Cyclic Codes II
We would now like to consider how the ideas we have previously discussed for linear codes are interpreted in this polynomial version of cyclic codes.

**Theorem 6:** If the generator polynomial \( g(x) \) of \( C \) has degree \( n-k \) then \( C \) is an \([n,k]\)-cyclic code. If \( g(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-k} x^{n-k} \) then a generator matrix for \( C \) is the \( k \times n \) matrix,

\[
\begin{bmatrix}
g(x) \\
x \cdot g(x) \\
x^2 \cdot g(x) \\
\vdots \\
x^{k-1} \cdot g(x)
\end{bmatrix} =
\begin{bmatrix}
a_0 & a_1 & a_2 & \cdots & a_{n-k} & 0 & 0 & \cdots & 0 \\
0 & a_0 & a_1 & \cdots & a_{n-k-1} & a_{n-k} & 0 & \cdots & 0 \\
0 & 0 & a_0 & \cdots & a_{n-k-2} & a_{n-k-1} & a_{n-k} & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & \cdots & a_{n-k}
\end{bmatrix}.
\]
Proof: The vectors \( g(x), xg(x), x^2 g(x), \ldots, x^{k-1} g(x) \) are linearly independent. If not, there would exist coefficients \( \{b_i\} \) so that
\[
b_0 g(x) + b_1 xg(x) + b_2 x^2 g(x) + \ldots + b_{k-1} x^{k-1} g(x) = 0,\
\]
\[
(b_0 + b_1 x + b_2 x^2 + \ldots + b_{k-1} x^{k-1}) g(x) = 0.
\]
But this product has degree \( k - 1 + n - k = n - 1 < n \), so it can not be \( \equiv 0 \mod (x^n - 1) \) unless all the \( b_i = 0 \).

Let \( c(x) \in C \), then \( c(x) = b(x) g(x) \) and we may assume that \( b(x) \) has degree \( \leq k - 1 \) (otherwise the product will have degree \( > n - 1 \) and we would reduce modulo \( (x^n - 1) \) to get a \( b'(x) \) which satisfies this degree constraint). Thus, \( c(x) \) can be written as a linear combination of the \( x^i g(x) \).

The set of \( \{x^i g(x) \} \), \( 0 \leq i \leq k - 1 \) is thus a basis for \( C \) and so this cyclic code has dimension \( k \) \( \square \)
Dual Code

Now that we have a polynomial approach to describe a cyclic code $C$, we consider the related polynomial representation of the dual code $C^\perp$ of $C$. We shall see that $C^\perp$ is a cyclic code if $C$ is cyclic.

Consider $h(x) = (x^n - 1)/g(x)$ where $g(x)$ is the generator of $C$. If the degree $g(x) = n - k$, then degree $h(x) = k$ and it is also monic, so $h(x)$ generates a cyclic code $C'$ of dimension $n - k$. Now consider $c_1(x) = a_1(x)g(x) \in C$ and $c_2(x) = a_2(x)h(x) \in C'$. Then

$$c_1(x) c_2(x) = a_1(x)g(x)a_2(x)h(x) = a_1(x)a_2(x)f(x) \equiv 0 \pmod{f(x)},$$

where $f(x) = x^n - 1$. Therefore, using polynomial multiplication mod $f(x)$, any codeword from $C$ multiplies with any codeword from $C'$ to give the polynomial $0$. Does this imply that $C'$ is the dual code of $C$? Unfortunately no, since the isomorphism that we set up does not preserve inner products. However, we now show that the codes $C'$ and $C^\perp$ are closely related - they are equivalent codes.
Dual Code

Consider two vectors
\[ \mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{C} \]
and
\[ \mathbf{b} = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{C}', \]
and the corresponding polynomial product
\[ a(x)b(x) = \left( \sum_{i=0}^{n-1} a_i x^i \right) \left( \sum_{i=0}^{n-1} b_i x^i \right) \equiv \sum_{i=0}^{n-1} c_i x^i \pmod{x^n-1} \]
for some \( c_i \in \mathbb{F} \). The constant term in this product is
\[ c_0 = a_0 b_0 + a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_{n-1} b_1, \]
since \( x^n \equiv 1 \pmod{f(x)} \). Now \( c_0 \) can be written as the inner product
\[ c_0 = \mathbf{a} \cdot \mathbf{b}' \]
where \( \mathbf{b}' \) is the vector obtained from \( \mathbf{b} \) by cyclically shifting \( \mathbf{b} \) one position to the left and then reversing the order of the components (i.e., \( b_0, b_{n-1}, b_{n-2}, \ldots, b_1 \)).
Dual Code

