Coding Theory: Cyclic Codes (III)
A linear cyclic code $C$ of length $n$ contains all $n$ cyclic shifts of any codeword.

$c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n \iff c(X) = c_0 + \ldots + c_{n-1}X^{n-1}$

$C = \{q(X)g(X), \ q(X) \in \mathbb{F}_q[X], \deg(q(X)) < n - r\}$, where $g(X)$ is the monic polynomial of lowest degree $r$ in $C$ called the generator polynomial.

$\dim(C) = n - r = k$

$g(X)h(X) = X^n - 1, \ h(X) = \text{check polynomial}$

Generator matrix is obtained by shifts of the coefficients of $g(X)$.

Divisors $g(X)$ of $X^n - 1 \iff$ cyclic codes of length $n$. 
If $C$ has check polynomial $h(X)$ then $C = \{c(X), \deg c(X) \leq n - 1, c(X)h(X) \equiv 0 \pmod{X^n - 1}\}$.

We prove both inclusions. If $c(X) \in C$, then $c(X) = q(X)g(X)$. Then $c(X)h(X) = q(X)g(X)h(X) = q(X)(X^n - 1)$.

Suppose now $c(X)$ is such that $c(X)h(X) = p(X)(X^n - 1) = p(X)g(X)h(X)$. Thus $[c(X) - p(X)g(X)]h(X) = 0$ but $h(X)$ cannot be 0. Then $c(X) - p(X)g(X) = 0 \Rightarrow c(X) = p(X)g(X)$ as desired.
Consider the (7, 3) linear binary code
\[ C = \{ q(X)(1 + X^2 + X^3 + X^4), \; q(X) \in \mathbb{F}_q[X], \; \deg(q(X)) < 3 \} : \]
\[
\begin{array}{cc}
q(X)g(X) & \text{codeword} \\
\hline
0 & (0, 0, 0, 0, 0, 0, 0) \\
1 + X^2 + X^3 + X^4 & (1, 0, 1, 1, 1, 0, 0) \\
X + X^3 + X^4 + X^5 & (0, 1, 0, 1, 1, 1, 0) \\
1 + X + X^2 + X^5 & (1, 1, 1, 0, 0, 1, 0) \\
X^2 + X^4 + X^5 + X^6 & (0, 0, 1, 0, 1, 1, 1) \\
1 + X^3 + X^5 + X^6 & (1, 0, 0, 1, 0, 1, 1) \\
X + X^2 + X^3 + X^6 & (0, 1, 1, 1, 0, 0, 1) \\
1 + X + X^4 + X^6 & (1, 1, 0, 0, 1, 0, 1) \\
\end{array}
\]
Since \((1 + X^2 + X^3)(1 + X^2 + X^3 + X^4) = X^7 - 1,\)
\[ h(X) = 1 + X^2 + X^3. \]
Does \( (1, 0, 1, 1, 1, 0, 0) \) belong to \( C \)?
Does \((1, 0, 1, 1, 1, 0, 0)\) belong to \(C\)?

\[
(1 + X^2 + X^3 + X^4)(1 + X^2 + X^3) = 1 + X^2 + X^3 + X^2 + X^4 + X^5 + X^3 + X^5 + X^6 + X^4 + X^6 + X^7 = 1 + X^7.
\]
Does \((1, 0, 1, 1, 1, 0, 0)\) belong to \(C\)?

\[
(1 + X^2 + X^3 + X^4)(1 + X^2 + X^3) = 1 + X^2 + X^3 + X^2 + X^4 + X^5 + X^3 + X^5 + X^6 + X^4 + X^6 + X^7 = 1 + X^7.
\]

Does \((1, 0, 1, 1, 1, 0, 1)\) belong to \(C\)?
Check polynomial
Example (2)

