Error-Correcting Codes: Solutions to a selection of the Exercises
Alfred Menezes

---

1. **Distance of a code**
   Let $C = \{c_1, c_2, c_3\}$ be an $[n, 3]$-binary code of distance d, and suppose that $d(C) = d > 2n/3$. Without loss of generality, we can suppose that $c_1 = 0$ and $d(c_1, c_2) = d$. Suppose that c_3 has d' 1's (and $n - d'$ 0's), where $d' \geq d$. Now, suppose that the number of coordinate positions in which c_2 has a 0 and c_3 a 1 is x, where $0 \leq x \leq n - d$. Then the number of coordinate positions in which c_2 and c_3 both have a 0 is $n - d - x$. Hence, the number of coordinate positions in which c_2 has a 1 and c_3 a 0 is $(n - d') - (n - d - x) = d - d' + x$. Thus,

   $$d(c_2, c_3) = x + (d - d' + x) = (d - d') + 2x \leq 2x \leq 2(n - d) < 2(n/3),$$

   which contradicts $d(C) > 2n/3$. Hence $d(C) \leq 2n/3$.

2. **Telephone numbers #1**

   (a) If the assignment were possible, then the set of telephone numbers would form a block code over the decimal alphabet (of size $q = 10$) with parameters $n = 10$, $M = 110,000,000$, and $d = 3$. For these parameters, the sphere packing bound is violated. Hence such a code does not exist, whence the assignment is not possible.

   (b) If the assignment were possible, then the set of telephone numbers would form a block code over the decimal alphabet (of size $q = 10$) with parameters $n = 10$, $M = 80,000,000$, and $d = 3$. For these parameters, the sphere packing bound satisfied. Hence such a code *might* exist. In fact, such a code *does* exist, but you wouldn't be expected to find it on your own. You will be asked to construct such a code in Problem #17.

4. **q-ary symmetric channels**

   (a) If $p = \frac{q-1}{q}$, then for any $1 \leq j, k \leq q$,

   $$Pr(Y_i = a_k | X_i = a_j) = \frac{1}{q}.$$

   The channel is thus useless since the input has no influence on the output.

   (b) Consider the 'modified' channel derived from the original channel as follows: If a symbol a_l is received by the original channel, then replace it with a symbol selected uniformly at random from the remaining symbols, $A \setminus \{a_l\}$. We claim that this 'modified' channel is a q-ary symmetric channel with symbol error probability $p' = 1 - \frac{p}{q-1}$.
   Proof of claim: Let Z_i be the i^{th} symbol output by the modified channel. Then for all $1 \leq j, k \leq q$,

   $$\begin{aligned} Pr(Z_i = a_k | X_i = a_j) &= \sum_{1 \leq l \leq q} Pr(Y_i = a_l | X_i = a_j) Pr(a_l \text{ is replaced with } a_k) \\ &= \sum_{1 \leq l \leq q, \quad l \neq k} Pr(Y_i = a_l | X_i = a_j) \frac{1}{q-1}, \end{aligned}$$

since $Pr(a_k \text{ is replaced with } a_k) = 0$. Now, by definition of a q-ary symmetric channel,

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

It follows that

$$Pr(Z_i = a_k | X_i = a_j) = \begin{cases} \frac{1}{q-1}\left((1-p) + (q-2)\frac{p}{q-1}\right) = \frac{1-\frac{p}{q-1}}{q-1} & \text{if } j \neq k \\ \frac{1}{q-1}\left((q-1)\frac{p}{q-1}\right) = 1 - \left(1 - \frac{p}{q-1}\right) & \text{if } j = k. \end{cases}$$

Hence the 'modified' channel is a q-ary symmetric channel with symbol error probability $p' = 1 - \frac{p}{q-1}$.

The result now follows since $\frac{q-2}{q-1} \leq p' < \frac{q-1}{q}$.

5. **Erasures**

   (a) Suppose that $c \in C$ is transmitted, $t \leq d-1$ symbols are erased during transmission, and r is received. Suppose that $c' \neq c$ is a codeword whose components are equal to those in c except possibly in the t erased positions. Then $1 \leq d(c, c') \leq t \leq d-1$, which contradicts $d(C) = d$. Hence, there is a unique codeword c which agrees with r in all its non-erased components. This codeword can be recovered from r by comparing r to all the codewords, and selecting the codeword that agrees with r in all its non-erased components.

   (b) Since $d(C) = d$, there exist $c, c' \in C$ with $c \neq c'$ and $d(c, c') = d$. Without loss of generality, suppose that c and c' differ in their first d components. Now, suppose that c is transmitted, the symbols in its first d positions are erased, and r is received. Since c and c' both agree with r in the $n-d$ non-erased positions, the channel decoder cannot determine with certainty whether c or c' was transmitted.

6. **Finite field computations #1**

   (a) $f(x)$ has no roots in $\mathbb{Z}_{11}$, so $f(x)$ has no linear factors over $\mathbb{Z}_{11}$ and thus is irreducible over $\mathbb{Z}_{11}$.

   (b) $8x + 1$.

   (c) $4x^2 + 10x$.

7. **Finite field computations #2**

   (a) $q = 5^5 = 3125$.

   (b) The polynomials in $\mathbb{Z}_5[x]$ of degree less than 5.

   (c) 5.

