Outline

- Convolutional Code Fundamentals
- Generator Matrices for a Convolutional Code.
- Canonical, Minimal, Systematic Generator Matrices
- The Corresponding Encoders
Block Code Fundamentals

• An \((n, k)\) linear block code \(\mathcal{C}\) is a \(k\)-dimensional subspace of \(F^n\).

• A generator matrix \(G\) for \(\mathcal{C}\) is a \(k \times n\) matrix over \(F\) whose rowspace is \(\mathcal{C}\).

• \(G\) can be used as an encoder: If \(u = (u_1, \ldots, u_k) \in F^k\) is an information word, the corresponding codeword \(x = (x_1, \ldots, x_n) \in F^n\) is given by

\[ x = uG. \]
Convolutional Code Fundamentals

- An \((n, k)\) convolutional code is a \(k\)-dimensional subspace of \(F(z^{-1})^n\).

- Here \(F(z^{-1})\) is the field of rational functions (quotients of polynomials) in the indeterminate \(z^{-1}\) over \(F\).

- A generator matrix \(G\) for \(\mathcal{C}\) is a \(k \times n\) matrix over \(F(z^{-1})\) whose rowspace is \(\mathcal{C}\).

- \(G(z)\) is called a polynomial generator matrix if the entries in \(G(z)\) are all polynomials.

- Every convolutional code has polynomial generator ma-
trices. (Proof?)
Examples

• Example: $n = 2, k = 1$. Here is a polynomial generator matrix for a $(2, 1)$ convolutional code over $GF(2)$:

\[
G = \begin{pmatrix}
1 + z^{-1} + z^{-2} & 1 + z^{-2}
\end{pmatrix}.
\]

• Here is another generator matrix for the same code:

\[
G' = \begin{pmatrix}
1 & \frac{1 + z^{-2}}{1 + z^{-1} + z^{-2}}
\end{pmatrix}.
\]
There are Lots of Possible Generator Matrices

- If $G$ is any generator matrix for $\mathcal{C}$, any matrix $G'$ which is row-equivalent to $G$ is also a generator matrix for $\mathcal{C}$.

- That is, $G'$ can be obtained from $G$ by a series of elementary row operations, or equivalently,

$$G' = UG,$$

where $U$ is a $k \times k$ nonsingular matrix over $F(z^{-1})$. 

Examples

\[ G_1(z) = \begin{pmatrix} \frac{1}{1+z^{-1}+z^{-2}} & 1 & \frac{1+z^{-2}}{1+z^{-1}+z^{-2}} & \frac{1+z^{-1}}{1+z^{-1}+z^{-2}} \\ 1 & \frac{1+z^{-1}+z^{-2}}{z^{-1}} & \frac{1}{z^{-1}} & \end{pmatrix}. \]

defines a (4, 2) convolutional code over \( GF(2) \). Clearing denominators,

\[ G_2(z) = \begin{pmatrix} 1 & 1+z^{-1}+z^{-2} & 1+z^{-2} & 1+z^{-1} \\ z^{-1} & 1+z^{-1}+z^{-2} & z^{-2} & 1 \end{pmatrix} \]

is a polynomial generator matrix for the same code.
Some More Generator
Matrices for the Same Code
\[ G_3 = \begin{pmatrix} 1 & 1 + z^{-1} + z^{-2} & 1 + z^{-2} & 1 + z^{-1} \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix} \]

\[ G_4 = \begin{pmatrix} 1 & z^{-1} & 1 + z^{-1} & 0 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix} \]

\[ G_5 = \begin{pmatrix} 1 + z^{-1} & 0 & 1 & z^{-1} \\ z^{-1} & 1 + z^{-1} + z^{-2} & z^{-2} & 1 \end{pmatrix} \]

\[ G_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix} \]

\[ G_7 = \begin{pmatrix} 1 + z^{-1} & 0 & 1 & z^{-1} \\ 1 & z^{-1} & 1 + z^{-1} & 0 \end{pmatrix} \]

\[ G_8 = \begin{pmatrix} 1 & 0 & \frac{1}{1+z^{-1}} & \frac{z^{-1}}{1+z^{-1}} \\ 0 & 1 & \frac{z^{-1}}{1+z^{-1}} & \frac{1}{1+z^{-1}} \end{pmatrix} \]
A Good Question

• Among all possible generator matrices, which ones are best?

