A Practical Guide to the MacWilliams Relations

Steven T. Dougherty

June, 2015

MacWilliams Relations

The MacWilliams relations are one of the foundations of coding theory.

MacWilliams Relations

The MacWilliams relations are one of the foundations of coding theory.

They were first proven by Jesse MacWilliams for codes over fields then extended to Frobenius rings by Jay Wood.

Notations

For an R-module M we denote $\widehat{M}$ as the homomorphisms from R to $\mathbb{C}^*$. Notice that in the literature, it is sometimes written that $\widehat{M} = Hom_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$.

Frobenius Rings

For a finite ring, the following statements are equivalent:

- R is Frobenius.
- As a left module $\widehat{R} \cong {}_R R$.
- As a right module $\widehat{R} \cong R_R$.

Codes

A code of length n over a ring R is a subset of R^n. If the code is a submodule then we say that the code is linear.

Codes

A code of length n over a ring R is a subset of R^n. If the code is a submodule then we say that the code is linear.

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$$

$$C^\perp = \{\mathbf{w} \mid [\mathbf{w}, \mathbf{v}] = 0, \ \forall \mathbf{v} \in C\}.$$

Complete Weight Enumerator

For a code over an alphabet $A = \{a_0, a_1, \ldots, a_{s-1}\}$, the complete weight enumerator is defined as:

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{s-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{s-1} x_{a_i}^{n_i(\mathbf{c})} \tag{1}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

Symmetric Weight Enumerator

Define $a \sim b$ if and only if $a = b\mu$ where μ is a unit in R. Let $[b_0], \ldots, [b_t]$ be the equivalence classes under this relation. Define the symmetrized weight enumerator, $(swe_C(x_{[b_0]}, x_{[b_1]}, \ldots, x_{[b_t]})$, as the weight enumerator formed by replacing x_{a_i} with $x_{[b_j]}$ where $a_i \in [b_j]$.

Hamming Weight Enumerator

The Hamming weight enumerator of a code C is defined to be

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n-wt(\mathbf{c})} y^{wt(\mathbf{c})},$$

where $wt(\mathbf{c}) = |\{i \mid c_i \neq 0\}|$. It is immediate that $W_C(x, y) = cwe(x, y, y, \ldots, y)$.

Jessie MacWilliams (1917-1990)

MacWilliams, Jessie A theorem on the distribution of weights in a systematic code. Bell System Tech. J. 42 1963 79-94.

Jessie MacWilliams (1917-1990)

Theorem

*(**MacWilliams Relations**) Let C be a linear code over $\mathbb{F}_q$ then*

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C(x+(q-1)y, x-y).$$

MacWilliams relations revisited

The matrix T_i is a $|R|$ by $|R|$ matrix given by:

$$(T_i)_{a,b} = (\chi(ab)) \tag{2}$$

where a and b are in R.

MacWilliams relations revisited

For a code C in R^n define

$$\mathcal{L}(C) = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in C\}$$

MacWilliams relations revisited

For a code C in R^n define

$$\mathcal{L}(C) = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in C\}$$

and

$$\mathcal{R}(C) = \{\mathbf{v} \mid [\mathbf{w}, \mathbf{v}] = 0, \forall \mathbf{w} \in C\}.$$

MacWilliams relations revisited

Theorem

(Generalized MacWilliams Relations – Wood) Let R be a Frobenius ring. If C is a left submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{R}(C)|} cwe_{\mathcal{R}(C)}(T^t \cdot (x_0, x_1, \ldots, x_k)).$$

If C is a right submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{L}(C)|} cwe_{\mathcal{L}(C)}(T \cdot (x_0, x_1, \ldots, x_k)).$$

MacWilliams relations revisited

For commutative rings $\mathcal{L}(C) = \mathcal{R}(C) = C^{\perp}$.

MacWilliams relations revisited

For commutative rings $\mathcal{L}(C) = \mathcal{R}(C) = C^{\perp}$.

Theorem

Let C be a linear code over a commutaive Frobenius rings R then

$$W_{C^{\perp}}(x_0, x_1, \ldots, x_k) = \frac{1}{|C|} W_C(T \cdot (x_0, x_1, \ldots, x_k)). \tag{3}$$

Corollary

Corollary

If C is a linear code over a Frobenius ring then $|C||C^{\perp}| = |R|^n$.

