Mac Williams identities for linear codes as Riemann-Roch conditions
Azniv Kasparian, Ivan Marinov

1 Partially supported by Contract 57/12.04.2016 with the Scientific Foundation of Kliment Ohridski University of Sofia.
Let $C$ be an $\mathbb{F}_q$-linear $[n, k, d]$-code.

The genus of $C$ is the deviation $g := n + 1 - k - d$ from the equality in the Singleton bound $n + 1 - k - d \geq 0$.

Let us denote by $g^\perp = k + 1 - d^\perp$ the genus of the dual code $C^\perp = \left\{ a \in \mathbb{F}_q^n \mid \langle a, c \rangle = \sum_{i=1}^{n} a_i c_i = 0 \text{ for } \forall c \in C \right\}$.
Let $C$ be an $\mathbb{F}_q$-linear $[n, k, d]$-code.

The genus of $C$ is the deviation $g := n + 1 - k - d$ from the equality in the Singleton bound $n + 1 - k - d \geq 0$.

Let us denote by $g^\perp = k + 1 - d^\perp$ the genus of the dual code $C^\perp = \left\{ a \in \mathbb{F}_q^n \mid \langle a, c \rangle = \sum_{i=1}^n a_i c_i = 0 \text{ for } \forall c \in C \right\}$. 

Mac Williams and Riemann-Roch
If $\mathcal{W}_C^{(w)}$ is the number of the words $c \in C$ of weight $1 \leq w \leq n$ then $\mathcal{W}_C(x, y) = x^n + \sum_{w=d}^{n} \mathcal{W}_C^{(w)} x^{n-w} y^w$ is called the homogeneous weight enumerator of $C$.

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

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

the homogeneous weight enumerator of an MDS-code with parameters $[n, n + 1 - s, s]$. 

Mac Williams and Riemann-Roch
The homogeneous weight enumerator of a linear code

If \( W_C^{(w)} \) is the number of the words \( c \in C \) of weight \( 1 \leq w \leq n \) then \( W_C(x, y) = x^n + \sum_{w=d}^{n} W_C^{(w)} x^{n-w} y^w \) is called the homogeneous weight enumerator of \( C \).

Denote by \( M_{n,s}(x, y) = x^n + \sum_{w=s}^{n} M_{n,s}^{(w)} x^{n-w} y^w \) with
\[
M_{n,s}^{(w)} = \binom{n}{w} \sum_{i=0}^{w-s} (-1)^i \binom{w}{i} (q^{w+1-s-i} - 1)
\]
the homogeneous weight enumerator of an MDS-code with parameters \([n, n + 1 - s, s]\).
Theorem (Duursma - 1999): For any linear code $C$ of genus $g \geq 0$ with dual $C^\perp$ of genus $g^\perp \geq 0$ there is a unique $\zeta$-polynomial $P_C(t) = \sum_{i=0}^{g+g^\perp} a_i t^i \in \mathbb{Q}[t]$ with

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

The quotient $\zeta_C(t) = \frac{P_C(t)}{(1-t)(1-qt)}$ is the $\zeta$-function of $C$. 

Mac Williams and Riemann-Roch
Theorem (Duursma - 1999): For any linear code $C$ of genus $g \geq 0$ with dual $C^\perp$ of genus $g^\perp \geq 0$ there is a unique $\zeta$-polynomial $P_C(t) = \sum_{i=0}^{g+g^\perp} a_i t^i \in \mathbb{Q}[t]$ with

$$\mathcal{W}_C(x, y) = \sum_{i=0}^{g+g^\perp} a_i M_{n,d+i}(x, y)$$

and $P_C(1) = 1$.

The quotient $\zeta_C(t) = \frac{P_C(t)}{(1-t)(1-qt)}$ is the $\zeta$-function of $C$. 

Mac Williams and Riemann-Roch
Let $X / \mathbb{F}_q \subset \mathbb{P}^N(\bar{\mathbb{F}}_q)$ be a smooth irreducible curve of genus $g$, $P_1, \ldots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q)$, $D = P_1 + \ldots + P_n$ and $G_1, \ldots, G_h$ be a complete set of representatives 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 $\forall 1 \leq i \leq h$. 

Mac Williams and Riemann-Roch
Let \( X / \mathbb{F}_q \subset \mathbb{P}^N(\mathbb{F}_q) \) be a smooth irreducible curve of genus \( g \), \( P_1, \ldots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q) \), \( D = P_1 + \ldots + P_n \) and \( G_1, \ldots, G_h \) be a complete set of representatives 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 \( \forall 1 \leq i \leq h \).
Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ be a smooth irreducible curve of genus $g$, $P_1, \ldots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q)$, $D = P_1 + \ldots + P_n$ and $G_1, \ldots, G_h$ be a complete set of representatives 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 $\forall 1 \leq i \leq h$. 