   (d) i. $2x^4 + 4x^3 + x + 4$.

   ii. $x^3 + 4x^2 + 2x + 3$.

   iii. By the frosh's dream, $(x+4)^5 = (x^5+4) = x+2$. Similarly, $(x+4)^{25} = (x+2)^5 = x^5+2 = x$, and $(x+2)^{125} = x^5 = x+3$. Since $6249 = q + (q-1)$, it follows that

$$\begin{aligned} (4x^3 + 2x^2 + x + 4)^{6249} &= (4x^3 + 2x^2 + x + 4)^{3125}(4x^3 + 2x^2 + x + 4)^{3124} \\ &= (4x^3 + 2x^2 + x + 4)(1) \\ &= 4x^3 + 2x^2 + x + 4. \end{aligned}$$

   Hence the answer is $(x+3)(4x^3 + 2x^2 + x + 4) = 4x^4 + 4x^3 + 2x^2 + 2x + 2$.

8. **Irreducibility of polynomials #1**

   (a) Long division of $f(x)$ by $(x-a)$ yields polynomials $\ell(x), r(x) \in F[x]$ such that

   $$f(x) = \ell(x)(x-a) + r(x), \text{ where } \deg(r) < 1, \tag{1}$$

   i.e., $r(x)$ is a constant polynomial, say $r(x) = c$. Now, substituting $x = a$ in (1) yields $f(a) = c$. Hence $f(a) = 0 \Leftrightarrow c = 0 \Leftrightarrow (x-a)|f(x)$.

   (b) Since f has degree 3, it is reducible over $\mathbb{Z}_5$ if and only if it has a linear factor in $\mathbb{Z}_5[x]$. By part (a), it has a linear factor in $\mathbb{Z}_5[x]$ if and only if $f(a) = 0$ for some $a \in \mathbb{Z}_5$. But $f(0) = 3$, $f(1) = 3$, and $f(2) = 4$, $f(3) = 2$, $f(4) = 3$. Hence, f is irreducible over $\mathbb{Z}_5$.

   (c) Since f has degree 4, it is reducible over $\mathbb{Z}_2$ if and only if it has a linear factor or an irreducible quadratic factor in $\mathbb{Z}_2[x]$. By part (a), it has a linear factor in $\mathbb{Z}_2[x]$ if and only if $f(a) = 0$ for some $a \in \mathbb{Z}_2$. But $f(0) = 1$ and $f(1) = 1$, so f has no linear factors. The only irreducible quadratic polynomial in $\mathbb{Z}_2[x]$ is $x^2 + x + 1$, which does not divide f (as seen by long division). Hence f is irreducible over $\mathbb{Z}_2$.

9. **Irreducibility of polynomials #2**

   (a) $x = 2$ is a root, so $x^7 + 5x^6 + x^3 + 5x + 3$ has a linear factor, and thus is reducible over $\mathbb{Z}_7$.

   (b) A degree-7 polynomial is irreducible if and only if it has no roots, no irreducible quadratic factors, and no irreducible cubic factors. Now, neither 0 nor 1 are roots of $f(x) = x^7 + x^6 + x^3 + x + 1$. Also, $f(x)$ is not divisible by the irreducible quadratic $x^2 + x + 1$, nor by the irreducible cubics $x^3 + x + 1$ and $x^3 + x^2 + 1$. Thus $f(x)$ is irreducible over $\mathbb{Z}_2$.

   (c) $f(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$ is divisible by the irreducible quadratic $x^2 + x + 1$. Hence, $f(x)$ is reducible over $\mathbb{Z}_2$.

10. **Orders of field elements**

    (a) $f(0) = 2$, $f(1) = 2$ and $f(2) = 2$, so $f(x)$ has no roots in $\mathbb{Z}_3$ and therefore no linear factors over $\mathbb{Z}_3$. Hence, $f(x)$ is irreducible over $\mathbb{Z}_3$.

    (b) Consider $\alpha = 2x$. Now the order of α is a divisor of $q - 1 = 27 - 1 = 26$, so $\mathrm{ord}(\alpha) = 1, 2, 13$ or 26. Now, $\alpha \neq 1$, and $\alpha^2 = (2x)^2 = x^2 \neq 1$. Also, $\alpha^{13} = (2x)^{13} = (-x)^{13} = -x^{13} = -1$ since x has order 13. Thus, we must have $\mathrm{ord}(\alpha) = 26$ and so α is a generator of $GF(3^3)^*$.

11. **Generators #1**

    (a) Let $x = \alpha^{(q-1)/2}$, where α is a generator of $GF(q)^*$. Then $x^2 = \alpha^{q-1} = 1$, so $x^2 - 1 = (x+1)(x-1) = 0$. Hence, $x + 1 = 0$ or $x - 1 = 0$. But α has order $q - 1$, whence $x - 1 \neq 0$, so we must have $x + 1 = 0$. Thus, $\alpha^{(q-1)/2} = -1$.

    (b) Let $q = 7$ and consider $GF(q) = \mathbb{Z}_7$. Let $\alpha = 6 \in \mathbb{Z}_7$. Then $\alpha^{(q-1)/2} = 6^3 = (-1)^3 = -1 \pmod 7$, but 6 has order 2 in $\mathbb{Z}_7$ and so is not a generator of $\mathbb{Z}_7^*$.

15. **Linear codes #1**

    (a) $n = 7$, $k = 3$ (since H has rank 4), $M = 3^3 = 27$.

(b) By performing elementary row operations on H, we get the matrix

$$H' = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = [A|I_4]$$

from which we can derive the generator matrix

$$G = \left[I_3| - A^T\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 & 1 & 0 \end{bmatrix}.$$

(c) Since H is a parity-check matrix for C, it is also a generator matrix for $C^\perp$.

(d) Length is 7, dimension is 4, number of codewords is $3^4 = 81$.