Corollary

Corollary

If C is a linear code over a Frobenius ring then $|C||C^{\perp}| = |R|^n$.

This often fails for codes over non-Frobenius rings.

MacWilliams Relation

Let S be the matrix, indexed by the equivalence class of the relation $\sim$, formed from T by $S_{[\alpha],[\beta]} = \sum_{\beta' \in [\beta]} T_{\alpha,\beta}$.
If C is a submodule of R^n, then

$$swe_C(y_0, y_1, \ldots, y_t) = \frac{1}{|C^\perp|} swe_{C^\perp}(S \cdot (y_0, y_1, \ldots, y_k)). \qquad (4)$$

MacWilliams Relation

Let S be the matrix, indexed by the equivalence class of the relation $\sim$, formed from T by $S_{[\alpha],[\beta]} = \sum_{\beta' \in [\beta]} T_{\alpha,\beta}$.
If C is a submodule of R^n, then

$$swe_C(y_0, y_1, \ldots, y_t) = \frac{1}{|C^\perp|} swe_{C^\perp}(S \cdot (y_0, y_1, \ldots, y_k)). \tag{4}$$

If C is a submodule of R^n, then

$$W_C(x, y) = \frac{1}{|C^\perp|} W_{C^\perp}(x + (|R| - 1)y, x - y)).$$

Chinese Remainder Theorem

Let R be a fintie commutative Frobenius ring, then R is isomorphic, via the Chinese Remainder Theorem to

$$R_1 \times R_2 \times \cdots \times R_s$$

where R_i is a local ring and Frobenius.

Chinese Remainder Theorem

Theorem

Let R be a Frobenius ring $R = CRT(R_1, R_2, \ldots, R_s)$ where each R_i is a local ring. Let χ_{R_i} be the generating character for R_i. Then the character χ for R defined by

$$\chi(a) = \prod \chi_{R_i}(a_i) \tag{5}$$

where $a = CRT(a_1, a_2, \ldots, a_s)$, is a generating character for R.

Wood's Lemma

Lemma

Let χ be a character of a finite ring R. The χ is a right generating character if and only if $\ker(\chi)$ *contains no nonzero right ideals of R.*

Frobenius Local Rings

Let R be a finite local commutative Frobenius ring with maximal ideal $\mathfrak{m}$.

Frobenius Local Rings

Let R be a finite local commutative Frobenius ring with maximal ideal $\mathfrak{m}$.

The Jacobson radical of R, $J(R) = \mathfrak{m}$ and the socle of the ring R is $Soc(R) = Ann(\mathfrak{m}) = \mathfrak{m}^{\perp}$.

Frobenius Local Rings

Let R be a finite local commutative Frobenius ring with maximal ideal $\mathfrak{m}$.

The Jacobson radical of R, $J(R) = \mathfrak{m}$ and the socle of the ring R is $Soc(R) = Ann(\mathfrak{m}) = \mathfrak{m}^{\perp}$.

Since $\mathfrak{m}$ is the maximal ideal we have that $R/\mathfrak{m}$ is isomorphic to a field K. We have that $dim_K(Ann(\mathfrak{m})) = 1$ which gives that $Soc(R)$ is isomorphic to K as R modules.

Frobenius Local Rings

Let R be a finite local commutative Frobenius ring with maximal ideal $\mathfrak{m}$.

The Jacobson radical of R, $J(R) = \mathfrak{m}$ and the socle of the ring R is $Soc(R) = Ann(\mathfrak{m}) = \mathfrak{m}^{\perp}$.

Since $\mathfrak{m}$ is the maximal ideal we have that $R/\mathfrak{m}$ is isomorphic to a field K. We have that $dim_K(Ann(\mathfrak{m})) = 1$ which gives that $Soc(R)$ is isomorphic to K as R modules.
The character of finite fields are well known.

Frobenius Local Rings

Let R be a finite local commutative Frobenius ring with maximal ideal $\mathfrak{m}$.

The Jacobson radical of R, $J(R) = \mathfrak{m}$ and the socle of the ring R is $Soc(R) = Ann(\mathfrak{m}) = \mathfrak{m}^{\perp}$.

