Linear codes over finite rings and modules:
The MacWilliams identities

Jay A. Wood

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

Coding Theory Seminar
Eastern Kentucky University
March 4, 2013
Acknowledgments

- Thanks to Edgar Martinez and Steve Szabo for inviting me to speak and for their kind hospitality.
Introduction

- The MacWilliams identities date from the 1962 doctoral dissertation of Florence Jessie MacWilliams.
- Dissertation title: Combinatorial properties of elementary abelian groups.
- Advisor: Andrew Gleason
- Title page says: Radcliffe College (the former women’s college under Harvard University)
Some basic definitions (a)

- Let $\mathbb{F}_q$ be a finite field of order $q$.
- A **linear code** of length $n$ is a linear subspace $C \subseteq \mathbb{F}_q^n$.
- The **dot product** on $\mathbb{F}_q^n$ is

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

for $x = (x_1, \ldots, x_n), \ y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$. 


Some basic definitions (b)

- The **dual code** of $C$ is
  \[ C^\perp = \{ y \in \mathbb{F}_q^n : x \cdot y = 0, \text{ for all } x \in C \}. \]

- The **Hamming weight** of $x \in \mathbb{F}_q^n$ is
  \[ \text{wt}(x) = |\{ i : x_i \neq 0 \}|, \]
  the number of nonzero entries in $x$. 

Some basic definitions (c)

- The *Hamming weight enumerator* of $C$ is the polynomial (or generating function)

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

$$= \sum_{i=0}^{n} A_i X^{n-i} Y^i,$$

where $A_i$ is the number of codewords in $C$ of Hamming weight $i$. 
The Model Theorem (MacWilliams, 1962)

Let $C$ be a linear code of length $n$ over $\mathbb{F}_q$. Then the dual code $C^\perp$ satisfies:

- $C^\perp \subseteq \mathbb{F}_q^n$;
- $C^\perp$ is a linear code of length $n$;
- $(C^\perp)^\perp = C$;
- $\dim C^\perp = n - \dim C$ (or $|C| \cdot |C^\perp| = |\mathbb{F}_q^n| = q^n$);
- (the MacWilliams identities)

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C(X + (q - 1)Y, X - Y).$$
The MacWilliams identities imply the size condition:

$$|C| \cdot |C^\perp| = |\mathbb{F}_q^n| = q^n.$$ 

Just set $X = Y = 1$. 

Size condition
Generalizations

- We will prove various generalizations of the model theorem, first for additive codes, then for linear codes defined over certain finite rings.
- While we will concentrate on the Hamming weight enumerator, there are comparable results for the complete weight enumerator and some symmetrized weight enumerators. (Prof. Heide Gluesing-Luerssen will speak more about this in her seminars in a few weeks.)
Primary tools

- The main tools to be used are:
  - characters on finite abelian groups,
  - the Fourier transform, and
  - the Poisson summation formula.

- Proving the MacWilliams identities with these tools was first done by Gleason.
Characters

- Let $A$ be a finite abelian group, written additively.
- A *character* is a group homomorphism $\pi : A \to \mathbb{C}^\times$, the multiplicative group of nonzero complex numbers. So, $\pi(a_1 + a_2) = \pi(a_1)\pi(a_2)$, $a_1, a_2 \in A$.
- The set of all characters on $A$ is denoted $\hat{A}$.
- $\hat{A}$ is an abelian group under point-wise multiplication: $(\pi_1\pi_2)(a) := \pi_1(a)\pi_2(a)$, $a \in A$. 
Example

- Let $A = \mathbb{Z}/N\mathbb{Z}$ under addition.
- For $b \in \mathbb{Z}/N\mathbb{Z}$, define
  \[
  \pi_b(a) = \exp\left(2\pi i ab/N\right), \quad a \in \mathbb{Z}/N\mathbb{Z}.
  \]

(Sorry for the overuse/abuse of $\pi$.)

- Every element of $\hat{A}$ is of the form $\pi_b$ for some $b$. 
Properties of $\hat{A}$

- $\hat{A}$ is isomorphic to $A$, but not naturally so.
- $A$ is naturally isomorphic to the double character group $(\hat{A})^\wedge$.
- $|\hat{A}| = |A|$.
- $(A_1 \times A_2)^\wedge \cong \hat{A}_1 \times \hat{A}_2$.
- As elements of $F(A, \mathbb{C}) := \{f : A \rightarrow \mathbb{C}\}$, the elements of $\hat{A}$ are linearly independent.
Let $B$ be a subgroup of $A$. Define the annihilator of $B$ in $\hat{A}$ by

$$ (\hat{A} : B) := \{ \pi \in \hat{A} : \pi(b) = 1, \text{ for all } b \in B \}. $$

$$(A : (\hat{A} : B)) = B.$$
Exact functor

- Given a short exact sequence of finite abelian groups

\[ 0 \to B \to A \to Q \to 0, \]

the character functor induces a short exact sequence

\[ 1 \to (\hat{A} : B) \to \hat{A} \to \hat{B} \to 1. \]