Mac Williams and Riemann-Roch
Let $X/F_q \subset \mathbb{P}^N(F_q)$ be a smooth irreducible curve of genus $g$, $P_1, \ldots, P_n \in X(F_q) = X \cap \mathbb{P}^N(F_q)$, $D = P_1 + \ldots + P_n$ and $G_1, \ldots, G_h$ be a complete set of representatives of the linear equivalence classes of the divisors of $F_q(X)$ of degree $2g - 2 < m < n$ with $\text{Supp}(G_i) \cap \text{Supp}(D) = \emptyset$ for $\forall 1 \leq i \leq h$. 

Mac Williams and Riemann-Roch
Let $X/F_q \subset \mathbb{P}^N(\overline{F}_q)$ be a smooth irreducible curve of genus $g$, $P_1, \ldots, P_n \in X(F_q) = X \cap \mathbb{P}^N(F_q)$, $D = P_1 + \ldots + P_n$ and $G_1, \ldots, G_h$ be a complete set of representatives of the linear equivalence classes of the divisors of $F_q(X)$ of degree $2g - 2 < m < n$ with $\text{Supp}(G_i) \cap \text{Supp}(D) = \emptyset$ for $\forall 1 \leq i \leq h$. 

Mac Williams and Riemann-Roch
The evaluation maps $\mathcal{E}_D : H^0(X, \mathcal{O}_X([G_i])) \rightarrow \mathbb{F}_q^n$, $\mathcal{E}_D(f) = (f(P_1), \ldots, f(P_n))$ of the global sections $f$ of the line bundles on $X$, associated with $G_i$ are $\mathbb{F}_q$-linear.

Their images $C_i = \mathcal{E}_D H^0(X, \mathcal{O}_X([G_i])) \subset \mathbb{F}_q^n$ are $\mathbb{F}_q$-linear codes of genus $g_i \leq g$, known as algebro-geometric Goppa codes.
The evaluation maps $\mathcal{E}_D : H^0(X, \mathcal{O}_X([G_i])) \rightarrow \mathbb{F}_q^n$, $\mathcal{E}_D(f) = (f(P_1), \ldots, f(P_n))$ of the global sections $f$ of the line bundles on $X$, associated with $G_i$ are $\mathbb{F}_q$-linear.

Their images $C_i = \mathcal{E}_D H^0(X, \mathcal{O}_X([G_i])) \subset \mathbb{F}_q^n$ are $\mathbb{F}_q$-linear codes of genus $g_i \leq g$, known as algebro-geometric Goppa codes.
The \( \zeta \)-functions of \( X \) and \( C_i \)

If \( |X(\mathbb{F}_{q^r})| \) is the number of the \( \mathbb{F}_{q^r} \)-rational points \( X(\mathbb{F}_{q^r}) := X \cap \mathbb{P}^N(\mathbb{F}_{q^r}) \) of \( X \) then the formal power series

\[
\zeta_X(t) := \exp \left( \sum_{r=1}^{\infty} |X(\mathbb{F}_{q^r})| \frac{t^r}{r} \right)
\]

is called the \( \zeta \)-function of \( X \).

Duursma’s considerations imply that the \( \zeta \)-functions of \( X \) and \( C_i \) satisfy the equality

\[
\zeta_X(t) = \sum_{i=1}^{h} t^{g_i-g_i} \zeta_{C_i}(t).
\]
If $|X(\mathbb{F}_{q^r})|$ is the number of the $\mathbb{F}_{q^r}$-rational points $X(\mathbb{F}_{q^r}) := X \cap \mathbb{P}^N(\mathbb{F}_{q^r})$ of $X$ then the formal power series

$$\zeta_X(t) := \exp \left( \sum_{r=1}^{\infty} \frac{|X(\mathbb{F}_{q^r})|}{r} t^r \right)$$

is called the $\zeta$-function of $X$.

Duursma’s considerations imply that the $\zeta$-functions of $X$ and $C_i$ satisfy the equality $\zeta_X(t) = \sum_{i=1}^{h} t^{g-g_i} \zeta_{C_i}(t)$. 

Mac Williams and Riemann-Roch
The absolute Galois group $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acts on any smooth irreducible curve $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ with finite orbits and

$$\deg \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(x) := \left| \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(x) \right|.$$ 

The $\mathbb{Z}$-linear combinations $D = a_1 \nu_1 + \ldots + a_s \nu_s$ of $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbits $\nu_j \subset X$ are called divisors on $X$.

The degree of $D$ is $\deg D = a_1 \deg \nu_1 + \ldots + a_s \deg \nu_s$. 

