A linear code $C \subseteq F^n$ is **cyclic** if

$$(a_n, a_1, ..., a_{n-1}) \in C \text{ for all } a = (a_1, ..., a_{n-1}, a_n) \in C.$$ 

In order to study cyclic codes, we need to introduce a few auxiliary algebraic concepts.

We have a unique $F$-linear isomorphism

$$\pi : F[x]_n \cong F[X]/(X^n - 1)$$

such that $x \mapsto [X]$. If $f \in F[X]$, its image $\bar{f} \in F[x]_n$ is determined by the substitution $X^j \mapsto x[j]_n = x^j \mod n$. We say that $\bar{f}$ is the **cyclic reduction of order $n$ of $f$**.
We can use the isomorphism $\pi$ to transport the ring structure of $F[X]/(X^n - 1)$ to a ring structure of the ring $F[x]_n$. This structure is determined by the ordinary sum and product of $F[x]$, except that the product is to be reduced modulo the relation $x^n = 1$.

On the other hand we have an $F$-linear isomorphism

$$F^n \cong F[x]_n = \{ \lambda_1 + \lambda_2 x + \cdots + \lambda_n x^{n-1} | \lambda_i \in F \}$$

$$a = (a_1, \ldots, a_n) \mapsto a(x) = a_1 + a_2 x + \cdots + a_n x^{n-1},$$

which allows us to transfer the ring structure of $F[x]_n$ to a ring structure of $F^n$. The sum in this ring is the ordinary sum of vectors, and the product $p = ab$ of the vectors $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ is obtained by accumulating the product $a_i b_j$ in the component $(i + j \mod n) - 1$ of $p$, $1 \leq i, j \leq n$.

**Notation.** If $f \in F[X]$ and $a \in F[x]$, $fa$ means $\bar{f}a$. 
Lemma. $s(a) = xa$, for all $a \in F[x]_n$, where
\[
\sigma(a_1 + a_2x + \cdots + a_nx^{n-1}) = a_n + a_1x + \cdots + a_{n-1}x^{n-1}.
\]

Proof. The product $xa$ is $a_1x + a_2x^2 + \cdots + a_nx^n$. Since $x^n = 1$, we have
\[
xa = a_n + a_1x + \cdots + a_{n-1}x^{n-1} = \sigma(a).
\]

Proposition. A linear code $C$ of length $n$ is cyclic if and only if it is an ideal of $F[x]_n$.

Proof. The lemma indicates that $C$ is cyclic if and only if $xC \subseteq C$. Now it is enough to observe that this condition implies that $x^jC \subseteq C$ for any positive integer $j$, and therefore that $aC \subseteq C$ for all $a \in F[x]_n$. 
Construction of cyclic codes

Given \( f \in F[X] \), we set \( C_f = (\bar{f}) \subseteq F[x]_n \). Note that \( C_f = \pi((f)) \).

**Lemma.** If \( g \) and \( g' \) are monic divisors of \( X^n - 1 \), then

1. \( C_g \subseteq C_{g'} \) if and only if \( g'|g \).
2. \( C_g = C_{g'} \) if and only if \( g = g' \).

**Proof.** The inclusion \( C_g \subseteq C_{g'} \) implies that \( \bar{g} = a \bar{g}' \), for some \( a \in F[x]_n \).
If \( a = \bar{f}, f \in F[X] \), the relation \( g = fg' \) holds mod \( X^n - 1 \). Since \( g' \) is a divisor of \( X^n - 1 \), say \( X^n - 1 = hg' \), we get \( g = fg' + hg' = (f + h)g' \), and so \( g'|g \). That \( g'|g \) implies \( C_g \subseteq C_{g'} \) is clear, and 2 is a direct consequence of 1 and the fact that \( g \) and \( g' \) are monic.

**Proposition.** Given a cyclic code \( C \) of length \( n \), there exists a unique monic divisor \( g \) of \( X^n - 1 \) such that \( C = C_g \).
**Proof.** Let \( g \in F[X] \) be a non-zero polynomial of minimal degree among those that satisfy \( g \in C \) (note that \( \pi(X^n - 1) = x^n - 1 = 0 \in C \), so that \( g \) exists and \( \deg(g) \leq n \)). We can assume that \( g \) is monic. Since \( C_g = (\bar{g}) \subseteq C \), we will end the proof of existence by establishing that

- \( g \) is a divisor of \( X^n - 1 \)
- \( C \subseteq C_g \).