Does \((1, 0, 1, 1, 1, 0, 0)\) belong to \(C\)?
\[
(1 + X^2 + X^3 + X^4)(1 + X^2 + X^3) = 1 + X^2 + X^3 + X^2 + X^4 + X^5 + X^3 + X^5 + X^6 + X^4 + X^6 + X^7 = 1 + X^7.
\]

Does \((1, 0, 1, 1, 1, 0, 1)\) belong to \(C\)?
\[
(1 + X^2 + X^3 + X^4 + X^6)(1 + X^2 + X^3) = 1 + X^2 + X^3 + X^2 + X^4 + X^5 + X^3 + X^5 + X^6 + X^4 + X^6 + X^7 + X^6 + X^8 + X^9 = 1 + X^7 + X^6 + X^8 + X^9 \equiv X^6 + X^8 + X^9 \equiv X^6 + X + X^2 \pmod{X^7 - 1}.
\]
Reverse code $C^{[-1]}$. The reverse code $C^{[-1]}$ of a cyclic code is cyclic.

Code obtained by reversing every codeword of $C$.

$$(c_0, \ldots, c_i, \ldots, c_{n-1}) \in C \iff (c_{n-1}, \ldots, c_{n-1-i}, \ldots, c_0) \in C^{[-1]}.$$
Reverse code $C^{[-1]}$.

Code obtained by reversing every codeword of $C$.

$$(c_0, \ldots, c_i, \ldots, c_{n-1}) \in C \iff (c_{n-1}, \ldots, c_{n-1-i}, \ldots, c_0) \in C^{[-1]}.$$ 

The reverse code $C^{[-1]}$ of a cyclic code is cyclic.

In polynomial notation: $c(X) \in C \iff X^{n-1}c(X^{-1}) \in C^{[-1]}$. 
Reciprocal polynomial.

\[ p^{[-1]}(X) = \sum_{i=0}^{d} p_{d-i} X^i = X^d p(X^{-1}). \]

For example, suppose \( h(X) = h_0 + h_1 X + \ldots h_k X^k \), then \( h^{[-1]}(X) = X^k (h_0 + h_1 X^{-1} + \ldots h_k X^{-k}) = h_k + h_{k-1} X + \ldots + h_0 X^k \).
Let $C$ be a cyclic code of length $n$ and check polynomial $h(X) = \sum_{i=0}^{k} h_i X^i$ of degree $k$. Then a parity-check matrix $H$ is:

$$
H = \begin{bmatrix}
    h_k & h_{k-1} & \ldots & h_1 & h_0 & 0 & \ldots & 0 \\
    0 & h_k & h_{k-1} & \ldots & h_1 & h_0 & 0 & \ldots & 0 \\
    \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots & \vdots \\
    0 & 0 & h_k & h_{k-1} & h_1 & h_0
\end{bmatrix}
$$

and $C^\perp$ is the cyclic code generated by the polynomial $h^{[-1]}(X)$. 
A polynomial \( c(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1} \) is a codeword from \( C \) if \( c(X)h(X) = 0 \). For \( c(X)h(X) \) to be 0, the coefficients of \( X^k, \ldots, X^{n-1} \) must be 0, i.e.,

\[
\begin{align*}
c_0h_k + c_1h_{k-1} + \ldots + c_kh_0 &= 0 \\
c_1h_k + c_2h_{k-1} + \ldots + c_{k+1}h_0 &= 0 \\
&\vdots \\
c_{n-k-1}h_k + c_{n-k}h_{k-1} + \ldots + c_{n-1}h_0 &= 0
\end{align*}
\]

Thus any codewords \((c_0, c_1, \ldots, c_{n-1}) \in C\) is orthogonal to \((h_k, h_{k-1}, \ldots, h_0, 0 \ldots, 0)\) and to its cyclic shifts.
A polynomial \( c(X) = c_0 + c_1X + \ldots + c_{n-1}X^{n-1} \) is a codeword from \( C \) if \( c(X)h(X) = 0 \). For \( c(X)h(X) \) to be 0, the coefficients of \( X^k, \ldots, X^{n-1} \) must be 0, i.e.,

\[
\begin{align*}
    c_0h_k &+ c_1h_{k-1} + \ldots + c_kh_0 = 0 \\
    c_1h_k &+ c_2h_{k-1} + \ldots + c_{k+1}h_0 = 0 \\
    &\vdots \\
    c_{n-k-1}h_k &+ c_{n-k}h_{k-1} + \ldots + c_{n-1}h_0 = 0
\end{align*}
\]

