Error-Correcting Codes: Problems

Alfred Menezes

---

1. **Distance of a code**
   Let C be a $[n, 3]$-binary code with distance d. Prove that $d \leq 2n/3$.

2. **Telephone numbers #1**
   Let C be an $[n, M]$-code with distance d over an alphabet A of size q. Let $e = \lfloor \frac{d-1}{2} \rfloor$. Recall that the sphere packing bound is $M \sum_{i=0}^{e} \binom{n}{i}(q-1)^i \leq q^n$.

   (a) Suppose that there are 110 million telephones in a country. Is it possible to assign 10-digit decimal numbers to these telephones so that a single error in dialing can always be (automatically) corrected? (Explain)

   (b) Suppose that there are 80 million telephones in a country. Is it possible to assign 10-digit decimal numbers to these telephones so that a single error in dialing can always be (automatically) corrected? (Explain)

3. **Existence of block codes**
   Let $q \geq 2$, and let n and d be positive integers with $d \leq n$. Define $T_q(n, d)$ to be the largest integer M such that there exists an $[n, M, d]$-code over an alphabet A of size q. Prove the following statements:

   (a) $T_q(n, d) \leq T_q(n-1, d-1)$.

   (b) If d is even, then $T_2(n, d) = T_2(n-1, d-1)$.

   (c) $T_2(n, 2) = 2^{n-1}$.

   (d) $T_2(8, 6) = 2$.

   (e) $T_2(9, 6) = 4$.

4. **q-ary symmetric channels**
   Recall the definition of a q-ary symmetric channel with symbol error probability p ($0 \leq p \leq 1$):

   - Let $A = \{a_1, a_2, \ldots, a_q\}$.
   - Let X_i be the i^{th} symbol transmitted ($i = 1, 2, \ldots$).
   - Let Y_i be the i^{th} symbol received ($i = 1, 2, \ldots$).
   - Then, for all $i \geq 1$ and $1 \leq j, k \leq q$,

$$Pr(Y_i = a_k | X_i = a_j) = \begin{cases} \frac{p}{q-1} & \text{if } j \neq k \\ 1-p & \text{if } j = k. \end{cases}$$

   (a) Show that if $p = \frac{q-1}{q}$, then a q-ary symmetric channel with symbol error probability p is "useless".

   (b) Show that if $\frac{q-1}{q} < p \leq 1$, then a q-ary symmetric channel with symbol error probability p can be converted to one with symbol error probability p', where $0 \leq p' < \frac{q-1}{q}$. (This justifies the assumption that we can, without loss of generality, assume that $0 \leq p < \frac{q-1}{q}$ for any q-ary symmetric channel.)

5. **Erasures**
Let C be an $[n, M]$-binary code of distance d. Suppose that the communications channel has the property that a transmitted symbol is either received correctly, or as a symbol * that is distinct from 0 and 1. A symbol that is received as * is said to be *erased*. For example, c =1011100 is transmitted and r =1*11**0 is received; note that the positions of the errors is known.

   (a) Suppose now that $c \in C$ is transmitted, and during transmission at most $d-1$ symbols are erased. Show that it is possible to determine c from the received word.

   (b) Suppose now that $c \in C$ is transmitted, and during transmission d symbols are erased. Is it always possible to determine c from the received word?

6. **Finite field computations #1**

   (a) Verify that the polynomial $f(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_{11}$.

   (b) Perform the following computation in $F = \mathbb{Z}_{11}[x]/(f)$ by hand: $(5x^2 + 8x + 6) \ + \ (6x^2 + 6)$.

   (c) Perform the following computation in $F = \mathbb{Z}_{11}[x]/(f)$ by hand: $(5x^2 + 8x + 6) \ \cdot \ (6x^2 + 6)$.

7. **Finite field computations #2**
The polynomial $f(x) = x^5 + 4x + 2$ is irreducible over $\mathbb{Z}_5$.

   (a) What is the order of the field $F = \mathbb{Z}_5[x]/(f(x))$?

