Decoding BCH Codes

Let $F = F_q$ be a field with q elements. Let $\alpha \in F_{q^s}$ be an element of order n, and let C be the corresponding BCH code of length n and design distance d (with generator polynomial equal to the product of the distinct minimal polynomials of $\alpha, \alpha^2, \ldots, \alpha^{d-1}$). Let g be the generator polynomial.
If we identify polynomials in $F_q[x]$ of degree $< n$ with the elements of $R_{q,n} = F_q[x]/(x^n - 1)$, then C may be thought of as the set of all polynomials of degree $< n$ with roots $\alpha, \alpha^2, \ldots, \alpha^{d-1}$. That is

$$C = \{f \in F_q[x] \mid \deg f < n; f(\alpha) = f(\alpha^2) = \cdots = f(\alpha^{d-1}) = 0\} = \{f \in (g) \mid \deg f < n\}$$

Notice that the elements in C are in one-to-one correspondence with their congruence classes in $R_{q,n}$; therefore, C corresponds to an ideal in $R_{q,n}$ (all elements divisible by $\bar{g}$ in $R_{q,n}$).

Since g divides $x^n - 1$, $f \in F_q[x]$ is divisible by g in $F_q[x]$ if and only if $\bar{f} \in R_{q,n}$ is divisible by $\bar{g}$: suppose $f = qg$, then $\bar{f} = \bar{q}\bar{g}$ in $R_{q,n}$ is clear. On the other hand, suppose $\bar{f} = \bar{q}\bar{g}$ for some polynomial q. Then $f = qg + (x^n - 1)r$ for a suitable polynomial r. Since $x^n - 1 = hg$, it follows that $f = (q + rh)g$ is divisible by g in $F_q[x]$ as well.

We are interested in C only as a vector space over F_q and are not really interested in the multiplicative structure. In that sense, it makes no difference whether we think of C as a subset of $F_q[x]$ or of $R_{q,n}$. It is worth keeping in mind though, that C is not an ideal when thought of as a subset of $F_q[x]$ (for starters, it is a finite set, but no nonzero ideal in $F_q[x]$ is finite), nor is it invariant under multiplication with x (this is true only modulo $x^n - 1$).

The decoding procedure for C is now as follows: Suppose a vector f is received, which we think of as a polynomial of degree $< n$. We assume that $d = 2t + 1$ is odd. We need to compute the coset leader e.

(1) **Compute the syndromes**: $S_1 = f(\alpha)$, $S_2 = f(\alpha^2)$, $\ldots$, $S_{d-1} = f(\alpha^{d-1})$. These are elements of F_{q^s}.

(2) If all of the S_i are zero, f is a codeword, go to Step (8) (with $e = 0$). Otherwise, for $k = 1, 2, 3, \ldots, t$ consider

$$M_k = \begin{bmatrix} S_1 & S_2 & \ldots & S_k \\ S_2 & S_3 & \ldots & S_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_k & S_{k+1} & \ldots & S_{2k-1} \end{bmatrix}$$

This is a $k \times k$ matrix with entries in F_{q^s}.

Find the maximum value k such that $\det M_k \neq 0$. We think of k as the number of errors that occurred (it will be in most instances). It is potentially possible that

$\det M_k = 0$ for all k but some S_i are nonzero nevertheless. In this case more than t errors occurred, and we have to seek retransmission.

Note that you always have to check $\det M_k$ until $k = t$, so you would typically start with $\det M_t$ and work your way down to the first k such that $\det M_k \neq 0$.

(If you start with $k = 1$, then $\det M_i = 0$ does not imply that $\det M_{i+1} = 0$, so you have to check all the way up to $k = t$).

We assume that k is the number of errors that actually occurred. (In rare circumstances, the number of errors could be actually bigger than k, but then it is also bigger than t and our decoding procedure does not yield a result.)

(3) **Solve the following system of linear equations (over F_{q^s}):**

$$M_k \mathbf{b} = -\mathbf{S}$$

with indeterminate

$$\mathbf{b} = \begin{bmatrix} b_k \\ b_{k-1} \\ \vdots \\ b_1 \end{bmatrix}$$

where

$$\mathbf{S} = \begin{bmatrix} S_{k+1} \\ S_{k+2} \\ \vdots \\ S_{2k} \end{bmatrix}.$$

Notice the order of the variables b_i and the sign on the right hand side!

