Characters and finite Frobenius rings

Jay A. Wood

Department of Mathematics
Western Michigan University
http://homepages.wmich.edu/~jwood/

Algebra for Secure and Reliable Communications Modeling
Morelia, Michoacán, Mexico
October 9, 2012
Recall from my last lecture that the MacWilliams identities for the Hamming weight hold for any finite ring $R$ that satisfies

$$\widehat{R} \cong R$$

as one-sided $R$-modules.

The extension theorem for Hamming weight will also hold for such rings (later).
Recall definitions

- Let $R$ be a finite associative ring with 1.
- Recall: the Jacobson radical $J$ is the intersection of all the maximal left ideals of $R$; $J$ is a two-sided ideal.
- Recall that the left socle $\text{Soc}(R_R)$ is the left ideal generated by all the simple left ideals of $R$.
- Similarly, for the right socle $\text{Soc}(R_R)$.
- Each $\text{Soc}(R)$ is a two-sided ideal.
Finite Frobenius rings

- A finite ring $R$ is Frobenius if $\mathcal{R}(R/J) \cong \text{Soc}(R_R)$ and $(R/J)_R \cong \text{Soc}(R_R)$.
- It is a theorem of Honold, 2001, that each of these isomorphisms implies the other.
- From my first lecture: $\mathbb{F}_q$ and $\mathbb{Z}/m\mathbb{Z}$ are Frobenius. Klemm’s example $\mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$ is not Frobenius.
Character modules

- Suppose $M$ is a finite left $R$-module.
- The character group $\hat{M}$ admits the structure of a right $R$-module via

  $$(\pi r)(m) := \pi(rm), \quad r \in R, m \in M, \pi \in \hat{M}.$$ 

- Similarly, if $N$ is a right $R$-module, then $\hat{N}$ is a left $R$-module.
Consider a finite field $\mathbb{F}_q$.

$\mathbb{F}_q$ is an $\mathbb{F}_q$-vector space.

Since $|\hat{\mathbb{F}}_q| = |\mathbb{F}_q|$, $\hat{\mathbb{F}}_q$ has dimension 1, and $\hat{\mathbb{F}}_q \cong \mathbb{F}_q$ as $\mathbb{F}_q$-vector spaces.

The character $\theta_q = \theta_p \circ \text{Tr}_{q/p}$ is a basis.
Matrix modules

- \( R = M_n(\mathbb{F}_q) \) is the ring of \( n \times n \) matrices over \( \mathbb{F}_q \).
- Let \( M = M_{n \times k}(\mathbb{F}_q) \) and \( N = M_{k \times n}(\mathbb{F}_q) \); \( M \) is a left \( R \)-module, and \( N \) is a right \( R \)-module.
- Define a character on \( R \): \( \rho = \theta_q \circ \text{Tr} \), where \( \text{Tr} \) is the matrix trace.
- \( M \cong \hat{N} \) via \( P \mapsto (Q \mapsto \rho(PQ)) \).
- \( N \cong \hat{M} \) via \( Q \mapsto (P \mapsto \rho(PQ)) \).
- In particular, \( \hat{R} \cong R \) as left and as right modules.
Main theorem

Theorem

Let $R$ be a finite ring with 1. The following are equivalent:

1. $R$ is Frobenius;
2. $\hat{R} \cong R$ as left $R$-modules;
3. $\hat{R} \cong R$ as right $R$-modules.

Short exact sequence

- $\hat{\cdot}$ is an exact contravariant functor on $R$-modules.
- A short exact sequence of left $R$-modules

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

induces a short exact sequence of right $R$-modules

$$0 \to (\hat{M}_2 : M_1) \to \hat{M}_2 \to \hat{M}_1 \to 0.$$ 

- Similarly with left-right reversed.
Theorem

Let $M$ be a finite left $R$-module. Then

$$\text{Soc}(\hat{M}) \cong (M/JM)^{\hat{}}.$$ 

- $J$ annihilates simple modules, so that $\text{Soc}(\hat{M}) = (\hat{M} : JM)$.
- Use $(M/JM)^{\hat{}} \cong (\hat{M} : JM)$. 
One direction

- Suppose \( \hat{\mathcal{R}} \cong R \) as right \( R \)-modules.
- \( R/J \) is a sum of matrix rings, so
  \[ (R/J)_R \cong (R(R/J))^{\hat{\ )} \).
- Use \( M = R \) (as left \( R \)-module) from Theorem.
- Then \( (R(R/J))^{\hat{\ )} \cong \text{Soc}(\hat{\mathcal{R}}_R) \cong \text{Soc}(R_R) \).
- Repeat on other side, or use Honold’s theorem.
Generating characters (a)

- Let $M$ be a finite left $R$-module.
- A character $\rho$ of $M$ is a (left) generating character if $\ker \rho$ contains no nonzero left submodules of $M$.
- Similarly for right modules.
Generating characters (b)

Theorem

$M$ has a left generating character iff $M$ injects into $\hat{R}$.

