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

26- Friday March 23, 2012.

Remark 26.1: For defining BCH codes, one considers F_q the field of size $q = p^k$ (unique up to an isomorphism), and then one considers F_{q^m} as a field extension of F_q of degree m, and one observes that if $\alpha \in F_{q^m}$, then $\alpha, \alpha^q, \alpha^{q^2}, \ldots$ have the same minimal polynomial.[1] BCH codes are then defined as follows.

For $q = p^k$, let c, d, n be positive integers such that $2 \le d \le n$, with n relatively prime with q (i.e. not a multiple of p). Let m be the least positive integer such that $q^m = 1 \pmod n$ (i.e. m is the order of q in the multiplicative group $\mathbb{Z}_n^*$ of units in $\mathbb{Z}_n$, so that m divides $\varphi(n)$ by Euler's theorem), so that n divides $q^m - 1$.

Let $\xi \in F_{q^m}$ be a primitive nth root of unity in F_{q^m}, which exists because n divides $q^m - 1$,[2] and let $P_i \in F_q[x]$ be the minimal polynomial of ξ^i, so that P_i divides $x^n - 1$ for each i. Let g be the product of distinct polynomials among P_i for $i = c, c+1, \ldots, c+d-2$, i.e. $g = lcm\{P_i \mid i = c, c+1, \ldots, c+d-2\}$, and since P_i divides $x^n - 1$ for each i, one deduces that g divides $x^n - 1$. Let C be the cyclic code with generator polynomial g in the ring $F_q[x]_n$: C is called a *BCH code* of *length* n over F_q with *designed distance* d.

If $n = q^m - 1$, then the BCH code C is called *primitive*. If $c = 1$, then C is called a *narrow sense BCH code.*

Remark 26.2: It means that $C = \{Q \in F_q[x]_n \mid Q(\xi^i) = 0 \text{ for } i = c, c+1, \ldots, c+d-2\}$, i.e. C is the null space of

$$H = \begin{bmatrix} 1 & \xi^c & \xi^{2c} & \ldots & \xi^{(n-1)\,c} \\ 1 & \xi^{c+1} & \xi^{2(c+1)} & \ldots & \xi^{(n-1)\,(c+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{c+d-2} & \xi^{2(c+d-2)} & \ldots & \xi^{(n-1)\,(c+d-2)} \end{bmatrix},$$

whose rows are not necessarily linearly independent, so that H is not exactly a parity check matrix, but one may use it as a *quasi parity check matrix.* Since H is a $(d-1)\times n$ matrix over F_{q^m}, it can be considered as a $m\,(d-1)\times n$ matrix over F_q, whose rank is then $\le m\,(d-1)$, so that the length of the code is $\ge n - m\,(d-1)$.

Since the minimum distance $d(C)$ of the code C is the minimal number of linearly dependent columns in a parity check matrix, one can show that it is $\ge d$ by checking that the above matrix H has rank $\ge d-1$, i.e. any $(d-1)\times(d-1)$ matrix extracted from H has a non-zero determinant, and it is the case since it is a Vandermonde determinant.[3]

Remark 26.3: The binary Hamming code $Ham(r,2)$ is a BCH code: one takes $q = 2$ and $n = 2^r - 1$, which gives $m = r$, so that $F_{q^m} = F_{2^r}$. Let ξ be a primitive nth root of unity in F_{2^r}, so that ξ generates $F_{2^r}^*$, and let g be the minimal polynomial of ξ, which has then degree r. Since ξ and ξ^2 have the same minimal polynomial, one has $g = lcm\{P_i \mid i = 1,2\}$, so that C is a narrow sense primitive BCH code of designed distance 3, but since it is equivalent to the binary Hamming code $Ham(r,2)$, one has $d(C) = 3$.

Remark 26.4: The binary Golay code is a BCH code: one takes $q = 2$ and $n = 23$, so that $m = 11$ and $F_{q^m} = F_{2^{11}}$ (i.e. F_{2048}).[4] Let ξ be a primitive 23rd root of unity in $F_{2^{11}}$, and g be the minimal polynomial of ξ, which is also the minimal polynomial of $\xi^2, \xi^4, \xi^8, \ldots$ and one checks that one power of 2 is $= 3 \pmod{23}$, namely $2^8 = 256 = 3 \pmod{23}$, so that $g = lcm\{P_i \mid i = 1,2,3,4\}$, and the cyclic code C is then a narrow sense BCH code of designed distance 5 over F_2. g divides $x^{23} - 1$ and its degree is 11 (since $1, \xi, \ldots, \xi^{10}$ is a

[1] From $\left(\sum_i a_i x^i\right)^p = \sum_i a_i^p x^{p\,i}$ one deduces that $\left(\sum_i a_i x^i\right)^q = \sum_i a_i^q x^{q\,i}$ and $\left(\sum_i a_i x^i\right)^{q^m} = \sum_i a_i^q x^{q^m i}$, and then one uses the fact that every $\beta \in F_{q^\ell}$ satisfies $\beta^{q^\ell} = \beta$.