Thus any codewords \((c_0, c_1, \ldots, c_{n-1}) \in C\) is orthogonal to \((h_k, h_{k-1}, \ldots, h_0, 0 \ldots, 0)\) and to its cyclic shifts. Rows of the matrix \( H \) are in \( C^\perp \). Since \( h_k = 1 \), the rows are linearly independent, and there are \( n - k = \dim(C^\perp) \). Hence \( H \) is a generator matrix for \( C^\perp \), and thus a parity-check matrix for \( C \).
Left to prove: $C^\perp$ is generated by the polynomial $h^{[-1]}(X)$. It is sufficient to show that $h^{[-1]}(X)$ is factor of $X^n - 1$.

Recall that $h^{[-1]}(X) = X^k h(X^{-1})$. Then

$h(X^{-1}) g(X^{-1}) = (X^{-1})^n - 1$, multiplying by $X^n$ gives

$X^k h(X^{-1}) X^{n-k} g(X^{-1}) = X^n ((X^{-1})^n - 1) = 1 - X^n$. 
**Exercise.** Consider the binary code of length 7 with generator polynomial \( g(X) = 1 + X^2 + X^3 + X^4 \). Construct its parity check matrix.
Exercise. Consider the binary code of length 7 with generator polynomial $g(X) = 1 + X^2 + X^3 + X^4$. Construct its parity check matrix.

Since $(1 + X^2 + X^3)(1 + X^2 + X^3 + X^4) = X^7 - 1,$
$h(X) = 1 + X^2 + X^3$.

$$H = \begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1
\end{bmatrix}$$
We can check that $HG^T = 0$:

\[
\begin{bmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
1 & 0 & 1 \\
1 & 1 & 0 \\
1 & 1 & 1 \\
0 & 1 & 1 \\
0 & 0 & 1
\end{bmatrix}
\]
For a linear \((n, k)\) cyclic code \(\mathcal{C}\) with generator polynomial \(g(X)\) of degree \(r\):

- Length is \(n\).
- Dimension is \(k = n - r\).
- Generator matrix is obtained by shifts of the coefficients of \(g(X)\).
- Parity check matrix is obtained by shifts of the coefficients of \(h[-1](X)\).
- \(\mathcal{C}^\perp\) is a cyclic code generated by \(h[-1](X)\).
A cyclic code is defined by its generator polynomial \( g(X) \), for \( g(X) \) a divisor of \( X^n - 1 \).

The polynomial \( g(X) \in \mathbb{F}_q[X] \) is factorized into a product of irreducible polynomials:

\[
g(X) = \prod_s M_s(X), \quad M_s(X) \in \mathbb{F}_q[X], \quad M_s(X)|X^n - 1.
\]

E.g. \( g(X) = 1 + X^2 + X^3 + X^4 = (X + 1)(X^3 + X + 1) \).

A cyclic code is defined by the irreducible factors \( M_s(X) \) of \( g(X) \), for \( M_s(X) \) a divisor of \( X^n - 1 \).
A cyclic code is defined by its generator polynomial \( g(X) \), for \( g(X) \) a divisor of \( X^n - 1 \).

The polynomial \( g(X) \in \mathbb{F}_q[X] \) is factorized into a product of irreducible polynomials:

\[
g(X) = \prod_s M_s(X), \quad M_s(X) \in \mathbb{F}_q[X], \quad M_s(X) | X^n - 1.
\]

E.g. \( g(X) = 1 + X^2 + X^3 + X^4 = (X + 1)(X^3 + X + 1) \).

