Mac Williams identities for linear codes as polarized Riemann-Roch conditions *

Azniv Kasparian, Ivan Marinov

Abstract

The present note shows that Mac Williams identities for the weight distribution of a pair $C, C^\perp \subset \mathbb{F}_q^n$ of mutually dual linear codes are equivalent to Polarized Riemann-Roch Conditions on their $\zeta$-functions $\zeta_C(t), \zeta_{C^\perp}(t)$. It provides some averaging and probabilistic interpretations of the coefficients of Duursma’s reduced polynomial of a linear code.

Let $C$ be an $\mathbb{F}_q$-linear $[n, k, d]$-code of genus $g := n + 1 - k - d$ with dual $C^\perp \subset \mathbb{F}_q^n$ of genus $g^\perp = k + 1 - d^\perp$. Throughout, denote by $W_C(x, y)$ the homogeneous weight enumerator of $C$ and put $M_{n,d}(x, y)$ for the MDS homogeneous weight enumerator of length $n$ and minimum distance $d$. In [1] and [2] Duursma introduces the $\zeta$-function of $C$ as the quotient

$$\zeta_C(t) = \frac{P_C(t)}{(1-t)(1/qt)}$$

of the unique polynomial $P_C(t) = \sum_{i=0}^{g+g^\perp} a_i t^i \in \mathbb{Q}[t]$ with

$$W_C(x, y) = \sum_{i=0}^{g+g^\perp} a_i M_{n,d+i}(x, y) \quad \text{and} \quad P_C(1) = 1.$$ 

The terminology arises from the algebro-geometric Goppa codes on a smooth irreducible curve $X/\mathbb{F}_q \subset \mathbb{P}^N(\mathbb{F}_q)$ of genus $g$, defined over a finite field $\mathbb{F}_q$. More precisely, suppose that there exist $\mathbb{F}_q$-rational points $P_1, \ldots, P_n \in X(\mathbb{F}_q)$ and a complete set of representatives $G_1, \ldots, G_h$ of the linear equivalence classes of the divisors of $\mathbb{F}_q(X)$ of degree $2g - 2 < m < n$ with $\text{Supp}(G_i) \cap \text{Supp}(D) = \emptyset$ for $D = P_1 + \ldots + P_n$ and $\forall 1 \leq i \leq h$. The evaluation maps

$$E_D : H^0(X, \mathcal{O}_X([G_i])) \to \mathbb{F}_q^n,$$

$$E_D(f) = (f(P_1), \ldots, f(P_n))$$

on the global sections $f \in H^0(X, \mathcal{O}_X([G_i]))$ of the line bundles, associated with $G_i$ are $\mathbb{F}_q$-linear. Their images $C_i = E_D H^0(X, \mathcal{O}_X([G_i]))$ are $\mathbb{F}_q$-linear codes of genus $g_i \leq g$.

* 2010 Mathematics Subject Classification: Primary: 94B27, 14G50; Secondary: 11T71.

Supported by Contract 57/12.04.2016 with the Scientific Foundation of Kliment Ohridski University of Sofia.
known as algebro-geometric Goppa codes. Duursma’s considerations from [1] imply that the $\zeta$-functions of $X$ and $C_i$ are related by the equality

$$\zeta_X(t) = \sum_{i=1}^{h} t^{g-g_i} \zeta_{C_i}(t).$$

Lemma 1 from the first section of the present note expresses the Riemann-Roch Theorem for $X$ in terms of $\zeta_X(t)$, in order to motivate Definition 2 for Riemann-Roch Conditions on a formal power series of one variable. Definition 3 is a polarized version of the Riemann-Roch Conditions. The main Theorem 4 establishes that Mac Williams identities for the weight distribution of $C_i C \subseteq \mathbb{P}_q^m$ are equivalent to the Polarized Riemann-Roch Conditions for $\zeta_C(t), \zeta_{C_i}(t)$. The proof of Theorem 4 is based on the properties of Duursma’s reduced polynomials $D_C(t), D_{C_i}(t)$, introduced and studied by the authors in [3].

Let $C$ be an $\mathbb{F}_q$-linear $[n, k, w]$-code of genus $g = n + 1 - k - w \geq 1$ with Duursma’s reduced polynomial $D_C(t)$. The second section provides sufficient conditions for the existence of a linear code $C_{\text{red}}$ with $\zeta$-polynomial $P_{C_{\text{red}}}(t) = \frac{D_C(t)}{D_C(1)}$. After observing that $C_{\text{red}}$ is of genus $g_{\text{red}} = g - 1$, we concentrate on three types of Duursma’s reductions $C_{\text{red}}$ of $C$. These are Duursma’s length, dimension and weight reductions $C_{\text{DLR}}, C_{\text{DDR}}, C_{\text{DWR}}$ of $C$, introduced by Definition 2. Propositions 2, 3, 4 provide sufficient conditions for the existence of $C_{\text{DLR}}$, respectively, $C_{\text{DDR}}, C_{\text{DWR}}$ and express the homogeneous weight enumerators of these linear codes by MDS homogeneous weight enumerators.