Since $\mathfrak{m}$ is the maximal ideal we have that $R/\mathfrak{m}$ is isomorphic to a field K. We have that $dim_K(Ann(\mathfrak{m})) = 1$ which gives that $Soc(R)$ is isomorphic to K as R modules.
The character of finite fields are well known.
Then simply extend the character to the ring R and you have a generating character.

Character

Once you have the generating character χ you use:
$\chi_a(b) = \chi(ab)$ and you can easily construct the matrix T in the MacWilliams relations.

Example 1

There is one commutative local ring of size 16 with characteristic 2 and Jacobson radical of size 4, namely $R = \mathbb{F}_4[x]/\langle x^2 \rangle$.

Example 1

There is one commutative local ring of size 16 with characteristic 2 and Jacobson radical of size 4, namely $R = \mathbb{F}_4[x]/\langle x^2 \rangle$.
The maximal ideal is $\langle x \rangle = \{0, x, \omega x, \omega^2 x\}$ which is isomorphic to $\mathbb{F}_4$ and is equal to the Socle.

Example 1

There is one commutative local ring of size 16 with characteristic 2 and Jacobson radical of size 4, namely $R = \mathbb{F}_4[x]/\langle x^2 \rangle$.
The maximal ideal is $\langle x \rangle = \{0, x, \omega x, \omega^2 x\}$ which is isomorphic to $\mathbb{F}_4$ and is equal to the Socle.
Then $\chi(0) = 1, \chi(x) = -1, \chi(\omega x) = -1, \chi(\omega^2 x) = 1$.

Example 1

There is one commutative local ring of size 16 with characteristic 2 and Jacobson radical of size 4, namely $R = \mathbb{F}_4[x]/\langle x^2 \rangle$.
The maximal ideal is $\langle x \rangle = \{0, x, \omega x, \omega^2 x\}$ which is isomorphic to $\mathbb{F}_4$ and is equal to the Socle.
Then $\chi(0) = 1, \chi(x) = -1, \chi(\omega x) = -1, \chi(\omega^2 x) = 1$.
Then we construct the generating character π as an extension of this character:

β	0	1	ω	ω^2	x	$1+x$	$\omega+x$	ω^2+x
$\pi(\beta)$	1	-1	-1	1	-1	1	1	-1
β	ωx	$1+\omega x$	$\omega+\omega x$	$\omega^2+\omega x$	$\omega^2 x$	$1+\omega^2 x$	$\omega+\omega^2 x+$	$\omega^2+\omega^2 x$
$\pi(\beta)$	-1	1	1	-1	1	-1	-1	1

Then $T_{i,j} = \pi(ij)$.

Example 1

There are three equivalence classes under the relation $\sim$, namely $\{0\}$, $\{1, \omega, \omega^2, 1+x, \omega+x, \omega^2+x, 1+\omega x, \omega+\omega x, \omega^2+\omega x, 1+\omega^2 x, \omega+\omega^2 x, \omega^2+\omega^2 x\}$ and $\{x, \omega x, \omega^2 x\}$.

Example 1

There are three equivalence classes under the relation $\sim$, namely $\{0\}$, $\{1, \omega, \omega^2, 1+x, \omega+x, \omega^2+x, 1+\omega x, \omega+\omega x, \omega^2+\omega x, 1+\omega^2 x, \omega+\omega^2 x, \omega^2+\omega^2 x\}$ and $\{x, \omega x, \omega^2 x\}$.

Then we have that

$$S = \begin{pmatrix} 1 & 12 & 3 \\ 1 & 0 & -1 \\ 1 & -4 & 3 \end{pmatrix}.$$

Example 2

Non-chain ring: $R = \mathbb{F}_2[u, v]/\langle u^2, v^2 \rangle$.

Example 2

Non-chain ring: $R = \mathbb{F}_2[u, v]/\langle u^2, v^2\rangle$.
The maximal ideal
$\mathfrak{m} = \langle u, v\rangle = \{0, u, v, uv, u + uv, v + uv, u + v, u + v + uv\} = J(R)$.
Then the socle is $Soc(R) = \{0, uv\}$.