(e) The parity-check matrix H of C has no zero columns, nor is any column a multiple of another column, so $d \geq 3$. However, column 1 of H is the sum of columns 2 and 7, so $d = 3$.

(f) G is a parity-check matrix for $C^\perp$. It has no zero columns, but the third and sixth columns are equal, so $d^\perp = 2$.

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

(a) We have $w(x + y) = w(x) + w(y) - 2t$, where t is the number of coordinate of positions in which both x and y are 1. So, if $w(x)$ and $w(y)$ are both even, then $w(x + y)$ is also even.

(b) The columns of H are nonzero (since they have odd weight) and distinct, and so $d(C) \geq 3$. Now suppose that three columns of H are linearly dependent over $\mathbb{Z}_2$. Without loss of generality, suppose that this is the first three columns, so $\alpha_1 h_1 + \alpha_2 h_2 + \alpha_3 h_3 = 0$ for $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_2$, and where the α_i are not all 0. Now, if any of the α_i is 0, then we have a linear dependency of one or two columns of H, which is impossible. Hence, each α_i is 1, so $h_1 + h_2 + h_3 = 0$. But since $w(h_1)$, $w(h_2)$ and $w(h_3)$ are odd, it follows from arguments similar to the one in (a) that $w(h_1 + h_2 + h_3)$ is odd, which contradicts $w(h_1 + h_2 + h_3) = w(0) = 0$. Hence, no three columns of H are linearly dependent over $\mathbb{Z}_2$, so $d(C) \geq 4$.

20. **Telephone numbers #2**

(a) Since H is a 2×10 matrix of rank 2, C is a $(10, 8)$ code. Since none of the columns of H are zero, and no column is a multiple of another column, it follows that C has distance at least 3. Finally, since C has at least one codeword of weight 3, e.g. $(1, 9, 1, 0, 0, 0, 0, 0, 0, 0)$, we have $d(C) = 3$.

(b) A generator matrix for C is

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

(c) Consider the codeword $c = (1, 9, 1, 0, 0, 0, 0, 0, 0, 0)$ in D; c is the first row of G. Now the word $10c = (10, 2, 10, 0, 0, 0, 0, 0, 0, 0)$ is not in D. Hence the codewords in D are not closed under scalar multiplication, and so D is not a linear code.

(d) Note that D is a subset of C, and $|D| \geq 2$. Therefore, since the distance between any two distinct codewords in C is at least 3, it follows that that the distance between any two distinct codewords in D is also at least 3. Now, consider the first two rows $c_1 = (1, 9, 1, 0, 0, 0, 0, 0, 0, 0)$ $c_2 = (2, 8, 0, 1, 0, 0, 0, 0, 0, 0)$ of G. Then $c_3 = 2c_1 = (2, 7, 2, 0, 0, 0, 0, 0, 0, 0) \in C$. Since none of the components of c_2 and c_3 are 10, we have $c_2, c_3 \in D$. And, since $d(c_2, c_3) = 3$, we have $d(D) = 3$.

(e) Since $D \subseteq C$, we can use the parity-check matrix H and any single-error correcting algorithm to decode r. However, we have to make sure that if the decoded word has a component that is 10 then it is rejected – since such words would have never been sent.
Let the columns of H be denoted h_i, $1 \leq i \leq 10$. The decoding algorithm is:

i) Compute the syndrome $s = Hr^T$.

ii) If $s = 0$ then
 If no component of r is 10 then accept r.
 Else reject r.

iii) Check whether $s = \lambda h_i$ for some $\lambda \in \mathbb{Z}_{11}$ and some $i \in [1, 10]$; if s cannot be written in this form then reject r.
Otherwise, let $c = r - \lambda e_i$, where e_i denotes the ith unit vector.
If any component of c is 10, then reject r; else decode r to c.

(f) Accept r.

(g) Reject r.

(h) Decode r to $(9, 2, 3, 0, 2, 4, 0, 6, 9, 9)$.

21. **Linear code over $GF(4)$**

(a) The matrix G is a 3×6 matrix over $GF(4)$ of rank 3. Hence, $n = 6$, $k = 3$.

(b) C has $M = q^k = 4^3 = 64$ codewords.

(c) Since G is of the form $[I|A]$, a parity-check matrix for C is $[-A^T|I]$. Hence

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

(d) The columns of H are nonzero, and no two are $GF(4)$-multiples of each other. Hence $d(C) \geq 3$. We are given that $d \neq 3$, so $d(C) \geq 4$. The first row of G is a codeword of weight 4. Hence, $d(C) = 4$.

22. **Distance of the dual code**
Let G be a generator matrix for C, whence G is also a PCM for $C^\perp$. Suppose that $d(C^\perp) \leq k$. Then G has k columns that are linearly dependent over $GF(q)$. Without loss of generality, suppose that the first k columns of G are linearly dependent over $GF(q)$. Let A be the $k \times k$ matrix that is the left submatrix of G, so $G = [A|B]$. Then A is non-singular, so the rows of A are linearly dependent over $GF(q)$. Thus, there is a nonzero linear combination of the rows of A that gives the 0 vector (of length k). Taking the same linear combination of the rows of G gives a nonzero

codeword $c \in C$ whose first k components are 0, so c has weight at most $n-k$. This contradicts $d(C) = n-k+1$. We conclude that $d(C^{\perp}) = k$.

