Exercise 1. In this exercise, we give an alternative proof of the BCH bound using the discrete Fourier Transform.

Let $n$ be an integer and $\mathbb{F}_q$ a finite field with $q$ prime to $n$. Let $\mathbb{F}_q(\zeta_n)$ be a finite extension of $\mathbb{F}_q$ containing all the $n$–th roots of 1, $\zeta_n$ denotes a primitive $n$–th root of 1. The discrete Fourier transform is defined as

$$\mathcal{F} : \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) \to \mathbb{F}_q(\zeta_n)[X]/(X^n - 1)$$

$$f \mapsto \sum_{i=0}^{n-1} f(\zeta_n^{-i})X^i.$$

1. Prove that $\mathcal{F}$ is an $\mathbb{F}_q$–linear map.

2. Prove that

$$\sum_{i=0}^{n-1} \zeta_n^{ij} = \begin{cases} n & \text{if } n|j \\ 0 & \text{else} \end{cases}.$$

3. Prove that $\mathcal{F}$ is an isomorphism with inverse:

$$\mathcal{F}^{-1} : \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) \to \mathbb{F}_q(\zeta_n)[X]/(X^n - 1)$$

$$f \mapsto \frac{1}{n} \sum_{i=0}^{n-1} f(\zeta_n^i)X^i.$$

**Indication:** it suffices to prove that $\mathcal{F}^{-1}(\mathcal{F}(X^i)) = X^i$ for all $i = 0, \ldots, n - 1$.

4. For all $f, g \in \mathbb{F}_q(\zeta_n)[X]/(X^n - 1)$, denote by $f \ast g$ the coefficientwise product:

if $f = \sum_{i=0}^{n-1} f_iX^i$ and $g = \sum_{i=0}^{n-1} g_iX^i$, then $f \ast g = \sum_{i=0}^{n-1} f_ig_iX^i$.

Prove that for all $f, g \in \mathbb{F}_q(\zeta_n)[X]/(X^n - 1)$, then

(i) $\mathcal{F}(fg) = \mathcal{F}(f) \ast \mathcal{F}(g)$;

(ii) $\mathcal{F}(f \ast g) = \frac{1}{n} \mathcal{F}(f) \mathcal{F}(g)$;

(iii) $\mathcal{F}^{-1}(fg) = n(\mathcal{F}^{-1}(f) \ast \mathcal{F}^{-1}(g))$;

(iv) $\mathcal{F}^{-1}(f \ast g) = \mathcal{F}^{-1}(f) \mathcal{F}^{-1}(g)$.
5. Let $g \in \mathbb{F}_q[X]/(X^n - 1)$ be a nonzero polynomial vanishing at $1, \zeta_n, \ldots, \zeta_n^{\delta - 2}$ (in particular, it vanishes at $\delta - 1$ roots of $X^n - 1$ with consecutive exponents). Prove that

$$\mathcal{F}^{-1}(g) \equiv X^{\delta - 1}h(X) \mod (X^n - 1)$$

for some $h \in \mathbb{F}_q[\zeta_n][X]$ where $h$ is nonzero and has degree $\leq n - \delta$.

6. Using $\mathcal{F}(\mathcal{F}^{-1}(g))$ prove that $g$ has at least $\delta$ nonzero coefficients.

7. Prove that if $g \in \mathbb{F}_q[X]/(X^n - 1)$ vanishes at $\zeta_n^a, \zeta_n^{a+1}, \ldots, \zeta_n^{a+\delta - 2}$, then $g$ also has at least $\delta$ nonzero coefficients.

8. Conclude.

**Exercise 2** (A decoding algorithm for BCH codes). Let $\mathbb{F}_q$ be a finite field and $n$ be an integer prime to $q$. Let $\mathbb{F}_q(\zeta_n)$ be the smallest extension of $\mathbb{F}_q$ containing all the $n$–th roots of 1. Let $g \in \mathbb{F}_q[x]$ be a polynomial of degree $< n$ vanishing at $\zeta_n, \ldots, \zeta_n^{\delta - 1}$ for some positive integer $\delta$. Let $C$ be the BCH code with generating polynomial $g$. The BCH bound asserts that $C$ has minimum distance at least equal to $\delta$. We will prove that the code is $t$–correcting, where $2t + 1 = \delta$ if $\delta$ is odd and $2t + 1 = \delta - 1$ if $\delta$ is even.

