21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

27- Monday March 26, 2012.

Remark 27.1: With the notation of Remark 26.7, with ξ a root of $P_1 = x^4 + x + 1$, and denoting P_i the polynomial associated to ξ^i, one has $P_1 = P_2 = P_4 = P_8 = x^4 + x + 1$, $P_3 = P_6 = P_9 = P_{12} = x^4+x^3+x^2+x+1 = \frac{x^5-1}{x-1}$, $P_5 = P_{10} = x^2+x+1 = \frac{x^3-1}{x-1}$, and $P_7 = P_{11} = P_{13} = P_{14} = x^4+x^3+1 = x^4 P_1\big(\frac{1}{x}\big)$.

Since $n = 2^m - 1$ with $m = 4$, the BCH codes considered are primitive, and if they start at ξ they are also narrow sense BCH codes.

If one uses $g = lcm\{P_i \mid i = 1, 2\}$, it gives $g = P_1 = x^4 + x + 1$, which gives a primitive narrow sense BCH code with designed distance 3. Since g has weight 3, the minimum distance of this code is 3.

If one uses $g = lcm\{P_i \mid i = 1, 2, 3, 4\}$, it gives $g = P_1 P_3 = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$, which gives a primitive narrow sense BCH code with designed distance 5. Since g has weight 5, the minimum distance of this code is 5.

If one uses $g = lcm\{P_i \mid i = 1, 2, 3, 4, 5, 6\}$, it gives $g = P_1 P_3 P_5 = (x^8 + x^7 + x^6 + x^4 + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$, which gives a primitive narrow sense BCH code with designed distance 7. Since g has weight 7, the minimum distance of this code is 7.

If one wants codes which are not narrow sense BCH codes, one may consider $g = P_3 P_5 = lcm\{P_i \mid i = 5, 6\} = lcm\{P_i \mid i = 9, 10\}$ which has designed distance 3, or one may consider $g = P_3 P_5 P_7 = lcm\{P_i \mid i = 5, 6, 7\} = lcm\{P_i \mid i = 9, 10, 11, 12, 13, 14\}$, which has designed distance 7, but it seems equivalent to the code with generator $P_1 P_3 P_5$ by replacing ξ by ξ^{-1}.

Remark 27.2: Suppose C is a binary narrow sense BCH code of length 31, and designed distance $d \geq 5$, and let us compute its dimension. One uses Remark 26.8, and since a claim is that $x^5 + x^2 + 1$ is a primitive polynomial, one can check it by noticing that if ξ is a root, then replacing ξ^5 by $1 + \xi^2$ permits to express all the powers of ξ as linear combinations of $1, \xi, \xi^2, \xi^3, \xi^4$, and by induction one constructs a table analogous to that of Remark 26.9, and one should arrive at ξ^{31} with all lower powers of ξ corresponding to different combinations.

Then $P_1 = x^5 + x^2 + 1 = (x - \xi)(x - \xi^2)(x - \xi^4)(x - \xi^8)(x - \xi^{16})$, and using the preceding table one computes the polynomial $P_j = (x - \xi^j)(x - \xi^{2j})(x - \xi^{4j})(x - \xi^{8j})(x - \xi^{16j})$ by developing it, for the values of j which are necessary, i.e. $j = 3$, and then $j = 5$, and the coefficients of these polynomials should be 0 or 1, i.e. belong to $\mathbb{Z}_2$ and not any power ξ^k with $1 \leq k \leq 4$. Since one has observed that $P_7(x) = x^5 P_3\big(\frac{1}{x}\big)$, P_7 is easily deduced from P_1; similarly, $P_{11}(x) = x^5 P_5\big(\frac{1}{x}\big)$, so that P_{11} is easily deduced from P_5, and $P_{15}(x) = x^5 P_1\big(\frac{1}{x}\big)$, so that P_{15} is easily deduced from P_5. One then recalls that P_1 has for roots the ξ^j with $j \in \{1, 2, 4, 8, 16\}$, P_3 has for roots the ξ^j with $j \in \{3, 6, 12, 17, 24\}$, P_5 has for roots the ξ^j with $j \in \{5, 9, 10, 18, 20\}$, P_7 has for roots the ξ^j with $j \in \{7, 14, 19, 25, 28\}$, P_{11} has for roots the ξ^j with $j \in \{11, 13, 21, 22, 26\}$, and P_{15} has for roots the ξ^j with $j \in \{15, 23, 27, 29, 30\}$. Of course, one does not need to do such computations explicitly if one is only interested in comparing the dimensions, hence the transmission rates, compared to the designed distance (which is $\leq$ than the minimum distance $d(C)$ of the code).