A cyclic code is defined by the irreducible factors \( M_s(X) \) of \( g(X) \), for \( M_s(X) \) a divisor of \( X^n - 1 \).

Every \( M_s(X) \) can be factorized as \( M_s(X) = \prod_{i \in C_s} (X - \alpha_i) \) over a finite field that contains all the roots of \( X^n - 1 = \prod_{i=0}^{n-1} (X - \alpha_i) \).

A cyclic code is defined by the roots of \( g(X) \), which form a subset of the roots of \( X^n - 1 \).
• If \( \alpha \) is a root of \( X^n - 1 \), then \( \alpha^n = 1 \) and \( \alpha \) is an \( n \)th root of unity.

• Roots of \( X^n - 1 \) may or not be repeated. E.g.
  \[ X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X + 1)^2 \]
  over \( \mathbb{F}_2 \), so it has 4 roots, all of them are 1 (and 1 is a 4rth root of unity).

• Claim: if \((n, q) = 1\), the roots of \( X^n - 1 \) are not repeated. From now on, we assume \((n, q) = 1\).
Cyclic Codes

■ Roots of $X^n - 1$

- If $\alpha$ is a root of $X^n - 1$, then $\alpha^n = 1$ and $\alpha$ is an $n$th root of unity.
- Roots of $X^n - 1$ may or not be repeated. E.g.
  $X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X + 1)^2$ over $\mathbb{F}_2$, so it has 4 roots, all of them are 1 (and 1 is a 4rth root of unity).
- Claim: if $(n, q) = 1$, the roots of $X^n - 1$ are not repeated. From now on, we assume $(n, q) = 1$.
- Since $X^n - 1 \in \mathbb{F}_q[X]$ has no repeated root when $(n, q) = 1$, this means that its $n$ roots are $n$ distinct $n$th roots of unity (that is all $n$th roots of unity).
Cyclic Codes

- Claim: Exactly when $n | q^t - 1$, $\mathbb{F}_{q^t}$ contains a primitive $n$th root of unity $\alpha$ that is an element $\alpha$ such that
  $$\alpha, \alpha^2, \alpha^3, \ldots \alpha^n = 1.$$ 

- When $n | q^t - 1$, we can find all the roots of $X^n - 1$ in $\mathbb{F}_{q^t}$. E.g. when $q = 2$, and $n = 7$, we need $t$ such that $7 | 2^t - 1$. 

For example take $t = 3$. Then $\mathbb{F}_{q^t} = \mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$:

- $\omega_3 = \omega + 1$,
- $\omega_4 = \omega^2 + \omega$,
- $\omega_5 = \omega^3 + \omega^2 = \omega^2 + 1$,
- $\omega_6 = \omega^3 + \omega^2 + \omega = \omega^2 + 1$,
- $\omega_7 = \omega^3 + \omega = 1$. Thus $\omega$ is a 7th root of unity and $(\omega^i)_7^{i=1} = (\omega^7)^i = 1$, $i = 1, \ldots, 7$ we thus have found the 7 roots of $X^7 - 1 = \prod_{i=1}^{7} (X - \alpha_i)$. 
- **Claim:** Exactly when $n|q^t - 1$, $\mathbb{F}_{q^t}$ contains a primitive $n$th root of unity $\alpha$ that is an element $\alpha$ such that

$$\alpha, \alpha^2, \alpha^3, \ldots \alpha^n = 1.$$

- When $n|q^t - 1$, we can find all the roots of $X^n - 1$ in $\mathbb{F}_{q^t}$. E.g. when $q = 2$, and $n = 7$, we need $t$ such that $7|2^t - 1$. For example take $t = 3$. Then

$$\mathbb{F}_{q^t} = \mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1): \omega^3 = \omega + 1, \omega^4 = \omega^2 + \omega, \omega^5 = \omega^3 + \omega^2 = \omega^2 + \omega + 1, \omega^6 = \omega^3 + \omega^2 + \omega = \omega^2 + 1, \omega^7 = \omega^3 + \omega = 1.$$  

