Combinatória e Teoria de Códigos
Exercises from the notes

Chapter 1

1.1. The following binary word

01111000000?001110000?0011001100101011100000000?01110

encodes a date. The encoding method used consisted in writing the date in 6 decimal digits (e.g. 290296 means February 29th, 1996), then converting it to a number in base 2 (e.g. 290296 becomes 1000110110111111000), and enconding the binary number using the rule

$$\begin{aligned} \{0,1\}^2 &\longrightarrow \mathcal{C} \subset \{0,1\}^6 \\ 00 &\longmapsto 000000 \\ 01 &\longmapsto 001110 \\ 10 &\longmapsto 111000 \\ 11 &\longmapsto 110011 \end{aligned}$$

The received word contains 3 unknown digits (which were deleted) and it may also contain some switched digits.
(a) Find the 3 deleted bits.
(b) How many, and in which positions, are the wrong bits?
(c) Which date is it?
(d) Repeat the problem switching the bits in positions 15 and 16, counting from the left. ("Switching a bit in position i" means replacing "1" by "0", and vice versa, in position i).

1.2. Consider the binary code $\{01101, 00011, 10110, 11000\}$. Using minimum distance decoding, decode the following received words:
(a) 00000;
(b) 01111;
(c) 01101;
(d) 11001.

1.3. Consider a binary channel with the following error probabilities

$$P(1 \text{ received} \mid 0 \text{ sent}) = 0,3 \qquad \text{and} \qquad P(0 \text{ received} \mid 1 \text{ sent}) = 0,2 \ .$$

For the binary code $\{000, 101, 111\}$, use maximum likelihood decoding, to decode the received words
(a) 010;
(b) 011;
(c) 001.

1.4. Prove that, for a symmetric binary channel, with crossover probability $p < \frac{1}{2}$, the minimum distance and maximum likelihood decoding schemes coincide.

1.5. What is the capacity of a code, with minimum distance d, for detecting and correcting errors *simultaneously*? State a decoding algorithm that corrects t errors and detects s errors and justify that it works.

1.6. Discuss the capacity of a code, with minimum distance d, for correcting erasure errors, and for correcting symbol errors and erasure errors *simultaneously*. State a decoding algorithm that corrects t symbol errors and a erasure errors and justify that it works.

1.7. (A Binary Hamming Code) We encode a message vector with 4 binary components $m = m_1 m_2 m_3 m_4$, $m_i \in \{0,1\}$, as a code word with 7 binary components $c = c_1 c_2 c_3 c_4 c_5 c_6 c_7$, $c_j \in \{0,1\}$, defined by

$$c_3 = m_1 \quad ; \qquad c_5 = m_2 \quad ; \qquad c_6 = m_3 \quad ; \qquad c_7 = m_4$$

and the other components:

$$c_4 \text{ is such that } \alpha = c_4 + c_5 + c_6 + c_7 \text{ is even}$$

$$c_2 \text{ is such that } \beta = c_2 + c_3 + c_6 + c_7 \text{ is even}$$

$$c_1 \text{ is such that } \gamma = c_1 + c_3 + c_5 + c_7 \text{ is even.}$$

Check that with this coding scheme we get a code which corrects an error in any position.
If we receive the vector $x = x_1 x_2 x_3 x_4 x_5 x_6 x_7$, we compute

$$\left.\begin{array}{l} \alpha = x_4 + x_5 + x_6 + x_7 \\ \beta = x_2 + x_3 + x_6 + x_7 \\ \gamma = x_1 + x_3 + x_5 + x_7 \end{array}\right\} \quad \text{mod } 2 \ ;$$

$\alpha\beta\gamma$ is the binary representation of the j component in which the error occured. If $\alpha\beta\gamma = 000$ we assume no error occured.
Study this example carefully.