The final, third section is devoted to some averaging and probabilistic interpretations of the coefficients $c_i$ of Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+q^+ - 2} c_i t^i \in \mathbb{Q}[t]$ of a linear code $C$. After showing that $c_i(n_i) \in \mathbb{Z}^\geq 0$ are non-negative integers for all $0 \leq i \leq g + q^+ - 2$, Proposition 6 establishes that $c_i$ with $0 \leq i \leq g - 1$ is the average cardinality of an intersection of the projectivization $\mathbb{P}(C)$ of $C$ with $n - d - i$ coordinate hyperplanes in the ambient projective space $\mathbb{P}(\mathbb{F}_q^n) = \mathbb{P}^{n-1}(\mathbb{F}_q)$. Proposition 7 expresses $c_i$ by the probabilities $\pi_{\mathbb{P}(C)}^{(w)}$, respectively $\pi_{\mathbb{P}(C)}^{(w)}$ for a word $[w] \in \mathbb{P}^{n-1}(\mathbb{F}_q)$ of weight $w$ to belong to $\mathbb{P}(C)$, respectively, to $\mathbb{P}(C^\perp)$. The coefficients $c_i$ of $D_C(t)$ with $0 \leq i \leq g - 1$ are related also to the probabilities $\pi_{\mathbb{P}(C)}^{(d+i)}$ of a $(d + i)$-tuple $\{\beta_1, \ldots, \beta_{d+i}\} \subseteq \{1, \ldots, n\}$ to contain the support of a word $[a] \in \mathbb{P}(C)$ of weight $d \leq \text{wt}[a] \leq d + i$. In the case of $g \leq i \leq g + q^+ - 2 = n - d - d^+$, the coefficients $c_i$ are described by the probabilities $\pi_{\mathbb{P}(C^\perp)}^{(n-d-i)}$ of $\{\beta_1, \ldots, \beta_{n-d-1}\} \subseteq \{1, \ldots, n\}$ to contain the support of a word $[b] \in \mathbb{P}(C^\perp)$ of weight $d^+ \leq \text{wt}[b] \leq n - d - i$.

1 Mac Williams identities for linear codes are equivalent to Polarized Riemann-Roch Conditions

The following fact motivates the notion of Riemann-Roch Conditions for a formal power series of one variable.
Lemma 1. Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\mathbb{F}_q)$ be a smooth irreducible curve of genus $g$, defined over a finite field $\mathbb{F}_q$ and $\zeta_X(t) = \sum_{m=0}^{\infty} \mathcal{A}_m(X)t^m$ be the $\zeta$-function of $X$. Then the Riemann-Roch Theorem for $X$ implies the Riemann-Roch Conditions

$$\mathcal{A}_m(X) = q^{m-g+1} \mathcal{A}_{2g-2-m}(X) + (q^{m-g+1} - 1) \text{Res}_1(\zeta_X(t)) \quad \text{for} \quad \forall m \geq g,$$

where $\mathcal{A}_m(X)$ is the number of the effective divisors of degree $m$ of the function field $\mathbb{F}_q(X)$ and $\text{Res}_1(\zeta_X(t))$ is the residuum of $\zeta_X(t)$ at $t = 1$.

Proof. For an arbitrary divisor $G$ of the function field $\mathbb{F}_q(X)$, let $H^0(X, \mathcal{O}_X([G]))$ be the space of the global sections of the line bundle, associated with $G$ and $l(G) := \dim_{\mathbb{F}_q} H^0(X, \mathcal{O}_X([G]))$. Riemann-Roch Theorem asserts the existence of a canonical divisor $K_X$ of degree $\deg K_X = 2g - 2$ with

$$l(G) = l(K_X - G) + \deg G - g + 1 \quad (1)$$

for all divisors $G$ of $\mathbb{F}_q(X)$. In particular, if $\deg G > 2g - 2$ then $l(G) = \deg G - g + 1$.

For any $k \in \mathbb{N}$ let $X(\mathbb{F}_q^k)$ be the set of the $\mathbb{F}_q^k$-rational points on $X$. The formal power series

$$\zeta_X(t) := \exp \left( \sum_{k=1}^{\infty} \frac{X(\mathbb{F}_q^k)}{k} t^k \right)$$

is called the $\zeta$-function of $X$. It is well known that

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

for a polynomial $P_X(t) \in \mathbb{Z}[t]$ of $\deg P_X(t) = 2g$ and the residuum

$$\text{Res}_1(\zeta_X(t)) = \frac{P_X(1)}{q-1} = \frac{h}{q-1}$$

for the class number $h$ of $\mathbb{F}_q(X)$. If $G_1, \ldots, G_h$ is a complete set of representatives of the linear equivalence classes of the divisors of $\mathbb{F}_q(X)$ of degree $m \in \mathbb{Z} \geq 0$ then $K_X - G_1, \ldots, K_X - G_h$ is a complete set of representatives of the linear equivalence classes of the divisors of $\mathbb{F}_q(X)$ of degree $\deg(K_X - G_i) = 2g - 2 - m$. The effective divisors of $\mathbb{F}_q(X)$, which are linearly equivalent to $G_i$ form the projective space $\mathbb{P}(H^0(X, \mathcal{O}_X([G_i]))) = \mathbb{P}^{l(G_i)-1}(\mathbb{F}_q)$. Thus, the number of the effective divisors of $\mathbb{F}_q(X)$ of degree $m$ is

$$\mathcal{A}_m(X) = \sum_{i=1}^{h} \left| \mathbb{P}^{l(G_i)-1}(\mathbb{F}_q) \right| = \sum_{i=1}^{h} \frac{q^{l(G_i)} - 1}{q-1}. \quad (2)$$