The solution to this system gives us the *error locator polynomial*

$$\sigma = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_1 x + 1.$$

The coefficients b_i of σ are elements of F_{q^s} in general, and need not be elements of F_q.

The error locator polynomial is defined as

$$\sigma = (-1)^k (\alpha_1 x - 1)(\alpha_2 x - 1) \cdots (\alpha_k x - 1).$$

(*Notice the sign. This way we can avoid the annoying $(-1)^k$ in all syndrome equations above. So σ is the unique polynomial in $F_{q^s}[x]$ with roots α_i^{-1} and constant term $\sigma(0) = 1$. This changes nothing compared to the discussion in class except for the sign. We still have $\sigma(\alpha_i^{-1}) = 0$ and then the deduction leads to the equation $M_k \mathbf{b} = -\mathbf{S}$ instead of $M_k \mathbf{b} = (-1)^{k+1} S$. We simply replace $\mathbf{b}$ by $(-1)^k \mathbf{b}$ from class.*)

(4) **Find the roots of the error locator polynomial**: We are working under the assumption that precisely k errors occurred (we know that at least k errors occurred, and if the number is not k then it is strictly greater than t and no decoding is possible with this method); therefore, σ must have precisely k *distinct* roots $\beta_1, \beta_2, \ldots, \beta_k$ *unless more than k errors occurred*. Again, the roots are in F_{q^s}. **If the roots do not exist, then we have to seek retransmission**.

(5) **Compute the error locations**: First compute $\alpha_i := \beta_i^{-1}$. Now find $l_1, l_2, \ldots, l_k$ such that

$$\alpha_i = \alpha^{l_i}.$$

Notice that the l_i are unique as long as we require $0 \leq l_i < n$ (the l_i are supposed to be the error positions so they need to be bewteen 0 and $n-1$; so for example $1 = \alpha^0$).

Again, if the l_i do not exist, we cannot decode further. (NB if α is primitive, then the l_i always exist.)

We now have worked our way to an error vector of the form

$$e = e_1 x^{l_1} + e_2 x^{l_2} + \cdots + e_k x^{l_k}.$$

We therefore conjecture the error locations to be $l_1, l_2, \ldots, l_k$ (keeping in mind that these positions are based on 0).

(6) **Determine the values of $e_1, e_2, \ldots, e_k$**:

This step is essentially void if $q = 2$, for then all e_i must be equal to 1 provided decoding is possible; If $q \neq 2$, we only know that they are nonzero (assuming decoding is possible). Solve the equations

$$S_i = e_1(\alpha^{l_1})^i + e_2(\alpha^{l_2})^i + \cdots + e_k(\alpha^{l_k})^i \qquad (i = 1, 2, \ldots, 2k)$$

for the e_j in F_q. (Notice that often not all $2k$ equations are needed to determine the e_i because each single equation corresponds to multiple linear equations over F_q, but you still need to check all $2k$ equations hold). Another way of doing it is by inverting the Vandermonde matrix V and V^t and computing the diagonal matrix

$$D = V^{-1} M_k (V^T)^{-1}.$$

Then the k entries of D are $e_1\alpha_1, e_2\alpha_2, \ldots, e_k\alpha_k$, determining the e_i uniquely.

It could potentially happen that the e_i computed in this manner are *not* elements of F_q but are in F_{q^s} rather. **In this case, decoding is not possible**, because of course our error vector must have coefficients in F_q.

(7) **Check for consistency**:

We now have a supposed error vector $e = e_1 x^{l_1} + e_2 x^{l_2} + \cdots + e_k x^{l_k}$. By construction, for $i = 1, 2, \ldots, 2k$, we know that $f(\alpha^i) = S_i = e(\alpha^i)$ (see remarks below).

However, if $k < t$, then we still need to check that

$$S_i = e(\alpha^i)$$

also for $i = 2k+1, 2k+2, \ldots, 2t = d-1$. If this fails for any i, more than t errors occurred, and decoding is not possible. Of course, if $k = t$, this step is empty.

(8) **Celebrate**!

We are done. The decoded codeword is now $c = f - e$. c is indeed a codeword, because $c(\alpha^i) = f(\alpha^i) - e(\alpha^i) = 0$ for $i = 1, 2, \ldots, d-1$.

In the special case that $q = 2$, this step simply means flipping the positions $l_1, l_2, \ldots, l_k$ in f.