   (b) Describe, in words, the elements of the field F.

   (c) What is the characteristic of the field F?

   (d) Perform the following computations in F by hand:

      i. $(4x^4 + 3x^2 + x + 3) \ + \ (3x^4 + 4x^3 + 2x^2 + 1)$.

      ii. $(4x^4 + 3x^2 + x + 3) \ \cdot \ (3x^4 + 4x^3 + 2x^2 + 1)$.

      iii. $(x + 4)^{125} \cdot (4x^3 + 2x^2 + x + 4)^{6249}$.

8. **Irreducibility of polynomials #1**

   (a) Recall the *division algorithm for polynomials:* Let F be a field and let $f, g \in F[x]$, with $g \neq 0$. Then long division of f by g yields unique polynomials $\ell, r \in F[x]$ such that

$$f = \ell g + r, \text{ where } \deg(r) < \deg(g).$$

   Prove the *Factor Theorem*: The linear polynomial $x - a \in F[x]$ is a factor of $f \in F[x]$ if and only if $f(a) = 0$.

   (b) Prove that $f(x) = x^3 + 4x + 3$ is irreducible over $\mathbb{Z}_5$.

   (c) Prove that $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$.

9. **Irreducibility of polynomials #2**
Determine the irreducibility of the following polynomials.
(You should do this question by hand, without the aid of a computer.)

   (a) $x^7 + 5x^6 + x^3 + 5x + 3$ over $\mathbb{Z}_7$.

   (b) $x^7 + 5x^6 + x^3 + 5x + 3$ over $\mathbb{Z}_2$.

   (c) $x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$ over $\mathbb{Z}_2$.

10. **Orders of field elements**
Let $f(x) = x^3 + 2x + 2 \in \mathbb{Z}_3[x]$, and let $GF(3^3) = \mathbb{Z}_3[x]/(x^3 + 2x + 2)$.

    (a) Prove that $f(x)$ is irreducible over $\mathbb{Z}_3$.

    (b) The element x has order 13 in $GF(3^3)$. Find a generator of $GF(3^3)^*$.

11. **Generators #1**
Let q be an odd prime power.

    (a) Prove that if α is a generator of $GF(q)^*$ then $\alpha^{(q-1)/2} = -1$.

    (b) Show that the converse of the statement in (a) is not always true.

12. **Generators #2**
Find a generator of $GF(2^4) = \mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$.

13. **Generators #3**
Let m be a positive integer such that $(3^m - 1)/2$ is prime. Let $f(x)$ be a monic irreducible polynomial of degree m in $\mathbb{Z}_3[x]$, and let $F = \mathbb{Z}_3[x]/(f(x))$.

    (a) Prove that either x or $-x$ is a generator of F, but not both.

    (b) Let $f(x) = x^3 + 2x + 1$. Given that x is a generator of F, find the order of $-x$.

14. **Finite fields**
Let q be a prime power. Prove that $\sum_{\alpha \in GF(q)} \alpha^d = 0$ for all $1 \leq d \leq q - 2$.
Hint: Let γ be a generator of $GF(q)^*$ and write $\alpha = \gamma^j$ where $0 \leq j \leq q - 2$.

15. **Linear codes #1**
Consider the following parity-check matrix H for a linear (n, k)-code C over $\mathbb{Z}_3$:

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

    (a) Determine the length n, the dimension k, and the number of codewords M of C.

    (b) Find a generator matrix G for C.

    (c) Find a generator matrix for the code $C^\perp$.

    (d) Determine the length, dimension, and number of codewords of $C^\perp$.

    (e) Determine the distance d of C.

    (f) Determine the distance $d^\perp$ of $C^\perp$.

16. **Linear codes #2**
Let C be a binary linear code with generator matrix:

$$G = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right].$$

(a) What is the length n of C?

(b) What is the dimension k of C?

(c) How many codewords does C have?

(d) Prove that G is also a parity-check matrix for C.

(e) Prove that $C = C^{\perp}$.