30. **New codes from old ones**

(a) Since $|C_1| \geq 2$, we also have $|C| \geq 2$ so C is non-empty.
Let $x = (u_1, u_1 + v_1)$, $y = (u_2, u_2 + v_2) \in C$, where $u_1, u_2 \in C_1$ and $v_1, v_2 \in C_2$. Then $x + y = (u_1 + u_2, u_1 + u_2 + v_1 + v_2)$. Since C_1 and C_2 are closed under addition, we have $u_1 + u_2 \in C_1$ and $v_1 + v_2 \in C_2$. Hence, $x + y \in C$, so C is closed under addition.
Let $\alpha \in GF(q)$. Then $\alpha x = (\alpha u_1, \alpha u_1 + \alpha v_1)$. Since C_1 and C_2 are closed under scalar multiplication, we have $\alpha u_1 \in C_1$ and $\alpha v_1 \in C_1$. Hence, $\alpha x \in C$, so C is closed under scalar multiplication.
Thus, C is a linear code under $GF(q)$.

(b) Let $u_1, u_2 \in C_1$ and $v_1, v_2 \in C_2$. Suppose that $(u_1, u_1 + v_1) = (u_2, u_2 + v_2)$. Then $u_1 = u_2$ and $u_1 + v_1 = u_2 + v_2$, the latter giving $v_1 = v_2$. Thus, if $(u_1, v_1) \neq (u_2, v_2)$, then $(u_1, u_1 + v_1) \neq (u_2, u_2 + v_2)$. Hence, $|C| = |C_1| \times |C_2| = q^{k_1} \times q^{k_2} = q^{k_1 + k_2}$. Since C is a vector space over $GF(q)$, it follows that the dimension of C is $k_1 + k_2$.

(c) Let $c = (u, u + v)$ be a nonzero word in C where $u \in C_1$ and $v \in C_2$. Suppose first that $u = 0$. Then $v \neq 0$, so $w(v) \geq 2d$ and hence $w(c) \geq 2d$. Suppose next that $u \neq 0$; let $w(u) = d + t$ where $t \geq 0$. Now, $w(u + v) \geq w(v) - w(u) \geq 2d - (d + t) = d - t$. Hence, $w(c) = w(u) + w(u + v) \geq (d + t) + (d - t) = 2d$. Also, if u is a weight-d word in C_1, then $c = (u, u)$ is in C and has weight $2d$. It follows that $w(C) = 2d$.

31. **Existence of linear codes**
Recall that a parity-check matrix H for an (n, k)-code over $GF(q)$ with distance $\geq d$ is an $(n-k) \times n$ matrix with entries from $GF(q)$ such that no $d-1$ (or fewer) columns of H are linearly dependent over $GF(q)$.
For $1 \leq j \leq n-1$, let H_j denote an $(n-k) \times j$ matrix having the property that no $d-1$ (or fewer) of its columns are linearly dependent over $GF(q)$. Now, the number of vectors in $GF(q)^{n-k}$ that are linear combinations of $d-2$ or fewer columns of H_j is at most

$$\sum_{i=0}^{d-2} \binom{j}{i} (q-1)^i.$$

Since $1 \leq j \leq n-1$, we have $\binom{j}{i} \leq \binom{n-1}{i}$ for all $0 \leq i \leq d-2$. Hence

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

and so there exists a vector $v \in GF(q)^{n-k}$ which is not a linear combination of $d-2$ or fewer columns of H_j. This vector can be added as a column to H_j, producing an $(n-k) \times (j+1)$ matrix H_{j+1} which also has the property that no $d-1$ of its columns are linearly dependent over $GF(q)$. Note that H_1 exists, since any non-zero vector in $GF(q)^{n-k}$ can be used as the column of H_1. By the above argument, we can construct a matrix $H_n = H$ by repeatedly adding columns to H_1. Hence an (n, k)-code over $GF(q)$ with distance $\geq d$ exists.

32. **Existence of perfect codes #1**

(a) Suppose that C is a perfect code of length $n = 27$ and distance $d = 3$ over $GF(27)$. Suppose that C has M codewords. Then the sphere packing bound says that

$$M(1 + n(q-1)) = q^n,$$

so $M = q^n/(1 + n(q-1))$. But the right hand side is not an integer when $q = 27$ and $n = 27$ (since the numerator is a power of 3, whereas the denominator is 703 which is not divisible by 3). Hence, such a code C does not exist.

(b) The Hamming code of order 2 over $GF(27)$ has length $n = 28$ and distance $d = 3$ (and dimension $k = 26$).

33. **Existence of perfect codes #2**

(a) If there exists a perfect binary code of length $n = 10$, having M codewords, and distance $d = 5$, then

$$M\left[\binom{10}{0} + \binom{10}{1} + \binom{10}{2}\right] = 2^{10}.$$

However,

$$M = 2^{10}/\left[\binom{10}{0} + \binom{10}{1} + \binom{10}{2}\right] = \frac{128}{7},$$

which is not an integer. Hence no such code exists.

(b) If C is a binary linear code of length $n = 10$, dimension k, and distance $d = 5$, then

$$2^k\left[\binom{10}{0} + \binom{10}{1} + \binom{10}{2}\right] \leq 2^{10}.$$

Hence

$$2^k \leq \frac{128}{7},$$

and so $k \leq 4$.

34. **Distance of perfect codes**

Let C be a code of even distance $d = 2t$. Then $e = \lfloor (d-1)/2 \rfloor = t - 1$. Let $c \in C$ and let r be a vector such that $d(c, r) = t$. Note that r is not in the sphere of radius e centered at c. Now, if r were in the sphere of radius e centered at some codeword $c' \neq c$, then we would have

$$d(c, c') \;\leq\; d(c, r) + d(r, c') \;\leq\; t + e \;<\; d,$$

which is impossible since the distance of C is d. Hence r is not contained in any of the radius-e spheres centered at codewords, and so C is not a perfect code. It follows that a perfect code must have odd distance.