Thus $\omega$ is a 7th root of unity and

$$(\omega^i)^7 = (\omega^7)^i = 1, \ i = 1, \ldots, 7$$

we thus have found the 7 roots of $X^7 - 1 = \prod_{i=1}^{7}(X - \alpha^i)$. 
• Claim: Exactly when $n|q^t - 1$, $\mathbb{F}_{q^t}$ contains a primitive $n$th root of unity $\alpha$. We will choose $t$ to be the smallest such $t$.

• E.g. when $q = 2$, and $n = 7$, we need $t$ such that $7|2^t - 1$. We already saw that we can choose $t = 3$. 
• Claim: Exactly when \( n | q^t - 1 \), \( \mathbb{F}_{q^t} \) contains a primitive \( n \)th root of unity \( \alpha \). We will choose \( t \) to be the smallest such \( t \).

• E.g. when \( q = 2 \), and \( n = 7 \), we need \( t \) such that \( 7 | 2^t - 1 \). We already saw that we can choose \( t = 3 \). We could also pick \( t = 6 \), but \( t = 3 \) is the smallest suitable \( t \), thus we will choose \( t = 3 \) over \( t = 6 \).
A cyclic code is defined by its generator polynomial

\[ g(X) = \prod_s M_s(X) = \prod_s \prod_{i \in C_s} (X - \alpha^i), \]

for \( g(X) \) a divisor of \( X^n - 1 \), thus by the roots \( \alpha^i \) of \( g(X) \), and since we only have powers of \( \alpha \), a cyclic code is defined by the sets \( C_s \).

E.g. \( g(X) = 1 + X^2 + X^3 + X^4 = (X + 1)(X^3 + X + 1) \):
\( C_0 = \{0\}, \ C_1 = \{1, 2, 4\} \).
For \( 0 \leq s < n \), the \( q \)-cyclotomic coset of \( s \) modulo \( n \) is

\[ C_s = \{ s, sq, \ldots, sq^{u-1} \} \pmod{n} \]

(\( \pmod{n} \)), \( u \) is the smallest positive integer such that \( q^u \equiv 1 \pmod{n} \).

When \( n = 7, q = 2, u = 3 \), since \( 2, 2^2 \equiv 4, 2^3 \equiv 1 \pmod{7} \). Then we have \( \{ 1, 2, q^{u-1} = 2^2 = 4 \} \):

\[
\begin{align*}
C_0 &= \{0\} \\
C_1 &= \{1, 2, 4\} = C_2 = C_4 \\
C_3 &= \{3, 6, 5\} = C_5 = C_6
\end{align*}
\]
For $n = 7$, $q = 2$: $X^7 - 1 = \prod_{i=1}^{7} (X - \alpha^i)$:

List all roots

$\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$

Group the roots

$\alpha^0, \alpha^1, \alpha^2, \alpha^4 \quad \alpha^3, \alpha^5, \alpha^6$

$C_0 \quad C_1 \quad C_2$

Compose $g(X)$

$X - 1$

$(X - \alpha)(X - \alpha^2)(X - \alpha^4)$

$(X - \alpha^3)(X - \alpha^5)(X - \alpha^6)$

$(X - 1)(X - \alpha)(X - \alpha^2)(X - \alpha^4)$

$(X - 1)(X - \alpha^3)(X - \alpha^5)(X - \alpha^6)$

$(X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^3)(X - \alpha^5)(X - \alpha^6)$

$X^7 - 1$
Cyclic Codes

Factors of $g(X)$

For $n = 7$, $q = 2$:

$$X^7 - 1 = \prod_{i=1}^{7} (X - \alpha^i):$$

List all roots: $\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$

Group the roots:

$C_0$: $\{\alpha^0, \alpha^1, \alpha^2, \alpha^4\}$
$C_1$: $\{\alpha^3, \alpha^5, \alpha^6\}$