Indeed, if \( q \) and \( r \) are the quotient and remainder of the division of \( X^n - 1 \) by \( g \), so that

\[
X^n - 1 = qg + r, \quad \deg(r) < \deg(g),
\]

then \( 0 = x^n - 1 = \bar{q}\bar{g} + \bar{r} \), and therefore \( \bar{r} = -\bar{q}\bar{g} \in C_g \subseteq C \). Consequently \( r = 0 \), by definition of \( g \), and hence \( g \mid X^n - 1 \).

Let now \( a \in C \). To see that \( a \in C_g \), let

\[
a_X = a_1 + a_2X + \cdots + a_nX^{n-1},
\]
so that \( a = a_1 + a_2x + \cdots + a_nx^{n-1} = \bar{a}_X \). Let \( q_a \) and \( r_a \) be the quotient and remainder of the Euclidean division of \( a_X \) by \( g \):

\[
a_X = q_ag + r_a, \quad \text{deg}(r_a) < \text{deg}(g).
\]

Thus \( \bar{r}_a = a - \bar{q}_a\bar{g} \in \mathcal{C}, r_a = 0 \) and \( a = \bar{q}_a\bar{g} \in C_g \).

The uniqueness of \( g \) is an immediate consequence of the previous lemma. \( \square \)

The monic divisor \( g \) of \( X^n - 1 \) such that \( \mathcal{C} = C_g \) is called the generating polynomial of \( \mathcal{C} \). The polynomial \( \hat{g} = (X^n - 1)/g \) is called the control polynomial of \( \mathcal{C} \) (we will see a reason for this term in a short while).

**Remark.** Given \( f \in F[X] \), the generating polynomial of \( C_f \) is \( g = \gcd(X^n - 1, f) \). Observe that

\[
C_f = (\bar{f}) = \pi((f)) = \pi((f) + (X^n - 1)) = \pi(\gcd(f, X^n - 1)).
\]
**Dimension of** $C_g$

**Proposition.** $\dim(C_g) = \deg(\hat{g}) = n - \deg(g)$.

**Proof.** It is enough to consider the $F$-linear map $F[X] \to F[x]^n, f \mapsto f\bar{g}$, and notice that its image is $(\bar{g}) = C_g$ and its kernel $(\hat{g})$. □

**Notations.** Instead of the set of indices $\{1, \ldots, n\}$, we will use the set $\{0,1,\ldots,n-1\}$. In this way $a = (a_0, a_1, \ldots, a_{n-1})$ is identified with the polynomial

$$a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$ 

Given $a \in F[x]^n$, we set $\ell(a) = a_{n-1}$ (the leading coefficient of $a$) and

$$\tilde{a} = a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1}.$$ 

Then we have that

$$\ell(\tilde{a}b) = a_0b_0 + \cdots + a_{n-1}b_{n-1}$$

(the scalar product of $a, b \in F[x]^n$).
If \( p \) is the characteristic of \( F \), suppose that \( p \nmid n \). In particular we have \( n \neq 0 \) in \( F \).

Since \( D(X^n - 1) = nX^{n-1} \sim X^{n-1} \) has no non-constant common divisors with \( X^n - 1 \), the irreducible factors \( f_1, \ldots, f_r \) of \( X^n - 1 \) are simple (i.e., have multiplicity 1):

\[
X^n - 1 = f_1 \cdots f_r .
\]

Thus the monic divisors of \( X^n - 1 \) have the form

\[
g = f_{i_1} \cdots f_{i_s}, \ 1 \leq i_1 < \cdots < i_s \leq r.
\]

From this it follows that there are exactly \( 2^r \) cyclic codes of length \( n \). Remark, however, that there may be non-trivial equivalences among these codes (we will see examples later on).
Generating matrices

The polynomials \( u_i = x^i \bar{g} \) \((0 \leq i < k)\) form a basis of \( C_g \). If

\[
g = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k},
\]

then the \( k \times n \) matrix

\[
G = \begin{pmatrix}
g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\
0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 \\
0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k}
\end{pmatrix}
\]

is a generating matrix of \( C = C_g \). Note that \( g_{n-k} = 1 \) (\( g \) is monic).