Mac Williams and Riemann-Roch
The absolute Galois group $\text{Gal}(\overline{F}_q/F_q)$ acts on any smooth irreducible curve $X/F_q \subset \mathbb{P}^N(\overline{F}_q)$ with finite orbits and 

$\deg \text{Orb}_{\text{Gal}(\overline{F}_q/F_q)}(x) := \left| \text{Orb}_{\text{Gal}(\overline{F}_q/F_q)}(x) \right|$. 

The $\mathbb{Z}$-linear combinations $D = a_1 \nu_1 + \ldots + a_s \nu_s$ of $\text{Gal}(\overline{F}_q/F_q)$-orbits $\nu_j \subset X$ are called divisors on $X$.

The degree of $D$ is $\deg D = a_1 \deg \nu_1 + \ldots + a_s \deg \nu_s$. 
The absolute Galois group $\text{Gal}(\overline{F}_q/F_q)$ acts on any smooth irreducible curve $X/F_q \subset \mathbb{P}^N(\overline{F}_q)$ with finite orbits and
\[ \text{deg Orb}_{\text{Gal}(\overline{F}_q/F_q)}(x) := \left| \text{Orb}_{\text{Gal}(\overline{F}_q/F_q)}(x) \right|. \]

The $\mathbb{Z}$-linear combinations $D = a_1 \nu_1 + \ldots + a_s \nu_s$ of $\text{Gal}(\overline{F}_q/F_q)$-orbits $\nu_j \subset X$ are called divisors on $X$.

The degree of $D$ is $\text{deg } D = a_1 \text{deg } \nu_1 + \ldots + a_s \text{deg } \nu_s$. 

Mac Williams and Riemann-Roch
A divisor $D = a_1 \nu_1 + \ldots + a_s \nu_s$ is effective if all of its non-zero coefficients $a_j > 0$ are positive.

There are finitely many $\text{Gal}(\overline{F}_q/F_q)$-orbits on $X$ of fixed degree and, therefore, a finite number $A_m(X) \in \mathbb{Z}^\geq 0$ of effective divisors on $X$ of degree $m \in \mathbb{Z}^\geq 0$.

The $\zeta$-function of $X$ is $\zeta_X(t) = \sum_{m=0}^{\infty} A_m(X)t^m$.  

Mac Williams and Riemann-Roch
A divisor $D = a_1 \nu_1 + \ldots + a_s \nu_s$ is effective if all of its non-zero coefficients $a_j > 0$ are positive.

There are finitely many $\text{Gal}(\overline{F_q}/F_q)$-orbits on $X$ of fixed degree and, therefore, a finite number $A_m(X) \in \mathbb{Z}_{\geq 0}$ of effective divisors on $X$ of degree $m \in \mathbb{Z}_{\geq 0}$.

The $\zeta$-function of $X$ is $\zeta_X(t) = \sum_{m=0}^{\infty} A_m(X)t^m$. 

Mac Williams and Riemann-Roch
A divisor $D = a_1 \nu_1 + \ldots + a_s \nu_s$ is effective if all of its non-zero coefficients $a_j > 0$ are positive.

There are finitely many $\text{Gal}(\overline{F}_q/F_q)$-orbits on $X$ of fixed degree and, therefore, a finite number $A_m(X) \in \mathbb{Z}^{\geq 0}$ of effective divisors on $X$ of degree $m \in \mathbb{Z}^{\geq 0}$.

The $\zeta$-function of $X$ is $\zeta_X(t) = \sum_{m=0}^{\infty} A_m(X)t^m$. 

Mac Williams and Riemann-Roch
Immediate consequences of the Riemann-Roch Theorem on a smooth irreducible curve $X/F_q \subset \mathbb{P}^N(F_q)$ of genus $g$ are the Riemann-Roch Conditions

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

for $\forall m \geq g$ and the residuum $\text{Res}_1(\zeta_X(t))$ of $\zeta_X(t)$ at $t = 1$. 

Riemann-Roch Conditions for a curve

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

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

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

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

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

Mac Williams and Riemann-Roch
Note that PRRC\((g, g^\perp)\) imply 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 \(m \geq g + g^\perp - 1\), which hold exactly when
\[
\zeta(t) = \frac{P(t)}{(1 - t)(1 - qt)}, \quad \zeta^\perp(t) = \frac{P^\perp(t)}{(1 - t)(1 - qt)}
\]
for polynomials \(P(t), P^\perp(t) \in \mathbb{C}[t]\).
Theorem: 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$(g, g^\perp)$ on their $\zeta$-functions $\zeta_C(t), \zeta_{C^\perp}(t)$. 

