

## Problems for ENEE626-2006 Coding Theory

Add problems on nonbinary cyclic codes: symbol field, locator field (see prob.2 in the final of 2006); minimal polynomials over  $F_q$

Last modified on 12/22/2006.

Computers can be used only in problems (or their parts) marked with a §.

1. Let  $F = \{0, 1\}^n$  be the binary Hamming space.

(a) What is the number of vectors  $\mathbf{x} \in F$  of weight  $w$ ? What is the number of vectors in  $F$  of even weight?

(b) Let  $\mathbf{x}, \mathbf{y} \in F$ ,  $d(\mathbf{x}, \mathbf{y}) = k$ . What is the number  $p_{ij}^k$  of vectors  $\mathbf{z}$  such that  $d(\mathbf{z}, \mathbf{x}) = i$ ,  $d(\mathbf{z}, \mathbf{y}) = j$ ? In particular, what is  $p_{ij}^0$ ?

2. Let  $F = \{0, 1, 2\}^n$  be the set of all  $n$ -vectors over the alphabet of 3 letters. Define the Hamming distance between  $\mathbf{x}, \mathbf{y} \in F$  as

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|.$$

(a) What is the number of vectors in  $F$  of weight  $w$ ?

(b) What is the number of vectors in  $F$  whose weight is even?

3. Write out the parameters  $[n, k, d]$ , a generator and a parity-check matrix for the binary linear codes  $C_1 = \{0^n\}$  (one vector),  $C_2 = F$  (the entire space),  $C_3 = \{0^n, 1^n\}$  (the repetition code),  $C_4 = \{\text{all even-weight vectors}\}$  (the single parity-check code).

4. Let  $C$  be an  $[n, k, d]$  linear binary code.

(a) Let  $i$  be a coordinate of the code. Prove that either  $x_i = 0$  for every codeword of  $C$  or exactly half of the codewords have  $x_i = 0$  (and the other half have  $x_i = 1$ ).

(b) Consider the codewords of  $C$  that contain zero in the last coordinate (assume that their number is less than  $|C|$ ). Form a code  $C_1$  by taking these codewords and deleting this coordinate. What are the parameters of  $C_1$ ? Let  $H$  and  $G$  be a parity-check and a generator matrix of  $C$ , respectively. What is the parity check matrix of  $C_1$ . What is its generator matrix?

(c) Consider the code  $C_2$  obtained from  $C$  by taking every codeword and appending to it the sum of its coordinates. For instance if  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in C$  then the corresponding vector of  $C_2$  has the form  $(x_1, x_2, \dots, x_n, \sum_{i=1}^n x_i)$ . Determine the dimension, distance and the parity check matrix of  $C_2$ .

5. Let  $C$  be a binary linear code. Show that if  $\mathbf{x} \notin C^\perp$  then  $\sum_{\mathbf{y} \in C} (-1)^{x_1 y_1 + \dots + x_n y_n} = 0$ .

6. Let  $d(\cdot, \cdot)$  be the Hamming distance.

(a) Prove that it is a metric.

(b) Prove that the distance between two even-weight binary vectors is even. Thus the sum of two even-weight binary vectors has even weight.

Let  $d(C)$  be the minimum distance of a linear code  $C$ . Prove that  $d(C) = \min_{\mathbf{x} \in C \setminus \{0\}} \text{wt}(\mathbf{x})$ .

8. Let  $\mathbf{x}, \mathbf{y}$  be binary  $n$ -vectors. Let  $\mathbf{x} \star \mathbf{y} = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$  be a vector that has ones exactly in those positions where both  $\mathbf{x}$  and  $\mathbf{y}$  have ones. Prove that  $\text{wt}(\mathbf{x} + \mathbf{y}) = \text{wt}(\mathbf{x}) + \text{wt}(\mathbf{y}) - 2 \text{wt}(\mathbf{x} \star \mathbf{y})$ .

9. Consider the  $[6, 3]$  linear binary code  $C$  from lecture 1.

(a) What is the minimum distance of  $C$ ?

(b) Determine the cosets that contain (111111), (110010), and (100000) respectively and find for each of these the coset leader.

(c) Let  $y = (111111)$ . Find  $c \in C$  closest to  $y$  by the Hamming distance.

10. Let  $C$  be an  $[n, k, 5]$  linear code and let  $H$  be its parity check matrix. Is it true that  $H(1110\dots 0)^T = H(001110\dots 0)^T$ ?

11. Determine a parity check matrix for a linear binary code whose set of coset leaders is (000000), (100000), (010000), (001000), (000100), (000010), (000001), (110000).

12. Let  $C = H_4[15, 11, 3]$  be the Hamming code in a systematic form. Write out a generator matrix of  $C$ .

13. Prove that the code  $C = H_{3, \text{ext}}$  is self-dual.

14. Decode the vectors 10110101, 11010010, 10011100 with the code  $H_{3, \text{ext}}$ . Decode the vector 101?0111 where ? denotes the erased symbol.

15. Show that any binary linear  $[2^m - 1, 2^m - m - 1, 3]$  code can be obtained from the Hamming code  $H_m$  by a permutation of coordinates.

16. Let  $C$  and  $D$  be linear codes. (a) Show that  $(C^\perp)^\perp = C$ . (b) Let  $C + D = \{x + y : x \in C, y \in D\}$ . Show that  $(C + D)^\perp = C^\perp \cap D^\perp$ .