- In particular, \( \hat{A}/\hat{B} = \hat{Q} \cong (\hat{A} : B) \) and \( |(\hat{A} : B)| = |A|/|B|. \)
Summation formulas

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

$$\sum_{\pi \in \hat{A}} \pi(a) = \begin{cases} |A|, & a = 0, \\ 0, & a \neq 0. \end{cases}$$
Function spaces

- Let $A$ be a finite abelian group and $V$ a complex vector space.
- Let $F(A, V) = \{ f : A \to V \}$ be the set of all functions from $A$ to $V$.
- $F(A, V)$ is a complex vector space under pointwise addition and scalar multiplication of functions.
- If $V$ is finite-dimensional, $\dim F(A, V) = |A| \cdot \dim V$. 
Fourier transform

Define the *Fourier transform* $\hat{\cdot} : F(A, V) \to F(\hat{A}, V)$:

$$\hat{f}(\pi) = \sum_{a \in A} \pi(a)f(a),$$

for $f \in F(A, V)$, $\pi \in \hat{A}$.
Inverse transform

The Fourier transform is invertible:

\[ f(a) = \frac{1}{|A|} \sum_{\pi \in \hat{A}} \pi(-a) \hat{f}(\pi). \]

Expand and use summation formulas.
Poisson summation formula

Let $B$ be a subgroup of $A$, a finite abelian group, and let $f : A \rightarrow V$. Then for any $a \in A$,

$$\sum_{b \in B} f(a + b) = \frac{1}{|\hat{A} : B|} \sum_{\pi \in \hat{A} : B} \pi(-a) \hat{f}(\pi).$$

If $a = 0$, then

$$\sum_{b \in B} f(b) = \frac{1}{|\hat{A} : B|} \sum_{\pi \in \hat{A} : B} \hat{f}(\pi).$$
Additive codes

- Let $A$ be a finite abelian group.
- An additive code $C$ of length $n$ over $A$ is a subgroup $C \subseteq A^n$.
- The MacWilliams identities for additive codes are due to Delsarte, 1972.
Model theorem for additive codes $C \subset A^n$

- $(\widehat{A^n} : C) \subset \widehat{A^n}$.
- $(\widehat{A^n} : C)$ is an additive code of length $n$.
- $(A^n : (\widehat{A^n} : C)) = C$.
- $|C| \cdot |(\widehat{A^n} : C)| = |A^n|$.
- (the MacWilliams identities)

$$W_{(\widehat{A^n} : C)}(X, Y) = \frac{1}{|C|} W_C(X + (|A| - 1)Y, X - Y).$$
Proof (a)

- Apply the Poisson summation formula with group $A^n$, subgroup $C$, and $V = \mathbb{C}[X, Y]$, the polynomial ring.
- Use $f : A^n \to \mathbb{C}[X, Y]$, $f(a) = X^{n-\operatorname{wt}(a)} Y^{\operatorname{wt}(a)}$.
- What is $\hat{f}$?
Proof (b)

To illustrate the argument, case $n = 1$:

$$\hat{f}(\pi) = \sum_{a \in A} \pi(a) X^{1-\text{wt}(a)} Y^{\text{wt}(a)}$$

$$= X + \sum_{a \neq 0} \pi(a) Y$$

$$= \begin{cases} 
  X + (|A| - 1) Y, & \pi = 1, \\
  X - Y, & \pi \neq 1,
\end{cases}$$

$$= (X + (|A| - 1) Y)^{1-\text{wt}(\pi)} (X - Y)^{\text{wt}(\pi)}$$

MacWilliams identities

March 4, 2013 24 / 39
Drawbacks

- The model theorem is very general, but it has the drawback that the dual code $(\hat{A}^n : C)$ lives in $\hat{A}^n$ not $A^n$.
- Although $\hat{A} \cong A$, there is no natural identification.
- Also, it has been customary to define $C^\perp$ via a dot product.
- We will explore these drawbacks for linear codes over finite rings.
Let $R$ be a finite associative ring with 1 (non-commutative is allowed).

A (left) linear code of length $n$ over $R$ is a left $R$-submodule $C \subset R^n$.

Hamming weight $\text{wt}(r)$ as before: $\text{wt}(0) = 0$, $\text{wt}(r) = 1$ for $r \neq 0$. Add up over vectors.

Dot product on $R^n$ as usual: $x \cdot y = \sum x_i y_i \in R$. 

Linear codes over finite rings
The character group $\hat{R}$ of a finite ring $R$ inherits an $R, R$-bimodule structure:

$$(s \pi)(r) := \pi(rs),$$

$$(\pi^s)(r) := \pi(sr),$$

for $r, s \in R, \pi \in \hat{R}$.