35. **Self-dual codes**

(a) Suppose first that C is self-dual, so $C = C^\perp$. Then $C \subseteq C^\perp$. Also, since C has dimension k and $C^\perp$ has dimension $n - k$, we have $k = n - k$, so $n = 2k$.
Conversely, suppose that C is self-orthogonal and $n = 2k$. Now C has dimension k and $C^\perp$ has dimension $n - k = 2k - k = k$. Hence $\dim(C)=\dim(C^\perp)$, so C is self-dual.

(b) Let $c = (c_1, c_2, \ldots, c_n) \in C$. Since C is self-orthogonal, we have $c \in C^\perp$ and hence $c \cdot c = 0$. Now, if $c_i = 0$ then $c_i^2 = 0$, and if $c_i = 1$ then $c_i^2 = 1$. Hence $c \cdot c = \sum_{i=1}^n c_i^2 = \sum_{c_i=1} 1 \equiv 0 \pmod 2$, and so c has even weight.

(c) Let $c = (c_1, c_2, \ldots, c_n) \in C$. Since C is self-orthogonal, we have $c \in C^\perp$ and hence $c \cdot c = 0$. Now, if $c_i = 0$ then $c_i^2 = 0$; if $c_i = 1$ then $c_i^2 = 1$; and if $c_i = 2$ then $c_i^2 = 1$. Hence $c \cdot c = \sum_{i=1}^n c_i^2 = \sum_{c_i=1 \text{ or } 2} 1 \equiv 0 \pmod 3$, and so c has weight divisible by 3.

43. **Cyclic codes #1**

(a) We need to prove that $C_1 \cap C_2$ is a vector subspace of $V_n(F)$.
First note that $0 \in C_1 \cap C_2$, so $C_1 \cap C_2$ is non-empty.
Let c_1, $c_2 \in C_1 \cap C_2$. Then, since C_1 and C_2 are closed under vector addition, we have $c_1 + c_2 \in C_1$ and $c_1 + c_2 \in C_2$. Hence $c_1 + c_2 \in C_1 \cap C_2$.
Let $c \in C_1 \cap C_2$ and $\lambda \in F$. Then, since C_1 and C_2 are closed under scalar multiplication, we have $\lambda c \in C_1$ and $\lambda c \in C_2$. Hence $\lambda c \in C_1 \cap C_2$.
We conclude that $C_1 \cap C_2$ is a linear code.
Let $c \in C_1 \cap C_2$. Since C_1 and C_2 are cyclic, $\pi(c)$ (the right cyclic shift of c) is in C_1 and in C_2. Hence $\pi(c) \in C_1 \cap C_2$, whence $C_1 \cap C_2$ is a cyclic code.

(b) Let $g(x) = \text{lcm}(g_1(x), g_2(x))$. Note that $g(x)$ is monic and divides $x^n - 1$.
Let $c(x) \in C_1 \cap C_2$. Since $c(x) \in C_1$ and $c(x) \in C_2$, it follows that $g_1(x)|c(x)$ and $g_2(x)|c(x)$. Hence $g(x)|c(x)$.
Conversely, if $c(x) = a(x)g(x)$, where $a(x) \in F[x]$, then $c(x) \in C_1$ since $g_1(x)|g(x)$, and $c(x) \in C_2$ since $g_2(x)|g(x)$. Hence $c(x) \in C_1 \cap C_2$.
It follows that $C_1 \cap C_2 = \{a(x)g(x) \,:\, a(x) \in F[x]\} = \langle g(x) \rangle$. Since $g(x)$ is a monic divisor of $x^n - 1$, it follows from the Theorem on slide 108 that $g(x)$ is *the* canonical generator of $C_1 \cap C_2$.

44. **Cyclic codes #2**

(a) The complete factorization of $x^6 - 1$ over $\mathbb{Z}_3$ is $x^6 - 1 = (x-1)^3(x+1)^3$. Thus, the number of cyclic subspaces in $V_6(\mathbb{Z}_3)$ is $4 \times 4 = 16$.

(b) We seek the monic divisor $g(x)$ of $x^6 - 1$ over $\mathbb{Z}_3$ of highest degree that is also a divisor of $v(x) = 1 + x + 2x^2 + x^3 + x^4$. Now, the complete factorization of $v(x)$ over $\mathbb{Z}_3$ is $v(x) = (x-1)^2(x^2+1)$. Thus, $g(x) = (x-1)^2$ and the dimension of the cyclic code that it generates is $k = 6 - 2 = 4$.

45. **Cyclic codes #3**
Note that since $k \geq 1$, C has at least one nonzero codeword, whence $w(C) \geq 1$. We will show that C cannot have any nonzero codewords of weight 1 or 2.
Let $v(x) = x^i$ be a weight-one word, where $0 \leq i \leq n-1$. Now, since $g(x) \neq 1$ (since $k \neq n$), we have $\deg(g) \geq 1$. Hence $g(x) \nmid x^0$. Also, since $g(x) \mid (x^n - 1)$ and $x \nmid (x^n - 1)$, we have $g(x) \nmid x^i$ for $1 \leq i \leq n-1$. Hence $g(x) \nmid v(x)$, so $v \notin C$.
Let $v(x) = x^i + x^j$ be a weight-two word, where $0 \leq i < j \leq n-1$. Then $v(x) = x^i(1 + x^{j-i})$. If $g(x) \mid v(x)$, then we must have $g(x) \mid (1 + x^{j-i})$ since $x \nmid g(x)$. But this is impossible since $1 \leq j - i < n$ and $g(x) \nmid x^\ell - 1$ for all $1 \leq \ell < n$. Thus, $g(x) \nmid v(x)$, and so $v \notin C$.
Hence $w(C) \geq 3$, whence $d(C) \geq 3$.