17. Let  $C$  be a binary  $[7, 4, 3]$  linear Hamming code. Consider the code  $D$  of length 14 whose codewords are all vectors of the form  $|x|x + y|$  where  $x \in C, y \in C^\perp$  and  $|a|b|$  means writing  $b$  next to  $a$ . Prove that the parameters of  $D$  are  $[14, 7, 4]$ .

18. Let  $\mathcal{H}_4$  be the binary linear Hamming code of length  $n = 15$ .

(a). Let  $C$  be a 1-shortening of the code  $\mathcal{H}_4$  What is the number of codewords of weight 3 in the code  $C$ ?

(b) Let  $C'$  be a puncturing of the code  $\mathcal{H}_4$  on one coordinate. What is the number of codewords of weight 3 in  $C'$ ?

(c) Let  $A$  be a 5-shortening of  $\mathcal{H}_4$ , i.e., the result of 5 successive shortenings. What are the parameters  $[n, k, d]$  of  $A$ ? Do they depend on the choice of the coordinates on which the code is shortened? Write out a generator matrix and a parity-check matrix of  $A$ . Do they depend on the choice of the coordinates?

19. Binomial coefficients. Below all the parameters are whole numbers. Prove that

- |   |  |
|---|--|
| (i) $\binom{n}{k} = \binom{n}{n-k}$ ;   | (viii) $\sum_{j=0}^{(r-1)/2} (-1)^j \binom{r}{j} (r-2j) = 0$ ( $r$ odd);   |
| (ii) $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$ ;                                 | (viii) $\sum_i (-1)^i \binom{p}{i} \binom{i}{s} = (-1)^p \delta_{p,s}$   |
| (iii) $(n-k) \binom{n}{k} = n \binom{n-1}{k}$ ;   | (ix) $\sum_k \binom{r}{m+k} \binom{s}{n-k} = \binom{r+s}{m+n}$ .   |
| (iv) $\sum_{k \text{ even}} \binom{n}{k} = \sum_{k \text{ odd}} \binom{n}{k} = 2^{n-1}$ ; | (x) $\sum_i i \binom{n}{i} = n 2^{n-1}$  |
| (v) $\sum_k (-1)^k \binom{n}{k} = 0$ ;  | (xi) $\sum_i i^2 \binom{n}{i} = \frac{n(n+1)}{4} 2^n$ .  |
| (vi) $\sum_{0 \leq k \leq n} \binom{k}{m} = \binom{n+1}{m+1}$ ;                           | (xii) $\sum_{i=0}^m (-1)^i \binom{n}{i} = (-1)^m \binom{n-1}{m}$ .   |
| (vii) $\binom{r}{j} \binom{j}{s} = \binom{r}{s} \binom{r-s}{j-s}$ ;                       | (xiii) $\sum_{m=k}^N \sum_{z=0}^{m-k} \binom{z+n-k-1}{n-k-1} \binom{N-z-n+k}{N-m-n+k} = \sum_{s=n}^N \binom{N}{s}$ |

(xiv) Let  $e = (e_1, e_1, \dots, e_r), e_i \geq 0$  be an  $r$ -tuple of integers such that  $\sum_{i=0}^r e_i \leq n$ . For  $i = 1, \dots, r$  evaluate in a closed form

$$\sum_e e_i \frac{n!}{e_1! \dots e_r! (n - \sum_i e_i)!} \prod_{j=1}^r ((q-1)q^{j-1})^{e_j}.$$

20. Covering radius of a code. Let  $C$  be a code. Define its covering radius as

$$\rho(C) = \max_{\mathbf{x} \in F_2^n} \min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}).$$

(a) Compute  $\rho(C)$  for the binary code  $C = \{\mathbf{x}, \mathbf{y}\}$  where  $d(\mathbf{x}, \mathbf{y}) = w$ .

(b) Let  $C$  be a linear code. Prove that  $\rho(C)$  is the weight of the coset of largest weight.

(c) Let  $C$  be a linear code. Prove that  $\rho(C)$  is the smallest number  $s$  such that every nonzero syndrome is a combination of  $s$  or fewer columns of  $H$ .

(d) What is the covering radius of the extended Hamming code  $H_{m,\text{ext}}$ ?

21. Consider a *ternary*  $[4,2]$  code  $C$  with a generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}.$$

Write out a standard array of  $C$ . (Generalize from the binary case; operations are now mod 3, so  $-1 = 2$ .)

22. A subset of  $k$  coordinates is called an information set of a linear code if the rank of the submatrix of  $G$  formed of the columns indexed by these coordinates equals  $k$ .

(a) Give an example of a 4-subset that forms an information set in  $H_3$  and an example of a 4-subset that does not.

(b) Given a vector  $\mathbf{y} = 0111010$  which equals a codeword  $\mathbf{c} \in H_3$  plus some error vector of weight 1 find an information set that does not contain errors; find  $\mathbf{c}$ .

23. Use the MacWilliams equation to compute the weight enumerator of the Hamming code  $H_m$  from the weight enumerator of its dual. Compute an explicit expression for the number  $A_w$  of codewords of weight  $w$  in  $H_m$ .

24. Find the weight enumerator of the extended Hamming code  $H_{m,\text{ext}}$  and of its dual code  $(H_{m,\text{ext}})^\perp = RM(1, m)$ .