(f) Determine the distance d of C.

(g) Correct (if possible) the received vector $r = (11100011)$.

17. **Linear codes #3**
Let $H = [I_5\ B]$ be the parity-check matrix for a binary linear code C, where

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

(a) Prove that all the codewords in C have even weight.

(b) Determine the distance d of C.

(c) Assuming the first 5 components of a codeword are the check symbols and the last 6 the information symbols, determine the codeword which contains the information symbols 110011.

(d) Assuming that at most one error occurs in transmission, list the 6 information bits corresponding to each of the following received words: (i) $v_1 = (11100\ 101000)$. (ii) $v_2 = (11011\ 110000)$.

(e) If $v = (01110\ 001111)$ is received at the decoder, what can we conclude? Explain.

18. **Two-dimensional parity code**
Suppose that source messages are binary strings of length st. A source message is mapped to a codeword as follows. Arrange message bits in an $s \times t$ array. Append parity bits at the end of each row, then at the end of each column, so the resulting codeword has $(s+1)(t+1)$ bits. Let C be the set of all such codewords.

(a) Prove that C is a linear code.

(b) Determine the distance of C.

(c) Determine the error-detecting capability of C.

(d) Determine the error-correcting capability of C.

19. **Even-weights and odd-weights**

(a) Let $x, y \in V_n(\mathbb{Z}_2)$. Prove that if both x and y have even weight, then so does $x + y$.

(b) Let H be a parity-check matrix for an (n, k)-binary code C with $n \geq 4$. Suppose that the columns of H are distinct and have odd weight. Prove that C has distance $d \geq 4$.

20. **Telephone numbers #2**
Let C be a linear code over $\mathbb{Z}_{11}$ with parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{bmatrix}$$

(a) Show that C is a $(10, 8)$-code with distance 3.

(b) Find a generator matrix for C.

Let D be the code over $\mathbb{Z}_{11}$ obtained from C by deleting all codewords that have a 10 in any position. (Note that D is a code over $\mathbb{Z}_{11}$ even though none of the codewords in D have a 10 in any position.)

(c) Show that D is not a linear code.

(d) Show that D has distance 3.

[Aside: It can be proven that the code D has size 82,644,629, and hence D can be used to assign telephone numbers as described in problem 2(b). The codewords in D are the telephone numbers.]

(e) Design a simple and efficient single error-correcting algorithm for D.

(f) Use your algorithm to decode $r = (6, 5, 2, 0, 8, 3, 0, 5, 6, 9)$.

(g) Use your algorithm to decode $r = (0, 3, 3, 0, 10, 4, 0, 6, 9, 9)$.

(h) Use your algorithm to decode $r = (9, 2, 3, 0, 2, 6, 0, 6, 9, 9)$.

21. **Linear code over $GF(4)$**
Let $GF(4) = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$. Consider the linear code C over $GF(4)$ with generator matrix

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

(a) Determine the length n and dimension k of C.

(b) How many codewords does C have?

(c) Find a PCM H for C.

(d) Determine the distance d of C, given that $d \neq 3$.

22. **Distance of the dual code**
Let C be an (n, k)-code over $GF(q)$ with distance $d = n - k + 1$. Prove that $C^\perp$ has distance $k + 1$.

23. **Binary Hamming codes**
Let C be a binary Hamming code of order r, and let $c \in C$. Prove that $\overline{c} \in C$ (where $\overline{c}$ denotes the bitwise complement of c).

24. **Dual of a binary Hamming code**
Let C be a binary Hamming code of order r. Show that $C^\perp$ has length $n = 2^r - 1$, dimension $k = r$, and distance $d = 2^{r-1}$.

25. **Linear codes**
Let C be a $(q + 1, 2)$-code over $GF(q)$ with distance q.

(a) Let $\alpha \in GF(q)$, and let $i, j \in [1, q + 1]$ with $i \neq j$. Prove that there is exactly one codeword in C which has α in positions i and j.

(b) Prove that each nonzero codeword has precisely one zero coordinate.

