nu_o}}{1 - q^{-\frac{1}{2}} \omega_j t}$$

is a sum of $2d$ geometric progressions with ratios $q^{-\frac{1}{2}} \omega_j t$ and the convergence of $S(t)$ for all $t \in \Delta(0,1)$ requires the rational function

$$-\sum_{j=1}^{2d} \frac{\left(q^{-\frac{1}{2}} \omega_j t \right)^{\nu_o}}{1 - q^{-\frac{1}{2}} \omega_j t}$$

of t to have no poles in $\Delta(0,1)$. In other words, all the poles $\frac{\sqrt{q}}{\omega_j}$ of this ratio of polynomials are from $\mathbb{C} \setminus \Delta(0,1)$, i.e.,

$$\left| \frac{\sqrt{q}}{\omega_j} \right| \geq 1. \tag{13}$$

Making use of (12), one observes that the convergence of the power series

$$S(t) = \sum_{\nu=\nu_o} S_\nu q^{-\frac{\nu}{2}} t^\nu = -\sum_{\nu=\nu_o}^{\infty} \left[\sum_{j=1}^{2d} \left(\frac{\sqrt{q}}{\omega_j} \right)^\nu \right] =$$

$$-\sum_{j=1}^{2d} \left[\sum_{\nu=\nu_o}^{\infty} \left(\omega_j^{-1} \sqrt{q} t \right)^\nu \right] = -\sum_{j=1}^{2d} \frac{\left(\omega_j^{-1} \sqrt{q} t \right)^{\nu_o}}{1 - \omega_j^{-1} \sqrt{q} t}$$

for all $t \in \Delta(0,1)$ implies that the poles $\frac{\omega_j}{\sqrt{q}}$ belong to $\mathbb{C} \setminus \Delta(0,1)$, i.e.,

$$\left| \frac{\omega_j}{\sqrt{q}} \right| \geq 1. \tag{14}$$

Combining (13) with (14), one concludes that

$$\left| \frac{\sqrt{q}}{\omega_j} \right| = 1 \quad \text{for all} \quad 1 \leq j \leq 2d.$$

Thus, all the roots $\frac{1}{\omega_j} \in \mathbb{C}$ of $P_M(t) = 0$ are from the circle

$$\partial\Delta \left(0, \frac{1}{\sqrt{q}} \right) := \left\{ z \in \mathbb{C} \,\middle|\, |z| = \frac{1}{\sqrt{q}} \right\}$$

and M satisfies the Riemann Hypothesis Analogue.

$\square$

References

[1] E. Bombieri, Counting points on curves over finite fields (d'après A. Stepanov), *Seminaire Bourbaki 1972/73, Exp. 430, Lecture Notes in Mathematics,* , **Vol. 383**, pp. 234 - 241, Springer, Berlin, 1974.

[2] I. Duursma, Weight distribution of geometric Goppa codes, *Transections of the American Mathematical Society*, **351** (1999), 3609 - 3639.

[3] I. Duursma, From weight enumerators to zeta functions, *Discrete Applied Mathematics*, **111** (2001), 55 - 73.

[4] H. Stichtenoth, *Algebraic Function Fields and Codes*, *Springer, Berlin*, 1992.