25. (the codes are binary linear) Let  $C \subset C^\perp$  (such a code is called *self-orthogonal*, or *weakly self-dual*). Prove that every codeword of  $C$  has even weight. If every row of the generator matrix is of weight divisible by 4, then every codeword of  $C$  is of weight divisible by 4. Is the last claim true if  $C$  is not self orthogonal?

26. Let  $\mathbf{x} = (x_1, \dots, x_n)$  be a coset leader of an  $[n, k]$  linear code and let  $G$  be its generator matrix. Letting  $E = \{i \in \{1, \dots, n\} : x_i = 0\}$  prove that the rank  $\text{rk}(G(E)) = k$  (i.e., the set of columns of  $G$  with numbers in  $E$  contains  $k$  linearly independent columns).

27. Fourier transform. Let  $f(\mathbf{x}) : \{0, 1\}^n \rightarrow \mathbb{R}$  be a function. Define the Fourier transform of  $f$  by  $\hat{f}(\mathbf{y}) = \frac{1}{2^n} \sum_{\mathbf{x} \in \{0, 1\}^n} (-1)^{(\mathbf{x}, \mathbf{y})} f(\mathbf{x})$ .

(a) Let  $K_k(i) = \sum_{\ell=0}^i (-1)^\ell \binom{i}{\ell} \binom{n-i}{k-\ell}$ . Prove that  $K_k(i) = 2^n \hat{L}_k(\mathbf{y})$ , where  $L_k(\mathbf{x}) = 1$  if  $\text{wt}(\mathbf{x}) = k$  and 0 otherwise, and  $\mathbf{y}$  is a vector of weight  $i$ .

(b) Let  $\text{wt}(\mathbf{y}) = i$ . Compute directly  $\hat{L}_1(\mathbf{y}) = 2^{-n} K_1(i)$ .

(c) The convolution of the functions  $f$  and  $g$  is defined by  $(f * g)(\mathbf{y}) = \frac{1}{2^n} \sum_{\mathbf{x} \in \{0, 1\}^n} f(\mathbf{x})g(\mathbf{y} + \mathbf{x})$ . Prove that

$$(f * L_1)(\mathbf{x}) = \frac{1}{2^n} \sum_{\mathbf{y} \in \{0, 1\}^n : d(\mathbf{x}, \mathbf{y})=1} f(\mathbf{y}).$$

(d) Prove that if  $h = f * g$  then  $\hat{h} = \hat{f}\hat{g}$ .

(e) Parseval identity. Given two functions  $f$  and  $\phi$  prove that

$$\sum_{\mathbf{x} \in \{0, 1\}^n} f(\mathbf{x})\phi(\mathbf{x}) = 2^n \sum_{\mathbf{y} \in \{0, 1\}^n} \hat{f}(\mathbf{y})\hat{\phi}(\mathbf{y}).$$

**28.** Let  $C$  be a linear binary  $[n, k]$  code of size  $M = 2^k$ .

(a) Prove that  $\sum_{x \in C} \text{wt}(x) \leq n2^{k-1}$ .

(b) Prove that  $d(C) \leq \frac{nM}{2(M-1)}$ . This inequality is called the *Plotkin bound*.

**29.** Consider a ternary code  $\mathcal{G}_{12}$  generated by  $G = [I_6|A]$  where

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix}$$

Prove that  $\mathcal{G}_{12}$  is a  $[12, 6, 6]$  ternary self-dual code.

**30.** Two binary codes  $C_1$  and  $C_2$  are called equivalent if one can permute the coordinates of  $C_1$  to obtain the set of codewords of  $C_2$ . Two binary codes,  $C_1$  and  $C_2$ , will be called *different* if they are not equivalent. Prove or disprove: the weight distributions  $(A_0(C_1), A_1(C_1), \dots, A_n(C_1))$  and  $(A_0(C_2), A_1(C_2), \dots, A_n(C_2))$  of two different binary linear codes  $C_1$  and  $C_2$  are different.

**31.** Take as a given that the polynomial  $f(x) = x^4 + x^3 + x^2 + x + 1$  is irreducible over  $\mathbb{F}_2$ .

(a) Show that  $f$  is not primitive.

(b) Construct  $\mathbb{F}_{16}$  by adding a root  $\beta$  of  $f$  to  $\mathbb{F}_2$ . More concretely, in every row of the table of  $\mathbb{F}_{16}$  write the coefficients of the expansion of the corresponding element into the basis  $1, \beta, \beta^2, \beta^3$ .

(c) Show that  $\beta + 1$  is primitive and find its minimal polynomial over  $\mathbb{F}_2$ .

**32.** Construct  $\mathbb{F}_{16}$  as an extension of  $\mathbb{F}_4$ . Namely, do the following:

Let  $\alpha$  be the primitive element of  $\mathbb{F}_{16}$  that satisfies  $\alpha^4 = \alpha + 1$  (refer to the table of  $\mathbb{F}_{16}$  from the class notes).

(a) Let  $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ . Using this notation, write out the multiplication and addition tables in  $\mathbb{F}_4$ . Find  $i$  such that  $\omega = \alpha^i$ , find  $j$  such that  $\bar{\omega} = \alpha^j$ .

(b) Prove that  $f(x) = x^2 + \omega x + 1$  is irreducible over  $\mathbb{F}_4$ .

(c) Let  $\beta$  be a root of  $f(x)$ . What is the order of  $\beta$ ? Is  $\beta$  primitive?

(d) Let  $\beta = \alpha^i$ . What is  $i$ ?