Chapter 2

2.1. Show that $A_q(n,d) < A_{q+1}(n,d)$.

2.2. Verify that the binary codes $C_1 = \{0000, 0011, 1100\}$ and $C_2 = \{0000, 0011, 1010\}$ have the same parameters but are not equivalent.

2.3. Show that, up to equivalence, there are precisely n binary codes with lenght n containing two words.

2.4. Show that any $(n,q,n)_q$-code is equivalent to a repetition code.

2.5. Show that $A_2(5,4) = 2$ and $A_2(8,5) = 4$.

2.6. (a) Prove Proposition 2.9, i.e., show that (i) $\mathrm{d}(x,y) = \mathrm{w}(x-y)$ and (ii) $\mathrm{d}(x,y) = \mathrm{w}(x)+\mathrm{w}(y)-2\,\mathrm{w}(x\cap y)$, for all $x,y \in \mathbb{Z}_2^n$.
(b) Give a counter-example to show that, in general, part (ii) of Proposition 2.9 is not true for vectors in $\mathbb{Z}_3^n$, $n > 1$.

2.7. Using Lemma 2.13, verify that the volume of the balls with radius n in $\mathcal{A}_q^n$ is q^n.

2.8. Show that there is a perfect code C with parameters $(n,M,d)_q$ if and only if $A_q(n,d) = M$ and equality holds in the Hamming Estimate with $t = \frac{d-1}{2}$.

2.9. Justify the statements in Example 2.22 by solving the following questions:
(a) Verify that a code containing a single word satisfies the equality in the Hamming Estimate.
(b) For $C = \mathcal{A}_q^n$, compute the packing radius $\rho_e(C)$ and the covering radius $\rho_c(C)$. Verify that C satisfies the equality in the Hamming Estimate.
(c) Repeat part (b) for the binary repetition codes with odd length.

2.10. Show that, in the definition of a perfect code, it isn't necessary to assume that the minimum distance is odd. That is, show that, if C has even minimum distance, then $\rho_e(C) < \rho_c(C)$.

2.11. Prove the binary and q-ary Plotkin Estimates:
(a) For a (n,M,d) binary code C with $n < 2d$, show that

$$M \le \begin{cases} \dfrac{2d}{2d-n} & \text{if } M \text{ is even} \\ \dfrac{2d}{2d-n} - 1 & \text{if } M \text{ is odd} \end{cases} .$$

(b) For q-ary codes, show that $A_q(n,d) \le \dfrac{d}{d-\theta n}$, where $d > \theta n$ and $\theta = \frac{q-1}{q}$.

2.12. (a) Given two vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_m)$, we define

$$(u,v) = (u_1, \ldots, u_n, v_1, \ldots, v_m) .$$

Let C_1 and C_2 be binary codes with parameters (n, M_1, d_1) and (n, M_2, d_2), respectively. The *Plotkin Construction* of the codes C_1 and C_2 is the code defined by

$$C_1 * C_2 = \{(u, u+v) \,:\, u \in C_1, v \in C_2\} .$$

Show that the parameters of $C_1 * C_2$ are $(2n, M_1 M_2, d)$, where $d = \min\{2d_1, d_2\}$.
(b) The important familly of Reed-Muller binary codes can be obtained as follows:

$$\begin{cases} \mathcal{RM}(0,m) = \{\vec{0}, \vec{1}\} & \text{the binary repetition code with length } 2^m \\ \mathcal{RM}(m,m) = (\mathbb{Z}_2)^{2^m} & \\ \mathcal{RM}(r,m) = \mathcal{RM}(r,m-1) * \mathcal{RM}(r-1,m-1)\ , & 0 < r < m \end{cases}$$

for $r,m \in \mathbb{N}_0$, where $C_1 * C_2$ denotes the Plotkin Construction obtained from the codes C_1 and C_2.
Show that the parameters of $RM(r,m)$ are $n = 2^m$, $M = 2^{\delta(r,m)}$, where $\delta(r,m) = \sum_{i=0}^{r} \binom{m}{i}$, and $d = 2^{m-r}$.

