MAD 6607: Coding Theory

Edoardo Persichetti Test 4 Solutions

Exercise 1 For the definition of Mattson-Solomon polynomial, see Chapter 8 of the book.

Exercise 2 Let $q = 2$ and $n = 31$.

a) We have $C_1 = \{1, 2, 4, 8, 16\}$, $C_3 = \{3, 6, 12, 24, 17\}$ etc.

b) It's obviously 5.

c) The parity-check matrix is given as in the textbook, where the first row has all powers of α, the second row has $1, \alpha^3, \alpha^6, \ldots$ and the third row has $1, \alpha^5, \alpha^{10}, \ldots$

d) The true minimum distance is in fact 7. You can check the criteria using binomial coefficients (Theorem 2, page 259).

e) The dimension is 16. The simplest method is to use Corollary 8, page 263 and check that $5 = 2t - 1 < 2^{\lceil m/2 \rceil} + 1 = 9$.

f) The generator polynomial for this code is $g(x) = M^{(1)}(x) \cdot M^{(3)}(x) \cdot M^{(5)}(x) = x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$. The corresponding generator matrix is given by 16 cyclic shifts of the binary word of its coefficients.

Exercise 3 The first stage consists of computing the syndrome of y, i.e. $Hy^T = (\alpha^{13}, \alpha^{29}, \alpha^4)$. Then, we find the locator polynomial: we use the special form of Newton's identities for binary codes, and after solving the system we get $\sigma_1 = \alpha^{13}, \sigma_2 = \alpha^{10}$ and $\sigma_3 = \alpha^{27}$ so the locator polynomial is $\sigma(z) = 1 + \alpha^{13}z + \alpha^{10}z^2 + \alpha^{27}z^3$. The roots of this polynomial are α, α^7 and α^{27} and so taking reciprocals we determine that the errors are in positions $4, 24$ and 30. Correcting the errors we obtain the codeword (00011110101110011000111110001 00).