Let $y \in \mathbb{F}_q^n$ be a word such that

$$y = c + e$$

where $c \in C$ and $e$ is a word of weight $f$ with $f \leq t$. In what follows, all the words of $\mathbb{F}_q^n$ are canonically associated to polynomials in $\mathbb{F}_q[z]/(z^n - 1)$. For instance

$$e(z) = e_{i_1}z^{i_1} + \cdots + e_{i_f}z^{i_f}$$

where the $e_{i_j}$’s are nonzero elements of $\mathbb{F}_q$.

We introduce some notation and terminology.

- The **syndrome** polynomial $S \in \mathbb{F}_q(\zeta_n)[z]$:

  $$S(z) \equiv \sum_{i=1}^{2t} y(\zeta_n^i) z^{i-1}.$$ 

- The **error locator polynomial** $\sigma \in \mathbb{F}_q(\zeta_n)[z]$:

  $$\sigma(z) \equiv \prod_{j=1}^{f} (1 - \zeta_n^{i_j} z).$$

1. Among the polynomials $S$ and $\sigma$, which one is known and which one is unknown from the point of view of the decoder?
2. Prove that
\[ S(z) = \sum_{i=1}^{2t} e(\zeta_n^i) z^{i-1} \]
and hence depends only on the error vector \( e \).

3. Let \( \omega \) be the polynomial defined as
\[ \omega(z) = \sum_{j=1}^{f} c_{ij} \zeta_n^{ij} \prod_{k \neq j}(1 - \zeta_n^{ik} z) \]
Prove that
(i) \( \deg \omega < t \);
(ii) \( S(z)\sigma(z) \equiv \omega(z) \mod (z^{2t}) \);
(iii) \( \sigma \) and \( \omega \) are prime to each other.

\textit{Indication: to prove that two polynomials are prime to each other, it is sufficient to prove that no root of one is a root of the other.}

4. Prove that if another pair \( (\sigma', \omega') \) of polynomials satisfying \( \deg \sigma' \leq t \), \( \deg \omega' < t \) and \( S(z)\sigma'(z) \equiv \omega'(z) \mod (z^{2t}) \) then, there exists a polynomial \( H \in \mathbb{F}_q(\zeta_n)[z] \) such that \( \sigma' = H\sigma \) and \( \omega' = H\omega \).

5. Let \( h \) be the largest integer such that \( z^h | S(z) \). Prove that \( h < t \). Deduce that the greatest common divisor of \( S \) and \( z^{2t} \) has degree \( < t \).

6. By proceeding to the extended Euclidean algorithm to the pair \( (S, z^{2t}) \), there exist sequences of polynomials \( P_0 = z^{2t}, P_1 = S, P_2, \ldots, P_r \) with \( \deg P_0 > \deg P_1 > \deg P_2 > \cdots \) where \( P_r \) is the GCD of \( (S, z^{2t}) \) and \( A_0, A_1, \ldots, B_0, B_1, \ldots \) such that for all \( i \),
\[ P_i = A_i z^{2t} + B_i S. \]
In particular, we have \( A_0 = B_1 = 1 \) and \( B_0 = A_1 = 0 \).
Prove the existence of a polynomial \( H \) and an index \( i \) such that \( P_i = H\omega \) and \( A_i = H\sigma \).
\textit{Indication: You need to analyze Euclid algorithm, and in particular to prove that for all \( i \geq 2 \), \( \deg B_i = \deg P_0 - \deg P_{i-1} \).}
\textit{Remark: Actually a deeper analysis of extends Euclid algorithm makes possible to prove that \( H \) has degree 0 and equals \( B_1(0) \).}

7. Describe a decoding algorithm for decoding BCH codes. What is its complexity?

\textbf{Exercise 3.} The goal of the exercise is to observe the strong relations between BCH and Reed-Solomon codes. Let \( \mathbb{F}_q \) be a finite field and \( n \) be an integer prime to \( q \).
1. We first consider the case \( n = q - 1 \).

(a) Prove that if \( n = q - 1 \) then \( \mathbb{F}_q \) contains all the \( n \)-th roots of 1.