Substituting (1) in (2), one obtains

$$\mathcal{A}_m(X) = q^{m-g+1} \sum_{i=1}^{h} \left( \frac{q^{l(K_X - G_i)} - 1}{q-1} \right) + h \left( \frac{q^{m-g+1} - 1}{q-1} \right).$$
Bearing in mind that

\[
\sum_{i=1}^{h} \left( \frac{q^i (K_X - G_i) - 1}{q - 1} \right) = A_{2g-2-m}(X),
\]

one concludes that

\[
A_m(X) = q^{m-g+1} A_{2g-2-m}(X) + h \left( \frac{q^{m-g+1} - 1}{q - 1} \right) \quad \text{for } \forall m \geq 0.
\]

Note that in the case of \( g \geq 2 \) the relations (3) for \( 0 \leq m \leq g - 2 \) are equivalent to the ones with \( g \leq m = 2g - 2 - i \leq 2g - 2 \), after multiplying by \( q^g - 1 \) and (3) is trivial for \( m = g - 1 \). If \( g = 0 \) then \( X = \mathbb{P}^1(\mathbb{F}_q) \) is the projective line and the equalities (3) reduce to \( A_m(X) = \frac{q^{m+1} - 1}{q - 1}, \forall m \geq 0 \). When \( g = 1 \), the curve \( X \) is elliptic and \( A_m(X) = h \left( \frac{q^m - 1}{q - 1} \right) \) for the class number \( h \) and all \( m \geq 0 \).

\[\square\]

**Definition 2.** A formal power series \( \zeta(t) = \sum_{m=0}^{\infty} A_m t^m \in \mathbb{C}[[t]] \) satisfies the Riemann-Roch Conditions RRC(\( g \)) of genus \( g \in \mathbb{Z}^{\geq 0} \) if

\[
A_m = q^{m-g+1} A_{2g-2-m} + \left( q^{m-g+1} - 1 \right) \text{Res}_1(\zeta(t)) \quad \text{for } \forall m \geq g,
\]

and the residuum \( \text{Res}_1(\zeta(t)) \) of \( \zeta(t) \) at \( t = 1 \).

Here is a polarized version of the Riemann-Roch Conditions.

**Definition 3.** Formal power series \( \zeta(t) = \sum_{m=0}^{\infty} A_m t^m \) and \( \zeta^\perp(t) = \sum_{m=0}^{\infty} A^\perp_m t^m \) satisfy the Polarized Riemann-Roch Conditions PRRC(\( g, g^\perp \)) for some \( g, g^\perp \in \mathbb{Z}^{\geq 0} \) if

\[
A_m = q^{m-g+1} A^\perp_{g+g^\perp-2-m} + \left( q^{m-g^\perp+1} - 1 \right) \text{Res}_1(\zeta(t)) \quad \text{for } \forall m \geq g^\perp,
\]

\[
A^\perp_m = q^{m-g^\perp+1} A^\perp_{g+g^\perp-2-m} + \left( q^{m-g^\perp+1} - 1 \right) \text{Res}_1(\zeta^\perp(t)) \quad \text{for } \forall m \geq g^\perp,
\]

where \( \text{Res}_1(\zeta(t)), \text{Res}_1(\zeta^\perp(t)) \) stand for the corresponding residuums at \( t = 1 \).

Note that PRRC(\( g, g^\perp \)) imply \( A_m = \kappa_1 q^m + \kappa_2, A^\perp_m = \kappa^\perp_1 q^m + \kappa^\perp_2 \) for all \( m \geq g+g^\perp-1 \) and some constants \( \kappa_1, \kappa^\perp_2 \in \mathbb{C} \). These are equivalent to the recurrence relations \( A_{m+2} - (q+1)A_{m+1} + qA_m = A^\perp_{m+2} - (q+1)A^\perp_{m+1} + qA^\perp_m = 0 \) for \( \forall m \geq g+g^\perp-1 \) and holds exactly when

\[
\zeta(t) = \frac{P(t)}{(1-t)(1-qt)} \quad \text{and} \quad \zeta^\perp(t) = \frac{P^\perp(t)}{(1-t)(1-qt)}
\]

for polynomials \( P(t), P^\perp(t) \).

The main result of the present note is the following
Theorem 4. Mac Williams identities for an $F_q$-linear $[n,k,d]$-code $C$ of genus $g := n+1-k-d \geq 0$ and its dual $C^\perp \subset F_q^n$ of genus $g^\perp = k+1-d^\perp \geq 0$ are equivalent to the Polarized Riemann-Roch Conditions PRRC$(g, g^\perp)$ on their $\zeta$-functions $\zeta_C(t), \zeta_{C^\perp}(t)$.

Proof. In [1], [2] Duursma observes that Mac Williams identities for an $F_q$-linear $[n,k,d]$-code $C$ of genus $g := n+1-k-d \geq 0$ and its dual $C^\perp \subset F_q^n$ of genus $g^\perp = k+1-d^\perp \geq 0$ are equivalent to the functional equation

$$P_{C^\perp}(t) = P_C \left( \frac{1}{qt} \right) q^g t^{g+g^\perp}. \quad (4)$$

The previous work [3] of the authors introduces Duursma’s reduced polynomial

$$D_C(t) := \frac{P_C(t) - t^g}{(1-t)(1-qt)} = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$$

of $\deg D_C(t) = g + g^\perp - 2$ for all pairs $C, C^\perp \subset F_q^n$ of mutually dual $F_q$-linear codes but the MDS ones.

