

ECE/MATH 641 FINAL, SPRING 2008

NIGEL BOSTON

For full credit you must explain your reasoning. Each question is worth an equal amount. Answer them in any order. Don't overlook any parts to a question!

1. (a) Let C be the binary linear code with generator matrix $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$

Find its minimum distance and its weight enumerator. Is C optimal?

ANS: Listing the 7 nonzero elements shows they all have weight 4, so the minimum distance is 4 and $A_0 = 1, A_4 = 7$. C is not optimal since e.g. 00001111 is at distance 4 from every codeword of C . (What's happening is that C is a subcode of the $[8, 4, 4]$ code \mathcal{H}_3^{ext} .)

(b) How many cosets does C have? Find a parity check matrix for C . Use syndrome decoding to decode the received vector 11000010.

ANS: It has $2^{n-k} = 2^5 = 32$ cosets. A parity check matrix is $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

Multiplying by the received vector transposed gives $(0 \ 0 \ 0 \ 0 \ 1)^T$, the last column of H . Subtracting e_8 from the received vector gives 11000011.

(c) State MacWilliams' Theorem relating the weight enumerators of a binary linear code and its dual.

ANS: $W^\perp(x, y) = W(y - x, y + x)/|C|$ if W and W^\perp denote the weight enumerators of C and C^\perp respectively.

(d) Find a generator matrix for the dual code C^\perp . Find its minimum distance and its weight enumerator.

ANS: H is a generator matrix. $W(x, y) = y^8 + 7x^4y^4$ and so $W^\perp(x, y) = ((y + x)^8 + 7(y - x)^4(y + x)^4)/8 = ((y + x)^8 + 7(y^2 - x^2)^4)/8 = (y^8 + 8y^7x + 28y^6x^2 + 56y^5x^3 + 70y^4x^4 + 56y^3x^5 + 28y^2x^6 + 8yx^7 + x^8 + 7(y^8 - 4y^6x^2 + 6y^2x^4 - 4y^2x^6 + x^8))/8 = (8y^8 + 8y^7x + 56y^5x^3 + 112y^4x^4 + 56y^3x^5 + 8yx^7 + 8x^8)/8 = y^8 + y^7x + 7y^5x^3 + 14y^4x^4 + 7y^3x^5 + yx^7 + x^8$. The minimum distance is 1 (in fact H has a row of weight 1.)

2. (a) Let $f(x) = x^3 + x^2 + 1 \in \mathbf{F}_2[x]$. Let α be a root of $f(x)$. Show that $f(x)$ is irreducible.

ANS: $f(0) = 1, f(1) = 1$. No roots implies no linear factors, and so, since f is cubic, f is irreducible.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$

(b) Define what a primitive element of a field is. Show that α is a primitive element of \mathbf{F}_8 . Write $1, \alpha, \alpha^2, \dots, \alpha^6$ as linear combinations of $1, \alpha, \alpha^2$ and give the minimal polynomial over \mathbf{F}_2 of each element of \mathbf{F}_8 .

ANS: β is a primitive element of a field F if every nonzero element of F is a power of β . $1, \alpha, \alpha^2$ stay the same and have minimal polynomials $x + 1, f, f$ respectively. $\alpha^3 = 1 + \alpha^2, \alpha^4 = 1 + \alpha + \alpha^2, \alpha^5 = 1 + \alpha, \alpha^6 = \alpha + \alpha^2$. Since all these powers are distinct, α is primitive. α^4 has minimal polynomial f . $\alpha^3, \alpha^5, \alpha^6$ have minimal polynomial $x^3 + x + 1$. 0 has minimal polynomial x .

(c) Using α , define the Hamming code \mathcal{H}_3 . Prove that its parameters are $[7, 4, 3]$ and that it is a perfect code.

ANS: $\mathcal{H}_3 = \{c(x) = c_0 + c_1x + \dots + c_6x^6 \mid c(\alpha) = 0\}$. $n = 7$ since $c(x)$ has 7 coefficients. $k = 4$ since writing each α^i as in (b) turns the condition $c(\alpha) = 0$ into 3 independent parity checks. The columns of the parity check matrix are the powers of α - since one is not a multiple of another, the minimum distance is at least 3. Since $f(\alpha) = 0$, $f \in \mathcal{H}_3$ and has weight 3, so $d = 3$. A ball of radius $(d - 1)/2 = 1$ contains $1 + 7 = 8$ vectors. The balls around the $2^4 = 16$ codewords are disjoint so yield 128 vectors, but that accounts for all the vectors.

(d) Show that \mathcal{H}_3 has no codewords of weight 5 or 6.

ANS: $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = (1 + x^2 + x^3)(1 + x + x^3)$ so is in \mathcal{H}_3 . Adding this to a codeword of weight 5 or 6 yields a codeword of weight 2 or 1, contradicting (c).

3. (a) Let α be a primitive element of \mathbf{F}_{64} . Let $m_i(x)$ denote the minimal polynomial of α^i over \mathbf{F}_2 . What are the degrees of $m_1(x), m_3(x)$, and $m_9(x)$?

ANS: The cyclotomic cosets are $\{1, 2, 4, 8, 16, 32\}, \{3, 6, 12, 24, 48, 33\}, \{9, 18, 36\}$, so the degrees are 6, 6, 3 respectively.