Let \( \zeta_n \) be such an \( n \)-th root, from now on the elements of \( \mathbb{F}_q \setminus \{0\} \) are denoted by 
\[ 1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}. \]

(b) Then, in this situation, describe the minimal cyclotomic classes and the cyclotomic classes in general.

(c) Still in case where \( n = (q - 1) \), let \( C \) be a BCH whose set of roots contains 
\( \zeta_n, \ldots, \zeta_n^{\delta-1} \). Prove that \( C \) has dimension \( n - \delta + 1 \). Then prove that \( C \) is MDS.

(d) Let \( C' \) be the generalised Reed–Solomon code \( C' \overset{\text{def}}{=} \text{GRS}_{\delta-1}(x, x) \) where \( x \overset{\text{def}}{=} (1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}) \). Recall that this code is defined as the image of the map
\[
\begin{align*}
\mathbb{F}_q[z]_{<\delta-1} & \longrightarrow \mathbb{F}_q^n \\
f & \longmapsto (f(1), \zeta_n f(\zeta_n), \zeta_n^2 f(\zeta_n^2), \ldots, \zeta_n^{n-1} f(\zeta_n^{n-1}))
\end{align*}
\]

Prove that \( C' = C'\perp \).

Indication : a nice basis for \( C' \) can be obtained from the images by the above map of the monomials \( 1, z, z^2, \ldots, z^{\delta-2} \).

(e) Conclude that \( C \) is a generalised Reed Solomon (GRS in short) code.

2. Now, consider the general case : \( n \) is prime to \( q \) and \( C \) denotes the BCH code whose set of roots contains \( \zeta_n, \ldots, \zeta_n^{\delta-1} \). Prove that \( C \) is contained in the subfield subcode of a GRS code with minimum distance \( \delta \).

3. Deduce from that a decoding algorithm based on the decoding of the GRS code. Compare its complexity with that of the algorithm presented in Exercise 2.
Solution to Exercise 1

1. For all \( f, g \in \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) \) and all \( \lambda, \mu \in \mathbb{F}_q \),

\[
\mathcal{F}(\lambda f + \mu g) = \sum_{i=0}^{n-1} (\lambda f(\zeta_n^{-i}) + \mu g(\zeta_n^{-i}))X^i = \lambda \mathcal{F}(f) + \mu \mathcal{F}(g).
\]

2. If \( n \mid j \), then \( \zeta_n^{ij} = 1 \) for all integer \( i \) and hence

\[
\sum_{i=0}^{n-1} \zeta_n^{ij} = n.
\]

Else, then the classical formula on the sum of elements of geometric sequence yields

\[
\sum_{i=0}^{n-1} \zeta_n^{ij} = \frac{1 - \zeta_n^j}{1 - \zeta_n^1} = 0.
\]

3. Let \( j \in \{0, \ldots, n-1\} \). Then

\[
\mathcal{F}(X^j) = \sum_{i=0}^{n-1} \zeta_n^{-ij} X^i.
\]

Set

\[
\mathcal{G} : \left\{ \begin{array}{c}
\mathbb{F}_q(\zeta_n)[X]/(X^n - 1) \longrightarrow \mathbb{F}_q(\zeta_n)[X]/(X^n - 1) \\
f \longmapsto \frac{1}{n} \sum_{h=0}^{n-1} f(\zeta_n^h)X^h
\end{array} \right.
\]

\[
\mathcal{G} \circ \mathcal{F}(X^j) = \frac{1}{n} \sum_{h=0}^{n-1} \sum_{i=0}^{n-1} \zeta_n^{-ij} \zeta_n^{hi} X^h
\]

\[
= \frac{1}{n} \sum_{h=0}^{n-1} \left( \sum_{i=0}^{n-1} \zeta_n^{i(h-j)} \right) X^h.
\]

And from Question 2, \( \sum_{i=0}^{n-1} \zeta_n^{i(h-j)} = 0 \) if \( h \neq j \) and \( n \) else. Thus,

\[
\mathcal{G} \circ \mathcal{F}(X^j) = X^j.
\]