- If $f : M \hookrightarrow \hat{R}$, set $\rho(m) = f(m)(1_R)$.
- If $\rho$ is a generating character, define $f(m) = (r \mapsto \rho(rm))$.
- If $m \in \ker f$, then $Rm \subset \ker \rho$.
- Because $|\hat{R}| = |R|$, $\hat{R} \cong R$ as left modules iff $R$ has a left generating character. Same for right.
Left generating iff right generating

Theorem
Let $\rho$ be a character of $R$. Then $\rho$ is left generating iff $\rho$ is right generating.

- If $\rho$ is right generating, then $\hat{R}_R \cong R_R$, so every $\pi \in \hat{R}$ has the form $\rho r$ for some $r \in R$.
- If $Ra \subset \ker \rho$, then for all $r \in R$, $1 = \rho(ra) = (\rho r)(a)$. Thus $\pi(a) = 1$ for all $\pi \in \hat{R}$. This implies $a = 0$, and $\rho$ is left generating.
Simple $R$-modules

- For any finite ring $R$, $R/J$ is a sum of matrix rings:

  $$R/J \cong \bigoplus_{i=1}^{k} M_{\mu_i}(\mathbb{F}_{q_i}).$$

- Let $T_i = M_{\mu_i \times 1}(\mathbb{F}_{q_i})$. $T_i$ is a simple left $M_{\mu_i}(\mathbb{F}_{q_i})$-module and a simple left $R$-module.

- Fact: the $T_i$ are the only simple left $R$-modules, up to isomorphism.
Structure of $R/J$ and $\text{Soc}(R)$

- As a left $R$-module, $R(R/J) \cong \bigoplus_{i=1}^{k} \mu_i T_i$.
- Because $\text{Soc}(R^R)$ is generated by simple modules, $\text{Soc}(R^R) \cong \bigoplus_{i=1}^{k} s_i T_i$, for some $s_i$, nonnegative integers.
- Thus, $R$ is Frobenius iff $\mu_i = s_i$ for all $i = 1, \ldots, k$.
- In general, $\text{Soc}(R^R)$ is a sum of matrix modules $M_{\mu_i \times s_i}(\mathbb{F}_{q_i})$. 

JW (WMU) 
Frobenius rings 
October 9, 2012 16 / 28
Generating characters for Soc\((R)\)

- If \(R\) is Frobenius, then \(\text{Soc}(R) \cong \bigoplus M_{\mu_i}(\mathbb{F}_{q_i})\).
- We saw earlier that \(M_{\mu_i}(\mathbb{F}_{q_i})\) admits a left generating character \(\theta_i\).
- The product of the \(\theta_i\) is a left generating character of \(\text{Soc}(R)\).
Theorem

Let $M$ be a finite left $R$-module. If $\text{Soc}(M)$ admits a left generating character $\theta$, then $\theta$ extends to a left generating character of $M$.

- $0 \to \text{Soc}(M) \to M \to M/\text{Soc}(M) \to 0$, induces $0 \to (\hat{M} : \text{Soc}(M)) \to \hat{M} \to \text{Soc}(M) \hat{} \to 0$.
- Let $\rho$ be any extension of $\theta$. 
Claim: $\rho$ is a left generating character of $M$.

Suppose $I$ is a left submodule of $\ker \rho$. Then

$$\text{Soc}(I) \subseteq \text{Soc}(M) \cap \ker \rho = \text{Soc}(M) \cap \ker \theta.$$ 

Since $\theta$ is a left generating character, $\text{Soc}(I) = 0$.

Thus, $I = 0$. 

Extending generating characters (b)
Other direction

- Suppose $R$ is Frobenius.
- $\text{Soc}(R) \cong \bigoplus M_{\mu_i}(\mathbb{F}_{q_i})$ admits a left generating character $\theta$.
- Any extension $\rho$ of $\theta$ is a left generating character of $R$.
- Thus $\hat{R} \cong R$ as left $R$-modules.
- Any left generating character is also right generating, so $\hat{R} \cong R$ as right $R$-modules.
Examples of Frobenius rings

- $\mathbb{F}_q$, $\rho = \theta_q$.
- $\mathbb{Z}/m\mathbb{Z}$, $\rho(a) = \exp(2\pi i a/m)$.
- Chain rings: all the left ideals form a chain under inclusion. $\text{Soc}(R) \cong \mathbb{F}_q$. Extend $\theta_q$ on $\text{Soc}(R)$ to $\rho$ on $R$. Examples of chain rings:
  - Any finite commutative local ring with principal maximal ideal.
  - $\mathbb{Z}/p^k\mathbb{Z}$.
  - Galois rings: Galois extensions of $\mathbb{Z}/p^k\mathbb{Z}$.
  - $\mathbb{F}_q[X]/(X^k)$.
  - Certain quotients of skew polynomial rings.
More examples

- $M_n(\mathbb{F}_q)$, $\rho = \theta_q \circ \text{Tr}$.
- $M_n(R)$, where $R$ is Frobenius. $\rho = \rho_R \circ \text{Tr}$.
- $R[G]$, the group ring of a finite group $G$ with coefficients in a Frobenius ring $R$. Every element of $R[G]$ is of the form $a = \sum_{g \in G} a_g g$, with $a_g \in R$. $\rho(a) = \rho_R(a_e)$, where $e$ is the identity of $G$.
- (Algebraic topology) Certain finite subalgebras of the Steenrod algebra.
Commutative case