26. **Direct product of two codes**
Let C_1 be an (n_1, k_1, d_1)-code over $\mathbb{Z}_2$, and let C_2 be an (n_2, k_2, d_2)-code over $\mathbb{Z}_2$. Suppose that C_1 and C_2 are both systematic. Define a new code C over $\mathbb{Z}_2$ as follows. A message m is an element of $\mathbb{Z}_2^{k_1 k_2}$, whose symbols are arranged in a $k_1 \times k_2$ array. The codeword $c \in C$ corresponding to m is derived as follows. First, the k_2 columns of m are encoded using C_1, and the resulting C_1-codewords are written as the columns of an $n_1 \times k_2$ array c'. Next, the n_1 rows of c' are encoded using C_2, and the resulting C_2-codewords are written as the rows of an $n_1 \times n_2$ array c.

(a) Prove that the last $n_2 - k_2$ columns of c are codewords in C_1.

(b) Prove that C is an $(n_1 n_2, k_1 k_2)$-linear code over $\mathbb{Z}_2$.

(c) Prove that C has distance $d_1 d_2$.

(d) One can use an analogous construction of a code D by first encoding the k_1 rows of m using C_2, and then encoding the resulting n_2 columns using C_1. Prove that $D = C$.

(e) Determine a generator matrix for C.

27. **Deducing distance from PCM**
Let H be a parity-check matrix for a binary (n, k, d)-code with $n \geq 4$. Suppose that the columns of H are distinct and all columns have odd weight. Prove that $d \geq 4$.

28. **Shortened codes**
Let C be a binary linear code. Fix a coordinate position ℓ, and consider the binary code C' obtained by taking all codewords in C that have a 0 in coordinate position ℓ, and then deleting the ℓth symbol in these words. Assume that $|C'| \geq 2$.

(a) Prove that C' is a binary linear code.

(b) Prove one of the following: (i) $d(C) \geq d(C')$; (ii) $d(C) = d(C')$; (iii) $d(C) \leq d(C')$.

(c) Prove or disprove: $\dim(C') < \dim(C)$.

29. **Punctured and shortened codes**
Let C be an (n, k, d)-code over $GF(q)$, and let T be any set of t coordinates. Let C^T be the *punctured code* obtained by deleting all components indexed by T from all codewords in C. Let C_T denote the *shortened code* obtained by taking all codewords in C that have 0's in the coordinate positions indexed by T, and then deleting these components.

(a) Let C be the $(6, 3)$-binary code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

and let $T = \{5, 6\}$. Find generator matrices in standard form for C^T and C_T.

(b) Prove that $(C^\perp)_T = (C^T)^\perp$ and $(C^\perp)^T = (C_T)^\perp$.

(c) Suppose that $t < d$. Prove that C^T and $(C^\perp)_T$ have dimensions k and $n - t - k$, respectively.

(d) Suppose that $t = d$ and T is the set of coordinates where a minimum weight codeword is nonzero. Prove that C^T and $(C^\perp)_T$ have dimensions $k - 1$ and $n - d - k + 1$, respectively.

30. **New codes from old ones**
Let C_1 be an (n, k_1, d)-code over $GF(q)$, and let C_2 be an $(n, k_2, 2d)$-code over $GF(q)$. Let C be code consisting of all words of the form $(u, u+v)$ where $u \in C_1$ and $v \in C_2$.

   (a) Prove that C is a linear code over $GF(q)$.

   (b) Determine the dimension of C.

   (c) Determine the distance of C.

31. **Existence of linear codes**
Prove that if

$$\sum_{i=0}^{d-2} (q-1)^i \binom{n-1}{i} < q^{n-k},$$

then there exists an (n, k)-code C over $GF(q)$ having distance $\geq d$.

32. **Existence of perfect codes #1**
You must answer this question without appealing to Tietäväinen's classification theorem.

   (a) Does there exist a perfect code of length 27 and distance 3 over $GF(27)$?