(e) Prove that  $(\beta, 1)$  form a basis of  $\mathbb{F}_{16}$  over  $\mathbb{F}_4$ . Write out coefficients of the expansion of every element in  $\mathbb{F}_{16}$  in this basis (in other words, write a representation of every element of  $\mathbb{F}_{16}$  as a polynomial over  $\mathbb{F}_4$ ).

(f) Find all monic irreducible polynomials of degree  $\leq 2$  over  $\mathbb{F}_4$ . For every element of  $\mathbb{F}_{16}$  list its minimal polynomial over  $\mathbb{F}_4$ .

**33.** Cyclotomic cosets.

(a) Let  $q = p^m$  where  $p$  is a prime and let  $\alpha$  be a primitive element of  $\mathbb{F}_q$ . Prove that if for some cyclotomic coset  $C = \{s, sp, sp^2, \dots\}$ , its size  $|C| < m$ , then  $\alpha^s$  lies in a subfield of  $\mathbb{F}_q$ .

(b) Let  $p = 2, n = 2^m - 1, m \geq 3$ . Prove that the cyclotomic cosets containing 1 and 3 (i.e., containing  $\alpha$  and  $\alpha^3$ ) are disjoint. Prove that the size of each of these cosets is  $m$  (thus,  $\deg m_1(x) = \deg m_3(x) = m$ ).

**34.** (a) Determine the number of primitive elements of  $\mathbb{F}_{32}$ .

(b) Show that the polynomial  $f(x) = x^5 + x^2 + 1$  is irreducible over  $\mathbb{F}_2$ .

(c) Are there elements  $\gamma \in \mathbb{F}_{32}$  of order 15?

(d) Is  $\mathbb{F}_{16}$  a subfield of  $\mathbb{F}_{32}$ ?

Let  $\alpha$  be a zero of  $f(x)$ .

- (e) Compute  $\prod_{i=0}^4 (x - \alpha^i)$ .
- (f) Compute the logarithm of  $\alpha^4 + \alpha^3 + \alpha$ .
- (g) Let  $\gamma \in \mathbb{F}_{32} \setminus \mathbb{F}_2$ . Show that  $\gamma$  is not a root of a polynomial of degree less than 5.
- (h) Show that  $1, \gamma, \gamma^2, \gamma^3, \gamma^4$  is a basis for  $\mathbb{F}_{32}$  as a linear space over  $\mathbb{F}_2$ .
- (i) What are the coordinates of  $\alpha^8$  with respect to the basis  $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ ?

35. For an element  $a \in \mathbb{F}_{p^m}$  define its trace as

$$Tr(a) = \sum_{j=0}^{m-1} a^{p^j}.$$

- (a) Prove that  $Tr(a) \in \mathbb{F}_p$  for any  $a \in \mathbb{F}_{p^m}$ .
- (b) Prove that  $Tr(a + b) = Tr(a) + Tr(b)$ .
- (c) Prove that  $Tr(\beta)$  takes every value in  $\mathbb{F}_p$  equally often.
- (d) Prove that  $Tr(\beta^p) = Tr(\beta)^p = Tr(\beta)$ .
- (e) Let  $g(x) = x^r + a_{r-1}x^{r-1} + \dots$  be the minimal polynomial of  $\beta \in \mathbb{F}_{p^m}$ . Prove that  $Tr(\beta) = -ma_{r-1}/r$ .

36. Factorize  $x^{73} + 1$  over  $F_2$ .

37. Factorize  $x^{10} + 1$  into irreducible polynomials over  $\mathbb{F}_2$ .

38. Let  $m$  be odd and let  $C$  be an  $[n = 2^m - 1, n - 2m, d]$  cyclic code with zeros  $\alpha, \alpha^{-1}$  (the *Melias code*). Show that  $d \geq 5$  (for instance, use the Hartmann-Tzeng bound).

39. (a) Let  $C$  be a cyclic code and let  $C^\perp$  be its dual. Prove that the zeros of  $C^\perp$  are inverses of the nonzeros of  $C$ .

(b) Prove that if the generator polynomial  $g(x)$  of a cyclic code  $C$  satisfies  $g(1) = 0$ , then all the codewords of  $C$  have even weight.

40. The polynomial  $x^{15} + 1$  factors over  $F_2$  as follows:

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

Let  $C$  be a  $[15, k, d]$  binary cyclic code of length 15 generated by  $g = (x + 1)(x^4 + x + 1)$ .

- (a) What are  $k$  and  $d$  (the designed distance). What about the true distance?
- (b) Is  $x^{14} + x^{12} + x^8 + x^4 + x + 1$  a codeword in  $C$ ?
- (c) List all  $[n = 15, k = 8]$  binary cyclic codes and their dual codes. For each code write its generator polynomial and check polynomial.
- (d) What is the total number of binary cyclic codes of length 15?

41. Let  $\beta$  be the root of  $f(x) = x^4 + x^3 + x^2 + x + 1$ . Show that  $\beta + 1$  is a primitive element of  $\mathbb{F}_{16}$  and find its minimal polynomial.

42. Let  $m \geq 4$  be even and let  $C$  be an  $[n = 2^m + 1, k, d]$  binary cyclic code whose zero is  $\omega$  (the  $n$ th degree primitive root of unity). Determine  $k$  and prove (using the Hartmann-Tzeng bound or otherwise) that  $d \geq 5$ .  $C$  is called the *Zetterberg code*.

