Linear Codes over Finite Rings and Modules

Jay A. Wood

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

Central China Normal University
Wuhan, Hubei
May 2, 2018
2. Representations and characters

- Representations of finite groups
- Irreducible representations
- Schur’s Lemma
- Case of finite abelian groups
- Additive codes and their dual codes
- Linear codes over finite modules
Representations and characters

Motivation (i)

- First lecture: the dual code is important.
- For linear codes defined over a finite field, the dual code was defined using the dot product:
  \[ C^\perp = \{ y \in \mathbb{F}^n : C \cdot y = 0 \} \].
- I want to generalize this to additive codes: subgroups of \( A^n \), where \( A \) is a finite abelian group.
- How to define \( C^\perp \)? There is no dot product!
- We will define the dual abstractly.
Motivation (ii)

- The abstract dual code will be defined in terms of **characters** on a finite abelian group.
- Two important techniques in these lectures are characters and the **Fourier transform** for complex-valued functions on a finite abelian group.
- I first want to discuss these ideas in the context of the **representation theory** of finite groups.
Representations

- Let $G$ be a finite group, and let $k$ be a field.
- A representation of $G$ over $k$ consists of a nonzero (finite-dimensional) $k$-vector space $V$ and a homomorphism $\rho : G \to \text{GL}_k(V)$.
- $\text{GL}_k(V)$ is the group of all invertible $k$-linear transformations from $V$ to itself.
- By choosing an ordered basis of $V$, $\text{GL}_k(V)$ is isomorphic to $\text{GL}(n, k)$, the group of invertible $n \times n$ matrices over $k$. Here, $n = \dim_k V$. 

Character of a representation

- Suppose $\rho : G \to \text{GL}_k(V)$ is a representation.
- Define the **character** $\chi$ of $\rho$ to be $\chi : G \to k$, $\chi(g) = \text{Tr} \, \rho(g)$.
- Here Tr is the **trace** of the linear transformation $\rho(g)$ (the sum of the diagonal terms of a matrix representing $\rho(g)$).
- $\chi$ is a **class function**: $\chi(aga^{-1}) = \chi(g), \ a, g \in G$.
- Note: if $\dim_k V = 1$, then $\chi = \rho$. 
Subrepresentations

- Given a representation $\rho : G \to \text{GL}_k(V)$, a **subrepresentation** is a vector subspace $W \subseteq V$ that is invariant under the representation $\rho$.

- That is, $\rho(g)W \subseteq W$, all $g \in G$.

- Then, $\rho|_W : G \to \text{GL}_k(W)$.

- A representation $\rho : G \to \text{GL}_k(V)$ is **irreducible** if the only invariant subspaces are 0 and $V$: no non-trivial subrepresentations.
Indecomposable representations

- A representation \( \rho : G \to \text{GL}_k(V) \) is **decomposable** if there exist two nonzero *invariant* subspaces \( W_1, W_2 \subseteq V \) such that \( V = W_1 \oplus W_2 \).
- A representation \( \rho : G \to \text{GL}_k(V) \) is **indecomposable** if it is not decomposable.
- If \( \rho \) is irreducible, then \( \rho \) is indecomposable.
- The converse is not true, in general.
- Converse is true when the characteristic of \( k \) does not divide the order of \( G \) (Maschke’s Theorem).
Intertwining maps

- Suppose $\rho_1 : G \to \text{GL}_k(V_1)$ and $\rho_2 : G \to \text{GL}_k(V_2)$ are representations of $G$.

- A linear transformation $\phi : V_1 \to V_2$ intertwines $\rho_1$ and $\rho_2$ if

\[
\phi \circ \rho_1(g) = \rho_2(g) \circ \phi, \quad g \in G.
\]

$$
\begin{array}{ccc}
V_1 & \xrightarrow{\rho_1(g)} & V_1 \\
\downarrow \phi & & \downarrow \phi \\
V_2 & \xrightarrow{\rho_2(g)} & V_2
\end{array}
$$
Equivalent representations

Two representations $\rho_1 : G \to \text{GL}_k(V_1)$ and $\rho_2 : G \to \text{GL}_k(V_2)$ are equivalent if there exists a linear isomorphism $\phi : V_1 \to V_2$ that intertwines $\rho_1$ and $\rho_2$. 
Intertwining maps for irreducible representations

