Mac Williams identities for linear codes as Riemann-Roch conditions

Azniv Kasparian, 1,2 Ivan Marinov 1,3

Faculty of Mathematics and Informatics
Sofia University "St. Kliment Ohridski"
5 James Bourchier Blvd., 1164 Sofia, Bulgaria

Abstract
The present note establishes the equivalence of Mac Williams identities for linear codes $C, C^\perp \subset \mathbb{F}_q^n$ with the Polarized Riemann-Roch Conditions for their $\zeta$-functions. It provides some averaging and probabilistic interpretations of the coefficients of Duursma’s reduced polynomial of $C$.

Keywords: Mac Williams identities, Duursma’s reduced polynomial, Polarized Riemann-Roch Conditions.

1 Introduction
Let $C$ be an $\mathbb{F}_q$-linear $[n, k, d]$-code of genus $g := n + 1 - k - d \geq 0$ with dual $C^\perp \subset \mathbb{F}_q^n$ of genus $g^\perp = k + 1 - d^\perp \geq 0$. Throughout, denote by $W_C(x, y)$ the homogeneous weight enumerator of $C$ and put $M_{n,s}(x, y)$ for the MDS homogeneous weight enumerator of length $n$ and minimum distance $s$. In [1] and [2] Duursma introduces the $\zeta$-function of $C$ as the quotient

---

1 Partially supported by the Science Foundation of Sofia University, Contract 57/2016.
2 Email: kasparia@fmi.uni-sofia.bg
3 Email: ivan.boychev.marinov@gmail.com
\[ \zeta_C(t) = \frac{P_C(t)}{(1-t)(1-qt)} \] of the unique polynomial \[ P_C(t) = \sum_{i=0}^{g+g^+} a_i t^i \in \mathbb{Q}[t] \]

\[ \mathcal{W}_C(x, y) = \sum_{i=0}^{g+g^+} a_i \mathcal{M}_{n,d+i}(x, y) \] and \[ P_C(1) = 1. \] The terminology arises from the algebrao-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 different \( \mathbb{F}_q \)-rational points \( P_1, \ldots, P_n \in X(\mathbb{F}_q) := X \cap \mathbb{P}^N(\mathbb{F}_q) \) 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

\[ \mathcal{E}_D : H^0(X, \mathcal{O}_X([G_i])) \longrightarrow \mathbb{F}_q^n, \quad \mathcal{E}_D(f) = (f(P_1), \ldots, f(P_n)) \]

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 \( C_i = \mathcal{E}_D H^0(X, \mathcal{O}_X([G_i])) \) are linear codes of genus \( g_i \leq g \), known as algebrao-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 2.1 from the first section of the present note expresses the Riemann-Roch Theorem on a curve \( X \) in terms of \( \zeta_X(t) \), in order to motivate Definition 2.2 for Riemann-Roch Conditions on a formal power series of one variable. Definition 2.3 is a polarized form of the Riemann-Roch Conditions. The main Theorem 2.4 establishes that Mac Williams identities for the weight distribution of \( C, C^\perp \subset \mathbb{F}_q^n \) are equivalent to the Polarized Riemann-Roch Conditions for \( \zeta_C(t), \zeta_{C^\perp}(t) \). Thus, Mac Williams duality can be viewed as a polarized version of the Serre duality on a smooth irreducible projective curve. The proof of Theorem 2.4 is based on the properties of Duursma’s reduced polynomials \( D_C(t), D_{C^\perp}(t) \), introduced and studied in [3].