47. **Error trapping**
The received words are decoded to:

(a) $c_1 = (11000\ 00000\ 10011)$.

(b) $c_2 = (11000\ 00010\ 11100)$.

(c) $c_3 = (10101\ 11010\ 11000)$.

48. **Interleaving two cyclic codes**

(a) For a codeword $c \in C^*$, we denote by (a, b) the codewords $a \in C_1$, $b \in C_2$ obtained by de-interleaving c.
Now, let $c_1, c_2 \in C^*$, and let $c_3 = c_1 + c_2$. Then clearly, $a_3 = a_1 + a_2$ and $b_3 = b_1 + b_2$. Since C_1 and C_2 are linear codes, we have $a_3 \in C_1$ and $b_3 \in C_2$. Hence $c_3 \in C^*$. This shows that C^* is closed under addition, so C^* is a linear code.

(b) The length of C^* is 14. Since C_1 and C_2 each have 2^4 codewords, the size of C^* is $2^4 \times 2^4 = 2^8$. Hence the dimension of C^* is 8.

(c) Let $\{a_1, a_2, a_3, a_4\}$ be a basis for C_1, and let $\{b_1, b_2, b_3, b_4\}$ be a basis for C_2. Let c_1, c_2, c_3, c_4 be the codewords in C^* obtained by interleaving a_1, a_2, a_3, a_4 with the zero codeword, and let c_5, c_6, c_7, c_8 be the codewords in C^* obtained by interleaving b_1, b_2, b_3, b_4 with the zero codeword. Then the c_i must be linearly independent over $\mathbb{Z}_2$ because if $\sum_{i=1}^{8} \lambda_i c_i = 0$ where $\lambda_i \in \mathbb{Z}_2$, then $\sum_{i=1}^{4} \lambda_i a_i = 0$ and $\sum_{i=5}^{8} \lambda_i b_{i+4} = 0$, from which it follows that $\lambda_i = 0$ for all $1 \le i \le 8$.
Recall now that $A = \{(1101000), (0110100), (0011010), (0001101)\}$ is a basis for C_1, and $B = \{(1011000), (0101100), (0010110), (0001011)\}$ is a basis for C_2. As a basis for C^*, we can take each vector from A and B interleaved with the zero vector. This gives the following generator matrix G^* for C^*:

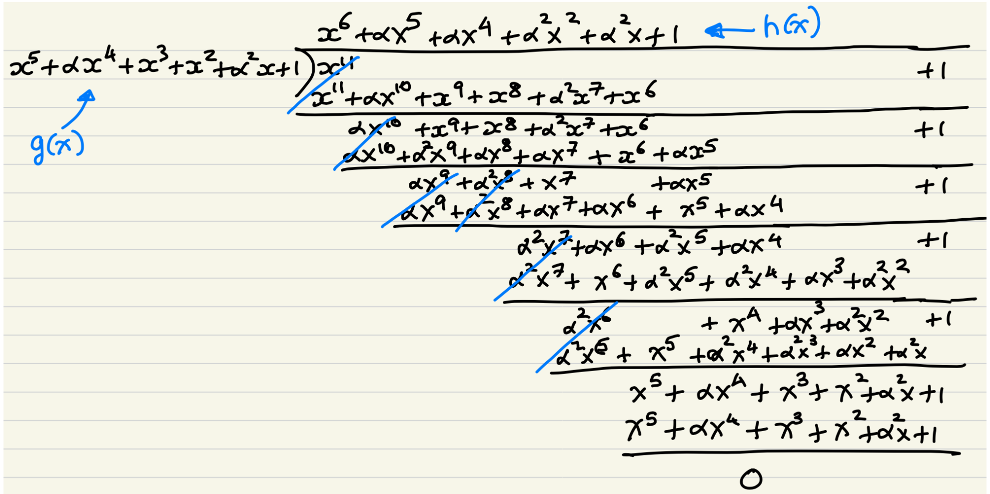
$$G^* = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0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

(d) The first row of G^* is the codeword $c = (1010001\ 0000000) \in C^*$, but its cyclic shift $c' = (0101000\ 100000)$ is not. To see this, note that de-interleaving c' and converting to polynomials gives 0 and $1 + x + x^3$. But $1 + x + x^3$ is not in C_2 since it is not divisible by $g_2(x)$.

49. **Cyclic codes over $GF(4)$**

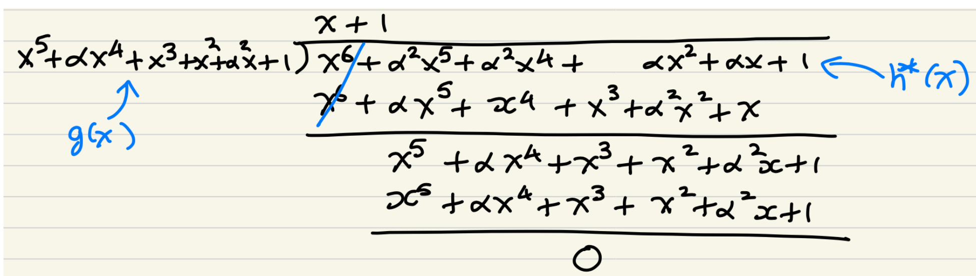
(a) Suppose first that $C \subseteq C^\perp$. Since $g(x) \in C$, we have $g(x) \in C^\perp$, and hence $g(x) = a(x)h^*(x)$, for some $a(x) \in GF(q)[x]$. Hence $h^*(x) | g(x)$.
Conversely, suppose that $h^*(x) | g(x)$. Then $g(x) = b(x)h^*(x)$ for some $b(x) \in GF(q)[x]$. Let $c \in C$. Then, since $g(x)$ generates C, we have $c(x) = d(x)g(x)$ for some $d(x) \in GF(q)[x]$. This implies that $c(x) = d(x)b(x)h^*(x)$, or $h^*(x) | c(x)$. Since $h^*(x)$ generates $C^\perp$, we have $c \in C^\perp$. Hence $C \subseteq C^\perp$.