First, we prove the theorem for $g, g^\perp \in \mathbb{N}$. A straightforward verification establishes that (4) reads as

$$D_{C^\perp}(t) = D_C \left( \frac{1}{qt} \right) q^{g-1} t^{g+g^\perp-2} \quad (5)$$

in terms of $D_C(t)$ and $D_{C^\perp}(t) = \frac{P_C(t)}{(1-t)(1-qt)} \in \mathbb{Q}[t]$. If Duursma’s $\zeta$-function $\zeta_C(t) := \sum_{m=0}^\infty A_m(C) t^m$ then

$$D_C(t) = \sum_{m=0}^\infty A_m(C) t^m - \sum_{m=g}^\infty \left( \frac{q^{m-g+1} - 1}{q-1} \right) t^m \quad (6)$$

by

$$\frac{t^g}{(1-t)(1-qt)} = t^g \left( \sum_{i=0}^\infty t^i \right) \left( \sum_{j=0}^\infty q^j t^j \right) = \sum_{m=g}^\infty (q^{m-g} + q^{m-g-1} + \ldots + q + 1) t^m = \sum_{m=g}^\infty \left( \frac{q^{m-g+1} - 1}{q-1} \right) t^m \in \mathbb{Z}[t].$$

Thus,

$$D_C(t) = \sum_{m=0}^{g-2} A_m(C) t^m + A_{g-1}(C) t^{g-1} + \sum_{i=g}^{g+g^\perp-2} c_i t^i = \sum_{m=0}^{g-2} A_m(C) t^m + A_{g-1}(C) t^{g-1} + \left( \sum_{m=0}^{g+g^\perp-2-m} c_{g+g^\perp-2-m} t^{-m} \right) t^{g+g^\perp-2} \quad (7)$$

$$= \sum_{m=0}^{g-2} A_m(C) t^m + A_{g-1}(C) t^{g-1} + \left( \sum_{m=0}^{g+g^\perp-2-m} c_{g+g^\perp-2-m} t^{-m} \right) t^{g+g^\perp-2}$$
and, respectively,
\[
D_{C^\perp}(t) = \sum_{m=0}^{g^\perp-2} A_m(C^\perp) t^m + A_{g^\perp-1}(C^\perp) t^{g^\perp-1} + \left( \sum_{m=0}^{g-2} c_{g^\perp-2-m} t^{-m} \right) t^{g + g^\perp - 2}
\]
for \( \zeta_{C^\perp}(t) := \frac{P_{C^\perp}(t)}{(1-t)(1-qt)} = \sum_{m=0}^{\infty} A_m(C^\perp) t^m \). According to (6),
\[
D_C \left( \frac{1}{qt} \right) q^{g-1} t^{g + g^\perp - 2} = \sum_{m=0}^{g-2} A_m(C) q^{g-1-m} t^{g + g^\perp - 2-m} + A_{g-1}(C) t^{g^\perp - 1} + \sum_{m=0}^{g^\perp-2} c_{g^\perp-2-m} q^{m-g^\perp+1} t^m = \sum_{m=0}^{g^\perp-2} c_{g^\perp-2-m} q^{m-g^\perp+1} t^m + A_{g-1}(C) t^{g^\perp - 1} + \left( \sum_{m=0}^{g-2} q^{m-g^\perp+1} A_m(C) t^{-m} \right) t^{g + g^\perp - 2},
\]
Mac Williams identities (5) for Duursma’s reduced polynomials of a pair \( C, C^\perp \subset \mathbb{F}_q^n \) of mutually dual linear codes of genus \( g \geq 1 \), respectively, \( g^\perp \geq 1 \) amount to
\[
c_{g^\perp-2-m} = q^{-m+g^\perp-1} A_m(C^\perp) \quad \text{for} \quad \forall 0 \leq m \leq g^\perp - 2,
\]
\[
A_{g^\perp-1}(C^\perp) = A_{g-1}(C) \quad \text{and}
\]
\[
c_{g^\perp-2-m} = q^{-m+g-1} A_m(C) \quad \text{for} \quad \forall 0 \leq m \leq g - 2.
\]
Substituting \( m = g + g^\perp - 2 - i \) and making use of (6), one observes that (8) is equivalent to
\[
A_i(C) = q^{i-g+1} A_{g+g^\perp-2-i}(C^\perp) + \left( \frac{q^{i-g+1} - 1}{q - 1} \right) \quad \text{for} \quad \forall g \leq i \leq g + g^\perp - 2.
\]
Exchanging \( C \) with \( C^\perp \), one expresses (10) in the form
\[
A_i(C^\perp) = q^{i-g^\perp+1} A_{g+g^\perp-2-i}(C) + \left( \frac{q^{i-g^\perp+1} - 1}{q - 1} \right) \quad \text{for} \quad \forall g^\perp \leq i \leq g + g^\perp - 2.
\]
According to (6),
\[
A_i(C) = \frac{q^{i-g+1} - 1}{q - 1} \quad \text{for} \quad \forall i \geq g + g^\perp - 1.
\]
Similarly,
\[
A_i(C^\perp) = \frac{q^{i-g^\perp+1} - 1}{q - 1} \quad \text{for} \quad \forall i \geq g + g^\perp - 1.
\]
Bearing in mind that \( \zeta_C(t) \) and \( \zeta_{C^\perp}(t) \) have no pole at \( t = 0 \), one introduces \( A_{-j}(C) = A_{-j}(C^\perp) = 0 \) for \( \forall j \in \mathbb{N} \) and expresses Mac Williams identities in the form
\[
A_i(C) = q^{i-g+1} A_{g+g^\perp-2-i}(C^\perp) + \left( \frac{q^{i-g+1} - 1}{q - 1} \right) \quad \text{for} \quad \forall i \geq g,
\]
\[ A_{g^+ - 1}(C) = A_{g-1}(C) \quad \text{and} \]
\[ A_i(C) = q^{i-g^+ + 1} A_{g^+ + g^+ - i - 1}(C) + \left( \frac{q^{i-g^+ + 1} - 1}{q - 1} \right) \quad \text{for } \forall i \geq g^+. \]

