

Coding Theory

(Midterm 2004 Fall)

Time: 18:40-21:30 11/18/2004

Venue: EC 122

(100 points in total, solve all problems)

[1] Given a linear code C with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

(1) Find another generator matrix in standard form by applying elementary row operations on G (show your steps) (5 points)

(2) Find a parity check matrix for C from the generator matrix obtained in (1). (3 points)

[2] (1) Give a parity check matrix for any Hamming code of length 15 ($r=4$). (3 points)

(2) Briefly explain that the minimal distance of a Hamming code of length 2^r-1 is 3. (3 points)

(3) Prove a Hamming code of length 2^r-1 is a perfect code. (3 points)

(4) Prove the Golay code C_{23} is a perfect code. (3 points)

[3] (1) List all of the linear cyclic codes of length 6. (In your answer you can use $\langle\langle g(x) \rangle\rangle$ to denote a cyclic code generated by $g(x)$ and no need to describe the contents of $\langle\langle g(x) \rangle\rangle$.) (3 points)

(2) Find the number of proper linear cyclic codes of length 120. (show your steps) (3 points)

(3) List all of the linear cyclic codes of length 14 and dimension 6. (4 points)

Hint: You may need following factorization of $1+x^n$ into irreducible polynomials:

$$1+x^3=(1+x)(1+x+x^2)$$

$$1+x^7=(1+x)(1+x+x^3)(1+x^2+x^3)$$

$$1+x^{15}=(1+x)(1+x+x^2)(1+x+x^2+x^3+x^4)(1+x+x^4)(1+x^3+x^4)$$

[4](1) Construct $GF(2^4)$ using $h(x)=1+x^3+x^4$. Let $\beta \leftarrow x \pmod{h(x)}$ and make a table similar to Table 5.1 in p.114. (8 points)

(2) Use the table constructed in (1) to answer the followings

(a) What is the multiplicative inverse of $1+x^2$? (3 points)

(b) Find all primitive elements in $GF(2^4)$. (5 points)

[5] $GF(2^4)$ is constructed by using $h(x)=1+x^3+x^4$ as shown in [4]

Let $g(x) = (\beta^2+x)(\beta^3+x)(\beta^4+x)(\beta^5+x)$ generate a linear cyclic code C over $GF(2^4)$.

(1) How many codewords does C have? (3 points)

(2) Construct a generating matrix G for C . (4 points)

(3) Encode the messages $m(x) = \beta^5x + x^2$ using G . (3 points)

(4) What is the minimum distance of C ? (2 points)

(5) Find the generator polynomial of the cyclic binary subfield subcode. (4 points)

[6] (1) Prove that in BCH decoding, if two errors occurred, say in position i and j , $i \neq j$, then β^i and β^j are roots of the quadratic equation

$$x^2 + s_1x + (s_3s_1^{-1} + s_1^2) = 0,$$

where $[s_1, s_3] = [w(\beta), w(\beta^3)]$ is the syndrome of the received word w . (8 points)

(2) Briefly describe how you can tell if a received word has no error, one error bits, two error bits, or more than two error bits. (8 points)

[7] Find all idempotent polynomials mod $1+x^{17}$, that is those polynomials $I(x)$ such that $I(x) = I(x)^2 \pmod{1+x^{17}}$. (10 points)

[8] (Derive a lower bound for general codes.)

The theorem of the Gilbert-Varshamov bound for linear codes is stated as:

There exists a binary linear code C of length n , minimum distance d with

$$|C| \geq \frac{2^{n-1}}{\binom{n-1}{0} + \binom{n-1}{1} + \binom{n-1}{2} + \dots + \binom{n-1}{d-2}}$$

Derive a lower bound for general codes by using the hint as below.

That is to prove that there exists a binary linear code C of length n , minimum distance d with $|C| \geq x$ for proper value x . (12 points)

(Hint: You may consider a maximal binary code C of length n , minimum distance d first. C is maximal in the sense that no word can be added to C without reducing the minimum distance. Then use the arguing approach similar to that of Hamming bound.)