Foundational Results on Linear Codes over Rings and Modules

Jay A. Wood

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

Centennial
Universidad Michoacana de San Nicolás de Hidalgo
Instituto de Física y Matemáticas
Morelia, Michoacán
March 5, 2018
Congratulations

- Congratulations to the Universidad Michoacana de San Nicolás de Hidalgo on its centennial!
- And congratulations on the 477th anniversary of the founding of the Colegio de San Nicolás Obispo!
- Thank you to the organizing committee for inviting me to speak to you on this joyous occasion.
- And my daughter Emily turns 25 today!
Michoacán and Michigan

- Universidad Michoacana de San Nicolás de Hidalgo has email address umich.mx.
- The University of Michigan has email address umich.edu.
- The state of Michigan has other public universities with email addresses such as cmich.edu, emich.edu, nmich.edu, wmich.edu.
Michoacán in/near Michigan

[Image of Carnicería Michoacán and Neveria Paletaria signs]
1. Codes and their duals

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

- Introduce some of the language of coding theory over finite fields.
- Introduce, with examples, some of the mathematical problems involving dual codes that will be discussed in the next lecture.
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 $P G$, $P$ invertible $k \times k$. 
Errors in transmission

- Error-correcting codes are designed to detect and correct errors in transmission in communication channels.
  \[ F^k \xrightarrow{\text{encode}} F^n \xrightarrow{\text{transmit}} F^n \xrightarrow{\text{decode}} F^n \xrightarrow{\text{unencode}} F^k \]

- 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

\[
C = \{ c \in \mathbb{F}^n : Hc^\top = 0 \}.
\]
Given linear $[n, k]$-code $C$, the dual code $C^\perp$ is the linear $[n, n-k]$-code generated by a 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

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

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

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$
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 $Hy^T = Hc^T + He^T = He^T$ (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** $\text{wt}(y)$ of a vector $y \in \mathbb{F}^n$ is the number of nonzero entries in $y$:
  \[ \text{wt}(y) = |\{i : y_i \neq 0\}|. \]

- The **Hamming distance** between two vectors $y, z \in \mathbb{F}^n$ is the Hamming weight of their difference:
  \[ d(y, z) = \text{wt}(y - z). \]

- 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**, \( \min \{ \text{wt}(c) : c \in C, c \neq 0 \} \).

- 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)

- $F = F_2$, $n = 7$, $k = 4$:

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

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

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

\[
H = \begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\end{bmatrix}
\]

- 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 $\text{wt}(e) = 1$, there is a single 1 in position $i$.
- The syndrome $He^T$ is the $i$th column of $H$.
- The $i$th 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 $Hy^T = 100^T$, so most likely $c = 1010101$ was sent.
Weight distributions

- Given $C$, its **weight distribution** is $(A_0, A_1, \ldots, A_n)$, where $A_i = |\{ c \in C : \text{wt}(c) = i \}|$, 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

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

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

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

\[
hwe_C(X, Y) = \frac{1}{|C^\perp|} \ hwe_{C^\perp}(X + Y, X - Y).
\]
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 lecture will be about generalizations of these properties.