Observe that multiplying the polynomial

\[
\sum_{i=0}^{n-1} c_i x^i
\]

by \( x^{n-t} \) results in \( c_t \) being the constant term, and hence the constant term in the product \( a(x)(x^{n-t} b(x)) \). Therefore,

\[
c_t = a \ b'
\]

where \( b' \) is now the vector associated with \( x^{n-t} b(x) \). In terms of \( b(x) \), \( b' \) is the vector obtained by cyclically shifting \( b \) \( t+1 \) positions to the left and then reversing the order of the components.
Example

Consider \( n = 3 \), and the vectors \( \mathbf{a} = (a_0 \ a_1 \ a_2) \) and \( \mathbf{b} = (b_0 \ b_1 \ b_2) \). Then modulo \( x^3 - 1 \),

\[
\mathbf{a}(x) \mathbf{b}(x) = (a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2)
\]

\[
= (a_0 \ b_0 + a_1 \ b_2 + a_2 \ b_1) + (a_0 \ b_1 + a_1 \ b_0 + a_2 \ b_2)x
\]

\[
+ (a_0 \ b_2 + a_1 \ b_1 + a_2 \ b_0)x^2.
\]

The coefficient of \( x^2 \) is \( \mathbf{a}(b_2 \ b_1 \ b_0) \). This \( \mathbf{b} \) vector is obtained from \( \mathbf{b} \) by shifting 3 (\( = 2 + 1 \)) positions to the left (putting \( \mathbf{b} \) back into its original order) and then reversing the order of the components from last to first. The \( \mathbf{b} \)-vector in the \( x \) coefficient is obtained from \( \mathbf{b} \) by shifting 2 (\( = 1 + 1 \)) to the left, obtaining \( (b_2 \ b_0 \ b_1) \) and then reversing the components.
Parity Check Matrix

Now since $a(x)b(x) \equiv 0 \pmod{(x^n - 1)}$, the coefficient of each power of $x$ must be 0. From the discussion above, this implies that $ac = 0$ (i.e., $a$ and $c$ are orthogonal) whenever $c$ is any cyclic shift of the vector obtained from $b$ by reversing the components of $b$. Since $h(x)$ generates $C'$, $\{h(x), xh(x), \ldots, x^{n-k-1}h(x) \}$ is a basis for $C'$ and $G' = [h(x), xh(x), \ldots, x^{n-k-1}h(x)]^T$ is a generator matrix for $C'$. Now $G'$ generates the code $C'$ which has the same dimension $n - k$ as $C^\perp$.

Furthermore, taking $b(x)$ in the above arguments to be $h(x)$ itself, we see that the reverse of every vector in $C'$ is orthogonal to every vector in $C$. It follows that if we reorder the columns of $G'$ last to first, we obtain a matrix $H$ which generates $C^\perp$, and hence is the parity-check matrix for $C$. 
Example

Suppose we wish to construct a generator matrix and a parity-check matrix for a \([7,4]\)-binary cyclic code. Since \(g(x) = 1 + x + x^3\) divides \(f(x) = x^7 - 1\), \(g(x)\) generates a \([7,4]\)-cyclic code \(C\). \(h(x) = f(x)/g(x) = 1 + x + x^2 + x^4\) generates a \([7,3]\)-cyclic code \(C'\). A generator matrix for \(C\) is

\[
G = \begin{bmatrix}
g(x) \\
x \cdot g(x) \\
x^2 \cdot g(x) \\
x^3 \cdot g(x)
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1
\end{bmatrix}.
\]
Example

A generator matrix for $C'$ is

$$G' = \begin{bmatrix} h(x) \\ x h(x) \\ x^2 h(x) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$ 