  • **Canonical** generator matrices.

  • **Systematic** generator matrices.

  • **Minimal** generator matrices
Generalizing the Definition of Degree

• The degree of a vector of polynomials is the maximum degree of any component. Example:

\[
\deg \left( \begin{array}{cccc}
1 & 1 + z^{-1} + z^{-2} & 1 + z^{-2} & 1 + z^{-1}
\end{array} \right) = 2.
\]

• The degree of a polynomial matrix is the sum of the row degrees. Example:

\[
\deg \left( \begin{array}{cccc}
1 & 1 + z^{-1} + z^{-2} & 1 + z^{-2} & 1 + z^{-1} \\
0 & 1 + z^{-1} & z^{-1} & 1
\end{array} \right) = 3.
\]
The Degree of a Convolutional Code

- The degree of a convolutional code is the minimum degree of any polynomial generator matrix for $C$.

**Notation.** An $(n, k)$ convolutional code whose degree is $m$ is called an $(n, k, m)$ convolutional code.

- A minimum degree polynomial generator matrix is called a canonical generator matrix.
Canonical Generator Matrices

• There are efficient algorithms for computing canonical generator matrices. We will not cover this.

• But there is an easy test for canonicity:

Theorem. A polynomial generator matrix is canonical iff it is basic and reduced.

• Basic: The gcd of the $k \times k$ minors is 1.

• Reduced: The indicator matrix $\overline{G}$ for the highest degree terms in each row has rank $k$. 
Basic and/or Reduced?

• Examples:

\[
G_4 = \begin{pmatrix}
1 & z^{-1} & 1 + z^{-1} & 0 \\
0 & 1 + z^{-1} & z^{-1} & 1
\end{pmatrix}
\]

\[
G_5 = \begin{pmatrix}
1 + z^{-1} & 0 & 1 & z^{-1} \\
z^{-1} & 1 + z^{-1} + z^{-2} & z^{-2} & 1
\end{pmatrix}
\]

\[
G_6 = \begin{pmatrix}
1 & 1 & 1 & 1 \\
0 & 1 + z^{-1} & z^{-1} & 1
\end{pmatrix}
\]
$G_4$ is Basic but not reduced

$$
G_4 = \begin{pmatrix}
1 & z^{-1} & 1 + z^{-1} & 0 \\
0 & 1 + z^{-1} & z^{-1} & 1
\end{pmatrix}.
$$

$$
\Delta_{1,2} = 1 + z^{-2}, \quad \Delta_{1,3} = z^{-1}, \ldots.
$$

$$
\bar{G} = \begin{pmatrix}
0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0
\end{pmatrix}.
$$
$G_5$ is Reduced but not Basic

$$G_5 = \begin{pmatrix} 1 + z^{-1} & 0 & 1 & z^{-1} \\ z^{-1} & 1 + z^{-1} + z^{-2} & z^{-2} & 1 \end{pmatrix}.$$ 

$$\Delta_{1,2} = 1 + z^{-3}, \quad \Delta_{1,3} = z^{-1} + z^{-2} + z^{-3}, \ldots.$$ 

$$\bar{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$
$G_6$ is Reduced and Basic

$$G_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix}.$$

$$\Delta_{1,2} = 1 + z^{-2}, \quad \Delta_{1,3} = z^{-1}, \ldots.$$

$$\bar{G} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$
Canonical generator Matrices are Not Unique

• Example:

\[ G_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix} \]

\[ G'_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & z^{-1} & 1 + z^{-1} & 0 \end{pmatrix} \]

both canonical.
Important Property I of Canonical Generator Matrices

“The Forney Indices”

• If \( G(z) \) and \( G'(z) \) are two canonical generator matrices for \( C \), then

\[
\deg g_i(z) = \deg g'_i(z) \quad \text{for } i = 1, \ldots, n,
\]

i.e., the list of row degrees is the same for any canonical generator matrix.

