Math 422 Winter 2008

Example. Let C be the Reed-Solomon Code of design distance $d = 3$ over $\mathbb{Z}_7$ where $\alpha = 5$. Find the generator and check polynomials of C.
Decode the received vector 652000.

Solution. Notice that α is primitive: $q = 7$ here, so $q - 1 = 6$. So the order of α is either $1, 2, 3$, or 6 since it must divide $q - 1$. Now $5 \neq 1$, and $5^2 = 25 = 4$, and $5^3 = 5 \cdot 4 = 20 = -1 \neq 1$. Thus 5 has order 6 as needed. (For a Reed-Solomon code, usually α is taken to be primitive).
The length is $n = q - 1 = 6$.

We need the minimal polynomials of $\alpha, \alpha^2, \ldots, \alpha^{d-1}$. With $d = 3$ this means, α and α^2. Since here α is an element of $\mathbb{Z}_7$, its minimal polynomial over $\mathbb{Z}_7$ is just $m_\alpha = x - \alpha$ and $m_{\alpha^2} = x - \alpha^2$. We have $m_\alpha = x - 5$ and $m_{\alpha^2} = x - 25 = x - 4$. Since these two polynomials are distinct, we get

$$g = (x - 5)(x - 4) = (x + 2)(x + 3) = x^2 + 5x + 6.$$

Now observe that $x^6 - 1$ has roots $1, 2, 3, 4, 5, 6$ in $\mathbb{Z}^7$, so

$$h = (x^6 - 1)/g = (x - 1)(x - 2)(x - 3)(x - 6) = x^4 + 2x^3 + 5x^2 + 5x + 1$$

(hopefully).
So the dimension of $C = n - \deg g = \deg h = 4$.
Let us decode 652000 which we interpret as $f = 6 + 5x + 2x^2$ (we already see that f differs from g at only one place, so g will be the decoded codeword).
First, compute syndromes: Here $d = 3$, so we need to compute only two: $S_1 = f(\alpha) = f(5) = 6 + 25 + 2 \cdot 25 = 6 + 4 + 1 = 4$. $S_2 = f(\alpha^2) = f(4) = 6 + 20 + 32 = 2$.
The syndrome equations to find the error locator polynomial is then

$$S_1 b_1 = -S_2$$

and hence $4 \cdot b_1 = -2 = 5$. Now $4^{-1} = 2$, so $b_1 = 10 = 3$.
Then $\sigma = b_1 x + 1 = 3x + 1$ has root $\beta = 2$. Thus $\alpha_1 = \beta^{-1} = 4$.
Now $4 = 5^2$, so the supposed error location is 2, i.e. in the coefficient of x^2, and the error vector is likely $e = e_1 x^2$.
To find e_1: we must compute D as in $M = VDV^T$. Here $V = [1]$ and so $D = M = S_1$. Thus $e_1 \alpha_1 = S_1 = 4$ gives $e_1 = 1$.
Strictly speaking, here no further consistency checks are needed, because here $k = t = 1$.
(And indeed, $e(\alpha) = 4$ and $e(\alpha^2) = e(4) = 4^2 = 2 = S_2$.)
The decoded codeword then is $c = f - e = 6 + 5x + 2x^2 - x^2 = g$, as we knew all along.

(Here is a side remark: We have seen that for Reed-Solomon codes we always have $d(C) = d$: here for example, since $d(C) \geq d$, we know that the first $n - d + 1$ symbols uniquely determine a codeword (the first $n-d+1$ symbols cannot be equal as otherwise there are two codewords with distance at most $d-1$): thus $M = |C| \leq q^{n-d+1}$. But the dimension of C is $n-d+1$, so $M = q^{n-d+1}$. Thus $d(C) \leq d$ because there are two codewords that differ only in one position among the first $n-d+1$ symbols (and hence must differ also at the remaining $d-1$ symbols), their distance is therefore equal to d. This is specific to Reed-Solomon codes and is not always true for BCH-codes in general, where we may have $d(C) > d$. The reason the argument does not work for BCH codes is that $d-1$ is not always the degree of the minimal polynomial (it may be larger) and hence $\dim C$ may be smaller than $n-d+1$.)