**Remark.** The coding \( F^k \rightarrow C_g, u \mapsto uG \), can be described, in terms of polynomials, as the map \( F[x]_k \rightarrow C_g, u \mapsto u\bar{g} \).
**Normalized generating matrix**

For $0 \leq j < k$, let

$$x^{n-k+j} = q_j g + r_j, \quad \text{deg}(r_j) < \text{deg}(g).$$

Then the $k$ polynomials $v_j = x^{n-k+j} - r_j$ form a basis of $C_g$ and the corresponding matrix of coefficients, $G'$, is normalized, in the sense that the submatrix formed by the last $k$ columns of $G'$ is the identity matrix $I_k$:

$$G' = -R|I_k, \quad R = \begin{pmatrix} r_{ji} \end{pmatrix}$$

Therefore, $H' = I_{n-k}|R^T$ is a normalized control matrix.

**Remark.** Let $u \in F^k \cong F[x]_k$. Then the coding of $u$ using the matrix $G'$ is obtained by substituting the monomials $x^j$ of $u$ by $v_j$ ($0 \leq j < k$):

$$u_0 + u_1 x + \cdots + u_{k-1} x^{k-1} \mapsto u_0 v_0 + u_1 v_1 + \cdots + u_{k-1} v_{k-1}.$$
Moreover, if $H'$ is the control matrix of $C_g$ associated to $G'$, then the syndrome $s \in F^{n-k} \cong F[x]_{n-k}$ of $a \in F^n \cong F[x]_n$ coincides with the remainder of the division of $a$ by $g$.

Notice that $s = aH'^T = a \begin{pmatrix} I_{n-k} \\ R \end{pmatrix}$.

The dual code

**Proposition.** $C_g^\perp = \tilde{C}_\hat{g}$, where $\tilde{C}_\hat{g}$ is the image of $C_\hat{g}$ by the map $a \mapsto \tilde{a}$.

**Proof.** Since $C_g^\perp$ and $\tilde{C}_\hat{g}$ have dimension $n - k$, it is enough to see that $\tilde{C}_\hat{g} \subseteq C_g^\perp$. But this is clear: if $a \in C_\hat{g}$ and $b \in C_g$, then $ab = 0$ and consequently $\langle \tilde{a} | b \rangle = \ell(\tilde{a}b) = \ell(ab) = 0$. \hfill \qed
Since $\hat{g}x^{n-k-1}, \ldots, \hat{g}x, \hat{g}$ form a basis of $C_{\hat{g}}$, if we let
\[
\hat{g} = h_0 + h_1X + \cdots + h_kX^k,
\]
then
\[
H = \begin{pmatrix}
  h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\
  0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\
  \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
  0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 & 0 \\
  0 & \cdots & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \\
\end{pmatrix}
\]

is a control matrix of $C_g$. 
Example (The ternary Golay code). The polynomial
\[ g = X^5 - X^3 + X^2 - X - 1 \]
is an irreducible factor of \( X^{11} - 1 \) over \( \mathbb{Z}_3 \). In fact, the irreducible factors of \( X^{11} - 1 \) over \( \mathbb{Z}_3 \) are \( X - 1, g, \) and \( X^5 + X^4 - X^3 + X^2 - 1 \) (notice that the 3-ciclotòmiques classes mod 11 are \( \{0\}, \{1,3,9,5,4\} \) and \( \{2,6,7,10,8\} \), and this shows that \( X^{11} - 1 \) two irreducible factors of degree 5).

Let \( q = 3, n = 11 \) and \( C = C_g \). Then the type of \( C \) is \([11,6]\). Let us see that the minimum distance of \( C \) is 5.

Let \( G \) be the normalized generating matrix of \( C \). The matrix \( \bar{G} \) (parity completion of \( G \)) satisfies that \( \bar{G}\bar{G}^T = 0 \) (in order to preserve the submatrix \( I_6 \) to the right, we place the parity symbols of the rows of \( G \) to the left, so that they form the first column of \( \bar{G} \)). It follows that the code \( \bar{C} = \langle \bar{G} \rangle \) is selfdual and therefore that the weight of any element of \( \bar{C} \) is a
multiple of 3. Since the rows of $\tilde{G}$ have weight 6, the minimum distance of $\tilde{C}$ is 3 or 6. But every row of $\tilde{G}$ has exactly one 0 in the first 6 columns, and the position of this 0 is different for different rows. This implies that a linear combination of two rows of $\tilde{G}$ has weight $\geq 2 + 2$ and hence $\geq 6$. Since the weight of this combination is clearly $\leq 12 - 4 = 8$, it must have weight 6. In particular, it contains exactly 2 zeros in its first six positions. This proves that a linear combination of 3 rows of $\tilde{G}$ has at least $1 + 3$ non-zero components, and therefore it has at least weight 6. Since the combinations of 4 or more rows of $\tilde{G}$ have weight $\geq 4$, this completes the proof.

