Character-Theoretic Tools for Studying Linear Codes over Rings and Modules

Jay A. Wood

Department of Mathematics
Western Michigan University
http://sites.google.com/a/wmich.edu/jaywood

Algebraic Methods in Coding Theory
CIMPA School
Ubatuba, Brazil
July 3, 2017

Acknowledgments

- Thanks to CIMPA, our other sponsors, and the organizing committees for organizing this school, for inviting me to speak, and for their hospitality.

1. Linear Codes over Finite Fields

- Definitions
- Error correction and the Hamming weight
- Syndrome decoding and the dual code
- Equivalence of codes

Objectives

- Introduce some the language of coding theory over finite fields.
- Introduce, with examples, some of the mathematical problems that will be discussed in later lectures.

Basic vocabulary

- Let $\mathbb{F}$ be a finite field.
- A **linear code** over $\mathbb{F}$ of **length** n is a vector subspace $C \subseteq \mathbb{F}^n$.
- Let $k = \dim_{\mathbb{F}} C$ be the dimension of C over $\mathbb{F}$.
- We say that C is a linear $[n, k]$-code.
- The elements of C are called **codewords**.

Encoding

- A linear code is often presented by an encoding map, represented by a **generator matrix** G.
- G will be a matrix of size $k \times n$ of rank k
- G defines a linear transformation $\mathbb{F}^k \to \mathbb{F}^n$, $x \mapsto xG$, with inputs written on the left. (Why? Tradition!)
- $\mathbb{F}^k$ is the **information space**. The linear code C is the image of the encoding map (row space of G).
- There are many possible encoding maps: use PG, P invertible $k \times k$.

Errors in transmission

- Error-correcting codes are designed to detect and correct errors in transmission in communication channels.

$$\mathbb{F}^k \xrightarrow[\text{encode}]{} \mathbb{F}^n \xrightarrow[\text{transmit}]{+\text{noise}} \mathbb{F}^n \xrightarrow[\text{decode}]{} \mathbb{F}^n \xrightarrow[\text{unencode}]{} \mathbb{F}^k$$

- The code adds redundancy which, if done properly, may allow errors to be corrected ("decoding").

Parity check matrix

- Given a linear $[n, k]$-code C, we can think of C as the solution space of a system of linear equations.
- A **parity check matrix** for C is an $(n-k) \times n$ matrix H of rank $n-k$ such that

$$C = \{c \in \mathbb{F}^n : Hc^{\mathsf{T}} = 0\}.$$

Dual code

- Given linear $[n, k]$-code C, the dual code $C^\perp$ is the linear $[n, n-k]$-code generated by the parity check matrix of C.
- Define the **dot product** on $\mathbb{F}^n$ by $a \cdot b = \sum_{i=1}^n a_i b_i$.
- Then $C^\perp = \{b \in \mathbb{F}^n : c \cdot b = 0, \text{ for all } c \in C\}$.
- Note that $(C^\perp)^\perp = C$.

Example

- $\mathbb{F} = \mathbb{F}_2$, $n = 7$, $k = 4$, $n - k = 3$:

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Syndromes

- Suppose $c \in C$ is transmitted, and suppose some error is introduced, so that $y = c + e$ is received. Here, e is the (yet to be determined) error vector.
- Applying the parity check matrix, we see that $Hy^{\mathsf{T}} = Hc^{\mathsf{T}} + He^{\mathsf{T}} = He^{\mathsf{T}}$ (the "syndrome").
- The error vector e lies in the same coset of C as the received vector y.

Likelihood

- Of all vectors in the coset $y + C$, which is the most likely to be the error vector?
- One model of a communication channel: the symmetric binary channel.
- Let $\mathbb{F} = \mathbb{F}_2$, the binary field. When an element of $\mathbb{F}_2$ is transmitted, there is a probability of p that the other element will be received. Assume $0 \leq p \leq 1/2$.

Hamming distance and Hamming weight

- The **Hamming weight** $\mathrm{wt}(y)$ of a vector $y \in \mathbb{F}^n$ is the number of nonzero entries in y; $\mathrm{wt}(y) = |\{i : y_i \neq 0\}|$.
- The **Hamming distance** between two vectors $y, z \in \mathbb{F}^n$ is the Hamming weight of their difference: $d(y, z) = \mathrm{wt}(y - z)$.
- The Hamming distance d is a distance, so $(\mathbb{F}^n, d)$ is a (discrete) metric space.

Likelihood, again

- Provided $p < 1/2$, an error vector with small Hamming weight is more likely to occur than one of larger Hamming weight.
- Syndrome decoding: given a received vector $y = c + e$, the most likely error vector is a vector of minimal Hamming weight in the coset $y + C$.
- Such an e exists, but it may not be unique.