43. Let  $C$  be a ternary  $[80, k, d \geq \delta]$  BCH code, where  $\delta$  is the BCH designed distance. Find  $k$  for  $\delta = 4, 7, 11$ .

44. Let  $C$  be a  $[15, k, d]$  16-ary RS code with zeros  $\alpha, \alpha^2, \dots, \alpha^6$ .

(a) What are  $k$  and  $d$ ?

(b) Write out the generator polynomial  $g(x)$ ?

(c) Find a codeword of weight 10 in  $C$ .

(d) Given a vector  $y = (\alpha^8, \alpha^{10}, 1, \alpha^8, \alpha^{10}, \alpha^3, \alpha^{12}, \alpha^6, \alpha^{10}, 1, 0, \alpha^4, 0, \alpha^7, 0)$ , perform the calculations of the Gorenstein-Peterson-Zierler algorithm to decode it. Use Forney's algorithm to determine the values of the errors.

(e) Let  $c$  be the decoding result. Suppose that  $y$  was received from the channel that transmits a 16-ary symbol correctly with probability  $1 - p$  and changes it to another symbol with probability  $p/15$ , where  $p = 0.01$ . What is the probability of transmitting  $c$  and receiving  $y$ ?

45. Let  $C$  be a ternary primitive BCH code of length 26 with zeros  $\alpha, \alpha^2, \alpha^4, \alpha^5$ .

(a) Determine the parameters and the generator polynomial of  $C$ .

(b)<sup>§</sup> Decode the vector  $y = (00000001200202020110002120)$ , i.e., find the vector  $c \in C$  closest to  $y$  by the Hamming distance (if you use a computer algebra system, show all the steps of the algorithm).

46. Let  $C$  be an  $[n = 15, k = 12, d]$  primitive Reed-Solomon code over  $\mathbb{F}_{16}$ . Construct 2 codewords of weight  $d$  which are not proportional to each other and are not cyclic shifts of each other.

47. Let  $C[n, k, d = n - k + 1]$  be a Reed-Solomon code. Prove that the covering radius  $\rho(C) \geq d - 1$ .

48. Let  $C$  be a  $[15, k, d]$  RS code over  $\mathbb{F}_{16}$  with zeros  $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ , where  $\alpha$  is a root of  $x^4 + x + 1$ .

(a) What are  $k$  and  $d$ ?

(b) Find the generator polynomial of  $C$ .

(c) Suppose that the vector received from the channel is  $(000\alpha^7 00\alpha^3 00000\alpha^4 00)$ . Compute the syndromes. What is the decoding result?

49<sup>§</sup>. Let  $C$  be an  $[n = 63, 53, 11]$  RS code over  $F_{64}$

The weight distribution of an RS code is found as  $A_0 = 1, A_1 = \dots = A_{10} = 0$ , and for  $w \geq 11$ ,

$$A_w = \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} (q^{w-d+1-j} - 1), \quad w \geq 11.$$

Suppose that the code is used over a  $q$ -ary symmetric channel with the parameter  $p$  and decoded to correct  $t$  errors.

(a) Suppose that  $t = 5$ . Compute the probability  $P_e$  of miscorrection and the probability  $P_x + P_e$  of failure or miscorrection for  $p = 10^{-i}, i = 2, 3, \dots, 6$ . Attach a table. Attach a plot for  $1 \leq i \leq 6$ .

(b) Compute the probabilities in (a) for  $t = 3, 4$ . Show the results for  $P_e$  in the same plot for  $t = 3, 4, 5$ . In another plot, show the results for  $P_x$  for  $t = 3, 4, 5$ . What happens to the probability  $P_e$  as  $t$  decreases and why? The same question for  $P_x$ .

(c) Suppose that  $t = 0$ , i.e., the code is used for pure error detection. Compute the probability of correct decoding  $P_c$  for  $p = 10^{-i}, i = 2, 3, \dots, 6$  (attach a table).

(d) In the same situation as in (c), write our a general expression for the probability of miscorrection  $P_e$  (in this case also called a probability of undetected error and denoted  $P_{ue}$ ) for an  $[n, k, d]$  linear  $q$ -ary code with weight enumerator  $A(x, y)$ .

(e) For the RS code in question compute  $P_{ue}$  for  $p = 63/64$ . Compare this number with  $64^{k-n} = 64^{-10}$ . Explain the result of the comparison.

(f) Compute exactly the fraction of the space  $(\mathbb{F}_{64})^{63}$  occupied by spheres of radius 5 about the codewords of  $C$ . Based on the outcome make an educated guess if max-likelihood decoding of the code  $C$  will have a much better performance than decoding up to 5 errors, and explain your answer.

**50<sup>§</sup>.** Let  $C$  be the binary Hamming code of length 31 used on a binary symmetric channel with the parameter  $p$ , denoted by  $\text{BSC}(p)$ .

(a) Let  $p = 0.004$ . Compute the probability of miscorrection  $P_e$  for bounded distance decoding that corrects one error. Compute the error probability  $P_{ml}$  of max-likelihood decoding of  $C$ . If your answers are different, you owe me a serious explanation.

(b) Estimate the *bit error rate*  $p_b$  for  $p = 10^{-i}$ ,  $i = 2, 3, \dots, 6$ : write out a formula that you used and attach a table of the results. Plot  $\log p_b$  vs  $\log p$ .