Note also that the rational function
\[ \zeta_C(t) = \frac{P_C(t)}{(1-t)(1-qt)} \]
has residuum
\[ \text{Res}_1(\zeta_C(t)) = \frac{P_C(1)}{q-1} = \frac{1}{q - 1} \]
at 1. Thus, for \( g \geq 1 \) and \( g^+ \geq 1 \), Mac Williams identities (11), (12), (13) for \( C, C^\perp \subset \mathbb{F}_q^n \) are equivalent to the polarized Riemann-Roch conditions PRRC\((g, g^+)\).

In the case of \( g = 0 \) the linear code \( C \) is Maximum Distance Separable, as well as its dual \( C^\perp \). The \( \zeta \)-functions
\[ \zeta_C(t) = \zeta_{C^\perp}(t) = \frac{1}{(1-t)(1-qt)} = \zeta_{P^1(\mathbb{F}_q)}(t) \]
coincide with the \( \zeta \)-function of the projective line \( P^1(\mathbb{F}_q) \) and satisfy the Riemann-Roch Conditions RRC\((0)\) of genus \( g = 0 \), which are equivalent to the Polarized Riemann-Roch Conditions PRRC\((0, 0)\).

Corollary 5. The lower parts \( \varphi_C(t) = \sum_{i=0}^{g^+ - 2} c_i t^i, \varphi_{C^\perp}(t) = \sum_{i=0}^{g^+ - 2} c_i^\perp t^i \) of Duursma’s reduced polynomials \( D_C(t) = \sum_{i=0}^{g + g^+ - 2} c_i t^i, D_{C^\perp}(t) = \sum_{i=0}^{g + g^+ - 2} c_i^\perp t^i \) of mutually dual linear codes \( C, C^\perp \subset \mathbb{F}_q^n \) of genus \( g \geq 1 \), respectively, \( g^+ \geq 1 \) and the number \( c_{g-1} = c_{g^+ - 1} \in \mathbb{Q} \) determine uniquely
\[ D_C(t) = \varphi_C(t) + c_{g-1} t^{g-1} + \varphi_{C^\perp} \left( \frac{1}{qt} \right) q^{g^+ - 1} t^{g^+ - 2}, \]
\[ D_{C^\perp}(t) = \varphi_{C^\perp}(t) + c_{g-1} t^{g^+ - 1} + \varphi_C \left( \frac{1}{qt} \right) q^{g^+ - 1} t^{g^+ - 2}. \]

Proof. The substitution of (8) in (7) yields
\[ D_C(t) = \varphi_C(t) + c_{g-1} t^{g-1} + \left( \sum_{m=0}^{g^+ - 2} c_m q^{-m} t^{-m} \right) q^{g^+ - 1} t^{g^+ - 2}, \]
whereas (14). Replacing \( C \) by \( C^\perp \), \( C^\perp \) by \( C \) and \( c_{g^+ - 1} \) by \( c_{g-1} \), one obtains (15).
2 Averaging and probabilistic interpretations of the coefficients of Duursma’s reduced polynomial

Let $C \subset \mathbb{F}_q^n$ be a linear code with Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+g^⊥-2} c_i t^i$ and $\mathbb{P}(C) \subset \mathbb{P}(\mathbb{F}_q^n) = \mathbb{P}^{n-1}(\mathbb{F}_q)$ the projectivization of $C$, viewed as a subspace of the projectivization of the ambient space $\mathbb{F}_q^n$. Note that the weight function
\[
\text{wt} : \mathbb{F}_q^n \rightarrow \{0, 1, \ldots, n\},
\]
\[
\text{wt}(a) = |\{1 \leq i \leq n \mid a_i \neq 0\}| \text{ for } \forall a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n
\]
descends to an weight function
\[
\text{wt} : \mathbb{P}(\mathbb{F}_q^n) \rightarrow \{0, 1, \ldots, n\},
\]
\[
\text{wt}([a]) = \text{wt}([a_1 : \ldots : a_n]) = |\{1 \leq i \leq n \mid a_i \neq 0\}|
\]
and define as usual the support of $[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q)$ as $\text{Supp}([a]) := \{1 \leq i \leq n \mid a_i \neq 0\}$. Denote by
\[
\mathbb{P}^{n-1}(\mathbb{F}_q)^{(s)} := \{[a] \in \mathbb{P}^{n-1}(\mathbb{F}_q) \mid \text{wt}([a]) = s\}
\]
the set of the words of $\mathbb{P}^{n-1}(\mathbb{F}_q)$ of weight $s$ and put
\[
\mathbb{P}(C)^{(s)} := \{[a] \in \mathbb{P}(C) \mid \text{wt}([a]) = s\} = \mathbb{P}^{n-1}(\mathbb{F}_q)^{(s)} \cap \mathbb{P}(C).
\]

Recall that a linear code $C \subset \mathbb{F}_q^n$ is non-degenerate if it is not contained in a coordinate hyperplane $V(x_i) = \{a \in \mathbb{F}_q^n \mid a_i = 0\}$ for some $1 \leq i \leq n$.

