Finite Frobenius Rings and the MacWilliams Identities

Jay A. Wood

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

Algebra and Communications Seminar
University College Dublin
November 14, 2011

Finite Frobenius Rings (from last week)

- Finite ring R with 1.
- The (Jacobson) *radical* $\mathrm{Rad}(R)$ of R is the intersection of all maximal left ideals of R; $\mathrm{Rad}(R)$ is a two-sided ideal of R.
- The (left/right) *socle* $\mathrm{Soc}(R)$ of R is the ideal of R generated by all the simple left/right ideals of R.
- R is *Frobenius* if $R/\mathrm{Rad}(R) \cong \mathrm{Soc}(R)$ as one-sided modules (both left and right).

Two Useful Theorems About Finite Frobenius Rings (also, last week)

- (Honold, 2001) $R/\operatorname{Rad}(R) \cong \operatorname{Soc}({}_R R)$ as left modules iff $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R_R)$ as right modules.
- R is Frobenius iff $R \cong \widehat{R}$ as left modules iff $R \cong \widehat{R}$ as right modules (Hirano, 1997; indep. 1999).
- Corollary: R is Frobenius iff there exists a character π of R such that $\ker \pi$ contains no nonzero left (right) ideal of R. This π is a *generating character*.

Characters on a Finite Ring

- Let R be a finite ring, with 1.
- A *character* of R is a homomorphism $\pi : (R, +) \to (\mathbb{C}^\times, \cdot)$.
- The set $\widehat{R}$ of all characters of R is an (R, R)-bimodule with scalar multiplications

$$({}^r\pi)(x) = \pi(xr),$$
$$(\pi^r)(x) = \pi(rx),$$

for $\pi \in \widehat{R}$, $r, x \in R$.

Generating Characters

- For any character $\pi \in \widehat{R}$, there are two homomorphisms $R \longrightarrow \widehat{R}$:

$$r \longmapsto {}^{r}\pi,$$
$$r \longmapsto \pi^{r}.$$

  The first is left linear; the second is right linear.
- A character π is a *left (right) generating character* if the first (second) map is surjective.

Equivalent Conditions

- Remember $|\widehat{R}| = |R|$.
- A map $R \longrightarrow \widehat{R}$ is surjective iff it is injective iff it is bijective.
- The first map $r \longmapsto {}^{r}\pi$ is injective iff $\ker \pi$ contains no nonzero left ideal of R.
- The second map $r \longmapsto \pi^{r}$ is injective iff $\ker \pi$ contains no nonzero right ideal of R.

Left-Right Symmetry

- A character χ is left generating iff it is right generating.
- Suppose χ is right generating and that $Rx \subset \ker \chi$.
- $\chi(rx) = 1$ for all $r \in R$; $\chi^r(x) = 1$ for all $r \in R$.
- Thus x is annihilated by every character of R, implying $x = 0$.

Generating Characters and Frobenius Rings

- Theorem. R is Frobenius iff R admits a generating character.
- All isomorphisms below are as one-sided modules.
- Fact: $(R/\operatorname{Rad}(R))\widehat{\ } \cong \operatorname{Soc}(\widehat{R})$.
- Matrix fact: $(R/\operatorname{Rad}(R))\widehat{\ } \cong R/\operatorname{Rad}(R)$.
- If $R \cong \widehat{R}$ (existence of generating character), then $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$, and R is Frobenius.

Producing a Generating Character

- The converse remains: if R is Frobenius, how to produce a generating character?
- Start with $\mathrm{Soc}(R) \cong R/\mathrm{Rad}(R)$, which is a sum of square matrix modules.
- Suppose θ is a character of $\mathrm{Soc}(R)$ such that $\ker\theta$ contains no nonzero left submodule of $\mathrm{Soc}(R)$.
- Take any extension of θ to a character χ of R.
- Theorem: χ is a generating character of R.