Example 2

Non-chain ring: $R = \mathbb{F}_2[u, v]/\langle u^2, v^2 \rangle$.
The maximal ideal
$\mathfrak{m} = \langle u, v \rangle = \{0, u, v, uv, u + uv, v + uv, u + v, u + v + uv\} = J(R)$.
Then the socle is $Soc(R) = \{0, uv\}$.
Then we have $\chi(0) = 1, \chi(uv) = -1$.

Example 2

Non-chain ring: $R = \mathbb{F}_2[u, v]/\langle u^2, v^2 \rangle$.
The maximal ideal
$\mathfrak{m} = \langle u, v \rangle = \{0, u, v, uv, u + uv, v + uv, u + v, u + v + uv\} = J(R)$.
Then the socle is $Soc(R) = \{0, uv\}$.
Then we have $\chi(0) = 1, \chi(uv) = -1$.
Then we construct π as an extension of this character:

β	0	1	u	$1+u$	v	$1+v$	uv	$1+uv$
$\pi(\beta)$	1	-1	1	-1	1	-1	-1	1
β	$u+uv$	$1+u+uv$	$v+uv$	$1+v+uv$	$u+v$	$1+u+v$	$u+v+uv$	$1+u+v+uv$
$\pi(\beta)$	-1	1	-1	1	1	-1	-1	1

Then $T_{i,j} = \pi(ij)$.

Example 2

The equivalence classes formed by the relation $\sim$ are: $\{0\}, \{1, 1+u, 1+u+uv, 1+v, 1+v+uv, 1+uv, 1+u+v+uv, 1+u+v\}, \{u, u+uv\}, \{v, v+uv\}, \{uv\}, \{u+v+uv, u+v\}$. We index S in the order given for these classes. Then we have that

$$S = \begin{pmatrix} 1 & 8 & 2 & 2 & 1 & 2 \\ 1 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 2 & -2 & 1 & -2 \\ 1 & 0 & -2 & 2 & 1 & -2 \\ 1 & -8 & 2 & 2 & 1 & 2 \\ 1 & 0 & -2 & -2 & 1 & 2 \end{pmatrix}. \tag{6}$$

Example 3

Non-chain ring $\mathbb{Z}_4[x]/\langle x^2 \rangle$.

Example 3

Non-chain ring $\mathbb{Z}_4[x]/\langle x^2 \rangle$.
The maximal ideal
$\mathfrak{m} = \langle 2, x \rangle = \{0, 2, x, 2 + x, 2x, 2 + 2x, 3x, 2 + 3x\} = J(R)$. Then the socle is $Soc(R) = \{0, 2x\}$.

Example 3

Non-chain ring $\mathbb{Z}_4[x]/\langle x^2 \rangle$.
The maximal ideal
$\mathfrak{m} = \langle 2, x \rangle = \{0, 2, x, 2+x, 2x, 2+2x, 3x, 2+3x\} = J(R)$. Then the socle is $Soc(R) = \{0, 2x\}$.
Then we have $\chi(0) = 1, \chi(2x) = -1$.
Then we construct π as an extension of this character:

β	0	1	2	3	x	$1+x$	$2+x$	$3+x$
$\pi(4,8)(\beta)$	1	i	-1	$-i$	i	-1	$-i$	1
β	$2x$	$1+2x$	$2+2x$	$3+2x$	$3x$	$1+3x$	$2+3x$	$3+3x$
$\pi(4,8)(\beta)$	-1	$-i$	1	i	$-i$	1	i	-1

Then $T_{i,j} = \pi(ij)$.

Example 3

The equivalence classes formed by the relation $\sim$ are: $\{0\}, \{1, 3, 1+x, 3+x, 1+2x, 3+2x, 1+3x, 3+3x\}, \{2, 2+2x\}, \{2+x, 2+3x\}, \{x, 3x\}, \{2x\}$.

$$S = \begin{pmatrix} 1 & 8 & 2 & 2 & 1 & 2 \\ 1 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 2 & -2 & 1 & -2 \\ 1 & 0 & -2 & 2 & 1 & -2 \\ 1 & -8 & 2 & 2 & 1 & 2 \\ 1 & 0 & -2 & -2 & 1 & 2 \end{pmatrix}. \tag{7}$$