If one uses $g = lcm\{P_i \mid i = 1, 2, 3, 4\}$, it gives $g = P_1 P_3$, which has degree 10, so that the code has dimension 21, hence a transmission rate 21/31 for a designed distance 5.

If one uses $g = lcm\{P_i \mid i = 1, 2, 3, 4, 5, 6\}$, it gives $g = P_1 P_3 P_5$, which has degree 15, so that the code has dimension 16, hence a transmission rate 16/31 for a designed distance 7.

If one uses $g = lcm\{P_i \mid i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, it gives $g = P_1 P_3 P_5 P_7$, which has degree 20, so that the code has dimension 11, hence a transmission rate 11/31 for a designed distance 11.

If one uses $g = lcm\{P_i \mid i = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \}$, it gives $g = P_1 P_3 P_5 P_7 P_{11}$, which has degree 25, so that the code has dimension 6, hence a transmission rate 6/31 for a designed distance 15.

The next one is the repetition code, which has transmission rate 1/31 for a designed distance 31.

The preceding codes are primitive, and non-primitive codes avoid the use of P_1: if one uses $g = lcm\{P_i \mid i = 9, 10, 11, 12, 13, 14, \}$, it gives $g = P_3 P_5 P_7 P_{11}$, which has degree 20, so that the code has dimension 11, hence a transmission rate 11/31 for a designed distance 7.

Remark 27.3: BCH codes are highly flexible, allowing control over block length and acceptable error thresholds, so that some codes can be designed to given specifications, but one important reason why BCH codes were so useful much before the power of computers increased so much is that their decoding can be done algebraically, so that the task was performed by very simple electronic hardware, without the need for a computer, hence decoding devices were small and low-powered.

One uses the syndrome decoding method, which for the $[n,k]$-code over $F = F_q$, and for each $y \in F^n$ defines the syndrome $S(y)$ of $y \in F^n$ as $S(y) = y\,H^T$ for a parity-check matrix H, but here one uses the quasi parity check matrix of Remark 26.2.

It means that for $a \in F^n$ one writes $a = (a_0, \ldots, a_{n-1})$ and $a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, and one computes

$$S(a) = a\,H^T = [\,a_0 \quad a_1 \quad \ldots \quad a_{n-1}\,] \begin{bmatrix} 1 & \xi^c & \xi^{2c} & \ldots & \xi^{(n-1)\,c} \\ 1 & \xi^{c+1} & \xi^{2(c+1)} & \ldots & \xi^{(n-1)\,(c+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{c+d-2} & \xi^{2(c+d-2)} & \ldots & \xi^{(n-1)\,(c+d-2)} \end{bmatrix}^T,$$

i.e.

$$S(a) = [\,S_c \quad S_{c+1} \quad \ldots \quad S_{c+d-2}\,], \text{ with}$$
$$S_j = a_0 + a_1\xi^j + \ldots + a_{n-1}\xi^{(n-1)\,j} = a(\xi^j) \text{ for } j = c, \ldots, c+d-2.$$

Suppose a codeword $z \in C$ is transmitted but the vector received is $a = z + e$, where e is the *error vector*, then $S(e) = S(a)$. Let $e = (e_0, \ldots, e_{n-1})$ and $e(x) = e_0 + e_1 x + \ldots + e_{n-1}x^{n-1}$, and let $i_1, \ldots, i_r$ be the positions where an error has occurred, so that $e_i \neq 0$ if and only if $i \in I = \{i_1, \ldots, i_r\}$; it means that $e(x) = \sum_{i \in I} e_i x^i$. The code C can correct up to t errors, where $t = \lfloor \frac{d-1}{2} \rfloor$, hence one assumes that $r \leq t$, i.e. $2r < d$.