Writing the columns of $G'$ last to first, a generator matrix for $C^\perp$ is

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

A simple check verifies that $GH^T = 0.$
Parity Check Matrix

Since $C'$ and $C^\perp$ can be obtained from each other by reversing the components in all vectors, $C'$ and $C^\perp$ are equivalent codes. Recall a definition that we have seen before,

**Definition**: Let $h(x) = a_0 + a_1 x + ... + a_k x^k$ be a polynomial of degree $k$ ($a_k \neq 0$). Define the *reciprocal polynomial* $h_R(x)$ of $h(x)$ by

$$h_R(x) = \sum_{i=0}^{k} a_{k-i} x^i.$$ 

Note that $h_R(x) = x^k h(1/x)$, where $k = \deg h(x)$.

**Theorem 7**: Let $g(x)$ be a monic divisor of $f(x) = x^n - 1$ of degree $n-k$, and hence the generator for a cyclic $[n,k]$-code $C$. Let $h(x) = f(x)/g(x)$. Then $h_R(x)$, the reciprocal poly of $h(x)$, generates $C^\perp$. 
Syndromes

Let us first consider an alternate form for the generator matrix of a cyclic code of the form \([R, I_k]\) when \(C\) is an \([n,k]\)-cyclic code. Let \(g(x)\) be the generator polynomial for the code.

Divide \(x^{n-k+i}\) by \(g(x)\) for \(0 \leq i \leq k-1\). This gives

\[
x^{n-k+i} = q_i(x)g(x) + r_i(x)
\]

where \(\deg r_i(x) < \deg g(x) = n-k\) or \(r_i(x) = 0\). Then

\[
x^{n-k+i} - r_i(x) = q_i(x)g(x) \in C
\]

is a set of \(k\) linearly independent code words and the matrix whose rows are these codewords is a generator matrix of the required form.
Example

Consider the binary $[7,4]$-cyclic code generated by $g(x) = 1 + x + x^3$. By the division algorithm we compute,

\[
x^3 = (1)(x^3 + x + 1) + (1+ x)
\]
\[
x^4 = (x)(x^3 + x + 1) + (x + x^2)
\]
\[
x^5 = (x^2 + 1)(x^3 + x + 1) + (1 + x + x^2)
\]
\[
x^6 = (x^3 + x + 1)(x^3 + x + 1) + (1 + x^2).
\]

A generator matrix for this code is

\[
G = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 \\
\end{bmatrix} = [RI_4]
\]

where

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

Notice that the rows of $R$ are just the remainder polynomials.
 Syndromes

The corresponding parity-check matrix for this generator is $H = [I_{n-k} - R^T]$. A reason for making this selection is that it affords a convenient polynomial interpretation for the syndrome of a vector.

**Theorem 8**: Let $r(x)$ and $s(x)$ be the respective polynomial representations of a vector $r$ and its syndrome $s = Hr^T$. Then $s(x)$ is the remainder polynomial when $r(x)$ is divided by $g(x)$.  
**Syndromes**

**Proof:** Suppose \( r(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \). Noting that column \( i, 0 \leq i \leq n-k-1 \), of \( H \) corresponds to the polynomial \( x^i \) and column \( j, n-k \leq j \leq n-1 \), corresponds to \( r_{j-n+k}(x) \), so that

\[
s(x) = a_0 + a_1 x + ... + a_{n-k-1} x^{n-k-1} + a_{n-k} r_0(x) + ... + a_{n-1} r_{k-1}(x)
\]
\[
= a_0 + a_1 x + ... + a_{n-k-1} x^{n-k-1} + a_{n-k} (x^{n-k} - q_0(x) g(x)) + ...
\]
\[
= r(x) - (a_{n-k} q_0(x) g(x) + ... + a_{n-1} q_{k-1}(x) g(x))
\]
\[
= r(x) - h(x) g(x)
\]

where \( h(x) = a_{n-k} q_0(x) + ... + a_{n-1} q_{k-1}(x) \). Thus \( r(x) = h(x) g(x) + s(x) \).