For a left $R$-submodule $C \subset R^n$, $(\hat{R}^n : C) \subset \hat{R}^n$ is a right $R$-submodule.
Drawbacks revisited

- Are there finite rings $R$ for which $\hat{R} \cong R$ as (say) one-sided $R$-modules?
- For $C \subset R^n$, what is the relationship between $(\hat{R}^n : C)$ and the two module-theoretic annihilators

\[ l(C) := \{ y \in R^n : y \cdot x = 0, \text{ for all } x \in C \} , \]
\[ r(C) := \{ y \in R^n : x \cdot y = 0, \text{ for all } x \in C \} . \]
It turns out that there is a class of finite rings, the finite *Frobenius* rings that are characterized by the property that $\hat{R} \cong R$ as one-sided $R$-modules.

The definition of a Frobenius ring is that $R/\text{Rad}(R) \cong \text{Soc}(R)$ as one-sided $R$-modules. (More on this at a later time.)

In addition, over a finite Frobenius ring the various annihilators: $(\hat{R}^n : C)$, $l(C)$, and $r(C)$, are all isomorphic as abelian groups.
Model theorem over finite Frobenius rings

- $l(C), r(C) \subset R^n$.
- $l(C), r(C)$ are (left/right, right) linear codes of length $n$.
- $l(r(C)) = C$.
- $|C| \cdot |l(C)| = |C| \cdot |r(C)| = |A^n|$.
- (the MacWilliams identities)

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

(Same for $r(C)$.)
Can we do better?

- Over finite Frobenius rings, we have everything we want in a model theorem.
- Do we really need the ring to be Frobenius?
- The double dual property \( l(r(C)) = C \) (plus its counterpart \( r(l(D)) = D \) for right linear codes \( D \subset R^n \)) actually characterizes quasi-Frobenius rings.
- If a ring \( R \) is quasi-Frobenius, but not Frobenius, there exist one-sided ideals \( R_I, J_R \subset R \) which violate the size condition: \( |I| \cdot |r(I)| < |R| \) and \( |J| \cdot |l(J)| < |R| \).
Linear codes over modules

- Let $R$ be a finite ring with 1 and $A$ be a finite left $R$-module.
- A left $R$-linear code of length $n$ over $A$ is a left $R$-submodule $C \subset A^n$.
- Due to Nechaev and collaborators and developed further by Greferath, Nechaev, and Wisbauer.
- The annihilator $(\hat{A}^n : C)$ is a right $R$-submodule of $\hat{A}^n$. 
Model theorem for codes over modules

- Mimics the additive code case.
- \((\hat{A}^n : C) \subset \hat{A}^n\).
- \((\hat{A}^n : C)\) is right \(R\)-linear code of length \(n\) over \(\hat{A}\).
- \((A^n : (\hat{A}^n : C)) = C\).
- \(|C| \cdot |(\hat{A}^n : C)| = |A^n|\).
- (the MacWilliams identities)

\[
W_{(\hat{A}^n:C)}(X, Y) = \frac{1}{|C|} W_C(X + (|A| - 1)Y, X - Y).
\]
How to make sense of self-dual codes?

- Over fields, a self-dual code satisfies $C^\perp = C$.
- Its weight enumerator is invariant under the MacWilliams identities.
- If $C \subset A^n$ is a left linear code, then the dual code is a right linear code in $\hat{A}^n$. How can we get self-dual codes?
- Follow ideas of Nebe, Rains, and Sloane.
Anti-isomorphisms

- Let $R$ be a finite ring with 1.
- An anti-isomorphism $\varepsilon : R \rightarrow R$ is an isomorphism of additive groups that satisfies $\varepsilon(rs) = \varepsilon(s)\varepsilon(r)$, $r, s \in R$. 
Modules: left to right

- Given a ring $R$ with anti-isomorphism $\varepsilon$.
- Let $M$ be a left $R$-module.
- Define $\varepsilon(M)$ to be the same abelian group as $M$, with right scalar multiplication defined by $mr := \varepsilon(r)m$, $r \in R$, $m \in M$, using the left scalar multiplication on $M$. Then $\varepsilon(M)$ is a right $R$-module.
- Similarly for right $R$-modules.
Making sense of self-dual codes

- Suppose $R$ is a finite ring with 1, equipped with an anti-isomorphism $\varepsilon$.
- Suppose the alphabet $A$ (a left $R$-module) admits an isomorphism $\psi : \varepsilon(A) \rightarrow \hat{A}$.
- For a left linear code $C \subset A^n$, define $C^\perp := \psi^{-1}(\hat{A}^n : C)$.
- With one additional technical assumption, the model theorem holds in this context too.
Special case

- Suppose the alphabet $A$ is the ring $R$ itself: $A = R$.
- Suppose $R$ admits an anti-isomorphism $\varepsilon$.
- Then an isomorphism $\psi : \varepsilon(R) \to \hat{R}$ exists if and only if $R$ is Frobenius.
Questions

Which finite rings admit anti-isomorphisms $\varepsilon$?
Which Frobenius rings?

Which modules over such rings admit isomorphisms $\psi : \varepsilon(A) \to \hat{A}$?

Some examples are known: group algebras; $H^*(\mathbb{R}P^{4k+3}; \mathbb{F}_2)$ over the subalgebra $A(1)$ of the mod 2 Steenrod algebra; some others.

Our ignorance is vast.