[2] The multiplicative group $F_{q^m}^*$ is cyclic, so that it has a generator α, and then if $q^m = n\,n'$ one deduces that $\xi = \alpha^{n'}$ is a primitive nth root of unity in F_{q^m}.

[3] Alexandre-Théophile VANDERMONDE, French mathematician, 1735–1796.

[4] Since $5^2 = 2 \pmod{23}$, 2 is a quadratic residue modulo 23, so that $2^{11} = 1 \pmod{23}$, hence the order of 2 divides 11, i.e. it is 11.

power basis of $F_{2^{11}}$ over F_2), hence C is the binary $[23, 12, 7]$ Golay code, which has $d(C) = 7$, a case where $d(C) > d$.

Remark 26.5: The ternary Golay code is a BCH code: one takes $q = 3$ and $n = 11$, so that $m = 5$ and $F_{q^m} = F_{3^5}$ (i.e. F_{243}).[5] Let ξ be a primitive 11rd root of unity in F_{3^5}, and g be the minimal polynomial of ξ, which is also the minimal polynomial of $\xi^3, \xi^9, \xi^{27}, \xi^{81}, \ldots$ and since $81 = 4 \pmod{11}$ and $27 = 5 \pmod{11}$, one has $g = lcm\{P_i \mid i = 3, 4, 5\}$, and the cyclic code C is then a BCH code of designed distance 4 over F_3. g divides $x^{11} - 1$ and its degree is 5 (since $1, \xi, \ldots, \xi^4$ is a power basis of F_{3^5} over F_3), hence C is the ternary $[11, 6, 5]$ Golay code, which has $d(C) = 5$, another case where $d(C) > d$.

Remark 26.6: Another example of a BCH code is a *Reed–Solomon* code. It corresponds to $n = q - 1$, so that $m = 1$. If ξ is a primitive element in F_q^*, its minimal polynomial of ξ over F_q is $x - \xi$. One takes $c = 1$ and $2 \le d \le n$, and the Reed–Solomon code is the cyclic code with generator polynomial $g = (x - \xi)\,(x - \xi^2) \cdots (x - \xi^{d-1})$, which is then a primitive narrow sense BCH code of designed distance d. Since g has degree $d - 1$, this code C has dimension $k = n - d + 1$, and since $d(C) \le n - k + 1 = d$, it has $d(C) = d$, hence it is a $[q - 1, q - d, d]$ code.

Remark 26.7: For constructing BCH codes of a given length n and designed distance d, one needs to know a primitive element $\xi \in F_{q^m}$, i.e. whose powers $\{1, \xi, \ldots, \xi^{m-1}\}$ form a (power) basis of $F_{q^m}^*$ over F_q, and know its associated monic irreducible polynomial ($\in F_q[x]$), which is then called a *primitive polynomial* over F_q, and has degree m.

For example, taking $q = 2$ (i.e. the basic field is $F_2 \simeq \mathbb{Z}_2$), the case $m = 2$ corresponds to $(x - \xi)\,(x - \xi^2) = x^2 + x + 1$ (i.e. the quotient of $x^3 - 1$ by $x - 1$). The case $m = 3$ corresponds $\xi^7 = 1$, and if $P = (x - \xi)\,(x - \xi^2)\,(x - \xi^4)$, and $Q = (x - \xi^3)\,(x - \xi^6)\,(x - \xi^{12})$, whose roots are ξ^3, ξ^5, ξ^7, i.e. the inverses of ξ^4, ξ^2, ξ, so that $Q(x) = x^3 P\big(\frac{1}{x}\big)$, one deduces that $P = x^3 + a\,x^2 + b\,x + 1$ and $Q = x^3 + b\,x^2 + a\,x + 1$, and one has $P\,Q = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ (i.e. the quotient of $x^7 - 1$ by $x - 1$). Since the coefficient of x^5 in $P\,Q$ gives $a + b = 1$, there are two primitive polynomials of degree 3, namely $x^3 + x + 1$ and $x^3 + x^2 + 1$.