Since \( \deg r_i(x) \leq n-k-1 \), it follows that \( \deg s(x) \leq n-k-1 \). By the uniqueness of the quotient and remainder in the division algorithm for polynomials, we conclude that \( s(x) \) is the remainder when \( r(x) \) is divided by \( g(x) \). \(\square\)
Syndromes

Thus the syndrome of a vector can be determined by polynomial division. Furthermore, the syndrome of a vector and its cyclic shift are closely related. Suppose

\[ r(x) = q(x)g(x) + s(x), \]

where \( \deg s(x) \) is at most \( n-k-1 \). By the above theorem \( s(x) \) is the syndrome of \( r(x) \). Now

\[ xr(x) = xq(x)g(x) + xs(x). \]

If \( xs(x) \) has degree at most \( n-k-1 \), then again by the above theorem it is the syndrome of \( xr(x) \). Otherwise, the syndrome of \( xr(x) \) is the remainder when \( xs(x) \) is divided by \( g(x) \). In this case, let

\[ s(x) = \sum_{i=0}^{n-k-1} s_i x^i = \hat{s}(x) + s_{n-k-1} x^{n-k-1}, \]

where degree \( \hat{s}(x) \leq n-k-2 \).
 Syndromes

Let the (monic) generator polynomial be,

\[ g(x) = \sum_{i=0}^{n-k} g_i x^i = \hat{g}(x) + x^{n-k}, \text{ degree } \hat{g}(x) \leq n-k-1. \]

Then

\[ x s(x) = x \hat{s}(x) + s_{n-k-1} (g(x) - \hat{g}(x)) \]

\[ = s_{n-k-1} g(x) + (x \hat{s}(x) - s_{n-k-1} \hat{g}(x)), \]

where degree \( x \hat{s}(x) - s_{n-k-1} \hat{g}(x) \leq n-k-1. \]

Now by the uniqueness of the remainder in the division algorithm and the previous theorem, we see that the syndrome of \( xs(x) \) is \( xs(x) - s_{n-k-1} g(x) \). We summarize this as,
Syndromes

**Theorem 9**: Let $C$ be a cyclic $[n,k]$-code over $F$ with generator polynomial $g(x)$, and let $r(x)$ be a polynomial with syndrome $s(x) = s_0 + s_1 x + \ldots + s_m x^m$. Then the syndrome of $xr(x)$ is

\[
xs(x) \quad \text{if } \deg s(x) < n-k-1, \text{ and }
\]

\[
xs(x) - s_{n-k-1} g(x), \quad \text{if } \deg s(x) = n-k-1.
\]

\[\square\]
Example

Consider the previous example with $g(x) = 1 + x + x^3$. From the generator matrix written there, we may form the parity check matrix,

$$H = [I_3 - R^T] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$ 

Consider $r = (1011011)$. The syndrome of $r$ is $Hr^T = (001)^T = s$. Now, $r(x) = 1 + x^2 + x^3 + x^5 + x^6$. If we divide $r(x)$ by $g(x)$, we get $r(x) = (x^3 + x^2 + x + 1)g(x) + x^2$. The remainder is, as expected, $s$.

To compute the syndrome of a cyclic shift of $r$, let $w = (1101101)$ which corresponds to the polynomial $xr(x)$. $Hw^T = (110)^T$. Using polynomial operations, since $\text{deg } s(x) = 2 = n-k-1$, the syndrome of $xr(x)$ is $xs(x) - 1g(x) = x^3 - (x^3 + x + 1) = 1 + x$. 
The preceding observations lead us to an interesting method of decoding certain error patterns in cyclic codes. The technique is sometimes referred to as *error trapping*.

Suppose $C$ is an $[n,k]$-code with minimum distance $d = 2t + 1$, and parity-check matrix $H = [I_{n-k} \ A]$. Let $c$ be a codeword and $e$ an error pattern of weight at most $t$. If $r = c + e$ is received, then the syndrome of $r$ is

