Finite Frobenius Rings as a Setting for Algebraic Coding Theory

Jay A. Wood

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

Hefei University of Technology, Hefei, Anhui
June 30, 2011

Acknowledgments

- I am pleased to be visiting the city of Hefei, and I thank my host, Professor Shixin Zhu, for the invitation and for his hospitality.

Two Classical Theorems of MacWilliams

- Traditionally, linear codes are defined as linear subspaces $C \subset \mathbb{F}_q^n$ over a finite field $\mathbb{F}_q$.
- Two theorems of MacWilliams, both in her 1962 Harvard doctoral dissertation, provide a foundation and an important tool for further research.
- The MacWilliams extension theorem provides the foundation for code equivalence.
- The MacWilliams identities relate the weight enumerators of a linear code and its dual code. The identities are an important tool for studying linear codes, especially self-dual codes.

Linear Codes Defined over Finite Rings

- Let R be a finite ring with 1. A *linear code* of length n defined over R is a left R-submodule $C \subset R^n$.
- There were some results on codes over rings in the 1970s, but the real breakthrough came in 1994. Hammons, Kumar, Calderbank, Sloane, and Solé showed that important duality properties of certain non-linear binary codes could be explained by linear codes defined over $\mathbb{Z}/4\mathbb{Z}$.
- Do the fundamental results of MacWilliams remain true over finite rings?

Code Equivalence

- When should two linear codes be considered the same?
- Monomial equivalence (external)
- Linear isometries (internal)
- These notions are the same over finite fields: the MacWilliams extension theorem.

Monomial equivalence

- Work over a finite ring R.
- A permutation σ of $\{1, \ldots, n\}$ and invertible elements (units) $u_1, \ldots, u_n$ in R determine a *monomial transformation* $T : R^n \longrightarrow R^n$ by

$$T(x_1, \ldots, x_n) = (x_{\sigma(1)}u_1, \ldots, x_{\sigma(n)}u_n).$$

- Two linear codes $C_1, C_2 \subset R^n$ are *monomially equivalent* if there exists a monomial transformation T such that $C_2 = T(C_1)$.

Linear Isometries

- The *Hamming weight* $\mathrm{wt}(x)$ of a vector $x = (x_1, \ldots, x_n) \in R^n$ is the number of nonzero entries in x.
- A linear isomorphism $f : C_1 \longrightarrow C_2$ between linear codes $C_1, C_2 \subset R^n$ is an *isometry* if it preserves Hamming weight: $\mathrm{wt}(f(x)) = \mathrm{wt}(x)$, for all $x \in C_1$.
- If T is a monomial transformation with $C_2 = T(C_1)$, then the restriction of T to C_1 is an isometry.
- Is the converse true? Does every linear isometry come from a monomial transformation?

MacWilliams Extension Theorem over Finite Fields

Assume C_1, C_2 are linear codes in $\mathbb{F}_q^n$. If a linear isomorphism $f : C_1 \longrightarrow C_2$ preserves Hamming weight, then f extends to a monomial transformation of $\mathbb{F}_q^n$.

- MacWilliams (1961); Bogart, Goldberg, Gordon (1978)
- Ward, Wood (1996)

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.
- Example: let $G = \mathbb{Z}/n\mathbb{Z}$ be the integers modulo n. For any $a \in \mathbb{Z}/n\mathbb{Z}$, $\pi_a(x) = \exp(2\pi iax/n)$, $x \in G$, is a character of G.
- Example: let $G = \mathbb{F}_q$. For any $a \in \mathbb{F}_q$, $\pi_a(x) = \exp(2\pi i \operatorname{Tr}(ax)/p)$, $x \in \mathbb{F}_q$, is a character of $\mathbb{F}_q$. ($\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace to the prime subfield.)

Character Group

- The set $\widehat{G}$ of all characters of G is itself a finite abelian group under pointwise multiplication of functions.
- $\widehat{G}$ is called the *character group*.
- $\widehat{G} \cong G$ (not naturally); in particular, $|\widehat{G}| = |G|$.
- $\widehat{\widehat{G}} \cong G$ (naturally).
- As elements of the vector space of all functions from G to $\mathbb{C}$, the characters are linearly independent.

Two Useful Formulas

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

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

Proof of Extension Theorem (a)

- View C_i as the image of a linear map $g_i : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, with $g_2 = f \circ g_1$.
- Component functionals $g_i = (g_{i,1}, \ldots, g_{i,n})$.
- Observe, for $x \in \mathbb{F}_q^k$:

$$\mathrm{wt}(g_i(x)) = n - \sum_{j=1}^{n} \frac{1}{q} \sum_{\pi \in \widehat{\mathbb{F}}_q} \pi(g_{i,j}(x)).$$

Proof of Extension Theorem (b)

- Denote the characters of $\mathbb{F}_q$ by π_a, $a \in \mathbb{F}_q$.
- Weight preservation yields, for all $x \in \mathbb{F}_q^k$,

$$\sum_{j=1}^{n} \sum_{a \in \mathbb{F}_q} \pi_a(g_{1,j}(x)) = \sum_{l=1}^{n} \sum_{b \in \mathbb{F}_q} \pi_b(g_{2,l}(x)).$$

- This is an equation of characters of $\mathbb{F}_q^k$.
- Use $\pi_a(x) = \pi_1(ax)$ and linear independence of characters to match up terms (with care).

Why Did this Proof Work?

- One key step was to replace $\sum_{\pi \in \widehat{\mathbb{F}}_q} \pi(g_{i,j}(x))$ with $\sum_{a \in \mathbb{F}_q} \pi_a(g_{i,j}(x))$.
- For a finite ring R, is $\widehat{R} \cong R$ (as one-sided modules)?