4. (4i) Obvious, since for all \( i \), \( f g(\zeta_n^{-i}) = f(\zeta_n^{-i})g(\zeta_n^{-i}) \). By the very same manner, one proves (4ii). (4ii) can be obtained from (4i) and (4iii) as follows

\[
\mathcal{F}(f \star g) = \mathcal{F}(\mathcal{F}^{-1}(\mathcal{F}(f)) \star \mathcal{F}^{-1}(\mathcal{F}(g)))
\]

\[
= \mathcal{F}\left( \frac{1}{n} \mathcal{F}^{-1}(\mathcal{F}(f)\mathcal{F}(g)) \right)
\]

\[
= \frac{1}{n} \mathcal{F}(f)\mathcal{F}(g),
\]

where the second equality is a consequence of (4i). Identity (4iv) can be obtained by the very same manner by exchanging \( \mathcal{F} \) and \( \mathcal{F}^{-1} \).
5. By the very definition of $F^{-1}$, the $\delta - 1$ first coefficients of $F^{-1}(g)$ are zero. This yields the result.

6. From (4i) and from the previous question, we get:

$$F(F^{-1}(g)) = F(X^\delta h(X)) = F(X^\delta) \ast F(h(X))$$

Now, observe that $F(X^\delta) = \sum i \zeta_i^{-\delta} X^i$ and hence has only nonzero coefficients. Therefore, the $i$-th coefficient of $F(F^{-1}(g)) = F(X^\delta) \ast F(h(X))$ is zero if and only if that of $F(h)$ is zero. Assume now that $F(F^{-1}(g))$ has strictly less than $\delta$ nonzero coefficients, which means that it has strictly more than $n - \delta$ zero coefficients. This entails that $F(h)$ has strictly more than $n - \delta$ zero coefficients. By definition of $F$, it means that $h$ vanishes at strictly more than $n - \delta$ distinct elements among the $\zeta_i^{-\delta}$’s which cannot happen since $h$ is nonzero and has degree $\leq n - \delta$ and hence has at most $n - \delta$ distinct roots.

7. In the general case, use the cyclic structure and observe that in this situation,

$$X^{n-a}F^{-1}(g) = X^\delta h(x)$$

for some polynomial $h$ of degree $\leq n - \delta$ and hence

$$F^{-1}(g) = X^{a+\delta} h(X).$$

The rest of the proof is exactly as in the previous question.

8. A nonzero polynomial vanishing at $\delta - 1$ roots with consecutive exponents has at least $\delta$ nonzero coefficients. This provides another proof of the BCH bound.

**Solution to Exercise 2**

1. $S$ is known and $\sigma$ is unknown.

2. We have,

$$S(z) = \sum_{i=1}^{2t} y(\zeta_i^n) z^{i-1} = \sum_{i=1}^{2t} c(\zeta_i^n) z^{i-1} + \sum_{i=1}^{2t} e(\zeta_i^n) z^{i-1}. $$

Then, by the very definition of the BCH code $C$, the term $\sum_{i=1}^{2t} c(\zeta_i^n) z^{i-1}$ is zero.

3. (i) Clearly, $\omega$ has degree $< f$ and since $f \leq t$, we get the result.
(ii) We have
\[
\omega(z) = \sum_{j=1}^{f} e_{ij} \zeta_{ij}^j \prod_{k \neq j} (1 - \zeta_{ik}^j z)
\]
\[
= \sigma(z) \sum_{j=1}^{f} e_{ij} \zeta_{ij}^j \frac{1}{1 - \zeta_{ij}^j z}
\]
\[
= \sigma(z) \sum_{j=1}^{f} e_{ij} \zeta_{ij}^j \sum_{k=0}^{+\infty} \zeta_{ij}^k z^k
\]
\[
= \sigma(z) \sum_{k=0}^{+\infty} z^k \left( \sum_{j=1}^{f} e_{ij} \zeta_{ij}^j (k+1) \right)
\]
\[
= \sigma(z) \sum_{k=0}^{+\infty} z^k e(\zeta_n^{k+1})
\]
\[
= \sigma(z) \sum_{\ell=1}^{+\infty} z^{\ell-1} e(\zeta_n^{\ell})
\]
\[
\equiv \sigma(z) S(z) \mod (z^{2t}).
\]

(iii) The polynomial \( \sigma \) is separable with \( f \) distinct roots which are \( \zeta_n^{-i_1}, \ldots, \zeta_n^{-i_f} \). Now, let \( 1 \leq \ell \leq f \).
\[
\omega(\zeta_n^{-i_\ell}) = \sum_{j=1}^{f} e_{ij} \zeta_{ij}^j \prod_{k \neq j} (1 - \zeta_{ik}^j \zeta_n^{-i_\ell}).
\]
and the product \( \prod_{k \neq j} (1 - \zeta_{ik}^j \zeta_n^{-i_\ell}) \) is zero unless \( j = \ell \). Therefore,
\[
\omega(\zeta_n^{-i_\ell}) = e_{i_\ell} \zeta_{i_\ell}^\ell \prod_{k \neq \ell} (1 - \zeta_{ik}^j \zeta_n^{-i_\ell})
\]
which is nonzero. Thus no root of \( \sigma \) cancels \( \omega \); hence the two polynomials are prime to each other.