Compose $g(X)$:

$X + 1$
$X^3 + X + 1$
$X^3 + X^2 + 1$
$X^4 + X^3 + X^2 + 1$
$X^4 + X^2 + X + 1$
$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
$X^7 - 1$
Defining set of $\mathcal{C}$

The set

\[ T = \bigcup_{s} C_s, \]

\[ C_s = \{s, sq, \ldots, sq^{u-1}\} \pmod{n}. \]

\[ Z = \{\alpha^i, \ i \in T\} \]

is called the set of zeros of $\mathcal{C}$.

\[ T = C_0 \cup C_1 = \{0, 1, 2, 4\} \]

is a defining set of $\mathcal{C}$ generated by $g(X) = 1 + X^2 + X^3 + X^4$ over $\mathbb{F}_2$. Also

\[ Z = \{1, \alpha, \alpha^2, \alpha^4\} \]

is the set of zeros of $\mathcal{C}$. 
Consecutive elements

The defining set
\[ T = \bigcup_s C_s \] contains \( v \) consecutive elements if there is a set
\[ S = \{b, b+1, \ldots, b+v-1\} \]
of \( v \) consecutive integers (mod \( n \)) such that
\[ S \subseteq T. \]

\[ T = C_0 \cup C_1 = \{0, 1, 2, 4\} \]
is a defining set of \( C \) generated by \( g(X) = 1 + X^2 + X^3 + X^4 \) over \( \mathbb{F}_2 \). Then \( T \) contains a set \( S \) of \( v = 3 \) consecutive elements:
\[ S = \{0, 1, 2\}. \]
BCH Bound

Let \( C \) be an \((n, k, d)\) cyclic code over \( \mathbb{F}_q \) with defining set \( T = \bigcup s \mathbb{C}_s \). If \( T \) contains \( \delta - 1 \) consecutive elements for some integer \( \delta \), then

\[ d \geq \delta. \]

Let \( C \) be the cyclic code generated by \( g(X) = 1 + X^2 + X^3 + X^4 \) over \( \mathbb{F}_2 \), with defining set \( T = C_0 \cup C_1 = \{0, 1, 2, 4\} \) which contains a set \( S = \{0, 1, 2\} \) of \( v = 3 = \delta - 1 \) consecutive elements. Thus

\[ d \geq 4. \]
**BCH Bound**

Let $\mathcal{C}$ be an $(n, k, d)$ cyclic code over $\mathbb{F}_q$ with defining set $T = \bigcup_s C_s$. If $T$ contains $\delta - 1$ consecutive elements for some integer $\delta$, then

$$d \geq \delta.$$ 

The code $\mathcal{C}$ has zeros that include $\alpha^b, \ldots, \alpha^{b+\delta-2}$. Let $c(X)$ be a nonzero codeword of $\mathcal{C}$ of weight $w$:

$$c(X) = \sum_{j=1}^{w} c_{ij} X^{ij}$$

Assume to the contrary that $w < \delta$. We have $c(\alpha^l) = 0$ for $b \leq l \leq b + \delta - 2$, since $g(X)$ divides $c(X)$. 

That \( c(\alpha^l) = 0 \) for \( b \leq l \leq b + \delta - 2 \) implies

\[
c(\alpha^l) = \sum_{j=1}^{w} c_{ij} (\alpha^l)^{ij}
\]

which gives the following system of equations:

\[
\begin{bmatrix}
\alpha^{i_1b} & \alpha^{i_2b} & \cdots & \alpha^{i_wb} \\
i_1(b+1) & \alpha^{i_2(b+1)} & \cdots & \alpha^{i_w(b+1)} \\
\vdots & \vdots & \ddots & \vdots \\
i_1(b+w-1) & \alpha^{i_2(b+w-1)} & \cdots & \alpha^{i_w(b+w-1)}
\end{bmatrix}
\begin{bmatrix}
c_{i_1} \\
c_{i_2} \\
\vdots \\
c_{i_w}
\end{bmatrix}
\neq 0
\]