Some Details

- Why does an extension exist?
- $0 \to \mathrm{Soc}(R) \to R \to R/\mathrm{Soc}(R) \to 0$ induces $0 \to (R/\mathrm{Soc}(R))\widehat{\ } \to \widehat{R} \to (\mathrm{Soc}(R))\widehat{\ } \to 0$.
- Suppose I is a left ideal with $I \subset \ker \chi$. Then $\mathrm{Soc}(I) \subset \mathrm{Soc}(R) \cap \ker \chi = \ker \theta$, because $\chi = \theta$ on $\mathrm{Soc}(R)$.
- By hypothesis on θ, $\mathrm{Soc}(I) = 0$. Thus $I = 0$.

Characters on Matrix Modules

- Let $R = M_m(\mathbb{F}_q)$ and $M = M_{m\times k}(\mathbb{F}_q)$; $q = p^e$.
- Theorem. M admits a character θ such that $\ker\theta$ contains no nonzero left R-submodule iff $m \geq k$.
- R itself has generating character: $\chi(P) = \exp(2\pi i \operatorname{Tr}_{q,p}(\operatorname{Tr} P)/p)$, where Tr is the matrix trace and $\operatorname{Tr}_{q,p} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ is the field trace, $\operatorname{Tr}_{q,p}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{e-1}}$ for $x \in \mathbb{F}_q$.
- For $m \geq k$, embed M into R and restrict χ to M.
- Failure when $m < k$ is an exercise in linear algebra.

Final Argument

- If R is Frobenius, then $\mathrm{Soc}(R) \cong R/\mathrm{Rad}(R)$ is a sum of square matrix modules.
- Each of these matrix modules admits a character with no nonzero left submodules in its kernel.
- The product of these characters is a character of $\mathrm{Soc}(R)$ with no nonzero submodules in its kernel.
- Extend this character (in any way) to a character of R, and the extension is a generating character of R

Examples

- Finite fields $\mathbb{F}_q$: $\chi(x) = \exp(2\pi i \operatorname{Tr}_{q,p}(x)/p)$.
- $\mathbb{Z}/n\mathbb{Z}$: $\chi(x) = \exp(2\pi i x/n)$.
- Galois rings (Galois extensions of $\mathbb{Z}/p^m\mathbb{Z}$). $\operatorname{Soc}(R) \cong \mathbb{F}_{p^m}$; use χ for $\mathbb{F}_{p^m}$ and extend.
- Finite chain rings (all ideals form a chain). Extend from $\operatorname{Soc}(R) \cong \mathbb{F}_q$.
- Products of Frobenius rings. Use product of the generating characters.
- Matrix rings over a Frobenius ring: $M_n(R)$. $\chi = \chi_R \circ \operatorname{Tr}$.
- Finite group rings over a Frobenius ring: $R[G]$. $\chi(\sum a_g g) = \chi_R(a_e)$, e is identity element.

MacWilliams Identities

- The MacWilliams identities relate the weight enumerator of a linear code to that of its dual code, via a linear change of variables.
- The identities date from 1962 in the doctoral dissertation of MacWilliams.
- The proof given here is modeled on a proof due to Gleason over finite fields.
- The proof uses the Poisson summation formula for the Fourier transform.

Definitions

- Let R be a finite Frobenius ring.
- A *linear code* over R of length n is a left R-submodule $C \subset R^n$.
- The *Hamming weight* $\mathrm{wt}(x) = |\{i : x_i \neq 0\}|$ for $x = (x_1, x_2, \ldots, x_n) \in R^n$.
- The *Hamming weight enumerator* of $C \subset R^n$ is

$$W_C(X, Y) = \sum_{x \in C} X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)} = \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

where A_i is the number of $x \in C$ of weight i.

Annihilators

- The *dot product* on R^n is

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \in R,$$

for $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in R^n$.