   (b) Does there exist a perfect code of length 28 and distance 3 over $GF(27)$?

33. **Existence of perfect codes #2**
You must answer this question without appealing to Tietäväinen's classification theorem.

   (a) Does there exist a perfect binary code of length $n = 10$ and distance $d = 5$?

   (b) Find an upper bound on the dimension k of a binary linear code of length $n = 10$ and distance $d = 5$.

34. **Distance of perfect codes**
Prove (without referring to Tietäväiren's classification theorem) that every perfect code must have odd distance.

35. **Self-dual codes**
Recall that an (n, k)-code C over F is said to be self-dual if $C = C^{\perp}$, and C is said to be self-orthogonal if $C \subseteq C^{\perp}$.

   (a) Prove that C is self-dual if and only if C is self-orthogonal and $n = 2k$.

   (b) Prove that if C is a binary self-orthogonal code, then every codeword in C has even weight.

   (c) Prove that if C is a self-orthogonal code over $\mathbb{Z}_3$, then every codeword in C has weight divisible by 3.

36. **MDS code characterization #1**
Let C be an (n, k, d)-code over $GF(q)$ with generator matrix G and parity-check matrix H. Then C is said to be an maximum distance separable (MDS) code of $d = n - k + 1$.
Prove that the following are equivalent.

   (a) C is MDS.

   (b) Every k columns of G are linearly independent over $GF(q)$.

   (c) Every $n - k$ columns of H are linearly independent over $GF(q)$.

37. **MDS code characterization #2**
Let C be an (n, k)-code over $GF(q)$ of distance d. Prove that $d = n - k + 1$ if and only if for each subset of d coordinate positions there is a codeword in C whose nonzero entries are precisely in these d coordinate positions.

38. **MDS code characterization #3**
Let C be an (n, k)-code over $GF(q)$ of distance d with generator matrix $G = [I|A]$ in standard form. Prove that $d = n - k + 1$ if and only if every square submatrix of A is non-singular.
{A square submatrix of A is a matrix formed from any i rows and i columns of A, for any $i = 1, 2, \ldots, \min(k, n - k).$}

39. **Hamming MDS codes**
Which, if any, of the Hamming codes are also MDS codes?

40. **Dual of an MDS code**
Let C be an (n, k)-code over $GF(q)$ of distance d.

    (a) Prove that $d \leq n - k + 1$.

    (b) Suppose that $d = n - k + 1$. Prove that $C^{\perp}$ has distance $k + 1$.

41. **Self-dual codes**
Let C be a self-dual binary code of length n. Prove that the all-ones vectors of length n is in C.

42. **Augmenting a self-orthogonal code**
Let n be an odd number and let C be an $(n, (n-1)/2)$-binary self-orthogonal code. Let $C' = C \cup \overline{C}$, where $\overline{C}$ denotes the set obtained by complementing every vector in C. Prove that $C = C^{\perp}$.

43. **Cyclic codes #1** Let C_1 and C_2 be cyclic codes of length n over $F = GF(q)$, with canonical generators $g_1(x)$ and $g_2(x)$, respectively.

    (a) Let C_3 be the set of words that belong to both C_1 and C_2. Prove that C_3 is a cyclic code.

    (b) Determine *the* canonical generator for C_3.

44. **Cyclic codes #2**

    (a) Determine the number of cyclic subspaces in $V_6(\mathbb{Z}_3)$.

    (b) Determine the canonical generator and dimension of the smallest cyclic code containing the vector $v = (112110) \in V_6(\mathbb{Z}_3)$.

45. **Cyclic codes #3**
Let C be an (n, k)-binary cyclic code with $1 \leq k < n$ and canonical generator $g(x)$, and where n is the smallest positive integer for which $g(x)$ divides $x^n - 1$. Prove that $d(C) \geq 3$.

46. **Cyclic codes #4**
Let q be an odd prime power.

    (a) Let C be a $(q + 1, 2)$-code over $GF(q)$ with distance q. Prove that C is not cyclic.
    Hint: Consider a nonzero codeword in C that has the same entry in coordinate positions that are $(q + 1)/2$ apart.