(b) As the following long division shows, $g(x) = x^5 + \alpha x^4 + x^3 + x^2 + \alpha^2 x + 1$ is a monic divisor of $x^{11} - 1$ over $GF(4)$.



Hence, $g(x)$ is the canonical generator for an $(11,6)$-cyclic code C over $GF(4)$.

(c) Since the dimension of $C^\perp$ is 5, it cannot be the case that $C = C^\perp$ or $C \subsetneq C^\perp$. To show that $C^\perp \subsetneq C$, it suffices to show that $g(x) \mid h^*(x)$, where $h(x) = (x^{11}-1)/g(x) = x^6+\alpha x^5+\alpha x^4+\alpha^2x^2+\alpha^2x+1$. This is shown below:



50. **Double-adjacent errors**

(a) Let $x^i + x^{i+1}$ and $x^j + x^{j+1}$ be two double-adjacent error patterns with $i < j$. If these are in the same coset of C, then $g(x) \mid (x^i + x^{i+1} + x^j + x^{j+1})$. But

$$x^i + x^{i+1} + x^j + x^{j+1} \;=\; x^i(1+x) + x^j(1+x) \;=\; (1+x)x^i(1+x^{j-i}).$$

Since $g(x) \mid (x^n - 1)$, then $\gcd(g(x), x) = 1$, and hence $\gcd(p(x), x) = 1$. If $g(x) \mid (1+x)x^i(1+x^{j-i})$, then $p(x) \mid (1 + x^{j-i})$, which contradicts the hypothesis that $p(x)$ does not divide $x^t - 1$ for any t, $1 \le t \le n-1$. Hence, no two distinct double-adjacent error patterns are in the same coset of C.

(b) We need to prove (i) that no two single error patterns are in the same coset; and (ii) that no single and double-adjacent error patterns are in the same coset.
For (i), observe that if $g(x) \mid (x^i + x^j)$ (where $i < j$), then $g(x) \mid x^i(1 + x^{j-i})$. This implies that $p(x) \mid (1 + x^{j-i})$, which is false.
For (ii), observe that if $g(x) \mid (x^i + x^j + x^{j+1})$, then $(1+x) \mid (x^i + x^j(x+1))$, whence $(1+x) \mid x^i$, which is impossible.

(c) $g(x) = (1+x)(1+x+x^4)$. Also, $g(x) = (1+x)(1+x^3+x^4)$.

51. **Minimal polynomials #1**

- $m_{\beta^2}(x) = (x - \beta^2)(x - \beta^4)(x - \beta^8)(x - \beta) = x^4 + x + 1$.
- $m_{\beta^5}(x) = (x - \beta^5)(x - \beta^{10}) = x^2 + x + 1$.
- $m_{\beta^{11}}(x) = (x - \beta^{11})(x - \beta^7)(x - \beta^{14})(x - \beta^{13}) = x^4 + x^3 + 1$.

52. **Minimal polynomials #2**

- $m_0(x) = x$.
- $m_1(x) = x + 1$
- $m_\alpha(x) = x^3 + x + 1$.
- $m_{\alpha+1}(x) = x^3 + x^2 + 1$.
- $m_{\alpha^2}(x) = x^3 + x + 1$.
- $m_{\alpha^2+1}(x) = x^3 + x^2 + 1$.
- $m_{\alpha^2+\alpha}(x) = x^3 + x + 1$.
- $m_{\alpha^2+\alpha+1}(x) = x^3 + x^2 + 1$.

55. **Reversible cyclic codes**
Let C be an (n, k)-cyclic code over $GF(q)$ with canonical generator $g(x)$. Let $c = (c_0, c_1, \ldots, c_{n-1}) \in V_n(GF(q))$. Let $c(x)$ be the associated polynomial, and suppose that $\deg(c) = n - \ell$ where $\ell \geq 1$. Then the vector associated with $c_R(x)$ is $c_R = (c_{n-\ell}, c_{n-\ell-1}, \ldots, c_1, c_0, c_{n-1}, \ldots, c_{n-\ell+1})$, and hence the polynomial associated with $\bar{c} = (c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$ is $x^{\ell-1} c_R(x)$.

(a) ($\Leftarrow$) Suppose C is reversible. Let $g = (g_0, g_1, \ldots, g_{\ell-1})$ be the vector associated with $g(x)$. Since $g \in C$, we have $\bar{g}(x) = x^{k-1} g_R(x) \in C$. Hence, $g(x) \mid x^{k-1} g_R(x)$. Since $x \nmid g(x)$, it follows that $g(x) \mid g_R(X)$. Finally, since $\deg(g_R) = \deg(g) = n - k$, it must be the case that $g_R(x) = \lambda g(x)$ for some $\lambda \in GF(q)^*$.
($\Rightarrow$) Suppose that $g_R(x) = \lambda g(x)$ for some $\lambda \in GF(q)^*$. Let $c \in C$, so $c(x) = a(x)g(x)$ for some polynomial $a(x) \in GF(q)[x]$ of degree at most $k - 1$. Then $c_R(x) = a_R(x) g_R(x)$, so $c_R(x) = \lambda a_R(x) g(x)$. Thus, $c_R \in C$ and, since C is cyclic, it follows that $\bar{c} \in C$. This shows that C is reversible.

