Foundational Aspects of Linear Codes: 
1. Characters and Frobenius rings

Jay A. Wood

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

On the Algebraic and Geometric Classifications of Projective Varieties
University of Messina
June 20, 2016
Acknowledgments

- Thanks to Gaetana Restuccia and Mustapha Lahyane for organizing the workshop, for inviting me to speak, and for their kind hospitality.
0. Overview of lectures

- Basic terminology
- Duality and weight enumerators
- Extension problem
Basic vocabulary

- Let $R$ be a finite associative ring with 1, not necessarily commutative.
- Let $A$ be a finite unital left $R$-module; $A$ will be the alphabet.
- A left $R$-linear code over $A$ of length $n$ is a left $R$-submodule $C \subseteq A^n$.
- Right linear codes are defined similarly.
- Module alphabets are due to Nechaev and collaborators, 1999.
Weights

- A **weight** on $A$ is any function $w : A \rightarrow \mathbb{C}$ with $w(0) = 0$.
- Extend to $w : A^n \rightarrow \mathbb{C}$ by

$$w(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} w(a_i).$$

- Restrict $w$ to linear code $C \subseteq A^n$. 
Examples

- For any alphabet $A$, define the **Hamming weight**: 
  $$\text{wt}(a) = \begin{cases} 
  1, & a \neq 0, \\
  0, & a = 0. 
  \end{cases}$$

- **Lee weight**: for $R = A = \mathbb{Z}/N\mathbb{Z}$, restrict $-N/2 < a \leq N/2$ and set $w_L(a) = |a|$ (ordinary absolute value).

- Homogeneous weight (later).
For a linear code $C \subseteq A^n$, define the **Hamming weight enumerator** of $C$ by

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

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

Hamming weight enumerator
Dual codes

- Let $A = R$ itself. Define the **dot product** on $R^n$ by
  \[
  x \cdot y = \sum_{i=1}^{n} x_i y_i,
  \]
  where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.

- For a linear code $C \subseteq R^n$, define **annihilators**
  \[
  l(C) = \{ y \in R^n : y \cdot C = 0 \}, \\
  r(C) = \{ y \in R^n : C \cdot y = 0 \}.
  \]
Questions

- Are the annihilators well-behaved?
- Is there a nice relationship between the Hamming weight enumerators of $C$ and its annihilators?
  - Yes: the MacWilliams identities.
- We will discuss these questions in the second lecture.
Isometries

- Let $C_1, C_2 \subseteq A^n$ be two linear codes. An $R$-linear isomorphism $f : C_1 \rightarrow C_2$ is a linear isometry with respect to a weight $w$ if $w(xf) = w(x)$ for all $x \in C_1$.

- I will usually write homomorphisms of left modules $M$ on the right side, so that $(rx)f = r(xf)$ for $r \in R$, $x \in M$. 
Symmetry groups

- Suppose the alphabet $A$ has weight $w$. Define symmetry groups by

$$G_{lt} = \{ u \in \mathcal{U}(R) : w(ua) = w(a), a \in A \},$$
$$G_{rt} = \{ \phi \in GL_R(A) : w(a\phi) = w(a), a \in A \}.$$

- Here, $\mathcal{U}(R)$ is the group of units of $R$, and $GL_R(A)$ is the group of invertible $R$-linear homomorphisms of $A$ to itself.
Monomial transformations

Let $G \subseteq GL_R(A)$ be a subgroup. A $G$-monomial transformation of $A^n$ is an invertible $R$-linear homomorphism $T : A^n \rightarrow A^n$ of the form

$$(a_1, a_2, \ldots, a_n) T = (a_{\sigma(1)}\phi_1, a_{\sigma(2)}\phi_2, \ldots, a_{\sigma(n)}\phi_n),$$

for $(a_1, a_2, \ldots, a_n) \in A^n$.

Here, $\sigma$ is a permutation of $\{1, 2, \ldots, n\}$ and $\phi_i \in G$ for $i = 1, 2, \ldots, n$. 
Monomial transformations are isometries

- Easy: $G_{rt}$-monomial transformations are isometries of $A^n$ with respect to the weight $w$.
- Let $C_1 \subseteq A^n$ be a linear code and let $T$ be a $G_{rt}$-monomial transformation of $A^n$. Set $C_2 = C_1 T$. Then the restriction of $T$ to $C_1$ is a linear isometry from $C_1$ to $C_2$.
- Is the converse true? That is, does every linear isometry between linear codes extend to a $G_{rt}$-monomial transformation? Call this the Extension Problem.
- More on this in the third and fourth lecture and in the research seminar.
1. Characters and Frobenius rings

- Definitions
- Properties
- Fourier transform
- Character modules
- Generating characters
Definitions

- Let $A$ be a finite abelian group (additive notation); $A$ will be a module later.
- A **character** of $A$ is a group homomorphism
  \[ \pi : A \to \mathbb{C}^\times, \]
  where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers.
- The set $\hat{A}$ of all characters of $A$ is a multiplicative abelian group under pointwise multiplication.
- Additive version: $\hat{A} \cong \text{Hom}_\mathbb{Z}(A, \mathbb{Q}/\mathbb{Z})$. 
Duality functor

- Pontryagin duality: $A \mapsto \hat{A}$
- $\hat{A} \cong A$, naturally.
- $\hat{A} \cong A$, but not naturally.
- $(A \times B) \hat{} \cong \hat{A} \times \hat{B}$.
- Exact contravariant functor: exact sequence

\[
0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0
\]

induces exact sequence

\[
0 \rightarrow \hat{A}_3 \rightarrow \hat{A}_2 \rightarrow \hat{A}_1 \rightarrow 0.
\]
Summation formulas