**Proposition 6.** Let $C$ be a non-degenerate $\mathbb{F}_q$-linear $[n, k, d]$-code of genus $g \geq 1$ with dual $C^⊥ \subset \mathbb{F}_q^n$ of minimum distance $d^⊥$ and genus $g^⊥ \geq 1$. If $D_C(t) = \sum_{i=0}^{g+g^⊥-2} c_i t^i \in \mathbb{Q}[t]$ is Duursma’s reduced polynomial of $C$ and
\[
\mathbb{P}(C)^{(\leq \beta)} := \{[a] \in \mathbb{P}(C) \mid \text{Supp}([a]) \subseteq \beta\}
\]
is the set of the words of $\mathbb{P}(C)$, whose support is contained in some $\beta \in \mathcal{Q}_{d+i}^{n}$ then:
\[i\]
\[
c_i \left( d+i \atop n \right) \in \mathbb{Z}^\geq \text{ for } \forall 0 \leq i \leq g + g^⊥ - 2;
\]
\[ii\]
\[
c_i = \left( d+i \atop n \right)^{-1} \left( \sum_{\beta \in \mathcal{Q}_{d+i}^{n}} \left| \mathbb{P}(C)^{(\leq \beta)} \right| \right) \text{ for } \forall 0 \leq i \leq g - 1
\]
is the average cardinality of an intersection of $\mathbb{P}(C)$ with $n - d - i$ coordinate hyperplanes, whenever $C$ is non-degenerate.
Proof. (i) For any \( d \leq w \leq n \) let \( W_C^{(w)} \) be the number of the words \( a \in C \) of weight \( wt(a) \). Formula (11) from Proposition 3 of [3] asserts that

\[
\begin{align*}
\frac{c_i}{d+i} = & \sum_{w=d}^{d+i} \left( \frac{n-w}{n-d-i} \right) \frac{W_C^{(w)}}{q-1} \quad \text{for} \quad \forall 0 \leq i \leq g-1.
\end{align*}
\]

(16)

Note that \( \frac{W_C^{(w)}}{q-1} = |\mathbb{P}(C)^{(w)}| \in \mathbb{Z}^\geq 0 \) is the number of the words of \( \mathbb{P}(C) \) of weight \( w \), in order to observe that \( c_i \left( \frac{n}{d+i} \right) \in \mathbb{Z}^\geq 0 \) are non-negative integers for \( \forall 0 \leq i \leq g-1 \). By (14) from Corollary 5, one has

\[
\sum_{i=g}^{g+g^+ - 2} c_i t^i = \sum_{j=0}^{g^+ - 2} c_j t^{g^+ - 1 - j} g^+ g^+ - 2 - j,
\]

whereas

\[
c_i = q^{-g+1} c_{g+g^+ - 2 - i} \quad \text{for} \quad \forall g \leq i \leq g + g^+ - 2.
\]

(17)

The application of (16) to the dual code \( C^\perp \) provides

\[
c_{g+g^+ - 2 - i} \left( \frac{n}{d+i} + g + g^+ - 2 - i \right) = c_{g+g^+ - 2 - i} \left( \frac{n}{n-d-i} \right) = c_{g+g^+ - 2 - i} \left( \frac{n}{d+i} \right) \in \mathbb{Z}^\geq 0
\]

for \( \forall g \leq i \leq g + g^+ - 2 \). Combining with (17), one concludes that

\[
c_i \left( \frac{n}{d+i} \right) = q^{-g+1} c_{g+g^+ - 2 - i} \left( \frac{n}{d+i} \right) \in \mathbb{Z}^\geq 0 \quad \text{for} \quad \forall g \leq i \leq g + g^+ - 2.
\]

(ii) Any projective \( [n,k,d] \)-system \( \mathcal{P} = \{P_1, \ldots, P_n\} \subset \mathbb{P}^{k-1}(\mathbb{F}_q) = \mathbb{P}(C^*) \), corresponding to a non-degenerate \( \mathbb{F}_q \)-linear code \( C \) is a subset of the projectivization of the space \( C^* = \text{Hom}_{\mathbb{F}_q}(C, \mathbb{F}_q) \) of the linear functionals on \( C \). More precisely, each point \( P_j \) lifts to the restriction \( \overline{P}_j = x_j|_C \subset C^* \) of the coordinate functional \( x_j : \mathbb{F}_q^n \to \mathbb{F}_q \). The hyperplane \( H_j \subset C \), associated with \( P_j \) can be identified with \( C \cap Z(x_j) \), where \( Z(x_j) = \{ x \in \mathbb{P}^n_q | x_j = 0 \} \). For any \( \alpha = \{\alpha_1, \ldots, \alpha_i\} \in \binom{1, \ldots, n}{i} \) with complement \( -\alpha = \{1, \ldots, n\} \setminus \alpha \), note that