\((w < \delta \iff w+1 \leq \delta \iff w \leq \delta - 1 \iff b+w-1 \leq b+\delta-2)\).
Then $M$ must satisfy $\det(M) = 0$ but

$$M = \begin{bmatrix}
\alpha^{i_1 b} & \ldots & \alpha^{i_w b} \\
\alpha^{i_1 (b+1)} & \ldots & \alpha^{i_w (b+1)} \\
\vdots & \ddots & \vdots \\
\alpha^{i_1 (b+w-1)} & \ldots & \alpha^{i_w (b+w-1)}
\end{bmatrix} = \begin{bmatrix}
1 & \ldots & 1 \\
\alpha^{i_1} & \ldots & \alpha^{i_w} \\
\vdots & \ddots & \vdots \\
\alpha^{i_1 (w-1)} & \ldots & \alpha^{i_w (w-1)}
\end{bmatrix} D$$

with $D = \text{diag}(\alpha^{i_1 b}, \ldots, \alpha^{i_w b})$. 
Then $M$ must satisfy $\det(M) = 0$ but

$$M = \begin{bmatrix}
\alpha^{i_1 b} & \ldots & \alpha^{i_w b} \\
\alpha^{i_1 (b+1)} & \ldots & \alpha^{i_w (b+1)} \\
\vdots & \ddots & \vdots \\
\alpha^{i_1 (b+w-1)} & \ldots & \alpha^{i_w (b+w-1)}
\end{bmatrix} = \begin{bmatrix}
1 & \ldots & 1 \\
\alpha^{i_1} & \ldots & \alpha^{i_w} \\
\vdots & \ddots & \vdots \\
\alpha^{i_1 (w-1)} & \ldots & \alpha^{i_w (w-1)}
\end{bmatrix} D$$

with $D = \text{diag}(\alpha^{i_1 b}, \ldots, \alpha^{i_w b})$. Thus

$$\det(M) = \alpha^{(i_1 + \ldots + i_w)b} \prod_{l<j} (\alpha^{i_j} - \alpha^{i_l}) \neq 0$$

a contradiction.
BCH codes

BCH = BoseChaudhuri-Hocquenghem. For $2 \leq \delta \leq n$, a cyclic code of length $n$ over $\mathbb{F}_q$ and designed distance $\delta$ with defining set

$$T = C_b \cup \ldots \cup C_{b+\delta-2}.$$ 

By construction, $d \geq \delta$.

1. Fix $q, n$.
2. Compute the $q$-cyclotomic cosets modulo $n$.
3. Compute consecutive elements to find possible designed distance $\delta$.
4. Find a primitive $n$th root of unity.
5. Map $q$-cyclotomic cosets to polynomials.
1. Let us fix $n = 13$ and $q = 3$.

2. By definition the $q$-cyclotomic coset of $s$ modulo $n$ is

$$C_s = \{s, sq, \ldots, sq^{u-1}\} \pmod{n},$$

where $u$ is the smallest positive integer such that $q^u \equiv 1 \pmod{n}$.
1. Let us fix $n = 13$ and $q = 3$.
2. By definition the $q$-cyclotomic coset of $s$ modulo $n$ is

$$C_s = \{s, sq, \ldots, sq^{u-1}\} \pmod{n},$$

$u$ is the smallest positive integer such that $q^u \equiv 1 \pmod{n}$. We have $3, 3^2 = 9, 3^3 = 27 \equiv 1 \pmod{13}$ so $C_s = \{s, s3, s9\}$. 
1. Let us fix $n = 13$ and $q = 3$.
2. By definition the $q$-cyclotomic coset of $s$ modulo $n$ is

$$C_s = \{s, sq, \ldots, sq^{u-1}\} \pmod{n},$$

$u$ is the smallest positive integer such that $q^u \equiv 1 \pmod{n}$.