Mac Williams and Riemann-Roch
Proposition (KM - 2014): Let $C$ be an $\mathbb{F}_q$-linear $[n, k, d]$-code of
genus $g = n + 1 - k - d \geq 1$, whose dual $C^\perp$ is of genus $g^\perp = k + 1 - d^\perp \geq 1$. Then there is a unique Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$, such that $\mathcal{W}_C(x, y) = M_{n,n+1-k}(x, y) + \sum_{i=0}^{g+g^\perp-2} (q - 1)c_i \binom{n}{d+i}(x - y)^{n-d-i}y^{d+i}$. 

Mac Williams and Riemann-Roch
$D_C$ and $D_{C\perp}$ are determined by $g + g^\perp - 1$ parameters.

**Corollary:** The lower parts $\varphi_C(t) = \sum_{i=0}^{g-2} c_i t^i$, $\varphi_{C\perp}(t) = \sum_{i=0}^{g^\perp-2} c^\perp_i t^i$

of Duursma’s reduced polynomials $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i$,

$D_{C\perp}(t) = \sum_{i=0}^{g+g^\perp-2} c^\perp_i t^i$ and the number $c_{g-1} = c^\perp_{g^\perp-1} \in \mathbb{Q}$

determine uniquely

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

$$D_{C\perp}(t) = \varphi_{C\perp}(t) + c_{g-1} t^{g^\perp-1} + \varphi_C \left( \frac{1}{qt} \right) q^{g-1} t^{g+g^\perp-2}.$$
Corollary: If $C$ is an $\mathbb{F}_q$-linear code of genus $g \geq 1$ with Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$, then

$$c_i \binom{n}{d+i} \in \mathbb{Z}_{\geq 0} \quad \text{for} \quad \forall 0 \leq i \leq g + g^\perp - 2.$$ 

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 $1 \leq i \leq n$. 

Mac Williams and Riemann-Roch
**Corollary:** If $C$ is an $\mathbb{F}_q$-linear code of genus $g \geq 1$ with Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$, then

$$c_i \left( \begin{array}{c} n \\ d + i \end{array} \right) \in \mathbb{Z}_{\geq 0} \quad \text{for} \quad \forall 0 \leq i \leq g + g^\perp - 2.$$ 

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 $1 \leq i \leq n$. 

Mac Williams and Riemann-Roch
Proposition: Let $C$ be a non-degenerate $\mathbb{F}_q$-linear code with Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$ and

$$\mathbb{P}(C)\langle \subseteq \beta \rangle = \{[a] \in \mathbb{P}(C) \subset \mathbb{P}(\mathbb{F}_q^n) \mid \text{Supp}([a]) \subseteq \beta\}$$

for $\beta = \{\beta_1, \ldots, \beta_{d+i}\} \subset \{1, \ldots, n\}$ with $0 \leq i \leq g - 1$. Then

$$c_i = \binom{n}{d + i}^{-1} \sum_{\beta = \{\beta_1, \ldots, \beta_{d+i}\} \subset \{1, \ldots, n\}} |\mathbb{P}(C)\langle \subseteq \beta \rangle|$$

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

Mac Williams and Riemann-Roch
Proposition: Let $C$ be an $\mathbb{F}_q$-linear code with Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$. If $\pi^{(w)}_{\mathbb{P}(C)}$, respectively, $\pi^{(w)}_{\mathbb{P}(C^\perp)}$ is the probability of $[b] \in \mathbb{P}(\mathbb{F}_q^n)$ with $wt([b]) = w$ to belong to $\mathbb{P}(C)$, respectively, to $\mathbb{P}(C^\perp)$, then
\[
c_i = \sum_{w=d}^{d+i} \pi^{(w)}_{\mathbb{P}(C)} \binom{d+i}{w} (q-1)^{w-1} \quad \text{for } \forall 0 \leq i \leq g - 1; \]
\[
c_i = q^{i-g+1} \left[ \sum_{w=d^\perp}^{n-d-i} \pi^{(w)}_{\mathbb{P}(C^\perp)} \binom{n-d-i}{w} (q-1)^{w-1} \right], \forall g \leq i \leq g+g^\perp-2.\]
Proposition: Let $C$ be an $\mathbb{F}_q$-linear code with Duursma’s reduced polynomial $D_C(t) = \sum_{i=0}^{g+g^\perp-2} c_i t^i \in \mathbb{Q}[t]$. If $\pi^{(w)}_{[a]}$ is the probability of $\beta = \{\beta_1, \ldots, \beta_w\} \subset \{1, \ldots, n\}$ to contain the support $\text{Supp}([a])$ of $[a] \in \mathbb{P}(\mathbb{F}_q^n)$, then

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

$$c_i = q^{i-g+1} \left( \sum_{[b] \in \mathbb{P}(C^\perp)} \pi^{(n-d-i)}_{[b]} \right) \text{ for } \forall g \leq i \leq g + g^\perp - 2.$$
Thank you for your attention!