**51.** Let  $C$  be a binary  $[16, 8, 6]$  code with weight enumerator  $A(x) = 1 + 112x^6 + 30x^8 + 112x^{10} + x^{16}$ .

Suppose that  $C$  is used on a  $\text{BSC}(p)$ .

(a) How many errors can  $C$  correct?

(b) What is the probability of decoding failure for  $p = 0.005$  if the code is used to correct 2 errors?

(c) Compute the number of error patterns of weight 4 and 6 that have distance 2 to a given codeword of weight 6.

**52.** A  $[32, 16, 8]$  binary code  $C$  has weight enumerator

$$A(x) = 1 + 620x^8 + 13888x^{12} + 36518x^{16} + 13888x^{20} + 620x^{24} + x^{32}.$$

(a) What is the number  $t$  of errors that the code can correct?

Suppose the code  $C$  is used on a  $\text{BSC}(p)$ .

(b<sup>§</sup>) Compute the error probability  $P_e(t)$  of bounded distance decoding correcting up to  $t$  errors for  $p = 10^{-i}$ ,  $i = 2, 3, 4, 5, 6, 7$ . Give a table.

(c<sup>§</sup>) For the same values of  $p$  as in (b), estimate the probability  $\overline{P_e}(t)$  by assuming that error patterns of weight  $\geq 8$  always lead to a decoding error. Give a table of the results in (b) and (c). Next time you compute the error probability of bounded distance decoding, will you need the entire weight enumerator?

(d<sup>§</sup>) Using the Poltyrev bound, estimate the error probability  $P_{e,ml}$  of maximum likelihood decoding for the code  $C$ . What is the optimizing value of the cutoff radius that you found (is it the same for different  $p$ )? Plot the results of (b) and (d) in the same plot for  $p = 10^{-i}$ ,  $2 \leq i \leq 7$ .

**53.** Suppose that  $\mathbf{0}$  is transmitted over a binary symmetric channel with crossover probability  $p$ . What is the probability that the received vector will be at most distance 1 away from a given vector  $\mathbf{c}$  of weight  $w$ ?

**54.** Let  $\Phi = \{C\}$  be a family of  $q$ -ary  $[n, k]$  linear codes such that every vector  $x \in \mathbb{F}_q^n$  is contained in the same number of codes from the family.

(a) Prove that if

$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i < \frac{q^n - 1}{q^k - 1},$$

then  $\Phi$  contains a code with distance  $d$ .

(b) Let  $q = 2$ . Conclude that for  $n \rightarrow \infty$ ,  $\Phi$  contains codes that meet the asymptotic GV bound.

**55.** Does there exist a  $[38, 9, 19]$  binary linear code?

**56.** The Johnson space  $J^{n,w}$  is the subset of the binary Hamming space  $\mathbb{F}_2^n$  formed of all the vectors of constant weight  $w$ .

(a) What is the volume of a ball of radius  $2r$  in  $J^{n,w}$ ?

(b) Formulate the Gilbert bound on codes for  $J^{n,w}$ .

(c) What is the asymptotic form of the bound that you found in (a)? In other words, express the code rate  $R$  as a function of the relative distance  $\delta$ .

**57.** Prove that  $RM(0, m)$  and  $RM(0, m)^*$  are repetition codes,  $RM(m-1, m)$  contains all vectors of even weight,  $RM(m, m) = (\mathbb{F}_2)^{2^m}$ ,  $RM(m, m)^* = (\mathbb{F}_2)^{2^m-1}$ . Prove directly that the dual of  $RM(1, m)$  is the extended Hamming code  $\mathcal{H}_{m, \text{ext}}$ .

**58.** Write out a parity-check matrix of the Reed-Muller code  $RM(2, 5)$ . Which submatrix of this matrix generates  $RM(1, 5)$ ?

**59.** Consider an  $n = 2, k = 1$  convolutional code with memory  $m = 3$  and polynomial generator matrix  $\mathbf{G}(x) = (1 + x^2, 1 + x + x^2 + x^3)$ .

(a) Is this code catastrophic?

(b) Draw the diagram of the encoder as a feedforward register; draw the first 5 steps of the trellis diagram of the code; label the branches.

**60.** Let  $A_w$  be the number of codewords in a random code from the ensemble of linear binary codes defined in class. Compute  $\mathbf{E}[A_w]$ ,  $\text{Var}(A_w)$ . Prove that  $\text{Var}(A_w) < \mathbf{E}[A_w]$ .

**61.** Construct a binary  $(n, M, d) = (5, 4, 3)$  code. Prove that there is no  $(5, 5, 3)$  code.

**62.** Find the coset leaders for a binary linear  $[n, n-1, 2]$  code.

**63.** We are given an  $[n, k, d]$  binary linear code with no all-zero coordinates.

(a) Prove that one can construct an  $[n+1, k, d]$  code with no all-zero coordinates.

(b) Let  $k \geq 1$  and  $n > d \geq 2$ . Prove that one can construct codes with the parameters

$$[n-1, k-1, d], \quad [n-1, k, d-1], \quad [n, k-1, d], \quad [n, k, d-1].$$

**64.** Let  $\mathbf{G}, \mathbf{H}$  be a generator and a parity-check matrix of a linear binary  $[n, k]$  code. For a given subset  $E \subset \{1, 2, \dots, n\}$  let  $E^c$  be its complement. For any  $E \subset \{1, 2, \dots, n\}$  prove that

$$k - \text{rk}(\mathbf{G}(E)) = |E^c| - \text{rk}(\mathbf{H}(E^c)).$$

**65.** (*Companion matrix representation of finite fields*). Let  $F$  be a finite field and let  $a(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in F[x]$ . Consider the companion matrix of  $a(x)$  defined as

$$C_a = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

(a) Prove that  $a(x) = \det(xI - C_a)$ . Deduce that  $a(C_a) = 0$ .