(b) Let $g(x) = m_1(x)m_3(x)$. What are the parameters $[n, k, d]$ of the cyclic code with generator polynomial $g(x)$ (you may give the designed lower bound for d)?

ANS: $n = 63$. Since g has degree $12 = n - k$, $k = 51$. Since $g(\alpha) = g(\alpha^2) = g(\alpha^3) = g(\alpha^4) = 0$, the designed distance $d = 5$.

(c) Let $v(x) = c(x) + e(x)$ be the received vector, where $c(x)$ is a codeword and $e(x)$ has at most 2 nonzero coefficients. If the syndromes $v(\alpha) = 1 + \alpha$ and $v(\alpha^3) = 1 + \alpha^3$, find $e(x)$.

ANS: $1 + \alpha = v(\alpha) = e(\alpha)$ and $1 + \alpha^3 = v(\alpha^3) = e(\alpha^3)$ are satisfied by $e(x) = 1 + x$.

(d) How many binary cyclic codes of length 63 are there?

ANS: The irreducible factors of $x^{63} - 1$ have degree 6 except for those producing the subfields $\mathbf{F}_2, \mathbf{F}_4, \mathbf{F}_8$. Namely, $x^{63} - 1 = (x - 1)(x^2 + x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ times several degree 6 irreducible polynomials. Comparing degrees, there are $(63 - 9)/6 = 9$ of these, so $x^{63} - 1$ has 13 factors in all. Thus there are 2^{13} binary cyclic codes of length 63.

4. (a) Give the Singleton bound and define what it means for a linear code to be Maximum Distance Separable (MDS). Show that for every n there exist $[n, 1]$ and $[n, n]$ MDS binary linear codes.

ANS: The Singleton bound says that for any linear code $d \leq n - k + 1$. An MDS code is one for which equality holds. The repetition code of length n has dimension 1 and minimum distance $n = n - 1 + 1$. The code containing all vectors of length n

has dimension n and minimum distance $1 = n - n + 1$. Both these are MDS codes.

(b) Carefully define the $[63, 53]$ Reed-Solomon code over \mathbf{F}_{64} . What is its minimum distance?

ANS: If α is a primitive element of \mathbf{F}_{64} , the code is $\{(f(1), f(\alpha), f(\alpha^2), \dots, f(\alpha^{62})) \mid f \in \mathbf{F}_{64}[x], \deg(f) < 53\}$. It is MDS so has minimum distance $63 - 53 + 1 = 11$.

(c) If C is a binary linear $[n, k, d]$ code, let $R(C) = k/n$ and $\delta(C) = d/n$. Consider the set $S = \{(\delta(C), R(C)) : C \text{ is a binary linear code}\}$. State briefly the main facts known about S .

ANS: Should state how the set of limit points of S is given by $R \leq \alpha(\delta)$ for some function α . Lower bounds (e.g. Gilbert-Varshamov $R = 1 - h(\delta)$) and upper bounds (e.g. Plotkin $R = 1 - 2\delta$) for α are known.

(d) Why do MDS codes produce very few points in S (and so do not contradict your answer to (c))?

ANS: MDS codes over \mathbf{F}_q are only known for lengths $\leq q + 2$ besides the trivial examples in (a). Here $q = 2$. These do not contribute to the limit set.

5. (a) Define the Binary Erasure Channel (BEC) and the Binary Symmetric Channel (BSC).

ANS: The BEC has inputs $0, 1$ and outputs $0, e, 1$ - with probability p , an input yields output e and otherwise it stays the same. The BSC has inputs and outputs $0, 1$ - with probability p , an input is changed and otherwise it stays the same.

(b) State Shannon's theorem for random codes on the BSC.

ANS: Given $\epsilon > 0$ and $R \leq 1 - h(p) - \gamma, \gamma > 0$, there exists n_0 such that for any $n \geq n_0$ there exists a code of length n whose error probability of decoding on the BSC is $\leq \epsilon$.

(c) Let C be the binary linear code with parity check matrix $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

Draw its Tanner graph. Suppose $10ee1e$ is received using a BEC (where e denotes an erased bit). Decode this word.

ANS: Draw 6 variable nodes and 3 check nodes, joining the 1st check node to variable nodes 1, 4, 5, the 2nd check node to variable nodes 2, 4, 6, and the 3rd check node to variable nodes 3, 4, 5, 6. Plugging $10ee1e$ into the checks, we have: $1 + x_4 + 1 = 0, 0 + x_4 + x_6 = 0, x_3 + x_4 + 1 + x_6 = 0$. Thus $x_4 = 0$, so $x_6 = 0$, so $x_3 = 1$, giving 101010 .

(d) Explain briefly how this can be interpreted as iterative decoding or belief propagation on the Tanner graph. Show that this method can fail if the 3 erased bits are in other positions.

ANS: Talk about how the variable nodes send the initial information on their values to the check nodes. Each check node does a local calculation - basically, if all variables but one are known, then it can send to that remaining variable node its value. Otherwise it sends the message that it knows nothing. If a variable node receives a value from some check, then it sticks with that and sends that to all adjacent checks. Otherwise, it sends out that it doesn't know its value. This process is iterated. So long as in each round at least one check finds itself adjacent to exactly one unknown variable, this process continues to completion. In our situation, the algorithm would stick if say $000eee$ were received since each check involves 2 or more unknown variables.