\[
\tilde{G} = \begin{pmatrix}
1 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 2 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
2 & 1 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\]
# Computation of normalized generating matrix
# of the complete ternary Golay code \([11,6,5]_3\)

```plaintext
F=Zn(3); u=1:F;
g=x^5-x^3+x^2-x-u;

R=[vec(-rem(x^j,g),5) with j in 5..10];

G=[-sum(r) with r in R]|R|identity_matrix(6)

[[2,2,2,1,2,0,1,0,0,0,0,0],
 [2,0,2,2,1,2,0,1,0,0,0,0],
 [0,2,2,0,1,1,0,0,1,0,0,0],
 [2,1,0,1,1,1,0,0,0,1,0,0],
 [1,1,2,2,2,1,0,0,0,1,0,0],
 [0,1,2,1,0,2,0,0,0,0,0,1]]
:: Matrix(Z3)
```
# Factorization of $X^{11}-1$ over $\mathbb{Z}/(3)$
# $e_{11}(3)=5$; $x^5-x+1$ is irreducible of degree 5

F=extension(Zn(3),x^5-x+1);
# order(x)=242: x is primitive

a=x^(242/11);  # element d'ordre 11

f1=(X-a)*(X-a^3)*(X-a^9)*(X-a^5)*(X-a^4)  # $X^5+X^4+2*X^3+X^2+2 :: \mathbb{Z}_3[x][X]

f2=(X-a^2)*(X-a^6)*(X-a^7)*(X-a^10)*(X-a^8)  # $X^5+2*X^3+X^2+2*X+2 :: \mathbb{Z}_3[x][X]

factor(X^11-1,Zn(3))
(X+2)*(X^5+2*X^3+X^2+2*X+2)*(X^5+X^4+2*X^3+X^2+2) :: Divisor
Roots of a cyclic code

Let $F$ be a finite field and $q = |F|$. Let $C$ be a cyclic $F$-code of length $n$ and $g$ its generating polynomial. The roots of $C$ are, by definition, the roots of $g$ in a splitting field $F'$ of $X^n - 1$ over $F$ (recall that $|F'| = q^m$, where $m = e_n(q)$).

If $\omega \in F'$ is a primitive $n$-th root of unity and we write $E_g$ to denote the set of those $k \in \mathbb{Z}_n$ such that $\omega^k$ is a root of $g$, then $E_g$ is the union of the $q$-cyclotomic classes corresponding to the monic irreducible divisors of $g$.

If $E'_g \subseteq E_g$ is a subset formed by an element of each $q$-cyclotomic class contained in $E_g$, we say that

$$M = \{\omega^k | k \in E'_g\}$$

is a minimal set of roots of $C = C_g$. 
**Proposition.** If $M$ is a minimal set of roots of a cyclic code $C$, then

$$C = \{a \in F[x]_n \mid a(\xi) = 0 \text{ for all } \xi \in M\}.$$ 

**Determination of a cyclic code by specifying its roots.** Let now $\xi_1, \ldots, \xi_r \in F'$ be $n$-th roots of unity

$$C_{\xi_1, \ldots, \xi_r} = \{a \in F[x]_n \mid a(\xi_j) = 0 \text{ for all } j = 1, \ldots, r\}.$$

Then $C_{\xi_1, \ldots, \xi_r}$ is an ideal of $F[x]_n$ and we say that it is the cyclic code determined by $\xi_1, \ldots, \xi_r$.

**Proposition.** The generating polynomial of $C_{\xi_1, \ldots, \xi_r}$ is

$$g = \text{lcm}(g_1, \ldots, g_r),$$

where $g_i$ is the minimal polynomial of $\xi_i$. 
Control matrix of $C_{\xi_1, \ldots, \xi_r}$. The condition $a(\xi_j) = 0$ can be seen as a linear relation on the components $a_0, \ldots, a_{n-1}$ of $a$ with coefficients $1, \xi_j, \ldots, \xi_j^{n-1}$:

$$a_0 + a_1\xi_j + \cdots + a_{n-1}\xi_j^{n-1} = 0. \tag{[*]}$$

In other words, the matrix $V_n(\xi_1, \ldots, \xi_r)^T \in M_n^r(F')$ is a control matrix of $C_{\xi_1, \ldots, \xi_r}$.