Remarks.
For step (7), for $i = 1, 2, 3, \ldots, 2k-1$ the equations $S_i = \sum_j e_j \alpha_j^i$ hold as a consequence of the fact that $M_k = VDV^T$, so $e(\alpha^i) = S_i$. For $i = 2k$ it follows from this together with

$$-S_{2k} = S_k b_k + S_{k+1} b_{k-1} + \cdots + S_{2k-1} b_1 = \sum_{i=1}^{k} \sum_{j=1}^{k} e_j \alpha_j^{2k-i} b_i = -\sum_{j=1}^{k} e_j \alpha_j^{2k}$$

which uses that $\sigma(\alpha_i^{-1}) = 0$, hence $-\alpha_i^{-1} = \sum_{j=1}^{k} b_j \alpha_i^{-j}$.
This procedure seems very elaborate. However, the number of cosets is at least q^{d-1} (or even bigger). Often $q = 256$, and $d = 33$, so the syndrome table would be huge.

Examples

Element	Minimal polynomial	Power of α
1	$x - 1 = x + 2$	$\alpha^0 = \alpha^8$
2	$x - 2 = x + 1$	α^4
a	$x^2 + 1$	α^6
$2a$	$x^2 + 1$	α^2
$1 + a$	$x^2 + x + 2$	α^1
$1 + 2a$	$x^2 + x + 2$	α^3
$2 + a$	$x^2 + 2x + 2$	α^7
$2 + 2a$	$x^2 + 2x + 2$	α^5

Table 1. Elements of F_9, their minimal polynomials over $\mathbb{Z}_3$, and their expression as powers of the primitive element.

a) Let C be the BCH code of length 8 and design distance 5 over $F_3 = \mathbb{Z}_3$ corresponding to the primitive element $\alpha = 1 + a \in F_9$. ($F_9 = \mathbb{Z}_3[x]/(1 + x^2)$ and $a = \bar{x}$; cf. Table 1.) So here $s = 2$, $q^s = 9$.

Suppose we receive $f = 2 + x^2 + x^3 + x^4 + x^5$. Then

(1)

$$\begin{aligned} S_1 = f(\alpha) = 2 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 = 2 + 2a + 1 + 2a + 2 + 2 + 2a = 7 + 6a &= 1 \\ S_2 = f(\alpha^2) = 2 + \alpha^4 + \alpha^6 + \alpha^8 + \alpha^{10} = 2 + 2 + a + 1 + 2a = 2 + 3a &= 2 \\ S_3 = f(\alpha^3) = f(\alpha)^3 &= 1 \\ S_4 = 2 + \alpha^8 + \alpha^{12} + \alpha^{16} + \alpha^{20} = 2 + 1 + 2 + 1 + 2 &= 2 \end{aligned}$$

NB it is an accident that all syndromes are actually in $F_q = \mathbb{Z}_3$ rather than in F_9.

(2) Notice that $t = 2$.

$$M_2 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

and $\det M_2 = 1 - 4 = 0$. Now we know that either 1 or more than 2 errors occurred.

$$M_1 = [1]$$

so $\det M_1 = 1 \neq 0$. We assume that 1 error occurred.

(3) The syndrome equations now take the form

$$M[b_1] = -[S_2]$$

or $1 \cdot b_1 = -2 = 1$. Thus $\sigma = 1 \cdot x + 1$.

(4) Obviously σ has just one root, namely, $-1 = 2$. Thus $\beta_1 = 2$, and $\alpha_1 = 2^{-1} = 2$. It is again an accident that β_1 is an element of $\mathbb{Z}_3$. In general, this need not happen.

(5) Find l_1 such that $\alpha_1 = \alpha_1^l$. A look at the table shows that $l_1 = 4$.
(NB if α_1 were 1, we would take $l_1 = 0$ *not* $l_1 = 8$, because our error vector must be a polynomial of degree at most 7).

(6) $e = e_1 x^4$. We need to compute e_1. $M_1 = VDV^T$ translates into $M = D$ as $V = [1]$.
Thus, here $e_1\alpha_1 = 2 \cdot e_1 = 1$. Thus $e_1 = 2$.
Alternatively, use the first syndrome equation $S_1 = 1 = e_1\alpha_1$ (which happens to be the same equation here).
$e_1 = 2$ is an element of $\mathbb{Z}_3$, so we are OK.