Finite Frobenius Rings

- 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) *socle* $\mathrm{Soc}(R)$ of R is the ideal of R generated by all the simple left ideals of R.
- R is *Frobenius* if $R/\mathrm{Rad}(R) \cong \mathrm{Soc}(R)$ as one-sided modules.

Two Useful Theorems About Finite Frobenius Rings

- (Honold, 2001) $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$ as left modules iff $R/\operatorname{Rad}(R) \cong \operatorname{Soc}(R)$ as right modules .
- R is Frobenius iff $R \cong \widehat{R}$ as left modules iff $R \cong \widehat{R}$ as right modules (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*.

Examples of Finite Frobenius Rings

- Finite fields $\mathbb{F}_q$: $\pi(x) = \exp(2\pi i \operatorname{Tr}(x)/p)$.
- $\mathbb{Z}/n\mathbb{Z}$: $\pi(x) = \exp(2\pi i x/n)$.
- Galois rings (Galois extensions of $\mathbb{Z}/p^m\mathbb{Z}$).
- Finite chain rings (all ideals form a chain).
- Products of Frobenius rings.
- Matrix rings over a Frobenius ring: $M_n(R)$.
- Finite group rings over a Frobenius ring: $R[G]$.
- $\mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$ is not Frobenius (Klemm, 1989).

MacWilliams Extension Theorem over Finite Rings

- Theorem (1999). Let R be a finite Frobenius ring. Assume C_1, C_2 are linear codes in R^n. If a linear isomorphism $f : C_1 \longrightarrow C_2$ preserves Hamming weight, then f extends to a monomial transformation of R^n.
- Because $\widehat{R} \cong R$, the same proof works. (Need some technical details to make the matching work.)

Converse of the Extension Theorem

- Theorem (2008). If R is a finite ring and every linear isometry between linear codes extends to a monomial transformation of R^n, then R is Frobenius.
- Earlier results in 2004–2005 by Dinh and López-Permouth in special cases and a general strategy proposed.
- A non-Frobenius ring has a left ideal of the form $M_{m,k}(\mathbb{F}_q)$, with $m < k$. One can build a counter-example from that.

Some Notation

- We now discuss dual codes and the MacWilliams identities, first over finite fields.
- Finite field $\mathbb{F}_q$ with q elements; q a prime power.
- Dot product on $\mathbb{F}_q^n$ (all operations in $\mathbb{F}_q$):

$$x \cdot y = \sum x_i y_i,$$

  for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.
- It is a nondegenerate, symmetric bilinear form.

Definitions

- The *Hamming weight* $\mathrm{wt}(x)$ of a vector $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is the number of nonzero entries in x.
- A *linear code* over $\mathbb{F}_q$ of *dimension* k and *length* n is a k-dimensional vector subspace $C \subset \mathbb{F}_q^n$.
- If $C \subset \mathbb{F}_q^n$ is a linear code, then the *dual code* is

$$C^{\perp} = \{y \in \mathbb{F}_q^n : x \cdot y = 0, \text{ all } x \in C\}.$$

Hamming Weight Enumerators

- Given a linear code $C \subset \mathbb{F}_q^n$, the *Hamming weight enumerator* of C is the two-variable polynomial (generating function):

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

- $W_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i$, where A_i is the number of elements of C of weight i.

"Standard Properties" of Dual Codes

1. $C^{\perp} \subset \mathbb{F}_q^n$.
2. $C^{\perp}$ is a linear code.
3. $\dim C + \dim C^{\perp} = n$; or $|C||C^{\perp}| = |\mathbb{F}_q^n|$.
4. $(C^{\perp})^{\perp} = C$.
5. The MacWilliams identities hold:

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

Ideas of Proofs

- The first four items are obvious or follow from basic linear algebra of nondegenerate forms over fields.
- There is a proof of the MacWilliams identities due to Gleason that is based on character theory and the Poisson summation formula.
- One key step is to identify $C^{\perp}$ with the character-theoretic annihilator $(\widehat{\mathbb{F}}_q^n : C) := \{\pi \in \widehat{\mathbb{F}}_q^n : \pi(C) = 1\}$.

What Happens over Finite Rings?

- Dot product on R^n (all operations in R):

$$x \cdot y = \sum x_i y_i,$$

  for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in R^n$.
- Non-degenerate, but not usually symmetric when R is non-commutative.
- Two annihilators of left submodule $C \subset R^n$:
  - $l(C) = \{y \in R^n : y \cdot x = 0, x \in C\}$ (left)
  - $r(C) = \{y \in R^n : x \cdot y = 0, x \in C\}$ (right)

Problems

- Always have $C \subset l(r(C))$ and $D \subset r(l(D))$.
- Equality may not hold, even when R is commutative.
- Equality always holding is equivalent to R being quasi-Frobenius (QF).
- QF is also equivalent to R being self-injective (injective as a module over itself).

More Problems

- Even when R is QF, one may not have $|C||r(C)|$ equal to $|R^n|$.
- Which would mean that the MacWilliams identities also fail: just set $X = Y = 1$.
- Need R to be Frobenius, especially $\widehat{R} \cong R$.

The MacWilliams Identities

- When R is Frobenius, one can identify $(\widehat{R}^n : C)$ with $r(C)$, and Gleason's proof of the MacWilliams identities goes through.
- The MacWilliams identities hold:

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

References

- These slides and other papers are available on the web: http://homepages.wmich.edu/~jwood
- Many references in the paper "Foundations of Linear Codes ... "

Thank You

- I thank again my host Professor Shixin Zhu.
- I thank you, the audience members, for your kind attention.