If we express each $\xi_j^i$ as a vector of the components relative to a basis of $F'$ over $F$, the relation $[*]$ is equivalent to $m$ linear relations with coefficients in $F$ that have to be satisfied by $a_0, \ldots, a_{n-1}$. In this way we obtain a control matrix $\overline{H} \in M_n^m(F)$ with coefficients in $F$, and from $\overline{H}$ we can form a control matrix $H \in M_n^{n-k}(F)$ by eliminating linearly dependent rows.
**Example** (some Hamming codes are cyclic). Let \( m \) be a positive integer such that \( \gcd(m, q - 1) = 1 \), and define

\[
n = \frac{(q^m - 1)}{(q - 1)}.
\]

Let \( \omega \in F' \) be an \( n \)-th of unity of order \( n \) (if \( \alpha \in F' \) is a primitive element, we can take \( \omega = \alpha^{q-1} \)). Then \( C_\omega \) is equivalent to the Hamming code of codimension \( m \), \( \text{Ham}_q(m) \). Indeed,

\[
n = (q - 1)(q^{m-2} + 2q^{m-3} + \cdots + m - 1) + m,
\]

as it can be easily checked, and hence \( \gcd(n, q - 1) = 1 \). It follows that \( \omega^{q-1} \) is an \( n \)-th of unity of order \( n \), and therefore \( \omega^{i(q-1)} \neq 1 \) for \( i = 1, \ldots, n - 1 \). In particular, \( \omega^i \notin F \). Moreover, \( \omega^i \) and \( \omega^j \) are linearly independent over \( F \) if \( i \neq j \). As \( n \) is the greatest number of elements of \( F' \) that are pair-wise linearly independent over \( F \), the claim follows from the description above of the control matrix \( C_\omega \) and the definition of the Hamming code \( \text{Ham}_q(m) \).
**BCH codes**

Let $\omega \in F'$ be a primitive $n$-th root of unity. Let $\delta \geq 2$ and $\ell \geq 1$ be integers. Let $BCH_\omega(\delta, \ell)$ denote the cyclic code of length $n$ generated by the least common multiple $g$ of the minimal polynomials $g_i = p_{\omega^\ell+i}$, $i \in \{0, \ldots, \delta - 2\}$, which is called the BCH code (stemming from Bose–Chaudhuri–Hocquenghem) with *design distance* (or *intentional*) $\delta$ and *offset* $\ell$. In the case $\ell = 1$, we write $BCH_\omega(\delta)$ instead of $BCH_\omega(\delta, 1)$ and we say that they are *strict BCH* codes. An $BCH$ is called *primitive* if $n = q^m - 1$ (note that this condition is equivalent to say that $\omega$ is a primitive element of $F'$).

**Theorem** (The BCH bound). If $d$ is the minimum distance of $BCH_\omega(\delta, \ell)$, then $d \geq \delta$.

**Proof.** First note that an element $a \in F[x]_n$ is in $BCH_\omega(\delta, \ell)$ if and only if $a(\omega^{\ell+i}) = 0$ for all $i \in \{0, \ldots, \delta - 2\}$. But the relation $a(\omega^{\ell+i}) = 0$ is equivalent to
\[ a_0 + a_1 \omega^{\ell+i} + \cdots + a_{n-1} \omega^{(n-1)(\ell+i)} = 0, \]

and hence
\[ \left( 1, \omega^{\ell+i}, \omega^{2(\ell+i)}, \ldots, \omega^{(n-1)(\ell+i)} \right) \]

is a control vector of \( BCH_\omega(\delta, \ell) \). Now we claim that the matrix \( H \) whose rows are the vectors \([*]\) has the property that any \( \delta - 1 \) of its columns are linearly independent. Indeed, the determinant formed by the columns \( j_1, \ldots, j_{\delta-1} \) is equal to
\[ \begin{vmatrix}
\omega^{j_1 \ell} & \cdots & \omega^{j_{\delta-1} \ell} \\
\omega^{j_1(\ell+1)} & \cdots & \omega^{j_{\delta-1}(\ell+1)} \\
\vdots & \ddots & \vdots \\
\omega^{j_1(\ell+\delta-2)} & \cdots & \omega^{j_{\delta-1}(\ell+\delta-2)}
\end{vmatrix} \]