Chapter 3

3.1. (a) Verify that the tables in Examples 3.21 and 3.22 are correct.
(b) Write a (ring) isomorphism between $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{F}_2[t]/\langle t^2+t\rangle$.

3.2. Find a primitive element in each of the following fields: $\mathbb{F}_5$, $\mathbb{F}_{11}$ and $\mathbb{F}_{13}$.

3.3. The field $\mathbb{F}_{16}$:
(a) Show that the polynomial t^4+t+1 is irreducible in $\mathbb{F}_2[t]$.
(b) Define $\mathbb{F}_{16} = \mathbb{F}_2[t]/\langle t^4+t+1\rangle$ by identifiying its elements and by sketching the addition and multiplication tables. Find a primitive element in $\mathbb{F}_{16}$.
Suggestion: in Remark 3.28, use (3.2) to describe the sum and (3.3) to describe the product of two elements. So, instead of writing two 16×16 tables, you only need to write a correspondence between (3.2) and (3.3), identifying a primitive element $\alpha \in \mathbb{F}_{16}$.

3.4. List all irreducible polynomials in $\mathbb{F}_2[t]$ with degrees 2, 3 and 4.

3.5. Let $I(p,n)$ be the number of irreducible monic polynomials of degree n in $\mathbb{F}_p[t]$.
(a) Show that $I(p,2) = \binom{p}{2}$.
(b) Show that $I(p,3) = \dfrac{p(p^2-1)}{3}$.
(c) Study Section 2.2 in the Apendix A for a proof of a formula for $I(p,n)$.

3.6. Let $\mathbb{F}$ be a field with characteristic p, with p a prime number. Show that $\mathbb{F}$ is a vector space over $\mathbb{F}_p$. Conclude that the order of any finite field is a power of a prime number.

3.7. (a) Justify that the polynomials t^3+t+1 and t^3+t^2+1 are irreducible in $\mathbb{F}_2[t]$.
(b) Justify that both quotients $A = \mathbb{F}_2[t]/\langle t^3+t+1\rangle$ and $B = \mathbb{F}_2[t]/\langle t^3+t^2+1\rangle$ are isomorphic to the field $\mathbb{F}_8$, and write an isomorphism $\phi : A \longrightarrow B$.
Sugestion: Let $\alpha \in A$ be a root of $1+t+t^3$ and $\beta \in B$ be a root of $1+t^2+t^3$. Find a relation between α and β or, more precisely, find a root of $1+t^2+t^3$ in A.
(c) For the description A of $\mathbb{F}_8$, determine a primitive element. Justify that A is a vector space over $\mathbb{F}_2$ and write a basis.

3.8. Let V be a vector subspace of $\mathbb{F}_q^n$, with dimention $1 \le k \le n$.
(a) How many vectors does V contain?
(b) How many distinct bases does V have?

3.9. (a) Determine the number of nonsingular[1] $n \times n$ square matrices with entries in a finite field $\mathbb{F}_q$.
(b) What is the probability $P(q,n)$ of a $n \times n$ matrix over $\mathbb{F}_q$ being nonsingular?

3.10. Consider the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. Denote by $\begin{bmatrix} n \\ k \end{bmatrix}_q$ the number of k dimentional subspaces of $\mathbb{F}_q^n$.
(a) Show that

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} .$$

(b) Show that

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q .$$

(c) Justify that

$$\lim_{q \to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k} .$$

[1]Recall that a square matrix A, with entries in any field, is non singular, or invertible, if and only if $\det(A) \neq 0$ if and only if its columns (or rows) are linearly independent.

3.11. (a) Show that $\mathbb{F}_{q^m}$ is a vector space over $\mathbb{F}_q$, with the vector sum and product by a scalar defined via the operations in $\mathbb{F}_{q^m}$.