For $a \in A$,

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

For $\pi \in \hat{A}$,

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

- Let $F(A, \mathbb{C}) = \{ f : A \rightarrow \mathbb{C} \}$, a complex vector space of dimension $|A|$.
- The elements of $\hat{A}$ form a basis for $F(A, \mathbb{C})$.
- In particular, characters are linearly independent over $\mathbb{C}$.
- Need multiplicative form of characters for linear independence and for the summation formulas.
Annihilators

- Let $B \subseteq A$ be any subgroup.
- Define the annihilator $(\hat{A} : B)$:
  \[
  (\hat{A} : B) = \{ \pi \in \hat{A} : \pi(B) = 1 \}.
  \]
- $(\hat{A} : B) \cong (A/B)^\hat{\cdot}$.
- $|B| \cdot |(\hat{A} : B)| = |A|$.
- Double annihilator: $(A : (\hat{A} : B)) = B$. 
Fourier transform

> Given a function $f : A \to V$, $V$ a complex vector space. Define its **Fourier transform** $\hat{f} : \hat{A} \to V$ by

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

> $\hat{F} : F(A, V) \to F(\hat{A}, V)$.

> Invert:

$$f(a) = \frac{1}{|A|} \sum_{\pi \in \hat{A}} \pi(-a)\hat{f}(\pi), \quad a \in A.$$
Let $B$ be any subgroup of $A$, and let $f : A \to V$. 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

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

- Now suppose $R$ is a finite ring with 1 and $A$ is a finite unital left $R$-module.
- Then $\hat{A}$ becomes a right $R$-module by
  \[ \pi^r(a) = \pi(ra), \quad a \in A. \]
  \[ (r \pi(a) = \pi(ar) \text{ for right to left case.}) \]
- $\hat{A}$ is an exact contravariant functor of $R$-modules.
- For left $R$-submodule $B \subseteq A$, $(\hat{A} : B)$ is a right $R$-submodule of $\hat{A}$. 
Top-bottom duality

- An $R$-module is **simple** if it has no nontrivial proper submodules.
- The Jacobson **radical** $\text{Rad}(R)$ is the intersection of all maximal left ideals of $R$; a two-sided ideal.
- For a left $R$-module $A$, the **socle** $\text{Soc}(A)$ is the left $R$-submodule generated by all simple left $R$-submodules of $A$.
- $(A / \text{Rad}(R)A) \hat{\cong} \text{Soc}(\hat{A})$
Generating characters

- Left $R$-module $A$.
- A character $\rho \in \hat{A}$ is a **generating character** if $\ker \rho$ contains no nonzero left $R$-submodules.
- Not every module admits a generating character.
Embedding

- Suppose $\rho$ is a generating character for $A$.
- Define $\alpha : A \rightarrow \hat{\mathbb{K}}$ by $(a\alpha)(r) = \rho(ra)$, $a \in A$, $r \in R$.
- $\alpha$ is an injective homomorphism of left $R$-modules.
- Dual map $R \rightarrow \hat{\mathbb{A}}$, $r \mapsto \rho^r$, is surjective homomorphism of right $R$-modules.
- $\rho$ generates $\hat{\mathbb{A}}$.
- Conversely: if $\hat{\mathbb{A}}$ is cyclic, or $A$ embeds in $\hat{\mathbb{K}}$, then $A$ has a generating character.
Frobenius rings

- Recall: $|\hat{R}| = |R|$. 
- Consider $R$ as a module over itself. 
- If $R$ has a generating character, then $\hat{R} \cong R$ as left and as right $R$-modules.
- $\text{Soc}(R) = \text{Soc}(\hat{R}) \cong (R/\text{Rad}(R)) \hat{\cong} \cong R/\text{Rad}(R)$.
- Such a finite ring is a **Frobenius** ring.
Some examples of generating characters

- \( \mathbb{Z}/N\mathbb{Z} \) admits \( \theta_N(a) = \exp(\frac{2\pi i a}{N}), \ a \in \mathbb{Z}/N\mathbb{Z} \).
- \( \exp \) is the standard complex exponential function.
- \( \mathbb{F}_q \) admits \( \theta_q(a) = \theta_p(\text{Tr}_{q \rightarrow p}(a)), \ a \in \mathbb{F}_q \).
- \( R = M_{k \times k}(\mathbb{F}_q) \) admits \( \rho(P) = \theta_q(\text{Tr} P), \ P \in R \).
- \( A = M_{k \times \ell}(\mathbb{F}_q), \ k > \ell, \) admits \( \rho|_A \).
- When \( k < \ell \), \( A \) does not admit a generating character. \( \pi_Q(P) = \theta_q(\text{Tr}(PQ)), \) for \( Q \in M_{\ell \times k}(\mathbb{F}_q) \). Find nonzero \( X \in M_{k \times \ell}(\mathbb{F}_q) \) with \( XQ = 0 \), as \( k < \ell \). Then \( RX \subseteq \ker \pi_Q \).
Cyclic socle

- Suppose $A$ has cyclic socle $\text{Soc}(A)$.
- $\text{Soc}(A)$ is a sum of matrix modules with $k \geq \ell$.
- $\text{Soc}(A)$ admits a generating character: multiply together those from matrix modules.
- Extension exists, by exactness. Any extension is a generating character for $A$.

Theorem

$R$-module $A$ has a generating character if and only if $\text{Soc}(A)$ is cyclic.