and this is non-zero if \( j_1, \ldots, j_{\delta-1} \) are distinct, as it is equal to
\[ \omega^{j_1 \ell} \cdots \omega^{j_{\delta-1} \ell} \cdot V_{\delta-1}(\omega^{j_1}, \ldots, \omega^{j_{\delta-1}}). \]
**Example** (The minimum distance of a **BCH** code can be greater than the design distance). Let \( q = 2 \) and \( m = 4 \). Let \( \omega \) be a primitive element of \( \mathbb{F}_{16} \). Since \( \omega \) has order 15, we can apply the previous results to the case \( q = 2, m = 4 \) and \( n = 15 \). The 2-cyclotomic classes mod \( n \) are

\[
\{1,2,4,8\}, \{3,6,12,9\}, \{5,10\}, \{7,14,13,11\}.
\]

This shows, if we set \( C_\delta = BCH_\omega (\delta) \) and \( d_\delta = d_{C_\delta} \), that

\[
C_4 = C_5, \text{ and hence } d_4 = d_5 \geq 5, \text{ and}
\]
\[
C_6 = C_7, \text{ and hence } d_6 = d_7 \geq 7.
\]

Note that the dimension of \( C_4 = C_5 \) is \( 15 - 2 \cdot 4 = 7 \), and that the dimension of \( C_6 = C_7 \) is \( 15 - 2 \cdot 4 - 2 = 7 \).

**Example.** It is similar to the preceding example, with \( q = 2 \) and \( m = 5 \). Let \( \omega \) be a primitive element of \( \mathbb{F}_{32} \). The 2-cyclotomic classes mod 31 are
\{1,2,4,8,16\}, \{3,6,12,24,17\}, \{5,10,20,9,18\},
\{7,14,28,25,19\}, \{11,22,13,26,21\}, \{15,30,29,27,23\}.

Thus we see, with similar conventions as in the previous example, that

\[ C_4 = C_5, \quad C_6 = C_7, \quad C_8 = C_9 = C_{10} = C_{11} \text{ and } C_{12} = C_{13} = C_{14} = C_{15}. \]

Therefore

\[ d_4 = d_5 \geq 5, \quad d_6 = d_7 \geq 7, \]
\[ d_8 = d_9 = d_{10} = d_{11} \geq 11, \text{ and } \]
\[ d_{12} = d_{13} = d_{14} = d_{15} \geq 15. \]

If we set \( k_\delta = \dim(C_\delta) \), then we have

\[ k_4 = 31 - 2 \cdot 5 = 21, \quad k_6 = 31 - 3 \cdot 5 = 16, \]
\[ k_8 = 31 - 4 \cdot 5 = 11, \quad k_{12} = 31 - 5 \cdot 5 = 6. \]
Exercise. If \( \omega \) is a primitive element \( \mathbb{F}_{64} \), prove that the minimum distance of \( BCH_\omega(16) \) is \( \geq 21 \) and that its dimension is 18.

In relation to the dimension of \( BCH_\omega(\delta, \ell) \), the following bound holds:

**Proposition.** If \( m = e_n(q) \), then

\[
\dim BCH_\omega(\delta) \geq n - m(\delta - 1).
\]

**Proof:** If \( g \) is the generating polynomial of \( BCH_\omega(\delta, \ell) \), then

\[
\dim BCH_\omega(\delta) = n - \deg(g).
\]

Since \( g \) is the least common multiple of the minimal polynomials

\[
p_i = p_{\omega^{\ell+i}}, i = 1, \ldots, \ell - 1, \text{ and }
\]

\[
\deg(p_{\omega^{\ell+i}}) \leq [F':F] = m,
\]

it is clear that \( \deg(g) \leq m(\delta - 1) \), and this implies the claimed inequality.
Improving the dimension bound in the binary case

The bound in the previous proposition can be improved considerably for strict binary \textit{BCH} codes. Let \( C_i \) be the 2-cyclotomic class of \( i \mod n \). If we set \( p_i \) to denote the minimal polynomial of \( \omega^i \), where \( \omega \) is a primitive \( n \)-th root of unity, then \( p_i = p_{2i} \), as \( (2i \mod n) \in C_i \). We get, if \( t \geq 1 \), that

\[
\text{lcm}(p_1, p_2, ..., p_{2t}) = \text{lcm}(p_1, p_2, ..., p_{2t-1}) \\
= \text{lcm}(p_1, p_3, ..., p_{2t-1}).
\]

Now the first of these equalities tells us that \( BCH_\omega(2t + 1) = BCH_\omega(2t) \), so that it is enough to consider, among the strict binary \textit{BCH} codes, those with odd design distance.

