TC10 / **Problems 46-60**

S. Xambó

46. If ω is a primitive element of $\mathbb{F}_{64}$, prove that the minimum distance of $BCH_\omega(16)$ is ≥ 21 and that its dimension is 18.

47. Let $f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}_2[X]$, $F = \mathbb{Z}_2[X]/(f)$ and α a primitive element of F. Find the dimension and a control matrix (over $\mathbb{Z}_2$) of $BCH_\alpha(5)$. Show that the minimum distance of this code is 7.

48. *Cyclotomic polynomials.* In the factorization of $X^n - 1 \in \mathbb{F}_q[X]$, let

$$Q_n = \prod_{\gcd(j,n)=1} (X - \omega^j)$$

(the degree of this polynomial is $\varphi(n)$ and it is called the n-th *cyclotomic polynomial over* $\mathbb{F}_q$). Prove that:

1. $X^n - 1 = \prod_{d|n} Q_d$.
2. $Q_n \in \mathbb{Z}_p[X]$ for all n, where p is the characteristic of $\mathbb{F}_q$.

3. $Q_n = \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}$, where μ is the Möbius function ($\mu(m)$ is 0 if m has repeated prime factors, and otherwise it is $+1$ or -1 according to whether the number of prime factors is even or odd).

4. If n is prime,

$$Q_n = X^{n-1} + X^{n-2} + \cdots + X + 1 \text{ and } Q_{n^k}(X) = Q_n(X^{n^{k-1}}).$$

5. If $m = e_n(q)$ and $\gcd(q, n) = 1$, then Q_n is the product of $\varphi(n)/m$ distinct irreducible polynomials of degree m.

49. Let g and g' be the irreducible factors of degree 5 of $X^{11} - 1$ over $\mathbb{Z}_3$. Show that the exponents j of the roots ω^j of g (of g') are the quadratic non-residues (the quadratic residues) modulo 11. If $k \in \mathbb{Z}_{11}^*$ is a quadratic non-residue ($k \in \{2,6,7,8,10\}$) and π_k is the permutation $i \mapsto ki$ of $\mathbb{Z}_{11} = \{0,1, \ldots ,10\}$, prove that $\pi_k(C_g) = C_{g'}$. This is an example of two distinct cyclic codes that are equivalent.

50. Let C be a cyclic linear binary code of odd length n. Prove that C contains a vector of odd weight if and only if it contains the vector $\mathbf{1}_n$. If this condition is satisfied, prove that the subcode of C formed by the even-weight vectors is a cyclic code.

51. Find the weight enumerators of the ternary Golay codes $\bar{\Gamma}_3$ and Γ_3.

52. Find the dimension and minimum distance of all the binary strict BCH codes of length 15. Ditto of length 31. Ditto of length 63.

53. Calculate a control matrix of a binary BCH code of length 31 that corrects 2 errors.

54. Find a generator polynomial of a binary BCH code of length 11 and design distance 5.

55. Compute the dimension of a BCH code over $\mathbb{Z}_3$ of length 80 that corrects 5 errors.

56. Calculate the generator polynomial of a ternary BCH code of length 26 and design distance 5. Find also its dimension.

57. Let $\alpha = 7 \bmod 17 \in \mathbb{Z}_{17}$. Prove that the minimum distance of $BCH_\alpha(7,3)$ is 7.

58. Let $G = I_6 | \binom{\mathbf{1}_5}{S_5}$, where S_5 is the Paley matrix of $\mathbb{Z}_5$ (is the 5×5 matrix with 0's along its diagonal and with $+1$ or -1 at the (i,j) entry according to whether $i-j \in \{1,4\}$ or $i-j \in \{2,3\}$). Prove that $\langle G \rangle$ is a ternary Golay code (that is, $\sim [11,6,5]_3$).

59. If $\boldsymbol{h}' = (h_1', \dots, h_n')$ is a non-zero vector of the kernel of the matrix $V_{n-1}(\alpha_1, \dots, \alpha_n) \cdot \mathrm{diag}(h_1, \dots, h_n)$, prove that the dual of $GRS(\boldsymbol{h}, \boldsymbol{\alpha}, k)$ is $GRS(\boldsymbol{h}', \boldsymbol{\alpha}, n-k)$.

60. (Alternative definition of classical Goppa codes)**.** Let $K = \mathbb{F}_q$ and $\bar{K} = \mathbb{F}_{q^m}$, m a positive integer. Let $g \in K[T]$ be a polynomial of degree $r > 0$ and $\boldsymbol{\alpha} = \alpha_1, \dots, \alpha_n \in \bar{K}$ the elements such that $g(\alpha_i) \neq 0$ for all i. Set, according to Goppa's original definition,

$$\Gamma'(g, \boldsymbol{\alpha}) = \left\{ a \in K^n \mid \sum_{i=1}^{n} \frac{a_i}{x - \alpha_i} \equiv 0 \bmod g \right\}. \qquad [*]$$

In this problem we will see that $\Gamma'(g,\boldsymbol{\alpha}) = \Gamma(g,\boldsymbol{\alpha})$.

1) Given $\alpha \in \overline{K}$ such that $g(\alpha) \neq 0$, show that $x-\alpha$ is invertible modulo g and that

$$\frac{1}{x-\alpha} = -\frac{1}{g(\alpha)}\frac{g(x)-g(\alpha)}{x-\alpha} \mod g$$

(note that $\frac{g(x)-g(\alpha)}{x-\alpha}$ is a polynomial of degree $< r$ with coefficients in $\overline{K}$).

2) Show that the condition

$$\sum_{i=1}^{n} \frac{a_i}{x-\alpha_i} \equiv 0 \mod g$$

is equivalent to

$$\sum_{i=1}^{n} \frac{a_i}{g(\alpha_i)}\frac{g(x)-g(\alpha_i)}{x-\alpha_i} = 0.$$

3) Use this relation to prove that the code defined by [*] admits a control matrix of the form

$$H^* = U \cdot H = U \cdot V_r(\alpha_1,\dots,\alpha_n) \cdot \mathrm{diag}(h_1,\dots,h_n),$$

where $h_i = 1/g(\alpha_i)$, $U = \left(g_{r-i+j}\right)_{1\le i,j\le r}$, with the convention that $g_l = 0$ si $l < 0$ o $l > r$ (here $g = g_0 + g_1 X + \cdots + g_r X^r$).

4) Since U is invertible, the code defined by $[*]$ also admits a control matrix of the form

$$H = V_r(\alpha_1, \dots, \alpha_n) \cdot \mathrm{diag}(h_1, \dots, h_n),$$

and this establishes $\Gamma'(g, \boldsymbol{\alpha}) = \Gamma(g, \alpha)$, as H is a control matrix for $\Gamma(g, \alpha)$.