(b) Let $f(t) \in \mathbb{F}_q[t]$ be an irreducible polynomial in $\mathbb{F}_q[t]$, with degree m, and let $\alpha \in \mathbb{F}_{q^m}$ be a root of $f(t)$. Show that $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

3.12. Let V be a finite dimentional vector space over $\mathbb{F}_{q^m}$.

(a) Show that V is also a vector space over $\mathbb{F}_q$ and

$$\dim_{\mathbb{F}_q}(V) = m \dim_{\mathbb{F}_{q^m}}(V) \ ,$$

where $\dim_{\mathbb{F}}(V)$ denotes the dimention of V as an $\mathbb{F}$-vector space.

(b) Let $\{v_1, \dots, v_k\}$ be a basis of V over $\mathbb{F}_{q^m}$, and $\{\alpha_1, \dots \alpha_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Show that $\{\alpha_i v_j \,:\, i = 1, \dots, m\,;\, j = 1, \dots, k\}$ is a basis of V over $\mathbb{F}_q$.

3.13. (a) Prove the *Freshman Dream Fromula*: $(a+b)^p = a^p + b^p$, for all $a, b \in \mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$.

(b) Show that $(a+b)^{q^i} = a^{q^i} + b^{q^i}$ for all $a, b \in \mathbb{F}_{q^m}$ and $i \in \mathbb{N}$.

(c) Justify that, for all $a \in \mathbb{F}_{q^m}$, $a \in \mathbb{F}_q \subset \mathbb{F}_{q^m}$ if and only if $a^q = a$.

(d) For each $x \in \mathbb{F}_{q^m}$, we define its trace by $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}$. Show that $\mathrm{Tr}(x) \in \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^m}$.

(e) Show that $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$, $x \longmapsto \mathrm{Tr}(x)$, is a linear map over $\mathbb{F}_q$.

3.14. Consider $\mathbb{F}_{16} = \mathbb{F}_2[t]/\langle t^4 + t + 1\rangle$, i.e., $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ where $\alpha^4 = \alpha + 1$.

(a) Identify $\mathbb{F}_4$ as a subfield of $\mathbb{F}_{16}$.
Suggestion: you may want to use part (c) of Exercise 3.13.

(b) Find a polynomial $f(t) \in \mathbb{F}_4[t]$ such that $\mathbb{F}_{16} = \mathbb{F}_4[t]/\langle f(t)\rangle$.

(c) Is $\mathbb{F}_8$ a subfield of $\mathbb{F}_{16}$? Justify your answer.

3.15. Given two fields $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$, with $m > n$, when is $\mathbb{F}_{q^n}$ a subfield of $\mathbb{F}_{q^m}$?

3.16. Let V and W be vector subspaces of $\mathbb{F}_q^n$. Show that the sum $V + W$ (defined by $V + W = \{v + w \in \mathbb{F}_q^n \,:\, v \in V, w \in W\}$), and the intersectione $V \cap W$ are vector spaces. Show also that the sum $V + W$ is the vector space generated by V and W.

3.17. Let $\langle \cdot, \cdot \rangle_H : \mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n \longrightarrow \mathbb{F}_{q^2}$ be defined by

$$\langle u, v \rangle_H = \sum_{i=1}^{n} u_i v_i^q \ ,$$

where $u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_{q^2}^n$. Show that $\langle \cdot, \cdot \rangle_H$ is an inner product in $\mathbb{F}_{q^2}^n$.
Remark: $\langle \cdot, \cdot \rangle_H$ is the *hermitian inner product*. The *hermitian dual* of a linear code C is defined as

$$C^{\perp_H} = \{v \in \mathbb{F}_{q^2}^n \,:\, \langle v, c \rangle_H = 0 \quad \forall\, c \in C\} \ .$$

3.18. Recall that $\mathbb{F}_4 = \mathbb{F}_2[t]/\langle t^2 + t + 1\rangle = \{0, 1, \alpha, \alpha^2\}$, where α is a root of $t^2 + t + 1 \in \mathbb{F}_2[t]$. Show that the following linear codes over $\mathbb{F}_4$ are self-dual with respect to the hermitian inner product defined in the previous problem:

(a) $C_1 = \langle (1, 1) \rangle \subset \mathbb{F}_4^2$,

(b) $C_2 = \langle (1, 0, 0, 1, \alpha, \alpha), (0, 1, 0, \alpha, 1, \alpha), (0, 0, 1, \alpha, \alpha, 1) \rangle \subset \mathbb{F}_4^6$.