\[
C \cap \left( \cap_{i=1}^i Z(x_{\alpha_i}) \right) = \{ a \in C | \text{Supp}(a) \subseteq -\alpha \} = C^{(\mathbb{Z} - \alpha)}
\]

consists of the words of \( C \), whose support is contained in \( -\alpha \). After denoting \( l(\alpha) := \dim_{\mathbb{F}_q}(C \cap \left( \cap_{i=1}^i Z(x_{\alpha_i}) \right)) \), one observes that \( \mathbb{P}(C)^{(<\mathbb{Z} - \alpha)} \) is of cardinality

\[
\left| \mathbb{P}(C)^{(<\mathbb{Z} - \alpha)} \right| = \frac{q^{l(\alpha)} - 1}{q - 1}.
\]

By Theorem 1.1.28 from [4], the homogeneous weight enumerator of \( C \) can be expressed in the form

\[
W_C(x, y) = x^n + \sum_{i=0}^{n-d} B_i (x - y)^i y^{n-i},
\]

(18)
where
\[ B_i = (q - 1) \sum_{\alpha \in \Sigma_i(1, \ldots, n)} \left| \mathbb{P}(C)(\leq -\alpha) \right| \]
by Exercise 1.1.29 from [4]. On the other hand, Proposition 3 from [3] establishes that
\[ W_C(x, y) = M_{n, n+1-k}(x, y) + \sum_{i=0}^{g+g^2-2} (q - 1)c_i \left( \begin{array}{c} n \\ d+i \end{array} \right)(x-y)^{n-d-i}y^{d+i}, \quad (19) \]
where \( M_{n, n+1-k}(x, y) \) stands for the MDS homogeneous weight enumerator of length \( n \) and minimum distance \( n + 1 - k \). The application of Theorem 1.1.28 from [4] to \( M_{n, n+1-k}(x, y) \) provides
\[ M_{n, n+1-k}(x, y) = x^n + \sum_{i=0}^{k-1} \left( \begin{array}{c} n \\ i \end{array} \right)(q^{k-i} - 1)(x-y)^iy^{n-i}. \]
Combining (18) and (19) with the above expression, one obtains
\[ \sum_{i=0}^{k-1} \left( \begin{array}{c} n \\ i \end{array} \right)(q^{k-i} - 1)(x-y)^iy^{n-i} + \sum_{i=0}^{g+g^2-2} (q - 1)c_i \left( \begin{array}{c} n \\ d+i \end{array} \right)(x-y)^{n-d-i}y^{d+i} = \sum_{i=0}^{n-d} B_i(x-y)^iy^{n-i}. \]
Let us introduce \( z := x - y \) and compare the coefficients of \( z^iy^{n-i} \) for \( k \leq i \leq n - d \), in order to conclude that
\[ (q - 1)c_{n-d-i} \left( \begin{array}{c} n \\ n-i \end{array} \right) = B_i \quad \text{for} \quad k \leq i \leq n - d. \]
In other words,
\[ c_j = \left( \begin{array}{c} n \\ d+j \end{array} \right)^{-1} (q - 1)^{-1}B_{n-d-j} = \left( \begin{array}{c} n \\ d+j \end{array} \right)^{-1} \sum_{\alpha \in \Sigma_{n-d-j}(1, \ldots, n)} \left| \mathbb{P}(C)(\leq -\alpha) \right| \]
for \( \forall 0 \leq j \leq g - 1 \). Bearing in mind that \( \beta = -\alpha \) runs over \( \left( \begin{array}{c} 1, \ldots, n \\ d+j \end{array} \right) \) while \( \alpha \) varies on \( \left( \begin{array}{c} 1, \ldots, n \\ n-d-i \end{array} \right) \), one concludes that
\[ c_j = \left( \begin{array}{c} n \\ d+j \end{array} \right)^{-1} \sum_{\beta \in \left( \begin{array}{c} 1, \ldots, n \\ d+j \end{array} \right)} \left| \mathbb{P}(C)(\leq \beta) \right| \quad \text{for} \quad \forall 0 \leq j \leq g - 1. \]

**Proposition 7.** Let \( C \) be an \( \mathbb{F}_q \)-linear \([n, k, d]_q\)-code of genus \( g \geq 1 \), whose dual \( C^\perp \) is an \([n, n-k, d^\perp]_q\)-code of genus \( g^\perp \geq 1 \) and \( D_C(t) = \sum_{i=0}^{g+g^2-2} c_it^i \in \mathbb{Q}[t] \) be Duursma’s reduced

\[ \text{Duursma’s reduced weight enumerator} \]
polynomial of $C$. For any $1 \leq w \leq n$ denote by $\pi_{P(C)}^{(w)}$ the probability of $[b] \in \mathbb{F}^{n-1}(\mathbb{F}_q)$ to belong to $\mathbb{P}(C)^{(w)}$ and put $\pi_a^{(w)}$ for the probability of $\beta \in \binom{1,...,n}{w}$ to contain $\text{Supp}(a)$ for some $[a] \in \mathbb{P}(C)$. Then:

