

Mac Williams identities for linear codes as
Riemann-Roch conditions
Azniv Kasparian, Ivan Marinov ¹

¹Partially supported by Contract 57/12.04.2016 with the Scientific
Foundation of Kliment Ohridski University of Sofia.

The genus of a linear code

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

The genus of a linear code

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

The homogeneous weight enumerator of a linear code

If $\mathcal{W}_C^{(w)}$ is the number of the words $c \in C$ of weight $1 \leq w \leq n$ then $\mathcal{W}_C(x, y) = x^n + \sum_{w=1}^n \mathcal{W}_C^{(w)} x^{n-w} y^w$ 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 $[n, n+1-s, s]$.

The homogeneous weight enumerator of a linear code

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 $[n, n + 1 - s, s]$.

The ζ -polynomial and the ζ -function of a linear code

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

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

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

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

The ζ -polynomial and the ζ -function of a linear code

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

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

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

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

Algebraic-geometric Goppa codes

Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}}_q)$ be a smooth irreducible curve of genus g , $P_1, \dots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q)$, $D = P_1 + \dots + P_n$ and G_1, \dots, 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 $\forall 1 \leq i \leq h$.

Algebraic-geometric Goppa codes

Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}}_q)$ be a smooth irreducible curve of genus g , $P_1, \dots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q)$, $D = P_1 + \dots + P_n$ and G_1, \dots, 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 $\forall 1 \leq i \leq h$.

Algebraic-geometric Goppa codes

Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}}_q)$ be a smooth irreducible curve of genus g , $P_1, \dots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q)$, $D = P_1 + \dots + P_n$ and G_1, \dots, 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 $\forall 1 \leq i \leq h$.

Algebraic-geometric Goppa codes

Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ be a smooth irreducible curve of genus g , $P_1, \dots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q)$, $D = P_1 + \dots + P_n$ and G_1, \dots, 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 $\forall 1 \leq i \leq h$.

Algebraic-geometric Goppa codes

Let $X/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}_q})$ be a smooth irreducible curve of genus g , $P_1, \dots, P_n \in X(\mathbb{F}_q) = X \cap \mathbb{P}^N(\mathbb{F}_q)$, $D = P_1 + \dots + P_n$ and G_1, \dots, 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 $\forall 1 \leq i \leq h$.

Algebraic-geometric Goppa codes

The evaluation maps $\mathcal{E}_D : H^0(X, \mathcal{O}_X([G_i])) \rightarrow \mathbb{F}_q^n$,
 $\mathcal{E}_D(f) = (f(P_1), \dots, f(P_n))$ 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 algebraic-geometric Goppa codes.

Algebraic-geometric Goppa codes

The evaluation maps $\mathcal{E}_D : H^0(X, \mathcal{O}_X([G_i])) \rightarrow \mathbb{F}_q^n$,
 $\mathcal{E}_D(f) = (f(P_1), \dots, f(P_n))$ 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 algebraic-geometric Goppa codes.

The ζ -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 ζ -function of X .

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

The ζ -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 ζ -function of X .

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

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

The \mathbb{Z} -linear combinations $D = a_1\nu_1 + \dots + a_s\nu_s$ 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 $\deg D = a_1 \deg \nu_1 + \dots + a_s \deg \nu_s$.

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 $D = a_1\nu_1 + \dots + a_s\nu_s$ 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 $\deg D = a_1 \deg \nu_1 + \dots + a_s \deg \nu_s$.

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 $D = a_1\nu_1 + \dots + a_s\nu_s$ 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 $\deg D = a_1 \deg \nu_1 + \dots + a_s \deg \nu_s$.

Effective divisors of fixed degree

A divisor $D = a_1\nu_1 + \dots + a_s\nu_s$ is effective if all of its non-zero coefficients $a_j > 0$ are positive.

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

The ζ -function of X is $\zeta_X(t) = \sum_{m=0}^{\infty} \mathcal{A}_m(X)t^m$.

