Cyclic Redundancy Check Codes

Lectures No. 17 and 18

Dr. Aoife Moloney

School of Electronics and Communications
Dublin Institute of Technology
Overview

These lectures will look at the following:

- Cyclic redundancy check (CRC) codes
- Generator and parity check matrices
- Decoding at the receiver
Cyclic Redundancy Check (CRC) Codes

- CRCs are very popular linear block codes.
- They are very effective for error detection and correction.
- The channel coders and decoders are easy to implement in hardware.
Cyclic Redundancy Check Codes

CRC Advantages

- CRC codes of length $n$ can be generated which detect:
  - All single and double errors
  - Any odd number of errors
  - Any burst error $\leq n$ and most larger error bursts
  - Sample questions
Generator and Parity Check Matrices

- All linear block codes can be generated from generator matrices and have error checking performed using parity check matrices and syndrome testing.

- We will use these matrix techniques to examine CRC codes here.
Generating the Codewords

- Let $x_{m1}, x_{m2}, ..., x_{mk}$ denote the $k$ information bits which are encoded to give the codeword $C_m$.

- The information bits are represented using a $1 \times k$ matrix (meaning 1 row $k$ columns). This matrix is called $X_m$ and is shown below:

$$X_m = \begin{bmatrix} x_{m1} & x_{m2} & \cdots & x_{mk} \end{bmatrix}$$

- The codeword is represented by a $1 \times n$ matrix as shown
Lectures No. 17 and 18: **Cyclic Redundancy Check Codes**

below:

\[
C_m = [c_{m1} \ c_{m2} \ \cdots \ c_{mn}]
\]

- Each element of the codeword \( C_m \) is given by:

\[
c_{mj} = x_{m1}g_{1j} \oplus x_{m2}g_{2j} \oplus \cdots \oplus x_{mk}g_{kj} \text{ for } j = 1, \ldots, n
\]

where \( g_{ij} \) is either a 1 or a 0. The products \( x_{mi}g_{ij} \) represent ordinary multiplication, and the \( \oplus \) operator indicates XOR (modulo-2 addition).

- The \( n \) linear equations that generate each codeword may
be written in matrix form as follows:

\[ C_m = X_m G \]

- \( G \) is called the generator matrix of the code and is given as:

\[
\begin{bmatrix}
  g_{11} & g_{12} & \cdots & g_{1n} \\
  g_{21} & g_{22} & \cdots & g_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  g_{k1} & g_{k2} & \cdots & g_{kn}
\end{bmatrix}
\]
Systematic Form

- The form of the generator matrix is not unique. However, it may always be reduced to systematic form as shown below:

\[
G = \begin{bmatrix}
1 & 0 & \cdots & 0 & p_{11} & p_{12} & \cdots & p_{1n-k} \\
0 & 1 & \cdots & 0 & p_{21} & p_{22} & \cdots & g_{2n-k} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & p_{k1} & p_{k2} & \cdots & g_{kn-k}
\end{bmatrix}
\]

- The generator matrix has the form \([I_k \quad P]\) where \(I_k\) is
the identity matrix (note: an identity matrix is a matrix which has a diagonal made up of 1s and has 0s everywhere else) and $\mathbf{P}$ is the $k \times (n - k)$ parity check matrix.

- This systematic form generator matrix generates codewords $C_m$ in which the $k$ information bits are followed by the $n - k$ parity bits.
The Parity Check Matrix H

- Since $G$ is a $k \times n$ matrix with all $k$ rows being linearly independent we can say that the rows of $G$ form a set of basis vectors in a $k$-dimensional subspace of the $n$-dimensional space defined by considering all valid and invalid codewords.

- There therefore must exist another matrix, $H$, consisting of $n - k$ linearly independent rows that forms a set of basis vectors in the $n - k$ subspace which is unreachable from $G$. It follows that each valid codeword $C_m$ will be
orthogonal to the basis vector set defined by $\mathbf{H}$, i.e.

$$C_m H' = 0$$

- As the basis vectors defined by $\mathbf{G}$ occupy a subspace unreachable by $\mathbf{H}$, it follows that every vector of $\mathbf{G}$ is orthogonal to every vector of $\mathbf{H}$, i.e.

$$G H' = 0$$
Constructing $H$

- So a codeword generated by $G$ cannot reach the subspace defined by $H$ unless a transmission error occurs. $H$ may therefore be used to verify that a received codeword is valid by verifying that it has not entered this forbidden sub-space.

- Due to this special property $H$ is called the **parity check matrix** of the generator matrix $G$.