The second section is devoted to some averaging and probabilistic interpretations of the coefficients \( c_i \) of Duursma’s reduced polynomial \( D_C(t) = \sum_{i=0}^{g+g^+} c_i t^i \) of a linear code \( C \). After showing that \( c_i \left( \begin{array}{c} n \\ d+i \end{array} \right) \in \mathbb{Z}^\geq0 \) for all \( 0 \leq i \leq g + g^+ - 2 \), Proposition 3.1 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 3.2 expresses \( c_i \) by the probabilities \( \pi_{\mathbb{P}(C)}^{(w)} \), respectively \( \pi_{\mathbb{P}(C)}^{(w)} \) of a word \([b] \in \mathbb{P}^{n-1}(\mathbb{F}_q) \) of weight \( w \) to belong to \( \mathbb{P}(C) \), re-
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 $\frac{1}{\pi[a]}^{d+i}$ of a $(d+i)$-tuple $\{\beta_1, \ldots, \beta_{d+i}\} \subseteq \{1, \ldots, n\}$ to contain the support of a word $[a] \in \mathbb{P}(C)$. In the case of $g \leq i \leq g+q^1 - 2 = n - d - d^1$, the coefficients $c_i$ are described by the probabilities $\frac{1}{\pi[b]}^{n-d-i}$ of $\{\beta_1, \ldots, \beta_{n-d-i}\} \subseteq \{1, \ldots, n\}$ to contain the support of a word $[b] \in \mathbb{P}(C^\perp)$.

2 Mac Williams identities for linear codes as Polarized Riemann-Roch Conditions on their $\zeta$-functions

**Lemma 2.1** 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 $\zeta_X(t) = \sum_{m=0}^{\infty} A_m(X) t^m$ be the $\zeta$-function of $X$. Then the Riemann-Roch Theorem on $X$ implies the Riemann-Roch Conditions

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

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

The above lemma motivates the following

**Definition 2.2** A formal power series $\zeta(t) = \sum_{m=0}^{\infty} A_m t^m \in \mathbb{C}[[t]]$ satisfies the Riemann-Roch Conditions RRC$_q(g)$ of base $q \in \mathbb{N}$ and genus $g \in \mathbb{Z}_{\geq 0}$ if

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

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 2.3** Formal power series $\zeta(t) = \sum_{m=0}^{\infty} A_m t^m$, $\zeta^\perp(t) = \sum_{m=0}^{\infty} A^\perp_m t^m$ satisfy the Polarized Riemann-Roch Conditions PRRC$_q(g, g^\perp)$ of base $q \in \mathbb{N}$ and genera $g, g^\perp \in \mathbb{Z}_{\geq 0}$ if

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

$$A_{g-1} = A_{g^\perp-1} \quad \text{and}$$

$$A^\perp_m = q^{m-g+1} A_{g+g^\perp-2-m} + (q^{m-g+1} - 1)\text{Res}_1(\zeta^\perp(t)) \quad \text{for } \forall m \geq g^\perp,$$

where $\text{Res}_1(\zeta(t))$, $\text{Res}_1(\zeta^\perp(t))$ stand for the corresponding residuums at $t=1$. 
Note that PRRC\(_q\)(\(g, g^\perp\)) imply \(A_m = \kappa_1 q^m + \kappa_2, A_m^\perp = \kappa_1^\perp q^m + \kappa_2^\perp\) for all \(m \geq g + g^\perp - 1\) and some \(\kappa_j, \kappa_j^\perp \in \mathbb{C}\). These are equivalent to the recurrence relations \(A_{m+2} - (q+1)A_{m+1} + qA_m = A_{m+2}^\perp - (q+1)A_{m+1}^\perp + qA_m^\perp = 0\) for all \(m \geq g + g^\perp - 1\) and some \(\kappa_j, \kappa_j^\perp \in \mathbb{C}\).

The main result of the present note is the following

**Theorem 2.4** Mac Williams identities for an \(\mathbb{F}_q\)-linear \([n, k, d]\)-code \(C\) of genus \(g := n + 1 - k - d \geq 0\) and its dual \(C^\perp \subset \mathbb{F}_q^n\) of genus \(g^\perp = k + 1 - d^\perp \geq 0\) are equivalent to the Polarized Riemann-Roch Conditions PRRC\(_q\)(\(g, g^\perp\)) on their \(\zeta\)-functions \(\zeta_C(t), \zeta_{C^\perp}(t)\).