4. We have,
\[
\omega(z) \sigma'(z) \equiv S(z) \sigma(z) \sigma'(z) \equiv \omega'(z) \sigma(z) \mod (z^{2t})
\]
Therefore, \( z^{2t} | \omega(z) \sigma'(z) - \omega'(z) \sigma(z) \). But the polynomial \( \omega \sigma' - \omega' \sigma \) has degree < 2t and hence is zero. Thus we have,
\[
\omega(z) \sigma'(z) = \omega'(z) \sigma(z)
\]
and since \( \sigma \) and \( \omega \) are prime to each other, we get \( \sigma | \sigma' \) which yields the existence of a polynomial \( H \) such that \( \sigma' = H \sigma \). Next one deduce easily that \( \omega' = H \omega \).
5. The coefficients of $S$ are obtained by evaluating $e$ which has degree $f \leq t$. Therefore, the number of roots of $e$ is less than or equal to $t$. Thus, $h < t$.

6. From Question 5, the GCD $P_r$ of $S$ and $z^{2t}$ equals up to multiplication by a nonzero scalar) $z^h$ for some $h < t$. Consequently, in the sequence $(P_i)_i$ of polynomials given by the Euclidian algorithm, there exists an index $i$ such that $\deg P_{i-1} \geq t$ and $\deg P_i < t$.

Set $\omega \overset{\text{def}}{=} P_i$. By construction, we have $\deg \omega < t$, moreover, the $i$–th step of Euclid Algorithm yields

$$\omega(z) \equiv B_i(z)S(z) \mod (z^{2t})$$

To conclude by applying the result of Question 4, we need to prove that $\deg A_i \leq t$. For this sake, we proceed to a deeper analysis of Euclid algorithm. Remind that there exists a sequence of quotients $Q_1, Q_2, \ldots$ such that for all $i \geq 2$,

$$P_i = Q_{i-1}P_{i-1} - P_{i-2} \quad (1)$$
$$B_i = Q_{i-1}B_{i-1} - B_{i-2}. \quad (2)$$

By induction, one proves that the sequence of degrees $\deg B_i$ is increasing for $i \geq 1$. Indeed, since $B_2 = Q_1B_1$ (remind that $B_0 = 0$), we clearly have $\deg B_2 \leq \deg B_1$. Then, by induction, for all $i \geq 2$, we assume that $\deg B_{i-1} \geq \deg B_{i-2}$ and hence from (2), we get

$$\deg(B_i) = \deg Q_{i-1} + \deg(B_{i-1}) \geq \deg B_{i-1} \quad (3)$$

since $Q_i$ is nonzero (it is a quotient in an Euclidian division).

Now, as specified in (1), for all $i \geq 2$, we have the Euclidian division $P_{i-2} = Q_{i-1}P_{i-1} + P_i$ where $P_i$ is the remainder. By the very definition of Euclidian division, we have

$$\forall i \geq 2, \quad \deg P_{i-2} = \deg(Q_{i-1}P_{i-1}) = \deg Q_{i-1} + \deg(P_{i-1}) \quad (4)$$

and, putting (3) and (4) together, we get

$$\forall i \geq 2, \quad \deg B_i = \deg B_{i-1} + \deg P_{i-2} - \deg P_{i-1}. \quad (5)$$

Finally, using (2) again, and since $B_1 = 0$, by induction, (5) leads to

$$\forall i \geq 2, \quad \deg B_i = \deg P_0 - \deg P_{i-1} = 2t - \deg P_{i-1}.$$ 

Next, by definition of $i$ we have $\deg P_{i-1} \geq t$ which leads to $\deg B_i \leq t$. Thus, from Question 4 we get the result.