Are these self-dual codes with respect to the euclidean inner product?

Chapter 4

4.1. Let C be a $[n, k]$ linear code over $\mathbb{F}_q$. For each $i \in \{1, \ldots, n\}$, show that either $x_i = 0$ for all $x = (x_1, \ldots, x_n) \in C$, or C contains $\frac{|C|}{q} = q^{k-1}$ words with $x_i = a$, for $a \in \mathbb{F}_q$ fixed.

4.2. Let C be a binary linear code. Show that either all words in C have even weight, or half of them have even weight and the other half odd weight.

4.3. Let C be a $[n, k, 2t+1]$ binary code and let $C' = \{x \in C : \mathrm{w}(x) \text{ is even}\}$ be the subcode of C consisting of the even weighted words.
(a) Show that C' is a linear code.
(b) Find the dimention of C'. Justify carefully your answer.

4.4. Let C be a binary self-dual linear code.
(a) Show that, if the weight of $x, y \in C$ is a multiple of 4, then the weight of $x + y$ is also a multiple of 4.
(b) Show that all words in C have weight a multiple of 4, or half has weight a multiple of 4 and the other half has even weight but not divisible by 4.
(c) Show that $\vec{1} = (1, \ldots, 1) \in C$.
(d) If C has length 6, find the minimum distance $\mathrm{d}(C)$.

4.5. Write a generating matrix, a parity-check matrix, and the parameters $[n, k, d]$ for the smallest linear code over $\mathbb{F}_q$ containing the set S, when
(a) $q = 3$, $S = \{110000, 011000, 001100, 000110, 000011\}$;
(b) $q = 2$, $S = \{10101010, 11001100, 11110000, 01100110, 00111100\}$.

4.6. Let C be a linear $[N, K, D]$-code over $\mathbb{F}_{q^m}$.
(a) The *trace code* is defined by

$$\mathrm{Tr}(C) := \{(\mathrm{Tr}(x_1), \ldots, \mathrm{Tr}(x_N)) : (x_1, \ldots, x_N) \in C\} ,$$

where $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ is the trace map defined in Exercise 3.13. Show that $\mathrm{Tr}(C)$ is a q-ary linear code, with length N and dimenstion $k \leq mK$.
(b) The *subfield subcode* is defined by

$$C|_{\mathbb{F}_q} := C \cap \mathbb{F}_q^N .$$

Justify that $C|_{\mathbb{F}_q}$ is a liner code over $\mathbb{F}_q$.

4.7. Consider the linear code $C = \langle(\alpha, \alpha^2, \alpha^4, 1, \alpha^3, \alpha^6, \alpha^5)\rangle$ over $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where $\alpha^3 = 1 + \alpha$.
(a) Find the parameters of C.
(b) Determine a generating matrix for the trace code $\mathrm{Tr}(C)$ (see Exercise 4.6).
(c) Find the parameters of the dual code $\mathrm{Tr}(C)^\perp$.
(d) Is $\mathrm{Tr}(C)$ a self-orthogonal or a self-dual code?
(e) Write a generating matrix for the dual code $C^\perp$ and for subfield subcode $(C^\perp)|_{\mathbb{F}_2}$.
(f) Verify[2] that $(C^\perp)|_{\mathbb{F}_2} = \mathrm{Tr}(C)^\perp$.