(b) Let  $u(x) = \sum_{i=0}^{n-1} u_i x^i$  and  $v(x) = \sum_{i=0}^{n-1} v_i x^i$ . Show that  $v(x) = xu(x) \pmod{a(x)}$  if and only if

$$\mathbf{v}^T = C_a \mathbf{u}^T,$$

where  $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$  and  $\mathbf{u} = (u_0, u_1, \dots, u_{n-1})$ .

(c) Let  $a(x)$  be irreducible. Prove that the set of matrices  $\{b(C_a), b(x) \in F, 0 \leq \deg(b(x)) \leq n-1\}$  forms a field (which is thus isomorphic to the  $n$ th degree extension of  $F$ ).

**66.** (*Quadratic residues*.) An element  $a \in \mathbb{F}_q$  is called a quadratic residue in  $\mathbb{F}_q$  if there exists an element  $x \in \mathbb{F}_q$  such that  $a = x^2$  and is called nonresidue otherwise.

Let  $q$  be odd, let  $R(N)$  be the set of quadratic residues (nonresidues) respectively.

(a) Prove that there are exactly  $(q-1)/2$  quadratic residues in  $F$ .

(b) Prove that  $\prod_{a \in R} (x - a) = x^{(q-1)/2} - 1$  and  $\prod_{a \in N} (x - a) = x^{(q-1)/2} + 1$ .

(c) Prove that  $-1 \in R$  if and only if  $q \equiv 1 \pmod{4}$ .

(d) Let  $q \neq 2$  be prime. Define the *Legendre symbol* as a function  $\chi : \mathbb{F}_q \rightarrow \{-1, 0, 1\}$  such that  $\chi(a) = 1$  if  $a \in R$ ,  $\chi(0) = 0$ , and  $\chi(a) = -1$  if  $a \in N$ . Prove that

$$\chi(ab) = \chi(a)\chi(b), \quad \chi(a) = a^{(q-1)/2}$$

$$\sum_{b \in \mathbb{F}_p} \chi(b)\chi(b+c) = -1 \quad (c \neq 0).$$

**67. (Product codes).** Let  $C_1[n_1, k_1, d_1]$  and  $C_2[n_2, k_2, d_2]$  be  $q$ -ary linear codes. Consider the code  $C = C_1 \otimes C_2$  of length  $n_1 n_2$  formed of matrices in which each row is a codeword in  $C_2$  and each column is a codeword in  $C_1$ .

(a) Let  $U$  be a  $k_1 \times k_2$  matrix of message symbols that corresponds to a codeword in  $C$ . Prove that  $C$  can be encoded by first encoding the rows of  $U$  with  $C_2$  and then encoding the columns of the obtained  $k_1 \times n_2$  matrix with  $C_1$ . Prove moreover that  $C$  can be encoded by first encoding the columns of  $U$  with  $C_1$  and then the rows of the obtained  $n_1 \times k_2$  matrix with  $C_2$ .

(b) Prove that the parameters of  $C$  are  $[n_1 n_2, k_1 k_2, d_1 d_2]$ .

(c) Write out a parity-check matrix of  $C$ .

(d) Give a decoding algorithm of  $C$  that corrects  $1/4(d_1 d_2 - 1)$  errors.

(e) Give a decoding algorithm of  $C$  of complexity at most  $O(\exp(n_1 + n_2))$  that corrects  $1/2(d_1 d_2 - 1)$  errors. Hint: To decode a row  $y_{i,1}, \dots, y_{i,n_2}$  with  $C_2$ , compute the total cost, in terms of the distance of columns to codewords of  $C_1$ , of using 0 and 1 in each of the coordinates  $(i, j), j = 1, \dots, n_2$ . This is called a *min-sum algorithm*.

(f) Take a complete bipartite graph  $G$  with  $n_2$  vertices in one part, call it  $V_1$ , and  $n_1$  vertices in the other part, denoted  $V_2$ , and all the possible edges between the parts. Consider the set of vectors  $C \subset \{0, 1\}^n$  with coordinates indexed by the edges of  $G$  such that all the edges incident to a vertex in  $V_1$  form a codeword in  $C_1$  and all the edges incident to a vertex in  $V_2$  form a codeword in  $C_2$ .

(i) Prove that  $C$  is a linear code.

(ii) How is the code  $C$  related to the product code above?

(iii) Compute directly the parameters of  $C$ .

(iv) Describe the processing of the decoding algorithms in parts (d) and (e) in terms of the graph.

(g) Replace the complete graph in part (e) with a  $\Delta$ -regular graph, i.e., a graph in which every vertex has degree  $\Delta$ . Replace the codes  $C_1$  and  $C_2$  with codes  $D_1[\Delta, k_1]$  and  $D_2[\Delta, k_2]$ . What are the parameters of the code obtained? Write out its parity-check matrix.

(h) In part (g) let  $C_1$  be a  $[\Delta, \Delta - 1]$  binary single parity check code and  $C_2$  a  $[\Delta, 1]$  repetition code. Write out a parity-check matrix of the code  $C$  thus obtained.