- Now suppose that both $\rho_1 : G \to \text{GL}_k(V_1)$ and $\rho_2 : G \to \text{GL}_k(V_2)$ are irreducible.
- If $\phi : V_1 \to V_2$ intertwines, then $\phi$ is either an isomorphism or the zero map.
- $\ker \phi \subseteq V_1$ is an invariant subspace: 0 or $V_1$.
- $\phi(V_1) \subseteq V_2$ is an invariant subspace: 0 or $V_2$. 
Schur’s Lemma (i)

- Given $\rho : G \rightarrow \text{GL}_k(V)$, define

$$I(V, V) = \{\phi : V \rightarrow V : \phi \text{ intertwines } \rho\}.$$ 

- $I(V, V)$ is a $k$-algebra: the **intertwining algebra**.
- $I(V, V)$ always contains $k \cong k \cdot \text{id}_V$.
- If $\rho$ is irreducible, then $I(V, V)$ is a division algebra.
- Any nonzero $\phi$ is an isomorphism.
Schur’s Lemma (ii)

- Suppose $\rho : G \to \text{GL}_k(V)$ is irreducible and $k$ is algebraically closed.
- Then $I(V, V) = k \cdot \text{id}_V$.
- Take any $\phi \in I(V, V)$, and let $\alpha \in k$ be an eigenvalue of $\phi$. Then $\phi' = \phi - \alpha \cdot \text{id}_V \in I(V, V)$.
- $\phi'$ is not an isomorphism, so $\phi' = 0$. Thus $\phi = \alpha \cdot \text{id}_V$. 
Abelian case (i)

- Assume $A$ is a finite abelian group.
- Let $\rho : A \rightarrow \text{GL}_k(V)$ be a representation.
- Fix $a \in A$, and let $\phi = \rho(a) : V \rightarrow V$.
- Then $\phi$ intertwines $\rho : A$ is abelian.
Abelian case (ii)

- Any irreducible representation of a finite abelian group over an algebraically closed field has dimension 1.
- Every $\rho(a)$, $a \in A$, is a scalar multiple of $\text{id}_V$.
- Every linear subspace of $V$ is invariant.
- Irreducible: $\dim_k V = 1$.
- Every irreducible representation of a finite abelian group over $\mathbb{C}$ equals its character.
Example (i)

1. The cyclic group $C_3$ acts on $V = k^3$ by cyclic permutation of entries:

\[
(a, b, c) \rightarrow (b, c, a) \rightarrow (c, a, b) \rightarrow (a, b, c).
\]

2. $W_2 = \{(a, b, c) : a + b + c = 0\}$ and $W_1 = \{(a, a, a) : a \in k\}$ are invariant subspaces.
Example (ii)

- If the characteristic of $k$ is 3, then $W_1 \subset W_2 \subset V$ with no invariant complements; $W_2$ and $V$ are indecomposable, but not irreducible.

- If the characteristic of $k$ is not 3, then $V = W_1 \oplus W_2$.

- For $(a, b, c) \in V$, set $m = (a + b + c)/3$. Then $(a, b, c) = (m, m, m) + (a - m, b - m, c - m) \in W_1 + W_2$. 


Example (iii)

- If $k$ also contains all third roots of unity $\{1, \zeta, \zeta^2\}$, then $W_2$ decomposes into

$$W_2 = \{(a, \zeta a, \zeta^2 a)\} \oplus \{(a, \zeta^2 a, \zeta a)\}.$$

- If $(a, b, c) \in W_2$, so that $a + b + c = 0$, then set

$$x = (a + \zeta^2 b + \zeta c)/3 \text{ and } y = (a + \zeta b + \zeta^2 c)/3.$$

- Then $(a, b, c) = (x, \zeta x, \zeta^2 x) + (y, \zeta^2 y, \zeta y)$. 
Characters of finite abelian groups

- Having discussed irreducible complex representations of finite abelian groups, we now discuss characters in a slightly different way.
- From here on, $A$ is a finite abelian group, written additively.
- A **character** of $A$ is a group homomorphism
  \[\pi : A \rightarrow \mathbb{C}^\times,\]
  where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers: $\pi(a + b) = \pi(a)\pi(b)$, $a, b \in A$. 
Character group

- The set $\hat{A}$ of all characters of $A$ is a multiplicative abelian group under pointwise multiplication.

\[(\pi \psi)(a) = \pi(a)\psi(a), \quad a \in A, \quad \pi, \psi \in \hat{A}.\]

- Every character of $\mathbb{Z}/k\mathbb{Z}$ has the form $\rho_b(a) = \exp(2\pi iab/k)$, $a \in \mathbb{Z}/k\mathbb{Z}$, for some $b \in \mathbb{Z}/k\mathbb{Z}$. [Consider where $a = 1$ is sent.]