4.8. Let C be a linear code with length $n \geq 4$. Let H be a parity-check matrix for C such that its columns are distinct and have odd weight. Show that $\mathrm{d}(C) \geq 4$.

4.9. Up to linear equivalence, find the number of linear codes over $\mathbb{F}_3$ with length n and dimension 1.

4.10. Let C be a linear $[n, k]_q$-code, with $k \geq 1$, and let G be a generating matrix show that

$$\begin{aligned} \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ m &\longmapsto G^T m , \end{aligned}$$

is a systematic coding scheme for C if and only if all columns in the identity $k \times k$-matrix are also columns in G.

[2]This relation between the trace code and the subfield subcode is valid for any linear code C over $\mathbb{F}_{q^m}$, it is the Delsarte's Theorem.

4.11. (a) Prove Proposition 4.29: For a q-ary linear code, with lenght n and minimum distance d, show that the vectors $x \in \mathbb{F}_q^n$ with weight $\mathrm{w}(x) \leq \lfloor \frac{d-1}{2} \rfloor$ are coset leaders of distinct cosets of this code.

(b) Let C be a perfect code with $\mathrm{d}(C) = 2t+1$. Show that the only coset leaders of C are the ones determined in part (a).

(c) Assuming that the perfect code C in part (b) is binary, let $\widehat{C}$ be the code obtained from C by adding a parity-check digit, i.e.,

$$\widehat{C} = \Big\{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_2^{n+1} : (x_1, \ldots, x_n) \in C\,, \sum_{i=1}^{n+1} x_i = 0\Big\}\ .$$

Show that the weight of any coset leader of $\widehat{C}$ is less or equal than $t+1$.

4.12. Consider the linear code over $\mathbb{F}_{11}$ with parity-check matrix

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

(a) Find the parameters $[n, k, d]$ of this code.
Suggestion: First show that in any field $\mathbb{F}$

$$\begin{vmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \end{vmatrix} = (a_3 - a_1)(a_2 - a_1)(a_3 - a_2)\ , \qquad \forall\, a_1, a_2, a_3 \in \mathbb{F}\ .$$

(b) Write a generating matrix for the code.

(c) Describe a decoding algorithm for this code that can correct 1 error and detect 2 errors in any position.

(d) Apply that algorithm to decode the received vectors

$$x = 0204000910 \qquad \text{e} \qquad y = 0120120120\ .$$

4.13. Solve the analogous problem to the previous one for the linear code over $\mathbb{F}_{11}$ with parity-check matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & X^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 & 8^3 & 9^3 & X^3 \end{bmatrix}\ .$$

Decode also the received vector $z = 1204000910$.

4.14. Let C be the linear code over $\mathbb{F}_5$ with the following parity-check matrix

$$H = \begin{bmatrix} 3 & 2 & 1 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 3 & 2 \\ 0 & 4 & 1 & 4 & 1 & 3 \end{bmatrix}\ .$$

(a) Show that C can correct all error vectors of the form

$$aa0000\,,\quad 0aa000\,,\quad 00aa00\,,\quad 000aa0 \quad \text{and} \quad 0000aa\ ,$$

for $a \in \mathbb{F}_5 \setminus \{0\}$, and decode the received vectors $y = 100011$ and $z = 023333$.

(b) Can C be used to correct all double errors?

4.15. Find a $[7, K]$ linear code with the largest possible rate which can correct the following error vectors: 1000000, 1000001, 1100001, 1100011, 1110011, 1110111 and 1111111.

4.16. Consider a linear code C over $\mathbb{F}_3 = \{0, 1, 2\}$ with parity-check matrix

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

(a) Determine the $[n, k, d]$ parameters of C.

