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

Motivation

- 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 $\mathrm{Soc}({}_R R)$ is the left ideal generated by all the simple left ideals of R.
- Similarly, for the right socle $\mathrm{Soc}(R_R)$.
- Each $\mathrm{Soc}(R)$ is a two-sided ideal.

Finite Frobenius rings

- A finite ring R is *Frobenius* if ${}_R(R/J) \cong \mathrm{Soc}({}_RR)$ and $(R/J)_R \cong \mathrm{Soc}(R_R)$.
- 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 $\widehat{M}$ admits the structure of a right R-module via

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

- Similarly, if N is a right R-module, then $\widehat{N}$ is a left R-module.

Finite fields

- Consider a finite field $\mathbb{F}_q$.
- $\widehat{\mathbb{F}_q}$ is an $\mathbb{F}_q$-vector space.
- Since $|\widehat{\mathbb{F}_q}| = |\mathbb{F}_q|$, $\widehat{\mathbb{F}_q}$ has dimension 1, and $\widehat{\mathbb{F}_q} \cong \mathbb{F}_q$ as $\mathbb{F}_q$-vector spaces.
- The character $\theta_q = \theta_p \circ \mathrm{Tr}_{q/p}$ 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: $\rho = \theta_q \circ \mathrm{Tr}$, where Tr is the matrix trace.
- $M \cong \widehat{N}$ via $P \mapsto (Q \mapsto \rho(PQ))$.
- $N \cong \widehat{M}$ via $Q \mapsto (P \mapsto \rho(PQ))$.
- In particular, $\widehat{R} \cong R$ 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. *$\widehat{R} \cong R$ as left R-modules;*
3. *$\widehat{R} \cong R$ as right R-modules.*

- Due independently to Hirano, 1997, and Wood, 1999.

Short exact sequence

- $\widehat{\quad}$ is an exact contravariant functor on R-modules.
- A short exact sequence of left R-modules
$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$
induces a short exact sequence of right R-modules
$$0 \longrightarrow (\widehat{M}_2 : M_1) \longrightarrow \widehat{M}_2 \longrightarrow \widehat{M}_1 \longrightarrow 0.$$
- Similarly with left-right reversed.

Socles of character modules

Theorem

Let M be a finite left R-module. Then

$$\mathrm{Soc}(\widehat{M}) \cong (M/JM)\widehat{\ } .$$

- J annihilates simple modules, so that $\mathrm{Soc}(\widehat{M}) = (\widehat{M} : JM)$.
- Use $(M/JM)\widehat{\ } \cong (\widehat{M} : JM)$.

One direction

- Suppose $\widehat{R} \cong R$ as right R-modules.
- R/J is a sum of matrix rings, so $(R/J)_R \cong ({}_R(R/J))\widehat{\ }$.
- Use $M = R$ (as left R-module) from Theorem.
- Then $({}_R(R/J))\widehat{\ } \cong \mathrm{Soc}(\widehat{R}_R) \cong \mathrm{Soc}(R_R)$.
- Repeat on other side, or use Honold's theorem.

Generating characters (a)

- Let M be a finite left R-module.
- A character ρ 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 $\widehat{R}$.

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

Left generating iff right generating

Theorem

Let ρ be a character of R. Then ρ is left generating iff ρ is right generating.

- If ρ is right generating, then $\widehat{R}_R \cong R_R$, so every $\pi \in \widehat{R}$ has the form ρr 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 $\pi \in \widehat{R}$. This implies $a = 0$, and ρ 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 $\mathrm{Soc}(R)$

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

Generating characters for Soc(R)

- If R is Frobenius, then $\mathrm{Soc}({}_R R) \cong \oplus M_{\mu_i}(\mathbb{F}_{q_i})$.
- We saw earlier that $M_{\mu_i}(\mathbb{F}_{q_i})$ admits a left generating character θ_i.
- The product of the θ_i is a left generating character of $\mathrm{Soc}({}_R R)$.

Extending generating characters (a)

Theorem

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

- $0 \to \operatorname{Soc}(M) \to M \to M/\operatorname{Soc}(M) \to 0$, induces $0 \to (\widehat{M} : \operatorname{Soc}(M)) \to \widehat{M} \to \operatorname{Soc}(M)\widehat{\ } \to 0$.
- Let ρ be any extension of θ.

Extending generating characters (b)

- Claim: ρ is a left generating character of M.
- Suppose I is a left submodule of $\ker \rho$. Then

$$\mathrm{Soc}(I) \subset \mathrm{Soc}(M) \cap \ker \rho = \mathrm{Soc}(M) \cap \ker \theta.$$

- Since θ is a left generating character, $\mathrm{Soc}(I) = 0$.
- Thus, $I = 0$.

Other direction

- Suppose R is Frobenius.
- $\mathrm{Soc}({}_RR) \cong \bigoplus M_{\mu_i}(\mathbb{F}_{q_i})$ admits a left generating character θ.
- Any extension ρ of θ is a left generating character of R
- Thus $\widehat{R} \cong R$ as left R-modules.
- Any left generating character is also right generating, so $\widehat{R} \cong R$ 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. $\mathrm{Soc}(R) \cong \mathbb{F}_q$. Extend θ_q on $\mathrm{Soc}(R)$ to ρ 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

- $M_n(\mathbb{F}_q)$, $\rho = \theta_q \circ \mathrm{Tr}$.
- $M_n(R)$, where R is Frobenius. $\rho = \rho_R \circ \mathrm{Tr}$.
- $R[G]$, 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 $\mathrm{Soc}(R_i) = \mathrm{ann}(\mathfrak{m}_i)$ has dimension 1 over $\mathbb{F}_q \cong R_i/\mathfrak{m}_i$. Extend θ_q on $\mathrm{Soc}(R_i)$ to ρ_i on R_i.

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

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

we have a short exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(C, R) \longrightarrow \mathrm{Hom}_R(B, R) \longrightarrow \mathrm{Hom}_R(A, R) \longrightarrow 0.$$

Frobenius implies QF

- In general, $\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^\times) \cong \mathrm{Hom}_R(M, \widehat{R})$, via $\pi \in \widehat{M} \mapsto (m \mapsto (r \mapsto \pi(rm)))$.
- $\widehat{\ }$ is an exact functor represented by $\widehat{R}$, so $\widehat{R}$ is always injective.
- If R is Frobenius, then $R \cong \widehat{R}$. 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 ${}_R C \subset R^n$ and $D_R \subset R^n$, recall the annihilators

$$\begin{aligned} l(D) &:= \{b \in R^n : b \cdot d = 0, d \in D\}, \\ r(C) &:= \{b \in R^n : a \cdot b = 0, a \in C\}. \end{aligned}$$

- 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.