(i) $c_i = \sum_{w=d}^{d+i} \pi_{P(C)}^{(w)} \binom{d+i}{w} (q-1)^{w-1}$ for $0 \leq i \leq g-1$, \hspace{1cm} (20)

$$c_i = q^{i-g+1} \left[ \sum_{w=d^\perp}^{n-d^\perp-i} \pi_{P(C)}^{(w)} \binom{n-d-i}{w} (q-1)^{w-1} \right] \text{ for } \forall g \leq i \leq g^{\perp} - 2; \hspace{1cm} (21)$$

(ii) $c_i = \sum_{[a] \in \mathbb{P}(C)^{\perp}} \pi_{a}^{(d+i)}$ for $0 \leq i \leq g-1$, \hspace{1cm} (22)

$$c_i = q^{i-g+1} \left( \sum_{[b] \in \mathbb{P}(C)^{\perp}} \pi_{[b]}^{n-d-i} \right) \text{ for } \forall g \leq i \leq g^{\perp} - 2 = n - d - d^\perp. \hspace{1cm} (23)$$

**Proof.** (i) If $C^{(w)} := \{a \in C \mid \text{wt}(a) = w\}$ is the set of the words of $C$ of weight $w$ then $\mathbb{P}(C)^{(w)} = C^{(w)}/\mathbb{F}_q^*$, whereas

$$|\mathbb{P}(C)^{(w)}| = \frac{|C^{(w)}|}{|\mathbb{F}_q^*|} = \frac{\mathcal{W}_C^{(w)}}{q-1} \text{ for } \forall 1 \leq w \leq n.$$

Bearing in mind that

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)^{(w)}| = \binom{n}{w} \frac{|\mathbb{F}_q^*|^w}{|\mathbb{F}_q^*|} = \binom{n}{w} (q-1)^{w-1},$$

one concludes that

$$\pi_{P(C)}^{(w)} = \frac{\mathcal{W}_C^{(w)}}{\binom{n}{w} (q-1)^{w-1}} \text{ for } \forall 1 \leq w \leq n.$$

The substitution of the above expression in (16) yields

$$c_i = \sum_{w=d}^{d+i} \binom{n}{d+i}^{-1} \binom{n}{w} \binom{n-w}{n-d-i} \pi_{P(C)}^{(w)} (q-1)^{w-1} \text{ for } 0 \leq i \leq g-1.$$

Combining with

$$\binom{n}{d+i}^{-1} \binom{n}{w} \binom{n-w}{n-d-i} = \binom{d+i}{w} \text{ for } \forall d \leq w \leq d+i,$$

one proves (20) for an arbitrary $\mathbb{F}_q$-linear $[n,k,d]$-code $C$. Applying this equality to the dual code $C^\perp$ of $C$, one concludes that

$$c_i^\perp = \sum_{w=d^\perp}^{d^\perp+i} \pi_{P(C)}^{(w)} \binom{d^\perp+i}{w} (q-1)^{w-1} \text{ for } \forall 0 \leq i \leq g^\perp - 1.$$
Plugging this in (17) and using that
\[ d^\perp + g + g^\perp - 2 - i = n - d - i, \tag{24} \]
one derives (21).

(ii) For arbitrary \([a] \in \mathbb{P}(C)\) and \(1 \leq w \leq n\), the probability of \(\beta \in \binom{1, \ldots, n}{w}\) to contain \(\text{Supp([a])} \in \binom{1, \ldots, n}{s}\) is
\[
\pi_{[a]}^{(w)} = \begin{cases} \binom{n-s}{w-s} & \text{if } s = \text{wt([a])} \leq w, \\ 0 & \text{if } s = \text{wt([a])} > w. \end{cases}
\]
That allows to represents (16) in the form
\[
c_i = \sum_{w=d}^{d+i} \binom{n-w}{d+i-w} \left| \mathbb{P}(C)^{(w)} \right| = \sum_{w=d}^{d+i} \sum_{[a] \in \mathbb{P}(C)^{(w)}} \binom{n-w}{d+i-w} = \sum_{w=d}^{d+i} \sum_{[a] \in \mathbb{P}(C)^{(w)}} \pi_{[a]}^{(d+i)} = \sum_{[a] \in \mathbb{P}(C)} \pi_{[a]}^{(d+i)}
\]
for \(0 \leq i \leq g - 1\). Similarly,
\[
c_j^\perp = \sum_{[b] \in \mathbb{P}(C^\perp)} \pi_{[b]}^{(d+j)} \quad \text{for } 0 \leq j \leq g^\perp - 1,
\]
combined with (17), (24) provides
\[
c_i = q^{i-g+1} \left( \sum_{[b] \in \mathbb{P}(C^\perp)} \pi_{[b]}^{(n-d-i)} \right) \quad \text{for } 0 \leq i \leq g + g^\perp - 2.
\]

\[\square\]

References

[1] I. Duursma, Weight distribution of geometric Goppa codes, Transactions of the American Mathematical Society, 351 (1999), 3609–3639.

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

[3] A. Kasparian, I. Marinov, Duursma’s reduced polynomial, arXiv:1505.01993v1[cs.IT] 8 May 2015

[4] M. Tsfasman, S. Vlăduţ, D. Nogin, Algebraic Geometry Codes: Basic Notions, Providence, RI: American Mathematical Society, 2007.