Minimum distance of a code

- Given a code C, the **minimum (Hamming) distance** of C is $d_C = \min\{d(b, c) : b, c \in C, b \neq c\}$.
- For linear codes, this equals the **minimum (Hamming) weight**, $\min\{\mathrm{wt}(c) : c \in C, c \neq 0\}$.
- Suppose C has minimum distance d_C. Let $t = \lfloor (d_C - 1)/2 \rfloor$.
- Nearest neighbor decoding corrects up to t errors.

Example (again)

- $\mathbb{F} = \mathbb{F}_2$, $n = 7$, $k = 4$:

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- Codewords: 0000000, 0001111, 0110011, 1010101, 1111111, 0111100, 1011010, 1110000, 1100110, 1001100, 0101010, 1101001, 1000011, 0100101, 0011001, 0010110. $d_C = 3$.

Example (and again)

- $\mathbb{F} = \mathbb{F}_2$, $n = 7$, $k = 3$:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

- Codewords: 0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 1100110, 1101001. $d_{C^\perp} = 4$.

Decoding C

- Because $d_C = 3$, we can correct one error.
- If $\mathrm{wt}(e) = 1$, there is a single 1 in position i.
- The syndrome He^{T} is the ith column of H.
- The ith column of H is the base 2 expression of i, so the syndrome tells us the location of the error.
- Suppose $y = 1011101$ is received. Syndrome $Hy^{\mathsf{T}} = 100^{\mathsf{T}}$, so most likely $c = 1010101$ was sent.

Weight distributions

- Given C, its **weight distribution** is $(A_0, A_1, \ldots, A_n)$, where $A_i = |\{c \in C : \mathrm{wt}(c) = i\}|$, the number of codewords of Hamming weight i.
- For our example, C has $(1, 0, 0, 7, 7, 0, 0, 1)$.
- $C^\perp$ has $(1, 0, 0, 0, 7, 0, 0, 0)$.
- In the next slide, we organize this information differently.

Hamming weight enumerator

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

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

- $\mathrm{hwe}_C(X, Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i$, where A_i is the number of codewords in C of Hamming weight i.
- In our example: $\mathrm{hwe}_{C^\perp}(X, Y) = X^7 + 7X^3Y^4$, $\mathrm{hwe}_C(X, Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$.

MacWilliams identities

- One can verify in our binary example that the weight enumerators are related in the following way:

$$\mathrm{hwe}_C(X, Y) = \frac{1}{|C^\perp|} \mathrm{hwe}_{C^\perp}(X + Y, X - Y).$$

Properties of dual codes

- Given a linear code $C \subseteq \mathbb{F}^n$.
- Dual $C^\perp$ is also a linear code in $\mathbb{F}^n$.
- Double dual: $(C^\perp)^\perp = C$.
- Dimension/size: $\dim C + \dim C^\perp = n$, or: $|C| \cdot |C^\perp| = |\mathbb{F}^n|$.
- The MacWilliams identities.
- The next several lectures will be about generalizations of these properties.

Equivalence of linear codes

- When should two linear codes be considered as being the same?
- "Extrinsic": differ by a monomial transformation of $\mathbb{F}^n$.
- "Intrinsic": related by a weight-preserving isomorphism.

Monomial transformations

- A **monomial transformation** $T : \mathbb{F}^n \to \mathbb{F}^n$ is an invertible linear transformation whose matrix has exactly one nonzero entry in each row and column (a "monomial matrix").
- Monomial transformations are precisely the invertible linear transformations $\mathbb{F}^n \to \mathbb{F}^n$ that preserve the Hamming weight.
- Linear codes $C_1, C_2 \subseteq \mathbb{F}^n$ are **monomially equivalent** if there exists a monomial transformation T with $T(C_1) = C_2$.

Weight-preserving maps

- If $T(C_1) = C_2$, then the restriction of T to C_1 is a linear isomorphism $C_1 \to C_2$ that preserves Hamming weight.
- Is the converse true?
- Yes!—MacWilliams (1961–62). Weight preserving maps extend to monomial transformations.
- Call this the "MacWilliams extension theorem".

Upcoming lectures

- Lectures 2 and 3 will address generalizations of dual codes and the MacWilliams identities for linear codes defined over finite rings and modules.
- Lecture 4 will discuss self-dual codes (where $C = C^{\perp}$) in a general setting. Lecture 5: exercises!
- Lectures 6–10 will deal with different aspects of the extension problem: do weight-preserving maps extend to monomial transformations?
- Many of the techniques are based on characters of finite abelian groups and the modules built out of these characters.