\textbf{Proposition.} If \( k \) is la dimension of the strict binary code \( BCH_\omega(2t + 1) \), then \( k \geq n - tm \), where \( m = e_n(2) \).
**Proof:** Let $g = \text{lcm}(p_1, p_2, ..., p_{2t})$ be the generating polynomial of $BCH_\omega(2t + 1)$. The we know that $k = n - \deg(g)$. But

$$g = \text{lcm}(p_1, p_3, ..., p_{2t-1})$$

and hence $\deg(g)$ is at most the sum of the degrees of $p_1, p_3, ..., p_{2t-1}$. Since the degree of $p_i$ is at most $m$, it follows that $\deg(g) \leq tm$ and this establishes the claim.

**Example.** If we apply the bound of the previous proposition to the code $BCH_\omega(8) = BCH_\omega(9)$ of the preceding example, we get that

$$k \geq n - tm = 31 - 4 \cdot 5 = 11.$$ 

Since the dimension of this code is exactly 11, we see that the bound in the proposition cannot be improved in general.
Exercise. Let

\[ f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}_2[X], \ F = \mathbb{Z}_2[X]/(f), \]

and let \( \alpha \) be a primitive element of \( F \). Find the dimension and a control matrix of \( BCH_\omega(8) \).

Example (The binary Golay code is cyclic). Let \( q = 2, \ n = 23 \) and \( m = e_n(2) = 11 \). The splitting field of \( X^{23} - 1 \in \mathbb{Z}_2[X] \) is \( L = \mathbb{F}_{2^{11}} \). The 2-cyclotomic classes mod 23 are

\[
C_0 = \{0\}, \\
C_1 = \{1,2,4,8,16,9,18,13,3,6,12\}, \\
C_5 = \{5,10,20,17,11,22,21,19,15,7,14\}.
\]

If \( \omega \in L \) is a primitive 23-rd root of unity, the generating polynomial of \( C = BCH_\omega(5) \) is \( g = \text{lcm}(p_1, p_2, p_3, p_4) = p_1 \). Since \( \deg(p_1) = |C_1| = 11 \), it turns out that \( \dim(C) = 23 - 11 = 12 \). Moreover, the minimum
distance of $C$ is 7 and therefore $C$ is a binary perfect code of type [23,12,7].

**Exercise.** Show that the minimum distance of the binary code in the previous example is 7. [**Hint.** Adapt the arguments in the presentation of the ternary Golay code as a cyclic code].

The RS codes with $n = q - 1$ turn out to be strict primitive BCH codes.

**Proposition.** If $\omega$ is a primitive element of a finite field $F = \mathbb{F}_q$ and $n = q - 1$, then

$$BCH_{\omega}(\delta) = RS_{1,\omega,\ldots,\omega^{n-1}}(n - \delta + 1).$$

**Proof:** The Vandermonde matrix $H = V_{1,\delta-1}(1, \omega, \ldots, \omega^{n-1})$ is a control matrix of $C = RS_{1,\omega,\ldots,\omega^{n-1}}(n - \delta + 1)$, **P36**. Since the $i$-th row of $H$ is $1, \omega^i, \ldots, \omega^{i(n-1)}$, the vectors $a = (a_0, a_1, \ldots, a_{n-1})$ of $C$ are those that satisfy $a_0 + a_1 \omega^i + \cdots + a_{n-1} \omega^{i(n-1)} = 0$ for $i = 1, \ldots, \delta - 1$. In terms of the polynomial $a_X$, this is equivalent to say that $\omega^i$ is a root of $a_X$ for
$i = 1, \ldots, \delta - 1$ and thereby $C$ coincides with the cyclic code corresponding to the roots $\omega, \ldots, \omega^{\delta-1}$. But this code is precisely $BCH_\omega(\delta)$. 