(7) We have $e = 2x^4$ and we believe that this is the sought after coset leader. We know that the first two syndrome equations are satisfied (cf. Remarks after (8) above).
We need to check $S_3 = e(\alpha^3)$ and $S_4 = e(\alpha^4)$. Now the first one follows because $e(\alpha^3) = e(\alpha)^3 = 1$. The second $e(\alpha^4) = 2\alpha^{16} = 2 = S_4$.

(8) We are done: $f - e$ is a codeword. Indeed,

$$f - e = 2 + x^2 + x^3 + 2x^4 + x^5$$

which we would recognize as the generator polynomial if we had computed the latter.

b) Let C be the same code as above, but this time suppose we receive $f = x + x^3 + 2x^4 + 2x^5 + x^6$.

(1)

$$\begin{aligned}
S_1 &= \alpha + \alpha^3 + 2\alpha^4 + 2\alpha^5 + \alpha^6 &&= 1 + a + 1 + 2a + 1 + 1 + a + a &&= 1 + 2a = \alpha^3 \\
S_2 &= \alpha^2 + \alpha^6 + 2\alpha^8 + 2\alpha^{10} + \alpha^{12} &&= 2a + a + 2 + a + 2 &&= 1 + a = \alpha \\
S_3 &= S_1^3 &&= 1 + 2a^3 &&= 1 + a = \alpha \\
S_4 &= \alpha^4 + \alpha^{12} + 2\alpha^{16} + 2\alpha^{20} + \alpha^{24} &&= 2 + 2 + 2 + 1 + 1 &&= 2
\end{aligned}$$

(2)

$$M_2 = \begin{bmatrix} \alpha^3 & \alpha \\ \alpha & \alpha \end{bmatrix}$$

So

$$\det M_2 = \alpha^4 - \alpha^2 = 2 + a \neq 0$$

and we conclude that 2 or more errors occurred. Notice the fact that $\det M_1 \neq 0$ is now irrelevant and we don't even have to compute it (well it's not much of a computation in the 1×1 case but this just serves to illustrate the principle).

(3) The syndrome equation is

$$\begin{bmatrix} \alpha^3 & \alpha \\ \alpha & \alpha \end{bmatrix} \begin{bmatrix} b_2 \\ b_1 \end{bmatrix} = - \begin{bmatrix} \alpha \\ 2 \end{bmatrix}$$

Recall that for an invertible 2×2 matrix we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Consequently, using $\det M_2 = 2 + a = \alpha^7 = \alpha^{-1}$

$$M_2^{-1} = \frac{1}{\alpha^7} \begin{bmatrix} \alpha & -\alpha \\ -\alpha & \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^2 & -\alpha^2 \\ -\alpha^2 & \alpha^4 \end{bmatrix}$$

and so

$$\begin{bmatrix} b_2 \\ b_1 \end{bmatrix} = - \begin{bmatrix} \alpha^2 & -\alpha^2 \\ -\alpha^2 & \alpha^4 \end{bmatrix} \begin{bmatrix} \alpha \\ 2 \end{bmatrix} = - \begin{bmatrix} \alpha^3 - 2\alpha^2 \\ -\alpha^3 + 2\alpha^4 \end{bmatrix} = - \begin{bmatrix} \alpha \\ \alpha^6 \end{bmatrix} = \begin{bmatrix} \alpha^5 \\ \alpha^2 \end{bmatrix}$$

The error locator polynomial becomes $\sigma = \alpha^5 x^2 + \alpha^2 x + 1$. Notice that this polynomial does not have all of its coefficients in $\mathbb{Z}_3$.

(4) Now we find its roots in F_9. Well, this basically just trial and error. One run through all 9 elements of F_9 suffices. We can always leave out 0 as this is never a root ($\sigma(0) = 1$).