Since $S(e) = S(a)$, one has $e(\xi^j) = S_j$ for $j = c, c+1, \ldots, c+d-2$, so that one has $2r$ unknowns ($i_1, \ldots, i_n$ and $e_{i_1}, \ldots, e_{i_r}$) satisfying the following linear system of $d-1$ linear equations in $e_{i_1}, \ldots, e_{i_r}$:

$$\sum_{i \in I} e_i \xi^{j\,i} = S_j, j = c, c+1, \ldots, c+d-2. \tag{1}$$

One first looks for the error positions $i_1, \ldots, i_r$, by defining the *error locator polynomial* f by

$$f(x) = \prod_{i \in I}(x - \xi^i) = f_0 + f_1 x + \ldots + f_{r-1}x^{r-1} + x^r,$$

and since $f(\xi^i) = 0$ for $i \in I$, one has

$$f_0 + f_1\xi^i + \ldots + f_{r-1}\xi^{i\,(r-1)} + \xi^{i\,r} = 0 \text{ for each } i \in I.$$

Multiplying this equation by $e_i\xi^{j\,i}$, summing the r equations for $i = i_1, \ldots, i_r$, and using (1), one has

$$f_0 S_j + f_1 S_{j+1} + \ldots + f_{r-1}S_{j+r-1} + S_{j+r} = 0 \text{ for } j = c, c+1, \ldots, c+d-2.$$

Selecting the first r equations (i.e. $j = c, \ldots, c+r-1$), one deduces that the r unknowns $f_0, \ldots, f_{r-1}$ satisfy the $r \times r$ system of linear equations

$$\begin{bmatrix} S_c & S_{c+1} & \ldots & S_{c+r-1} \\ S_{c+1} & S_{c+2} & \ldots & S_{c+r} \\ \vdots & \vdots & \ddots & \vdots \\ S_{c+r-1} & S_{c+r} & \ldots & S_{c+2r-2} \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{r-1} \end{bmatrix} = \begin{bmatrix} -S_{c+r} \\ -S_{c+r-1} \\ \vdots \\ -S_{c+2r-1} \end{bmatrix}. \tag{2}$$

If S denotes the coefficient matrix of the system (2), one can check that $S = V\,D\,V^T$ with

$$V = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \xi^{i_1} & \xi^{i_2} & \ldots & \xi^{i_r} \\ \vdots & \vdots & \ddots & \vdots \\ \xi^{i_1(r-1)} & \xi^{i_2(r-1)} & \ldots & \xi^{i_r(r-1)} \end{bmatrix}, D = \begin{bmatrix} e_{i_1}\xi^{i_1 c} & 0 & \ldots & 0 \\ 0 & e_{i_2}\xi^{i_2 c} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & e_{i_r}\xi^{i_r c} \end{bmatrix}.$$

Since V is a Vandermonde matrix, ξ is a primitive nth root of unity in F_{q^m}, and $i_1, \ldots, i_r$ are distinct integers $\in \{0, \ldots, n-1\}$, then $\xi^{i_1}, \ldots, \xi^{i_r}$ are all distinct, and $det(V) \neq 0$. Since $e_{i_1}, \ldots, e_{i_r}$ are non-zero, $det(D) \neq 0$, so that $det(S) \neq 0$, hence (2) has a unique solution.

If the actual number of error positions is $< r$, then $det(D) = 0$, henre r is the greatest positive integer $\leq t$ such that (2) has a unique solution, and one finds the value of r by taking successively $r = t, t-1, \ldots$ in (2) until one has a value for which (2) has a unique solution.

The unique solution of (2) gives the error locator polynomial f, and one finds the roots of f by trying $x = \xi^i$ for $i = 0, 1, \ldots$, and by definition they are $\xi^{i_1}, \xi^{i_2}, \ldots, \xi^{i_r}$. If the code C is binary, then $e_{i_1} = \ldots = e_{i_r} = 1$, and in the general case one solves (1).