(b) We have $g_R(x) = x^{n-k} g(1/x)$. If α is a root of $g(x)$, then $g_R(1/\alpha) = 0$ so $1/\alpha$ is a root of $g_R(X)$. Since $\deg(g) = \deg(g_R)$, it follows that α is a root of g iff $1/\alpha$ is a root of g_R. Now, C is reversible iff $g(x) = \lambda g_R(x)$ for some $\lambda \in GF(q)^*$. Since g_R and λg_R have the same roots, it follows that C is reversible iff $1/\alpha$ is a root of g for every root α of g.

(c) Let m be the smallest positive integer such that $q^m \equiv 1 \pmod{n}$, and let β be an element of order n in $GF(q^m)$. Since -1 is a power of q modulo n, we can write $-1 = q^j \bmod n$ for some $j \geq 1$. Now, $\beta^{-i} = \beta^{q^j i} = (\beta^i)^{q^j}$, which is also a root of $g(x)$ since $(\beta^i)^{q^j}$ is a conjugate of β^i with respect to $GF(q)$. It follows from (b) that C is reversible.

(d) Let $g(x) = \text{lcm}\{m_{\beta^i}(x) : -t \leq i \leq i\}$. Let α be a root of $g(x)$. Suppose that α is a root of $m_{\beta^i}(x)$ where $-t \leq i \leq t$ whence $\alpha = (\beta^i)^{q^j}$ for some $j \geq 0$. Then, $\alpha^{-1} = (\beta^{-i})^{q^j}$, so α^{-1} is a root of $m_{\beta^{-i}}(x)$ where $-t \leq -i \leq t$. It follows that α^{-1} is a root of $g(x)$, and so by (b) the BCH code with canonical generator $g(x)$ is reversible.

58. **Constructing BCH codes**
The cyclotomic cosets of 2 modulo 31 are:

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4, 8, 16\}, \quad C_3 = \{3, 6, 12, 24, 17\}, \quad C_5 = \{5, 10, 20, 9, 18\}$$

$$C_7 = \{7, 14, 28, 25, 19\}, \quad C_{11} = \{11, 22, 13, 26, 21\}, \quad C_{15} = \{15, 30, 29, 27, 23\}.$$

(a) The set $C_1 \cup C_3 \cup C_5 \cup C_7$ contains the elements 1 to 10, and has cardinality 20. Hence

$$\begin{aligned} g(x) &= m_\alpha(x)m_{\alpha^3}(x)m_{\alpha^5}(x)m_{\alpha^7}(x) \\ &= 1 + x^2 + x^4 + x^6 + x^7 + x^9 + x^{10} + x^{13} + x^{17} + x^{18} + x^{20} \end{aligned}$$

is a canonical generator for the required code.

(b) Let $g(x) = m_1(x)m_\alpha(x)m_{\alpha^3}(x)m_{\alpha^5}(x)$. Then $g(x)$ the canonical generator for a (31,15)-cyclic code C with designed distance 8, since α^i, $0 \leq i \leq 6$, are among its roots. Now, let $h(x) = (x^{31} - 1)/g(x)$. Since,

$$h(x) = (1 + x + x^2 + x^3 + x^5)(1 + x + x^3 + x^4 + x^5)(1 + x^3 + x^5),$$

we have

$$\begin{aligned} h^*(x) = h_R(x) &= (1 + x^2 + x^3 + x^4 + x^5)(1 + x + x^2 + x^4 + x^5)(1 + x^2 + x^5) \\ &= m_{\alpha^3}(x)m_{\alpha^5}(x)m_\alpha(x). \end{aligned}$$

Hence $h^*(x)$ divides $g(x)$. If follows that C is self-orthogonal.

59. **Reed-Solomon codes**

For $f \in GF(q)[x]$ with $\deg(f) \leq k - 1$, define the vector $c(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n))$.

(a) C is clearly non-empty. Now, let $f, g \in GF(q)[x]$ be two polynomials of degree at most $k - 1$, and let $\lambda \in GF(q)$. Then $c(f) + c(g) = c(f + g)$, where $f + g \in GF(q)[x]$ has degree at most $k-1$; hence C is closed under addition. Also, $\lambda \cdot c(f) = c(\lambda f)$, where $\lambda f \in GF(q)[x]$ has degree at most $k-1$; hence C is closed under scalar multiplication. Thus, C is a vector subspace over $GF(q)$.

(b) Clearly, C has length n.

If $f, g \in GF(q)[x]$ are two polynomials of degree at $k-1$ and $c(f) = c(g)$, then $(f - g)(\alpha_i) = 0$ for all $1 \leq i \leq n$, so $f - g$ has at least n roots in $GF(q)$. But $f - g$ has degree $\leq k - 1 < n$, so it must be the case that $f - g = 0$, so $f = g$. It follows that $|C| = q^k$, whence C has dimension k over $GF(q)$.

Let f be a nonzero polynomial of degree at most $k - 1$ in $GF(q)[x]$. Then f can have at most $k-1$ roots in $GF(q)$, and so $c(f)$ has weight at least $n-k+1$. Thus, $d(C) \geq n-k+1$. Now, any (n, k)-linear code over $GF(q)$ has distance at most $n - k + 1$. Thus, we have $d(C) = n - k + 1$.