- Thus, $(\mathbb{Z}/k\mathbb{Z})\hat{\sim} \mathbb{Z}/k\mathbb{Z}$, via $\rho_b \longleftrightarrow b$. 
Additive form of character group

- Original, multiplicative form: \( \hat{A} = \text{Hom}_\mathbb{Z}(A, \mathbb{C}^\times) \).
- Additive version: \( \hat{A} \cong \text{Hom}_\mathbb{Z}(A, \mathbb{Q}/\mathbb{Z}) \).
- \( \varrho \in \text{Hom}_\mathbb{Z}(A, \mathbb{Q}/\mathbb{Z}) \) corresponds to \( \rho \in \text{Hom}_\mathbb{Z}(A, \mathbb{C}^\times) \) by \( \rho(a) = \exp(2\pi i \varrho(a)) \).
- \( \rho(a + b) = \rho(a)\rho(b) \), while \( \varrho(a + b) = \varrho(a) + \varrho(b) \).
Duality functor

- Pontryagin duality: \( A \mapsto \hat{A} \)
- Exact contravariant functor:

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

induces

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

- \( \hat{A} \cong A \), but not naturally. (Uses fundamental theorem of finitely generated abelian groups.)

- \( \hat{A} \cong A \), naturally: \( a \mapsto (\pi \mapsto \pi(a)) \).
- \( (A \times B) \hat{=} \cong \hat{A} \times \hat{B} \).
Let $B \subseteq A$ be any subgroup.

Define the **annihilator** $(\hat{A} : B)$:

$$(\hat{A} : B) = \{\rho \in \hat{A} : \rho(B) = 1\} = \{\varrho \in \hat{A} : \varrho(B) = 0\}.$$ 

$(\hat{A} : B) \cong (A/B)^\hat{}$.

$|B| \cdot |(\hat{A} : B)| = |A|$.

Double annihilator: $(A : (\hat{A} : B)) = B$. 


Additive codes and their duals

- An **additive code** of length $n$ over $A$ is an additive subgroup $C \subseteq A^n$.
- View $C \subseteq A^n$ as an example of “$B \subseteq A$”.
- The **dual code** of $C \subseteq A^n$ is the annihilator $(\hat{A}^n : C) \subseteq \hat{A}^n$. 

Good duality properties

- Given an additive code $C \subseteq A^n$.
- Dual $(\hat{A}^n : C) \subseteq \hat{A}^n$ is an additive code over $\hat{A}$.
- Double annihilator: $(A^n : (\hat{A}^n : C)) = C$.
- Size: $|C| \cdot |(\hat{A}^n : C)| = |A^n|$.
- The MacWilliams identities. (Next lecture.)
Adding structure: linear codes over modules

- Let $R$ be a finite ring with 1, and let $A$ be a finite unital left $R$-module. **Unital**: $1 \cdot a = a$, $a \in A$.
- $\hat{A}$ inherits the structure of a right $R$-module: $(\varrho r)(a) = \varrho(ra)$, $\varrho \in \hat{A}$, $r \in R$, $a \in A$.
- Multiplicative form: $\rho^r(a) = \rho(ra)$.
- Similarly, if $M$ is a finite right $R$-module, then $\hat{M}$ is a left $R$-module.
Suppose $B \subseteq A$ is a left $R$-submodule.
Then $(\hat{A} : B)$ is a right $R$-submodule of $\hat{A}$.
For $\varrho \in (\hat{A} : B)$, $(\varrho r)(B) = \varrho(rB) \subseteq \varrho(B) = 0$.
Other features of $(\hat{A} : B)$ still hold.
Good duality properties

- Given left $R$-linear code $C \subseteq A^n$.
- Dual $(\hat{A}^n : C) \subseteq \hat{A}^n$ is a right $R$-linear code over $\hat{A}$.
- Double annihilator: $(A^n : (\hat{A}^n : C)) = C$.
- Size: $|C| \cdot |(\hat{A}^n : C)| = |A^n|$.
- The MacWilliams identities. (Lecture 3.)
For linear codes over finite fields, the linear code $C$ and its dual code $C^\perp$ were both contained in $\mathbb{F}^n$.

Is it possible to identify $(\widehat{A}^n : C)$ with a submodule of $A^n$?

That will be a topic for Lectures 3 and 4.