$$\begin{aligned}
\sigma(1) &= \alpha^5 + \alpha^2 + 1 && = a \neq 0 \\
\sigma(\alpha) &= \alpha^7 + \alpha^3 + 1 && = 1 \neq 0 \\
\sigma(\alpha^2) &= \alpha^9 + \alpha^4 + 1 && = \alpha \neq 0 \\
\sigma(\alpha^3) &= \alpha^{11} + \alpha^5 + 1 && = a \neq 0 \\
\sigma(\alpha^4) &= \alpha^{13} + \alpha^6 + 1 && = 3 + 3a = \mathbf{0} \\
\sigma(\alpha^5) &= \alpha^{15} + \alpha^7 + 1 && = 2a \neq 0 \\
\sigma(\alpha^6) &= \alpha^{17} + \alpha^8 + 1 && = 2 + \alpha \neq 0 \\
\sigma(\alpha^7) &= \alpha^{19} + \alpha^9 + 1 && = \alpha^3 + \alpha + 1 = \mathbf{0}
\end{aligned}$$

As a side remark, this table neatly illustrates that here $\sigma(\alpha^3)$ is *not* equal to $\sigma(\alpha)^3$, due to the fact that some coefficients of σ are not in $\mathbb{Z}_3$.

We conclude that the two roots are $\beta_1 = \alpha^4 = 2$ and $\beta_2 = \alpha^7$.

(5) The table gives $\alpha_1 = 2^{-1} = 2 = \alpha^4$ and $\alpha_2 = \beta_2^{-1} = \alpha = \alpha^1$. The supposed error locations are therefore $l_1 = 4$ and $l_2 = 2$.

(6) We must have

$$S_1 = \alpha^3 = e_1\alpha^{l_1} + e_2\alpha^{l_2} = e_1 \cdot 2 + e_2 \cdot \alpha$$

Looking at Table 1, this translates into

$$1 + 2a = e_1 \cdot 2 + e_2(1 + a) = (2e_1 + e_2) \cdot 1 + e_2 \cdot a \qquad (*)$$

Now we use the fact that F_9 is a vector space over $\mathbb{Z}_3$ with basis $1, a$. It follows that the coefficients of 1 and a on both sides have to coincide; thus,

$$\begin{aligned}
1 &= 2e_1 + e_2 \\
2 &= e_2
\end{aligned}$$

Notice that the one equation (*) becomes a system of equations (in general as many as there are basis vectors, hence the number is usually equal to the dimension of F_{q^s} as F_q-vector space, i.e. s). This is now a system of equations with coefficients in $\mathbb{Z}_3$ and so we can hopefully solve it over $\mathbb{Z}_3$: $e_2 = 2$ and $2e_1 + 2 = 1$ implies $e_1 = 1$.

We conclude $e = x^4 + 2x$.

In theory, we would now need to check that also the other three syndrome equations are satisfied, because we only know the first one holds (we have a total of four syndrome equations, resulting in 8 equations over $\mathbb{Z}_3$ with 2 indeterminates,

so potentially the system could be overdetermined and have no solution; here however this does not happen.)

Alternatively,

$$V^{-1} = \frac{1}{\alpha+1}\begin{bmatrix}\alpha & -1\\ -2 & 1\end{bmatrix} = \alpha\begin{bmatrix}\alpha & 2\\ 1 & 1\end{bmatrix} = \begin{bmatrix}\alpha^2 & \alpha^5\\ \alpha & \alpha\end{bmatrix}$$

Because $(V^T)^{-1} = (V^{-1})^T$ we have

$$\begin{aligned} D = V^{-1}M_2(V^{-1})^T &= \begin{bmatrix}\alpha^5+\alpha^6 & \alpha^3+\alpha^6\\ \alpha^4+\alpha^2 & \alpha^2+\alpha^2\end{bmatrix}(V^{-1})^T = \begin{bmatrix}2 & 1\\ \alpha^5 & \alpha^6\end{bmatrix}(V^{-1})^T \\ &= \begin{bmatrix}2 & 1\\ \alpha^5 & \alpha^6\end{bmatrix}\begin{bmatrix}\alpha^2 & \alpha\\ \alpha^5 & \alpha\end{bmatrix} = \begin{bmatrix}2 & 0\\ 0 & 2\alpha\end{bmatrix}\end{aligned}$$

We end up with the two equations $e_1\alpha_1 = 2$ and $e_2\alpha_2 = 2\alpha$ which because of $\alpha_1 = 2$ and $\alpha_2 = \alpha$ means $e_1 = 1$ and $e_2 = 2$. Here no further checks are necessary.

(7) We do not have to do any consistency checks, because $k = t = 2$.

(8) The codeword is therefore $f - e = 2x + x^3 + x^4 + 2x^5 + x^6$, which we recognize as xg where g is the codeword of the previous example.