    (b) Let C be a Hamming code of order 2 over $GF(q)$. Show that C is not cyclic.
    Hint: Consider the dual code of C.

47. **Error trapping**
Let C be the $(15, 9)$-binary cyclic code generated by $g(x) = 1 + x^3 + x^4 + x^5 + x^6$. It is known that C is a 3-cyclic burst error correcting code. Decoding each of the following received vectors using the error trapping algorithm that was presented in class.

(a) $r_1 = (11000\ 01110\ 10011)$.

(b) $r_2 = (01000\ 00010\ 11111)$.

(c) $r_3 = (10101\ 11010\ 11100)$.

48. **Interleaving two cyclic codes**
Let C_1, C_2 be the $(7, 4)$-binary cyclic codes with canonical generators $g_1(x) = 1+x+x^3$, $g_2(x) = 1+x^2+x^3$, respectively. Let C^* be the binary code obtained by interleaving C_1 and C_2. In other words, the codewords of C^* are obtained by taking pairs of codewords $a = (a_0, a_1, a_2, a_3, a_4, a_5, a_6) \in C_1$ and $b = (b_0, b_1, b_2, b_3, b_4, b_5, b_6) \in C_2$, to obtain $c = (a_0, b_0, a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4, a_5, b_5, a_6, b_6) \in C^*$.

(a) Prove that C^* is linear.

(b) Find the length and dimension of C^*.

(c) Find a generator matrix for C^*.

(d) Is C^* a cyclic code? Justify your answer.

49. **Cyclic codes over** $GF(4)$
Recall that if $g(x)$ is the canonical generator for an (n, k)-cyclic code C over $GF(q)$, then $h^*(x)$ (where $h(x) = (x^n - 1)/g(x)$) is the canonical generator for the dual code $C^\perp$.

(a) Let $x^n - 1 = g(x)h(x)$ over $GF(q)$. Prove that a cyclic code C with canonical generator $g(x)$ is self-orthogonal if and only if $h^*(x)$ divides $g(x)$.

(b) Recall that $GF(4) = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$. Let $g(x) = x^5 + \alpha x^4 + x^3 + x^2 + \alpha^2 x + 1 \in GF(4)[x]$. Show that $g(x)$ is the canonical generator for an $(11, 6)$-cyclic code C over $GF(4)$.

(c) Referring to the code C defined in (b), prove one of the following: (i) $C = C^\perp$; (ii) $C \subseteq C^\perp$; (iii) $C^\perp \subseteq C$.

50. **Double-adjacent errors**
Let C be a (n, k)-binary cyclic code with canonical generator $g(x) = (x + 1)p(x)$, where $p(x)$ does not divide $x^t - 1$ for any t, $1 \leq t \leq n-1$. An error pattern of the form $e(x) = x^i + x^{i+1}$ $(0 \leq i \leq n-1)$ is called a *double-adjacent* error pattern.

(a) Prove that no two double-adjacent error patterns can be in the same coset of C.

(b) Prove that C is capable of correctly decoding all single errors and all double-adjacent errors.

(c) Construct a canonical generator for a $(15, 10)$-binary cyclic code that is capable of correctly decoding all single errors and all double-adjacent error patterns.

51. **Minimal polynomials #1**
Consider $GF(2^4) = \mathbb{Z}_2[\alpha]/(\alpha^4 + \alpha + 1)$. Compute the minimal polynomials of β^2, β^5 and β^{11} over $GF(2)$, where $\beta = \alpha$. (See slide 151.)

52. **Minimal polynomials #2**
Find the minimal polynomials over $\mathbb{Z}_2$ of all elements in $GF(2^3) = \mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$.

53. **Minimal polynomials #3**
Consider $GF(3^3) = \mathbb{Z}_3[\alpha]/(\alpha^3 + 2\alpha^2 + 1)$. Compute the minimal polynomials of β^{11} and and β^{12} over $GF(3)$, where $\beta = \alpha^2$. (See slides 155 and 156.)