- Define the *right annihilator* of $C \subset R^n$ by

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

MacWilliams Identities over Finite Frobenius Rings

Theorem (1999)

Let R be a finite Frobenius ring. If $C \subset R^n$ is a left linear code, then the MacWilliams identities hold:

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

Characters of Finite Abelian Groups

- Let $(G, +)$ be a finite abelian group.
- A *character* π of G is a group homomorphism $\pi : (G, +) \to (\mathbb{C}^\times, \times)$, where $(\mathbb{C}^\times, \times)$ is the multiplicative group of nonzero complex numbers.
- The set $\widehat{G}$ of all characters of G is itself a finite abelian group called the *character group*.
- $|\widehat{G}| = |G|$.

Two Useful Formulas

$$\sum_{x \in G} \pi(x) = \begin{cases} |G|, & \pi = 1, \\ 0, & \pi \neq 1. \end{cases}$$

$$\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & x = 0, \\ 0, & x \neq 0. \end{cases}$$

Fourier Transform

- Given a function $f : G \longrightarrow V$, with V a complex vector space, its *Fourier transform* is a function $\hat{f} : \widehat{G} \longrightarrow V$ defined by

$$\hat{f}(\pi) = \sum_{x \in G} \pi(x) f(x), \quad \pi \in \widehat{G}.$$

- Fourier inversion:

$$f(x) = \frac{1}{|G|} \sum_{\pi \in \widehat{G}} \pi(-x) \hat{f}(\pi), \quad x \in G.$$

Poisson Summation Formula

- For a subgroup $H \subset G$, define its *annihilator* $(\widehat{G} : H) = \{\pi \in \widehat{G} : \pi(H) = 1\}$.
- $|(\widehat{G} : H)| = |G|/|H|$.
- For a subgroup $H \subset G$ and any $a \in G$,

$$\sum_{h \in H} f(a+h) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G}:H)} \pi(-a)\hat{f}(\pi).$$

- In particular, for a subgroup $H \subset G$,

$$\sum_{h \in H} f(h) = \frac{1}{|(\widehat{G} : H)|} \sum_{\pi \in (\widehat{G}:H)} \hat{f}(\pi).$$

Proof of the MacWilliams Identities (a)

- The proof follows a proof due to Gleason (1970).
- Let R be Frobenius with generating character χ.
- Let $G = R^n$, an abelian group under addition.
- Let $H = C$, a left linear code.
- Let $V = \mathbb{C}[X, Y]$, a complex vector space.
- Let $f : G \longrightarrow V$ be

$$f(x) = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}.$$

Proof of the MacWilliams Identities (b)

- By Frobenius hypothesis, every character of $G = R^n$ has the form π_a, for some $a \in R^n$, with

$$\pi_a(x) = \chi(x \cdot a), \quad x \in R^n.$$

- $\pi_a \in (\widehat{G} : H)$ if and only if $a \in r(C)$.
- $|(\widehat{G} : H)| = |r(C)|$.

Proof of the MacWilliams Identities (c)

- For $f(x) = X^{n-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$,

$$\hat{f}(\pi_a) = (X + (|R| - 1)Y)^{n-\mathrm{wt}(a)}(X - Y)^{\mathrm{wt}(a)}.$$

- This requires some manipulations and use of $\sum \pi(x)$ formulas. (Next slide.)
- Recognize $\hat{f}(\pi_a)$ as summand of $W_{r(C)}(X + (|R| - 1)Y, X - Y)$.

Idea of Manipulation

- Let $n = 1$, $f(x) = X^{1-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)}$.

$$\begin{aligned}
\hat{f}(\pi_a) &= \sum_{x \in R} \pi_a(x) X^{1-\mathrm{wt}(x)} Y^{\mathrm{wt}(x)} \\
&= X + \sum_{x \neq 0} \pi_a(x) Y \\
&= \begin{cases} X + (|R| - 1)Y, & a = 0, \\ X - Y, & a \neq 0, \end{cases} \\
&= (X + (|R| - 1)Y)^{1-\mathrm{wt}(a)} (X - Y)^{\mathrm{wt}(a)}
\end{aligned}$$

References

- These slides and other papers are available on the web: http://homepages.wmich.edu/~jwood
- Many references and generalizations (complete weight enumerators, additive codes, etc.) in the paper "Foundations of Linear Codes ... "