• These row degrees are called the Forney indices of the code.
Important Property I of Canonical Generator Matrices

- For Example,

\[ G_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix} \]

\[ G'_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & z^{-1} & 1 + z^{-1} & 0 \end{pmatrix} \]

The Forney indices are \((0, 1)\).
Important Property II of Canonical Generator Matrices

“The Predictable Degree Property”

• If \( u(z) = (u_1(z) \cdots u_k(z)) \) is a vector of polynomials, and \( x(z) = u(z)G(z) \), i.e.,

\[
x(z) = \sum_{1 \leq i \leq k} u_i(z)g_i(z)
\]

Then
\[ \deg \mathbf{x}(z) = \max_{1 \leq i \leq k} \left( \deg u_i(z) + \deg g_i(z) \right). \]

- (Any reduced generator matrix has this property.)
Important Property III of Canonical Generator Matrices

“Polynomial Out → Polynomial In”

- If $u(z)G(z)$ is a polynomial vector, then so is $u(z)$.
- (Any basic generator matrix has this property.)
Examples

• The following GM does not have the predictable degree property.

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

• The following GM does not have the POPI property:

\[
G = (1 + w^3, 1 + w + w^2 + w^3).
\]
• The set of row degrees is the same for any canonical generator matrix.

\[
G_6 = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 \\
0 & 1 + z^{-1} & z^{-1} & 1 \\
\end{pmatrix}
\]

\[
G'_6 = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & z^{-1} & 1 + z^{-1} & 0 \\
\end{pmatrix}
\]

These row degrees are called the Forney indices of the code, in this case (0, 1).
Important Properties of Canonical Generator Matrices

• The predictable degree property. If

\[ u(z) = \begin{pmatrix} u_1(z) & \cdots & u_k(z) \end{pmatrix}, \]

and

\[ G(z) = \begin{pmatrix} g_1(z) \\ \vdots \\ g_k(z) \end{pmatrix}, \]

\[ u(z)G(z) = \sum_{1 \leq i \leq k} u_i(z)g_i(z) \]

\[ \deg u(z)G(z) = \max_{1 \leq i \leq k} \left( \deg u_i(z) + \deg g_i(z) \right). \]
The Realizability Theorem

**Theorem.** An \((n, k, m)\) convolutional code \(C\) possesses an encoder which uses exactly \(m\) delay elements. No encoder for \(C\) has fewer than \(m\) memory elements.

**Definition.** An encoder that uses exactly \(m\) memory elements is called a minimal encoder.
One Way to Construct a Minimal Encoder

A minimal encoder can be realized via a canonical generator matrix in the “obvious way” (direct form realization).

\[(1 + z^{-1} + z^{-2}, 1 + z^{-2})\]
Canonical Generator
Matrix $\rightarrow$ Minimal Encoder

$$G_6 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ u_1 & u_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix}$$
Non-Canonical Generator
Matrix $\rightarrow$ Minimal Encoder

$$G_4 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ u_1 & z^{-1} & 1 + z^{-1} & 0 \\ u_2 & 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix}$$
Systematic Generator Matrices

\[ G_6 = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ 1 & 1 & 1 & 1 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix} \]

- Multiply row 2 by \( \frac{1}{1 + z^{-1}} \) and add it to row 1:

\[ G_8 = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ 1 & 0 & \frac{1}{1 + z^{-1}} & \frac{z^{-1}}{1 + z^{-1}} \\ 0 & 1 & \frac{z^{-1}}{1 + z^{-1}} & \frac{1}{1 + z^{-1}} \end{pmatrix} \]
In General

**Theorem.** Any convolutional code has a systematic generator matrix. Every systematic generator matrix can be realized by an encoder with $m$ delay elements.
Example: Systematic and Minimal, Not Canonical

\[ G_8 = \begin{array}{l}
\begin{array}{cc}
\begin{array}{cccc}
 x_1 & x_2 & x_3 & x_4 \\
 1 & 0 & \frac{1}{1+z^{-1}} & \frac{z^{-1}}{1+z^{-1}} \\
 0 & 1 & \frac{z^{-1}}{1+z^{-1}} & \frac{1}{1+z^{-1}} \\
\end{array}
\end{array}
\end{array}
\]
Outline

• Convolutional Code Fundamentals: Review

• The Important Special Case $k = 1$.