We have $3, 3^2 = 9, 3^3 = 27 \equiv 1 \pmod{13}$ so $C_s = \{s, s3, s9\}$. We compute $C_0 = \{0\}, C_1 = \{1, 3, 9\}, C_2 = \{2, 6, 5\}, C_4 = \{4, 12, 10\}, C_7 = \{7, 8, 11\}$. 
3. $C_0 = \{0\}, C_1 = \{1, 3, 9\}, C_2 = \{2, 6, 5\}, C_4 = \{4, 12, 10\}, C_7 = \{7, 8, 11\}.

$C_1$: it has $\delta - 1 = 1$ consecutive element, so designed distance $\delta = 2$.

$C_0 \cup C_1 = \{0, 1, 3, 9\}$: it has $\delta - 1 = 2$ consecutive elements, so designed distance $\delta = 3$.

$C_0 \cup C_1 \cup C_2 = \{0, 1, 2, 3, 5, 6, 9\}$: it has $\delta - 1 = 4$ consecutive elements, so designed distance $\delta = 5$. 
4. To find a primitive 13th root of unity, we know we need to find the smallest \( t \) such that \( n = 13|(q^t - 1) \), that is \( 13|3^t - 1 \). When \( t = 3 \), \( 3^3 - 1 = 26 \) which is divisible by 13.
4. To find a primitive 13th root of unity, we know we need to find the smallest $t$ such that $n = 13|(q^t - 1)$, that is $13|3^t - 1$. When $t = 3$, $3^3 - 1 = 26$ which is divisible by 13. We thus look for a primitive 13th root in $\mathbb{F}_{3^3}$. The polynomial $X^3 + 2X + 1 = 0$ is irreducible modulo 3. Let $\alpha$ be such that $\alpha^3 + 2\alpha + 1 = 0$, so $\alpha^3 = \alpha - 1$. Then $\alpha^6 = \alpha^2 + \alpha + 1$, $\alpha^{12} = \alpha^4 - \alpha^3 + 2\alpha + 1 = \alpha^2 - 1$ so $\alpha^{13} = \alpha^3 - \alpha = -1$. This shows that $\alpha^2$ is a primitive 13th root of unity.
5. We have $\alpha^2$ a primitive 13th root of unity for $\alpha$ such that $\alpha^3 + 2\alpha + 1 = 0$. Thus

\[
\begin{align*}
C_0 &= \{0\} & X - 1 \\
C_1 &= \{1, 3, 9\} & (X - \alpha^2)(X - \alpha^6)(X - \alpha^{18}) = X^3 + X^2 + X + 2 \\
C_2 &= \{2, 6, 5\} & (X - \alpha^4)(X - \alpha^{12})(X - \alpha^{10}) = X^3 + X^2 + 2 \\
C_4 &= \{4, 12, 10\} & (X - \alpha^8)(X - \alpha^{24})(X - \alpha^{20}) = X^3 + 2X^2 + 2X + 2 \\
C_7 &= \{7, 8, 11\} & (X - \alpha^{14})(X - \alpha^{16})(X - \alpha^{22}) = X^3 + 2X + 2
\end{align*}
\]
BCH codes

For $2 \leq \delta \leq n$, a cyclic code of length $n$ over $\mathbb{F}_q$ and designed distance $\delta$ with defining set $T = C_b \cup \ldots \cup C_{b+\delta-2}$. When $b = 1$, $C$ is called a narrow-sense BCH code. If $n = q^t - 1$, then $C$ is called a primitive BCH code.

For $n = 13$ and $q = 3$, $q^t - 1 = 3^3 - 1 = 26$, so $n = 13|q^t - 1$ so we are not getting primitive BCH codes.

The code with generator polynomial $(X - \alpha^2)(X - \alpha^6)(X - \alpha^{18})$ is a narrow-sense BCH.
Parity check matrix
Dual code
BCH bound
BCH codes (narrow-sense, primitive)