The proof of Theorem 2.4 makes use of Duursma’s reduced polynomial

\[
D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]
\]

of \(C\) with the homogeneous weight enumerator \(\mathcal{M}_{n,n+1-k}(x, y)\) of an MDS-code of the same length \(n\) and dimension \(k\) as \(C\) (cf.\([3]\)). It reveals that Randriambololona’s Riemann-Roch Theorem 44 for linear codes from \([4]\) implies the Polarized Riemann-Roch Conditions PRRC\(_q\)(\(g, g^\perp\)), stated by Definition 2.3.

As a byproduct, we obtain the following

**Corollary 2.5** The lower parts \(\varphi_C(t) = \sum_{i=0}^{g-2} c_i t^i, \varphi_{C^\perp}(t) = \sum_{i=0}^{g^\perp-2} c_i^\perp t^i\) of Duursma’s reduced polynomials \(D_C(t), D_{C^\perp}(t)\) of \(C, C^\perp \subset \mathbb{F}_q^n\) with genera \(g \geq 1,\) respectively, \(g^\perp \geq 1\) and the number \(c_{g-1} = c_{g^\perp-1}^\perp \in \mathbb{Q}\) determine uniquely

\[
D_C(t) = \varphi_C(t) + c_{g-1} t^{g-1} + \varphi_{C^\perp} \left( \frac{1}{ql} \right) q^{g^\perp-1} t^{g^\perp-2},
\]

\[
D_{C^\perp}(t) = \varphi_{C^\perp}(t) + c_{g-1} t^{g^\perp-1} + \varphi_C \left( \frac{1}{ql} \right) q^{g-1} t^{g^\perp-2}.
\]
3 Averaging and probabilistic interpretations of the coefficients of Duursma’s reduced polynomial

Let \( C \subseteq \mathbb{F}_q^n \) be a linear code with Duursma’s reduced polynomial \( D_C(t) = \sum_{i=0}^{g+q^g-2} c_i t^i \) and \( \mathbb{P}(C) \subseteq \mathbb{P}(\mathbb{F}_q^n) = \mathbb{P}^{n-1}(\mathbb{F}_q) \) be the projectivization of \( C \), viewed as a subspace of the projectivization \( \mathbb{P}(\mathbb{F}_q^n) = \mathbb{P}^{n-1}(\mathbb{F}_q) \) of the ambient space \( \mathbb{F}_q^n \). Note that the weight \( wt : \mathbb{F}_q^n \to \{0, 1, \ldots, n\}, \{\{1 \leq i \leq n \mid a_i \neq 0\}\mid \forall \) for all words \( a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n \) descends to a weight function \( wt : \mathbb{P}(\mathbb{F}_q^n) \to \{0, 1, \ldots, n\}, \{\{1 \leq i \leq n \mid a_i \neq 0\}\mid \forall \) where \( \mathbb{P}(\mathbb{F}_q^n) \to \{0, 1, \ldots, n\}, \{\{1 \leq i \leq n \mid a_i \neq 0\}\mid \forall \)

Let us denote by \( \mathbb{P}^{n-1}(\mathbb{F}_q)^{(\cdot)} := \{\{a\} \in \mathbb{P}^{n-1}(\mathbb{F}_q) \mid wt([a]) = s\} \) the set of the words of \( \mathbb{P}^{n-1}(\mathbb{F}_q) \) of weight \( 1 \leq s \leq n \) and put \( \mathbb{P}(C)^{(\cdot)} := \mathbb{P}^{n-1}(\mathbb{F}_q)^{(\cdot)} \cap \mathbb{P}(C) = \{\{a\} \in \mathbb{P}(C) \mid wt([a]) = s\} \). For an arbitrary \( 1 \leq s \leq n \), let \( \binom{n}{s} \) be the collection of the subsets \( \alpha = \{a_1, \ldots, a_s\} \subseteq [n] := \{1, \ldots, n\} \) of cardinality \( |\alpha| = s \).