$$s = H \ r^T = H \ (c + e)^T = H \ e^T.$$ 

Let $e^* = (s^T, 0)$, where $0$ is the $k$-tuple of all 0's. Then $H \ e^{*T} = s$, and $e^*$ and $e$ have the same syndrome, so are in the same coset of $C$. Now suppose $\text{wt}(s) \leq t$. Then $\text{wt}(e^*) \leq t$ and it follows that $e = e^*$ since a coset can contain at most one vector of weight less than or equal to $t$. Hence, the error is known to be $e = (s^T,0)$ in this case.
Now suppose $C$ is cyclic with generating polynomial $g(x)$. Let $e$ be an error pattern of weight at most $t$ with a cyclic run of at least $k$ 0's. Then there is some $i$, $0 \leq i \leq n-1$, such that a cyclic shift of $e$ through $i$ positions is a vector whose non-zero components all lie within the first $n-k$ components. For this $i$, $\text{wt}(s_i(x)) \leq t$, where $s_i(x)$ is the syndrome of $x^i e(x) \mod (x^n - 1)$. If we compute $s_i(x)$ as the remainder of $x^i r(x)$ divided by $g(x)$, then when $\text{wt}(s_i(x)) \leq t$, for this $i$ by the above argument $x^i e(x) = (s_i, 0)$. Thus $e(x) = x^{n-i}(s_i, 0)$. 
Error Trapping

This gives rise to the following algorithm (stated for the binary case, but easily modifiable for the q-ary case):

(1) Compute the syndrome $s_0(x)$ of $r(x)$ from the division algorithm.
(2) Set $i = 0$.
(3) If $\text{wt}(s_i(x)) \leq t$, then set $e(x) = x^{n-i}(s_i,0)$, and decode to $r(x) - e(x)$.
(4) Set $i = i + 1$.
(5) If $i = n$ then stop; the error pattern is not trappable.
(6) If $\deg s_{i-1}(x) < n-k-1$, then set $s_i(x) = xs_{i-1}(x)$;
    otherwise $s_i(x) = xs_{i-1}(x) - g(x)$.
(7) Go to (3).
Example

g(x) = 1 + x^2 + x^3 generates a binary [7,4]-cyclic code having minimum distance 3 (and so is 1-error correcting). Consider the codeword \(1 + x + x^5 = (1 + x + x^2) \ g(x)\), if upon transmission \(r(x) = 1 + x + x^5 + x^6\) is received we would decode as follows. Divide \(r(x)\) by \(g(x)\) to find the syndrome,

\[ r(x) = (x^3 + 1)g(x) + (x + x^2), \]

so \(s(x) = x + x^2\). Since the weight of \(s(x)\) is > 1 (= t), we compute the syndrome \(s_1(x)\) of \(xr(x)\). As the degree of \(s(x) = 2 = n - k - 1\), we multiply \(s(x)\) by \(x\) and subtract \(g(x)\) to get \(s_1(x) = 1\). As this has weight 1, we obtain the error pattern

\[ e(x) = x^{7-1}(s_1,0) = x^6(1000000) = x^6. \]

Since for \(n = 7\) all error patterns of weight 1 have a cyclic run of six 0's and \(6 > k = 4\), this technique will correct all single errors.
Example

g(x) = 1 + x^4 + x^6 + x^7 + x^8 generates a binary [15,7]-cyclic code. If the minimum distance of this code is 5, then t = 2. Any (at most) weight 2 error pattern must contain a run of at least 7 0's and so can be trapped. If a received 15-tuple is

\[ r = (1100 \ 1110 \ 1100 \ 010) \]

we calculate,

\[ r(x) = (x + x^2 + x^4 + x^5)g(x) + (1 + x^2 + x^5 + x^7). \]

We then compute the syndrome \( s_i(x) \) of \( x^i r(x) \) until \( \text{wt}(s_i(x)) \leq 2 \).

\[
\begin{align*}
  s_0(x) &= 10100101 & s_1(x) &= 11011001 & s_2(x) &= 11100111 \\
  s_3(x) &= 11111000 & s_4(x) &= 01111100 & s_5(x) &= 00111110 \\
  s_6(x) &= 00011111 & s_7(x) &= 10000100
\end{align*}
\]

Thus the error pattern is

\[ e = x^{15-7}(s_7,0) = x^8(100001000000000000) = (0000 \ 0000 \ 1000 \ 010), \]

and we decode \( r(x) \) to \( r - e = (1100 \ 1110 \ 0100 \ 000) \).