Remark 27.4: The matrix H is determined by the numbers c, d, n and by ξ, which is a primitive nth root of unity in F_{q^m}, root of a primitive polynomial P, so that for decoding one does not need to know what the generator polynomial g of the BCH code is.

If the code is over F_q, then $S_{j\,q} = (S_j)^q$, so that it is not necessary to use the same procedure for computing all the desired S_j (for $j = c, \ldots, c+d-2$), and the computation can be simplified by using the Euclidean division algorithm: if a is the received vector which one considers as the polynomial $a(x)$, then only the remainder of the Euclidean division of $a(x)$ by P is necessary for computing $a(\xi)$, and similarly for computing $a(\xi^j)$ one first computes the remainder of the division of the polynomial $a(x^j)$ by P, so that for decoding one does not need to use the table expressing all the powers of ξ on the basis $1, \xi, \ldots, \xi^{m-1}$.

If only one error has occurred, in ith position, then $S(a)$ is equal to the ith column of H, so that it is easy to correct, hence it is only in the case where $S(a)$ is non-zero and does not coincide with a column of H that there has been at least two errors and that one uses the described procedure.

Example 27.5: For the [15,5,7] BCH code of Remark 27.1, corresponding to generator polynomial $g = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ (i.e. $g = P_1 P_3 P_5 = lcm\{P_i \mid i = 1, \ldots, 6\}$ with $P_1 = x^4 + x + 1$, $P_3 = x^4 + x^3 + x^2 + x + 1$, $P_5 = x^2 + x + 1$), suppose that one receives $a = 110001001101000 \in F_2^{15}$, what is the corrected codeword and what is the message word?

The polynomial $a(x)$ is $1 + x + x^5 + x^8 + x^9 + x^{11} \in F_2[x]_{15}$, and the entry S_i of $S(a)$ is $a(\xi^i)$ for $i = 1, \ldots, 6$. Using the table of Remark 26.9, one finds that $S_1 = \xi^2, S_2 = (S_1)^2 = \xi^4, S_3 = 1 + \xi^2 = \xi^8, S_4 = (S_2)^2 = \xi^8, S_5 = 1, S_6 = (S_3)^2 = \xi$, so that there has been at least one error because $S(a) \neq 0$, and there has been at least two errors because $S(a)$ is not a column of H (which would have $S_i = (S_1)^i$ for $i = 1, \ldots, 6$). Since the code is designed to correct 3 errors, one first assumes that there are 3 errors and the error locator polynomial $f(x) = f_0 + f_1 x + f_2 x^2 + x^3$ has it coefficients satisfying the system

$$\begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ f_2 \end{bmatrix} = - \begin{bmatrix} S_4 \\ S_5 \\ S_6 \end{bmatrix},$$

and one computes the determinant

$$\det(S) = \begin{vmatrix} \xi^2 & \xi^4 & \xi^8 \\ \xi^4 & \xi^8 & \xi^8 \\ \xi^8 & \xi^8 & 1 \end{vmatrix} = \xi^{10} + \xi^{20} + \xi^{20} - \xi^{18} - \xi^8 - \xi^{24} = \xi^3 + \xi^8 + \xi^9 + \xi^{10} = 0,$$

so that $r \neq 3$, i.e. $r = 2$ (or there are more than 3 errors) and the error locator polynomial $f(x) = f_0 + f_1 x + x^2$ has it coefficients satisfying the system

$$\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \end{bmatrix} = - \begin{bmatrix} S_3 \\ S_4 \end{bmatrix},$$

and one has

$$\det(S) = \begin{vmatrix} \xi^2 & \xi^4 \\ \xi^4 & \xi^8 \end{vmatrix} = \xi^{10} - \xi^8 = \xi \neq 0,$$

and the solution is $f_0 = \xi^{12}, f_1 = \xi^2$. One then uses the table of Remark 26.9 for checking that the roots of $\xi^{12} + \xi^2 x + x^2$ are ξ^{13} and ξ^{14}: the corrected code polynomial is then $1 + x + x^5 + x^8 + x^9 + x^{11} + x^{13} + x^{14}$, the message word is then the quotient by the generator polynomial, which is $x^4 + x^3 + x^2 + 1$, so that the message word is $10111 \in F_2^5$.