54. **Existence of linear codes**
Does there exist a $(41, 16)$-code over $GF(3^3)$ of distance at least 14?

55. **Reversible cyclic codes**
A code C is reversible if $(c_0, c_1, c_2, \ldots, c_{n-1}) \in C$ implies that $(c_{n-1}, \ldots, c_2, c_1, c_0) \in C$.

(a) Let C be a cyclic code over $GF(q)$ with canonical generator $g(x)$. Prove that C is reversible if and only if $g_R(x)$ is a nonzero scalar multiple of $g(x)$.

(b) Let C be a cyclic code over $GF(q)$ with canonical generator $g(x)$. Prove that a cyclic code is reversible iff the reciprocal of every root of $g(x)$ is also a root of $g(x)$.

(c) Prove that if -1 is a power of $q \bmod n$ then every cyclic code over $GF(q)$ of length n is reversible.

(d) Prove that the BCH code with canonical generator $g(x) = \text{lcm}\{m_{\beta^i}(x) : -t \leq i \leq t\}$ is reversible.

56. **Concatenation of linear codes #1**
Let C be an (n, k, d)-code over $GF(q)$ with generator matrix G, and let C' be an (n', k', d')-code over $GF(q^k)$. Since $GF(q^k)$ is a k-dimensional vector space over $GF(q)$, we can represent each element m of $GF(q^k)$ as a k-tuple $(m_1, m_2, \ldots, m_k)$ in $V_k(GF(q))$. Define $\phi : GF(q^k) \to C$ by

$$\phi(m) = mG.$$

Define

$$D = \{(\phi(c_1), \phi(c_2), \ldots, \phi(c_{n'})) \mid (c_1, c_2, \ldots, c_{n'}) \in C'\}.$$

(So, each component c_i is replaced by the n-tuple $\phi(c_i)$.)

(a) Prove that D is a linear code over $GF(q)$.

(b) Determine the length and dimension of D.

(c) Find (and justify) a non-trivial lower bound on the distance of D.

57. **Concatenation of linear codes #2**
Let C' be the code over $GF(4)$ defined in #21, and let C be the $(2, 2)$-binary code $\{00, 10, 01, 11\}$. Define $\phi : GF(4) \to C$ by $\phi(0) = 00$, $\phi(1) = 10$, $\phi(\alpha) = 01$, $\phi(\alpha + 1) = 11$.

(a) Determine the length, dimension and distance of the code D that was defined in #56.

(b) Find a generator matrix for D in standard form.

58. **Constructing BCH codes**
Consider the finite field $GF(2^5) = \mathbb{Z}_2[x]/(x^5 + x^2 + 1)$. Then $\alpha = x$ is a generator of $GF(2^5)$. We have the following minimal polynomials:

$$m_0(y) = y \qquad m_{\alpha^5}(y) = 1 + y + y^2 + y^4 + y^5$$
$$m_1(y) = 1 + y \qquad m_{\alpha^7}(y) = 1 + y + y^2 + y^3 + y^5$$
$$m_\alpha(y) = 1 + y^2 + y^5 \qquad m_{\alpha^{11}}(y) = 1 + y + y^3 + y^4 + y^5$$
$$m_{\alpha^3}(y) = 1 + y^2 + y^3 + y^4 + y^5 \qquad m_{\alpha^{15}}(y) = 1 + y^3 + y^5.$$

(a) Construct a canonical generator for a $(31, 11)$-binary cyclic code which has designed distance 11.

(b) Construct a canonical generator for a $(31, 15)$-binary cyclic code which has designed distance 8 and is self-orthogonal.

59. **Reed-Solomon codes**
Let $q > n > k$, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct elements in $GF(q)$. Define

$$C = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \ : \ f \in GF(q)[x], \ \deg(f) \leq k-1\}.$$

(a) Prove that C is a linear code over $GF(q)$.

(b) Determine the length, dimension, and distance of C.