(b) Find a generator matrix in standard form for the code C.
(c) What is the capacity of C for correcting erasure errors? Give a detailed justification.
(d) Decode, if possible, the following received words

$$x = 2101?? \ , \qquad y = 1???12 \qquad \text{and} \qquad z = ???210 \ .$$

4.17. Prove Proposition 4.32. Show also that, for a perfect code, we also have that $\alpha_i = 0$ for all $i > t$.

4.18. Let C be a binary perfect linear code with length n and let

$$\widehat{C} = \{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_2^{n+1} : (x_1, \ldots, x_n) \in C \, , \sum_{i=1}^{n+1} x_i = 0\}$$

be its parity-check extension. For a symmetric binary transmission channel, with crossover probability $0 < p < \frac{1}{2}$, show that $P_{corr}(C) = P_{corr}(\widehat{C})$.

4.19. (a) Show that the minimum distance of the ISBN code (see Example 4.24) is 2.
(b) How many words in the ISBN code end with the symbol $X \in \mathbb{F}_{11}$?
(c) How many words in the ISBN code end with the symbol $a \in \{0, 1, \ldots, 9\} \subset \mathbb{F}_{11}$?
(d) Let C be the linear code over $\mathbb{F}_{11}$ defined in Example 4.36 and let $C' \subset C$ be the subcode defined by

$$C' = \{x \in C \, : \, x_i \neq X \quad \forall \, i = 1, \ldots, 10\} \ .$$

Show that $|C'| = 82644629$.

Sugestion: use the Inclusion-Exclusion Principle and Exercise 4.1.

Chapter 5

5.1. Prove Lemma 5.4.

5.2. Check the equalities (5.2) in Example 5.5.

5.3. Show that, if C is a linear code, then the code $\bar{C} = C \cup C^c$ in Example 5.5 is linear, and find its parameters.

5.4. (a) Let C be a linear $[n, k]_q$-code and let C' be the contraction of C obtained by puncturing the i-coordinate in the section $C_{i,0}$, where $i \in \{1, \dots, n\}$. Show that C' is a linear code, find its dimension and write a parity-check matrix for C'.

(b) Let $C = E_n$ be the binary even weight code with length $n \geq 2$. Justify that the punctured section $C_{i,1}$ is not a linear code.

5.5. If there is a $[n, k, d]_q$ code, show that there is also a $[n - r, k - r, d]$ code for any $1 \leq r \leq k - 1$.

5.6. Given a $[n, k, d]_q$ code C,

(a) is there always a $[n + 1, k, d + 1]_q$ code?

(b) is there always a $[n + 1, k + 1, d]_q$ code?

5.7. (a) Let G_1 and G_2 be generating matrices for the q-ary linear codes C_1 and C_2, respectively. show that

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$$

is a generating matrix for the sum code $C_1 \oplus C_2$.

(b) Write a parity-check matrix for $C_1 \oplus C_2$ in terms of parity-check matrices H_1 and H_2 for C_1 and C_2, respectively.

5.8. Repeat the previous exercise for the Plotkin construction:

(a) If C_1 and C_2 are linear codes, show that $C_1 * C_2$ is also linear.

(b) Let G_1 and G_2 be generating matrices for the q-ary linear codes C_1 and C_2, respectively, both with length n. Show that

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$$

is a generating matrix for $C_1 * C_2$.

(c) If H_1 and H_2 are parity-check matrices for C_1 and C_2, respectively, write a parity-check matrix for $C_1 * C_2$ in terms of H_1 and H_2.

5.9. Consider the linear codes C_1 and C_2 over $\mathbb{F}_q$, with length n and dimentions $\dim(C_i) = k_i$, $i = 1, 2$, and define

$$C = \{(a + x, b + x, a + b + x) \, : \, a, b \in C_1, x \in C_2\} \, .$$

(a) Show that C is a lienar code with parameters $[3n, 2k_1 + k_2]$.

(b) Write a generating matrix for C in terms of generating matrices G_1 and G_2 for C_1 and C_2, respectively.

(c) Write a parity-check matrix for C in terms of parity-check matrices H_1 and H_2 for C_1 and C_2, respectively.