**68. (from an exam)** We are studying a  $[10, 6]$  RS code  $C$  over  $\mathbb{F}_{11}$ .

(a) Prove that  $\alpha = 2$  is a primitive element of  $F = \mathbb{F}_{11}$ . Is it true that all the elements  $\{2, \dots, 10\}$  are primitive mod 11?

(b). Write out a parity-check  $H$  matrix of  $C$ . How many codewords does  $C$  contain?

(c) Reduce  $H$  to a systematic form  $H' = [I_4 | A]$ . Hint:  $\begin{bmatrix} 1 & 2 & 4 & 8 \\ 1 & 4 & 5 & 9 \\ 1 & 8 & 9 & 6 \\ 1 & 5 & 3 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} 2 & 1 & 8 & 1 \\ 6 & 0 & 10 & 6 \\ 2 & 5 & 0 & 4 \\ 7 & 7 & 2 & 6 \end{bmatrix} \pmod{11}$ .

In which coordinates are the message symbols located?

Then reduce  $H$  to a systematic form  $H''$  in which the message symbols are located in coordinates 1, 2, 4, 6, 8, 10.

$$\text{Hint: } \begin{bmatrix} 4 & 5 & 9 & 3 \\ 5 & 3 & 4 & 9 \\ 9 & 4 & 3 & 5 \\ 3 & 9 & 5 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} 7 & 6 & 3 & 5 \\ 6 & 5 & 7 & 3 \\ 3 & 7 & 5 & 6 \\ 5 & 3 & 6 & 7 \end{bmatrix} \pmod{11}.$$

(d). Using  $H'$ , write out a generator matrix  $G$  of  $C$  in a systematic form.

(e). Using  $H'$ , find the codeword  $c_0$  that corresponds to the message symbols  $(1, 1, 1, 1, 1, 1)$ . Then find the codeword that corresponds to these message symbols using  $G$  for encoding. Are the codewords the same? Explain the outcome.

(f). What is the polynomial  $f$  such that  $\text{eval}(f) = c_0$ ?

(g). Is it true that  $(c_0, c_1, \dots, c_9) \in C$  implies that  $(c_9, c_0, c_1, \dots, c_8) \in C$ ?

(h). Let  $c \in C$  be a vector of weight 5. Prove that if  $c' \in C$  is such that  $\text{supp}(c) = \text{supp}(c')$  then  $c' = ac$  where  $a \in F \setminus \{0\}$  is some constant.

(i). Using problem (h), compute directly, with proof, the number of vectors of weight 5 in  $C$  (your answer should be a number, not an expression).

(j). Let  $r = (3, 0, 0, 10, 5, 4, 0, 6, 10, 0)$  be a received vector. Perform the Peterson-Gorenstein Zierler algorithm to determine the number of errors and to decode the vector.

(k). Use the codeword found in part (j) to find the polynomial  $f$  such that  $\text{eval}(f)$  equals to this codeword.

**69.** (from an exam) Consider a ternary linear code  $C$  with the generator matrix

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 2 & 0 \\ 1 & 0 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

(a) Find a parity-check matrix of  $C$ .

(b) What are the parameters  $[n, k, d]$  of the code  $C$ ?

(c) How many cosets does  $C$  have? Name 10 coset leaders.

**70.** (from an exam) Let  $f(x) = x^4 + x^3 + 1$  and let  $\alpha$  be a root of  $f$ .

(a) Is  $f$  a primitive polynomial?

(b) Let  $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$  be the field of 4 elements. Is it a subfield of  $\mathbb{F}_{16}$ ? Write out the addition table of  $\mathbb{F}_4$ .

Given a basis  $(a, b)$  of  $\mathbb{F}_{16}$  over  $\mathbb{F}_4$ , each element of  $\mathbb{F}_{16}$  can be expressed uniquely as  $\mu a + \nu b$ , where  $\mu, \nu \in \mathbb{F}_4$ .

(c) Is  $(1, \omega)$  a basis of  $\mathbb{F}_{16}$  over  $\mathbb{F}_4$ ?

(d) Let  $g(x) = x^2 + \omega x + 1$ . Is it irreducible over  $\mathbb{F}_4$ ?

(e) Let  $\beta$  be a root of  $g(x)$ . Find the order of  $\beta$ . Is it primitive?

(f) Express  $\beta$  as a power of  $\alpha$ .

(g) Find the representation of  $\alpha^7$  in the basis  $(1, \beta)$  over  $\mathbb{F}_4$ .

(h) Find the cyclotomic coset mod 4 that contains  $\alpha^7$ . Find the minimal polynomial of  $\alpha^7$  over  $\mathbb{F}_4$ .

**71.** Let  $C$  be a linear  $[n, Rn]$  binary code whose weight distribution satisfies  $A_w \leq n \binom{n}{w} 2^{(R-1)n}$ ,  $w = 1, \dots, n$ . Derive the error probability of max-likelihood decoding of  $C$  on a BSP( $p$ ) using the Bhattacharyya bound. Does the result show that the code achieves capacity?

**72.** Find an RS code and a received vector  $r$  for which the calculations of a list-decoding algorithm (Sudan's or GS) give more than one solution; show the decoding steps of  $r$ . Hint: Such vectors  $r$  are found around the midpoint of the distance between two codewords.

**73.** Consider a binary linear code  $C$  with the generator matrix