The case $m = 4$ corresponds $\xi^{15} = 1$, and if $P = (x - \xi)\,(x - \xi^2)\,(x - \xi^4)\,(x - \xi^8)$, and $Q = (x - \xi^7)\,(x - \xi^{14})\,(x - \xi^{28})\,(x - \xi^{56})$, whose roots are $\xi^7, \xi^{11}, \xi^{13}, \xi^{14}$, i.e. the inverses of ξ^8, ξ^4, ξ^2, ξ, so that $Q(x) = x^4 P\big(\frac{1}{x}\big)$, one deduces that $P = x^4 + a\,x^3 + b\,x^2 + c\,x + 1$ and $Q = x^4 + c\,x^3 + b\,x^2 + a\,x + 1$, but one must find what $P\,Q$ is. One has $R = (x - \xi^3)\,(x - \xi^6)\,(x - \xi^{12})\,(x - \xi^{24}) = x^4 + x^3 + x^2 + x + 1$ (i.e. the quotient of $x^5 - 1$ by $x - 1$), because its roots are $\xi^3, \xi^6, \xi^9, \xi^{12}$, which are the fifth roots of unity different from 1. One has $S = (x - \xi^5)\,(x - \xi^{10}) = x^2 + x + 1$ (i.e. the quotient of $x^3 - 1$ by $x - 1$), because its roots are ξ^5, ξ^{10}, which are the cube roots of unity different from 1. From $(x - 1)\,P\,Q\,R\,S = x^{15} - 1$ and $(x - 1)\,R = x^5 - 1$, one deduces that $P\,Q\,S = x^{10} + x^5 + 1$ (i.e. the quotient of $x^{15} - 1$ by $x^5 - 1$), so that $P\,Q$ is the quotient of $x^{10} + x^5 + 1$ by $x^2 + x + 1$, and the Euclidean division algorithm gives $P\,Q = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$. Since the coefficient of x^7 in $P\,Q$ gives $a + c = 1$, and the coefficient of x^4 then gives $b^2 = 0$, there are two primitive polynomials of degree 4, namely $x^4 + x + 1$ and $x^4 + x^3 + 1$.

Remark 26.8: Still with $q = 2$, the case $m = 5$ for a primitive root ξ satisfying $\xi^{31} = 1$ leads to define the polynomials $P_j = (x - \xi^j)\,(x - \xi^{2j})\,(x - \xi^{4j})\,(x - \xi^{8j})\,(x - \xi^{16j})$, because if a has monic irreducible polynomial P then it is the same for $a^2, a^4, \ldots$. Because 31 is prime, one has $\varphi(31) = 30$, and there are 6 such polynomials: P_1 (powers of ξ being 1, 2, 4, 8, 16), P_3 (powers of ξ being 3, 6, 12, 17, 24), P_5 (powers of ξ being 5, 9, 10, 18, 20), P_7 (powers of ξ being 7, 14, 19, 25, 28), P_{11} (powers of ξ being 11, 13, 21, 22, 26), P_{15} (powers of ξ being 15, 23, 27, 29, 30). One has $P_{15}(x) = x^5 P_1\big(\frac{1}{x}\big)$, $P_7(x) = x^5 P_3\big(\frac{1}{x}\big)$, and $P_{11}(x) = x^5 P_5\big(\frac{1}{x}\big)$.

I do not know how one identifies these primitive polynomials,[6] but a book lists $x^5 + x^2 + 1$ as one such primitive polynomial for degree 5, $x^6 + x + 1$ as one for degree 6, $x^7 + x + 1$ as one for degree 7, and $x^8 + x^4 + x^3 + x^2 + 1$ as one for degree 8.

---

[5] Since $6^2 = 3 \pmod{11}$, 3 is a quadratic residue modulo 11, so that $3^5 = 1 \pmod{11}$, hence the order of 3 divides 5, i.e. it is 5.

[6] One may proceed as in Remark 26.9, and check that the following polynomials are indeed primitive by writing the decompositions of all powers of ξ on the power basis: for example, in order to check that $x^5 + x^2 + 1$ is a primitive polynomial for the case $m = 5$, one uses $\xi^5 = 1 + \xi^2$ and one then writes all the powers of ξ up to ξ^{31} as linear combinations of $1, \xi, \xi^2, \xi^3, \xi^4$ with coefficients 0 or 1, and one observes that the 32 powers of ξ have different components on the basis.

Remark 26.9: In order to construct binary codes of length 15 with various designed distances, one chooses the primitive polynomial $P = x^4 + x + 1$ obtained at Remark 26.7, one lets ξ be any of its four roots, and one uses the (power) basis $1, \xi, \xi^2, \xi^3$ for F_{16} over F_2, and since $\xi^4 = 1 + \xi$ one constructs easily by induction the formula expressing ξ^j:

$$\begin{array}{ccc} \xi^4 = 1 + \xi & \xi^8 = 1 + \xi^2 & \xi^{12} = 1 + \xi + \xi^2 + \xi^3 \\ \xi^5 = \xi + \xi^2 & \xi^9 = \xi + \xi^3 & \xi^{13} = 1 + \xi^2 + \xi^3 \\ \xi^6 = \xi^2 + \xi^3 & \xi^{10} = 1 + \xi + \xi^2 & \xi^{14} = 1 + \xi^3 \\ \xi^7 = 1 + \xi + \xi^3 & \xi^{11} = \xi + \xi^2 + \xi^3 & \xi^{15} = 1 \end{array}.$$