- Every finite commutative ring $R$ splits as a sum of local rings $(R_i, \mathfrak{m}_i)$, where $\mathfrak{m}_i$ is the unique maximal ideal of $R_i$. $R$ is Frobenius iff each $R_i$ is Frobenius. $\rho = \prod \rho_i$.
- A local commutative ring $(R_i, \mathfrak{m}_i)$ is Frobenius iff $\text{Soc}(R_i) = \text{ann}(\mathfrak{m}_i)$ has dimension 1 over $\mathbb{F}_q \cong R_i/\mathfrak{m}_i$. Extend $\theta_q$ on $\text{Soc}(R_i)$ to $\rho_i$ on $R_i$. 

$\rho$ denotes the Frobenius endomorphism of $R$. 

$\mathbb{F}_q$ denotes the finite field with $q$ elements. 

$\mathfrak{m}_i$ denotes the maximal ideal of $R_i$. 

$\text{Soc}(R_i)$ denotes the socle of $R_i$, which is the sum of all simple submodules of $R_i$. 

$\text{ann}(\mathfrak{m}_i)$ denotes the annihilator of $\mathfrak{m}_i$ in $R_i$. 

$\theta_q$ denotes the Frobenius map on $\mathbb{F}_q$. 

$\mathbb{F}_q \cong R_i/\mathfrak{m}_i$ denotes the quotient field of $R_i/\mathfrak{m}_i$. 

$\rho_i$ denotes the Frobenius endomorphism of $R_i$. 

$\rho = \prod \rho_i$ denotes the product of all Frobenius endomorphisms $\rho_i$. 

$\rho$ is a Frobenius ring if and only if each $R_i$ is a Frobenius ring. 

$\theta_q$ is a Frobenius map on $\mathbb{F}_q$ if and only if $\theta_q$ is a Frobenius map on $R_i$. 

$\mathbb{F}_q \cong R_i/\mathfrak{m}_i$ is a field if and only if $\mathbb{F}_q \cong R_i/\mathfrak{m}_i$ is a field.
Quasi-Frobenius rings

- Let $R$ be a finite ring with 1.
- $R$ is quasi-Frobenius (QF) if $R$ is an injective left (or right) $R$-module.
- That is, for every short exact sequence of $R$-modules

$$0 \to A \to B \to C \to 0,$$

we have a short exact sequence

$$0 \to \text{Hom}_R(C, R) \to \text{Hom}_R(B, R) \to \text{Hom}_R(A, R) \to 0.$$
Frobenius implies QF

- In general, $\hat{M} = \text{Hom}_\mathbb{Z}(M, \mathbb{C}^\times) \cong \text{Hom}_R(M, \hat{R})$, via $\pi \in \hat{M} \mapsto (m \mapsto (r \mapsto \pi(rm)))$.
- $\hat{\cdot}$ is an exact functor represented by $\hat{R}$, so $\hat{R}$ is always injective.
- If $R$ is Frobenius, then $R \cong \hat{R}$. Thus $R$ is injective, hence QF.
Benson’s example

Let $R$ be a ring consisting of all matrices over $\mathbb{F}_2$ of the following form:

$$
\begin{pmatrix}
  a_1 & 0 & a_2 & 0 & 0 & 0 \\
  0 & a_1 & 0 & a_2 & a_3 & 0 \\
  a_4 & 0 & a_5 & 0 & 0 & 0 \\
  0 & a_4 & 0 & a_5 & a_6 & 0 \\
  0 & 0 & 0 & 0 & a_9 & 0 \\
  a_7 & 0 & a_8 & 0 & 0 & a_9 \\
\end{pmatrix}.
$$

This $R$ is QF but not Frobenius.
Role of QF rings in duality

- Recall the dot product on $R^n$: $a \cdot b = \sum a_i b_i$.
- For $R \mathcal{C} \subset R^n$ and $D_R \subset R^n$, recall the annihilators

  $$l(D) := \{ b \in R^n : b \cdot d = 0, d \in D \},$$

  $$r(C) := \{ b \in R^n : a \cdot b = 0, a \in C \}.$$

- For all $C, D$, $l(r(C)) = C$ and $r(l(D)) = D$ iff $R$ is QF.
Role of Frobenius rings in duality

- The MacWilliams identities are true over Frobenius rings:

\[ W_C(X, Y) = \frac{1}{|r(C)|} W_{r(C)}(X + (|R| - 1)Y, X - Y). \]

- Setting \( X = Y = 1 \), yields \( |C||r(C)| = |R|^n \), for \( R \) Frobenius.

- If \( R \) is QF but not Frobenius, there exists a left ideal \( I \subset R \) with \( |I||r(I)| < |R| \).

- The MacWilliams identities (in standard form) cannot hold over a non-Frobenius ring.