- Because of the relationship between $G$ and $H$, $H$ may be
written as:

\[ H = \begin{bmatrix} P' & I_{n-k} \end{bmatrix} \]

when \( G = [I_k \quad P] \) and \( GH' = 0 \)
Example

- Find the $H$ matrix given that the generator matrix $G = [I_k \quad P]$ is:

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

$$H = [P' \quad I_{n-k}] \text{ (note: } P' \text{ means the transpose of the matrix } P, \text{ the transpose is found by making the columns}$$
of $P$ into rows) giving:

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$
Decoding at the Receiver

• A simple method for decoding at the receiver would be to add (modulo-2) each received codeword to the complete set of allowed codewords \( C_i \quad i = 1, 2, ..., m \) to obtain the error vector set \( e_r \).

• The error vector \( e_i \) with the smallest number of 1s is the one with the minimum distance to an allowed codeword and therefore the transmitted codeword is deemed to be \( C_i \).

• Ideally \( e_i \) consists of all 0s, i.e. no error occurs.
The Syndrome of the Error Pattern

- The previous method is easy to understand but is inefficient. It involves comparing each received codeword $Y$ with $2^n$ possible valid codewords.

- In general $Y$ may be written as:

$$Y = C_m + e$$
Lectures No. 17 and 18: Cyclic Redundancy Check Codes

Multiply $Y$ by $H'$ the parity check matrix gives:

$$YH' = (C_m + e)H'$$
$$= C_m H' + eH'$$
$$= 0 + eH'$$
$$= eH'$$
$$= S$$

- The $n - k$ vector $S$ is called the syndrome of the error pattern.
Syndrome Testing

• To correct a received codeword, \( Y \), follow the 3 step process outlined below:
  
  – Calculated \( S \)
    \[
    S = Y H'
    \]
  
  – Use \( S \) to find the most likely error \( e_m \) from a syndrome look-up table.
  
  – Correct the codeword by adding \( e_m \) to \( Y \):
    \[
    C_m = Y \oplus e_m
    \]
Sample Questions

• Question 1
  (a) A (7, 4) CRC code has the following generator matrix:

\[
G = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1
\end{pmatrix}
\]

Noting that this matrix is given in the \([I_k \quad P]\) form, write down the parity check matrix H.
(b) Hence calculate the syndromes for the following received code words:

\[ Y_1 = (1 1 0 0 1 0 1) \]
\[ Y_2 = (1 1 0 0 0 0 1) \]
\[ Y_3 = (1 1 1 1 0 1 0) \]

(c) The syndrome table for this code is:
### Syndrome Error Pattern

<table>
<thead>
<tr>
<th>Syndrome</th>
<th>Error Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0</td>
<td>0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>0 0 1</td>
<td>0 0 0 0 0 0 0 1</td>
</tr>
<tr>
<td>0 1 0</td>
<td>0 0 0 0 0 0 1 0</td>
</tr>
<tr>
<td>0 1 1</td>
<td>0 0 0 1 0 0 0 0</td>
</tr>
<tr>
<td>1 0 0</td>
<td>0 0 0 0 1 0 0 0</td>
</tr>
<tr>
<td>1 0 1</td>
<td>1 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>1 1 0</td>
<td>0 0 1 0 0 0 0 0</td>
</tr>
<tr>
<td>1 1 1</td>
<td>0 1 0 0 0 0 0 0</td>
</tr>
</tbody>
</table>
• **Question 2:**

A (7, 3) CRC code has the following generator matrix:

\[
\begin{pmatrix}
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1
\end{pmatrix}
\]

1. Calculate the entire code book for this codeword, i.e. the set of eight allowable codewords generated from input messages 000, 001, 010, ..., 111.

2. Calculate the Hamming distance between the all-zero codeword \(C_0 = [0 0 0 0 0 0 0]\) and each of the other
Lectures No. 17 and 18: Cyclic Redundancy Check Codes

non-zero code words (a total of seven Hamming distance calculations).

• **Question 3:**
  A (7, 4) Hamming Linear Block code has the following generator matrix:

\[
G = \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1
\end{pmatrix}
\]

1. Noting that this matrix is given in the \([I_k \ P] \) form,
write down the parity check matrix \( \mathbf{H} \).

2. Using \( \mathbf{H} \), verify that the following code words are valid:

\[
C_1 = [1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0] \\
C_2 = [0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0] \\
C_3 = [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1]
\]
Conclusion

These lectures have looked at the following:

- Cyclic redundancy check (CRC) codes
- Generator and parity check matrices
- Decoding at the receiver
- Sample questions