Recall that a linear code \( C \subseteq \mathbb{F}_q^n \) 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 3.1** Let \( C \) be an \( \mathbb{F}_q \)-linear \([n, k, d]\)-code of genus \( g \geq 1 \) with dual \( C^\perp \subseteq \mathbb{F}_q^n \) of minimum distance \( d^\perp \) and genus \( g^\perp \geq 1 \). Denote by \( D_C(t) = \sum_{i=0}^{g+q^g-2} c_i t^i \in \mathbb{Q}[t] \) Duursma’s reduced polynomial of \( C \).

(i) Then \( c_i \binom{n}{d+i} \in \mathbb{Z}_{\geq 0} \) are non-negative integers for \( \forall 0 \leq i \leq g + g^\perp - 2 \).

(ii) If \( C \) is non-degenerate and \( \mathbb{P}(C)^{(\subseteq \beta)} := \{\{a\} \in \mathbb{P}(C) \mid Supp([a]) \subseteq \beta\} \) is the set of the words of \( \mathbb{P}(C) \), whose support is contained in some \( \beta \in \binom{[n]}{s} \) then

\[
c_i = \binom{n}{d+i}^{-1} \left( \sum_{\beta \in \binom{[n]}{s}} |\mathbb{P}(C)^{(\subseteq \beta)}| \right) \text{ for } 0 \leq i \leq g - 1
\]

is the average cardinality of an intersection of \( \mathbb{P}(C) \) with \( n - d - i \) coordinate hyperplanes.

By Theorem 1.1.28 and Exercise 1.1.29 from [5], the homogeneous weight enumerator of a non-degenerate \( \mathbb{F}_q \)-linear code \( C \subseteq \mathbb{F}_q^n \) can be expressed in the form \( W_C(x, y) = x^n + \sum_{i=0}^{n-d} B_i (x-y)^i y^{n-i} \) with \( B_i = (q-1) \left( \sum_{\alpha \in \binom{[n]}{i}} |\mathbb{P}(C)^{(\subseteq \alpha)}| \right) \).
Thus, our Proposition 3.1 (ii) reveals that Tsfasman-Vlădut-Nogin’s coefficients $B_{d+i} = \binom{n}{d+i}(q-1)c_i$ for $0 \leq i \leq g - 1$ and the coefficients $c_i$ of Duursma’s reduced polynomial $D_C(t)$.

**Proposition 3.2** Let $C$ be an $\mathbb{F}_q$-linear $[n, k, d]$-code of genus $g \geq 1$, whose dual $C^\perp$ is an $[n, n-k, d^\perp]$-code of genus $g^\perp \geq 1$ and $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$ be Duursma’s reduced polynomial of $C$. For any $1 \leq w \leq n$ denote by $\pi^{(w)}_{\mathbb{P}(C)}$ the probability of $[b] \in \mathbb{P}^{n-1}(\mathbb{F}_q)^{(w)}$ to belong to $\mathbb{P}(C)^{(w)}$ and put $\pi^{(w)}_{[a]}$ for the probability of $\beta \in \binom{[n]}{w}$ to contain the support $\text{Supp}([a])$ of some $[a] \in \mathbb{P}(C)$. Then:

(i) $\quad c_i = \sum_{w=d}^{d+i} \pi^{(w)}_{\mathbb{P}(C)} \binom{d+i}{w} (q-1)^{w-1}$ for $\forall 0 \leq i \leq g - 1$,

(ii) $\quad c_i = q^{g+1} \sum_{[a] \in \mathbb{P}(C)} \pi^{(d+i)}_{[a]}$ for $\forall 0 \leq i \leq g - 1$,

$\quad c_i = q^{g+1} \sum_{[b] \in \mathbb{P}(C^\perp)} \pi^{(n-d-i)}_{[b]}$ for $\forall g \leq i \leq g + g^\perp - 2 = n - d - d^\perp$.

**References**