7. Step 1. Compute $S$ from the received word $y$.

Step 2. Proceed to Euclid Algorithm to compute $P_i$ and $B_i$.

Step 3. Compute the GCD $H$ of $P_i$ and $B_i$ and set $\omega = \frac{P_i}{H}$, $\sigma = \frac{B_i}{H}$ (actually a deeper analysis of Euclidian Algorithm would lead to $\deg H = 1$).
Step 4. Compute the inverse of the roots of $\sigma$ in $\mathbb{F}_q(\zeta_n)$. Call them $\zeta_{i_1}^n, \ldots, \zeta_{i_f}^n$.

Step 5. Compute the vector $e$ defined as $e_k = 0$ for all $k \notin \{i_1, \ldots, i_f\}$ and

$$\forall j \in \{1, \ldots, f\}, \quad e_{i_j} \overset{\text{def}}{=} \frac{\omega(\zeta_n^{-i_j})\zeta_n^{-i_j}}{\prod_{k \neq j}(1 - \zeta_n^{i_k}\zeta_n^{-i_j})}.$$ 

Step 6. Return $y - e$.

The most expensive part of the algorithm is Euclid algorithm whose complexity is $O(t^2)$ operations in $\mathbb{F}_q(\zeta_n)$.

**Solution to Exercise 3**

1. (a) It is well-known in finite field theory that

$$z^{q-1} - 1 = \prod_{a \in \mathbb{F}_q^*} (z - a).$$

(b) Cyclotomic classes are any subset of $\mathbb{Z}/(q - 1)\mathbb{Z}$ and minimal cyclotomic classes are subsets of cardinality 1.

(c) Let $g$ be the polynomial $g(z) \overset{\text{def}}{=} \prod_{i=1}^{\delta-1}(z - \zeta_n^i)$. Since the $\zeta_n^i$ are all in $\mathbb{F}_q$, $g \in \mathbb{F}_q[z]$ and is a generating polynomial of the code. Since its degree is $\delta - 1$ its dimension is $n - \delta + 1$ and by the BCH bound its minimum distance is $\geq \delta$. Thanks to Singleton bound we see that its distance is actually equal to $\delta$ and hence it is an MDS code.

(d) From the basis of polynomials $1, z, z^2, \ldots, z^{\delta-2}$, the code $C'$ has a basis given by

$$v_i \overset{\text{def}}{=} (1, \zeta_n^{i+1}, \zeta_n^{2i+2}, \ldots, \zeta_n^{i(n-1)+(n-1)})$$

for $i \in \{0, \ldots, \delta - 2\}$. Let $c \in C$, then the inner product $\langle c, v_i \rangle$ is nothing but $c(\zeta_n^{i+1})$ regarding $c$ as a polynomial. Then, since, by definition of $C$, we know that $c(\zeta_n^j) = 0$ for all $j \in \{1, \ldots, \delta - 1\}$, which proves that

$$\forall i \in \{0, \ldots, \delta - 2\}, \quad \langle c, v_i \rangle = 0.$$

Therefore, $C' \subset C^\perp$. Next, since $C'$ has dimension $\delta - 1$ and $C$ has dimension $n - \delta + 1$, we conclude that

$$C' = C^\perp.$$

(e) The dual of a GRS code is a GRS code. Hence $C$ is GRS code.

2. Consider the BCH code $D$ over $\mathbb{F}_q(\zeta_n)$ (and not $\mathbb{F}_q$) associated to the roots $\zeta_n, \ldots, \zeta_n^{\delta-1}$. The code $C$ is contained in $D|_{\mathbb{F}_q}$. Moreover, from the previous question, $D$ is a GRS code.

3. The code $D$ considered in the previous question has minimum distance $\delta$. Thus an approach to correct up to $\lfloor \frac{\delta - 1}{2} \rfloor$ errors would be to proceed as follows:
- Given a received word $y = c + e$ where $c \in C$ and $w_H(e) \leq \frac{\delta - 1}{2}$. Solve the decoding problem in $D$ using Berlekamp Welch algorithm.

By uniqueness of the solution of this decoding problem in $C$ and in $D$, we know that the solution is the closest element in $C$ to $y$ and hence is $c$.

Compared to the algorithm presented in Exercise 2 whose complexity was quadratic in $\delta$, the present algorithm includes a part of linear algebra which will be cubic.