Effective divisors of fixed degree

A divisor $D = a_1\nu_1 + \dots + a_s\nu_s$ is effective if all of its non-zero coefficients $a_j > 0$ are positive.

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

The ζ -function of X is $\zeta_X(t) = \sum_{m=0}^{\infty} \mathcal{A}_m(X)t^m$.

Effective divisors of fixed degree

A divisor $D = a_1\nu_1 + \dots + a_s\nu_s$ is effective if all of its non-zero coefficients $a_j > 0$ are positive.

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

The ζ -function of X is $\zeta_X(t) = \sum_{m=0}^{\infty} \mathcal{A}_m(X)t^m$.

Riemann-Roch Conditions for a curve

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

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

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

Polarized Riemann-Roch Conditions

Definition: Formal power series $\zeta(t) = \sum_{m=0}^{\infty} \mathcal{A}_m t^m$ and

$\zeta^\perp(t) = \sum_{i=0}^{\infty} \mathcal{A}_m^\perp t^m$ satisfy the Polarized Riemann-Roch

Conditions PRRC(g, g^\perp) for some $g, g^\perp \in \mathbb{Z}^{\geq 0}$ if

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

$$\mathcal{A}_{g-1} = \mathcal{A}_{g^\perp-1}^\perp \quad \text{and}$$

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

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

Note that $\text{PRRC}(g, g^\perp)$ imply the recurrence relations

$$\mathcal{A}_{m+2} - (q+1)\mathcal{A}_{m+1} + q\mathcal{A}_m = \mathcal{A}_{m+2}^\perp - (q+1)\mathcal{A}_{m+1}^\perp + q\mathcal{A}_m^\perp = 0$$

for $\forall m \geq g + g^\perp - 1$, 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 $\text{PRRC}(g, g^\perp)$ on their ζ -functions $\zeta_C(t), \zeta_{C^\perp}(t)$.

Definition of Duursma's reduced polynomial

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 $\mathcal{W}_C(x, y) =$

$$\mathcal{M}_{n, n+1-k}(x, y) + \sum_{i=0}^{g+g^\perp-2} (q-1)c_i \binom{n}{d+i} (x-y)^{n-d-i} y^{d+i}.$$

D_C and D_{C^\perp} are determined by $g + g^\perp - 1$ parameters

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

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

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

determine uniquely

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

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

The coefficients of Duursma's reduced polynomial

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

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

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 $1 \leq i \leq n$.

The coefficients of Duursma's reduced polynomial

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

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

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 $1 \leq i \leq n$.

An averaging interpretation of the coefficients of Duursma's reduced polynomial

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

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

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

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

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

Probabilistic interpretations of the coefficients of Duursma's reduced polynomial

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 $\pi_{\mathbb{P}(C)}^{(w)}$, respectively, $\pi_{\mathbb{P}(C^\perp)}^{(w)}$ is the probability of $[b] \in \mathbb{P}(\mathbb{F}_q^n)$ with $\text{wt}([b]) = w$ to belong to $\mathbb{P}(C)$, respectively, to $\mathbb{P}(C^\perp)$, then

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

$$c_i = q^{i-g+1} \left[\sum_{w=d^\perp}^{n-d-i} \pi_{\mathbb{P}(C^\perp)}^{(w)} \binom{n-d-i}{w} (q-1)^{w-1} \right], \quad \forall g \leq i \leq g+g^\perp-2.$$

Probabilistic interpretations of the coefficients of Duursma's reduced polynomial

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 $\bar{\pi}_{[a]}^{(w)}$ is the probability of $\beta = \{\beta_1, \dots, \beta_w\} \subset \{1, \dots, n\}$ to contain the support $\text{Supp}([a])$ of $[a] \in \mathbb{P}(\mathbb{F}_q^n)$, then

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

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

Thank you for your attention!