• Three Important Properties of Canonical Generator Matrices.

• The Free Distance.
Convolutional Code Fundamentals

- An \((n, k)\) **convolutional code** is a \(k\)-dimensional sub-space of \(F(z^{-1})^n\).

- \(G(z)\) is called a **generator matrix** for the convolutional code \(C\) if its rowspace is \(C\).

- Every convolutional code has polynomial generator matrices that are basic and reduced: Canonical.

- Every convolutional code has a systematic GM.

- Canonical and Systematic GM’s lead to minimal encoders.
Special Case: \( k = 1 \)

**Theorem.** A canonical generator matrix for an \((n, 1)\) convolutional code is of the form

\[
G = (g_1(z), \ldots, g_n(z)),
\]

where

\[
gcd(g_1(z), \ldots, g_n(z)) = 1.
\]

**Proof:** Basic? Yes, because \( gcd(g_1(z), \ldots, g_n(z)) = 1 \). Reduced? yes, automatically. \( \blacksquare \)
A Canonical Encoder for $k = 1$
Special Case: $k = 1$

**Theorem.** A systematic generator matrix for an $(n, 1)$ convolutional code is of the form

$$G = \begin{pmatrix} 1, \frac{g_2(z)}{g_1(z)}, \ldots, \frac{g_n(z)}{g_1(z)} \\ \frac{g_1(z)}{g_2(z)}, 1, \ldots, \frac{g_n(z)}{g_2(z)} \\ \vdots \\ \frac{g_1(z)}{g_n(z)}, \frac{g_2(z)}{g_n(z)}, \ldots, 1 \end{pmatrix}.$$
Systematic Encoders for $k = 1$
Back to Canonical Generator Matrices

Let $G(z)$ be a canonical generator matrix for a convolutional code $C$, with $g_i(z) = (g_{1,1}(z), \ldots, g_{1,n}(z))$ being the $i$th row:

$$G(z) = \begin{pmatrix} g_1(z) \\ \vdots \\ g_k(z) \end{pmatrix},$$

with $\deg g_1 \leq \deg g_2 \leq \cdots \leq \deg g_n$. 
\[ G_6 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 + z^{-1} & z^{-1} & 1 \end{pmatrix} \]
The Free Distance of a Convolutional Code

• A block code has a minimum distance:

**Definition.** The minimum distance of an \((n, k)\) linear block code is the minimum Hamming weight among all nonzero codewords.

• A convolutional code has a free distance:

**Definition.** The free distance of a convolutional code is the minimum weight among all polynomial codewords.
Example 1

• The \((2, 1, 2)\) code, described by the generator matrix

\[
G = \begin{pmatrix} 1 + w + w^2 & 1 + w^2 \\ 1 & 1 + w^2 \end{pmatrix} 
= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + w \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + w^2 \begin{pmatrix} 1 & 1 \end{pmatrix}
\]

• The general polynomial codeword is a finite linear combination of

\[G, wG, w^2 G, \ldots\]
The Free Distance is 5

- The general polynomial codeword is a finite linear combination of:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>1</th>
<th>w</th>
<th>w</th>
<th>w²</th>
<th>w²</th>
<th>w³</th>
<th>w³</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wG</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>w²G</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>w³G</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example 2

• The $(4, 2, 1)$ code described by the generator matrix

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

• The general polynomial codeword is a finite linear combination of

\[g_1, g_2, wg_1, wg_2, w^2g_1, w^2g_2, \ldots\]
The Free Distance is 4

- The general polynomial codeword is a finite linear combination of:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>w</th>
<th>w</th>
<th>w</th>
<th>w</th>
<th>w²</th>
<th>w²</th>
<th>w²</th>
<th>w²</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$wG$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$w²G$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>