Chapter 6

6.1. Let C be the binary Hamming code $\mathrm{Ham}(3,2)$ in Example 6.2. Decode the received vectors $y = 1101101$ and $z = 1111111$.

6.2. Let C be a $\mathrm{Ham}(5,2)$ code and assume that column j of the parity-check matrix is the binary representation of the integer j. Find the parameters of C and decode the received vector $y = \vec{e}_1 + \vec{e}_3 + \vec{e}_{15} + \vec{e}_{20}$, where $\vec{e}_i$ is the vector with a 1 in the i-th coordinate and 0 in all the others.

6.3. Write the parameters and a parity-check matrix H for $\mathrm{Ham}(2,5)$. Using your matrix H, decode the received vector $y = 3\vec{e}_1 + \vec{e}_3 + 2\vec{e}_4$.

6.4. Write the parameters and a parity-check matrix for $\mathrm{Ham}(3,4)$.

6.5. Describe a decoding algorithm for the extended Hamming code $\widehat{\mathrm{Ham}}(r,2)$ that corrects any simple error and detects double errors simultaneously.

6.6. Let C be the binary code with the following parity-check matrix

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

(a) Determine the $[n,k,d]$ parameters of the code C.
(b) Show that C can be used to correct all errors with weight 1 and all errors with weight 2 with a nonzero n-th component. Can this code correct simultaneously all these errors plus a few more with weight 2?
(c) Describe a decoding algorithm that corrects all errors mentioned in part (b), and decode the received vector $y = 10111011$.

6.7. (a) Show that
$$\mathcal{RM}(r,m)^{\perp} = \mathcal{RM}(m-r-1,m),\ \forall\, 0 \le r < m.$$
(b) Show that $\mathcal{RM}(1,m)$ contains a unique word of weight 0, namely the zero word, a unique word of weight 2^m, namely the word whose components are all 1, and $2^{m+1}-2$ words of weight 2^{m-1}.
(c) Show that $\mathcal{RM}(1,m)$ is equivalent to the dual of an extended binary Hamming code.
(d) Conclude that the words in the dual of a Hamming code of redundancy r are all equidistant and have weight 2^{r-1}.

6.8. Given a binary code C with parameters (n, M, d), where $d \ge 3$, define
$$C_\lambda = \{(x, x+c, \pi(x) + \lambda(c)) \,:\, x \in \mathbb{F}_2^n, c \in C\} ,$$
where $\lambda : C \longrightarrow \mathbb{F}_2$ is an arbitrary map and $\pi : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is given by
$$\pi(x) = \begin{cases} 0 & \text{if } \mathrm{w}(x) \text{ is even,} \\ 1 & \text{if } \mathrm{w}(x) \text{ is odd .} \end{cases}$$

(a) Determine the (n', M', d') parameters of C_λ. Justify your answer.
(b) If C is a linear code, show that C_λ is a linear code if and only if λ is a linear map.
(c) Assuming that C is a linear code with generating matrix G and that λ is a linear map, write a generating matrix for C_λ.
(d) Show that, if C is a perfect code with $\mathrm{d}(C) = 3$, then C_λ is perfect.
(e) Let $C = \mathrm{Ham}(r,2)$, with $r \ge 2$, and let λ be the zero map. Is C_λ a Hamming code? Justify your answers.
(f) Let $C = \mathrm{Ham}(r,2)$, with $r \ge 2$, and let λ be the constant map with value $1 \in \mathbb{F}_2$. Is C_λ a Hamming code? Justify your answer.
(g) Let $C = \vec{e}_1 + \mathrm{Ham}(r,2) := \{\vec{e}_1 + c \,:\, c \in \mathrm{Ham}(r,2)\}$, where $r \ge 2$ and $\vec{e}_1 = (1,0,\ldots,0)$, and let λ be the zero map. Is C_λ a Hamming code? Justify your answer.

6.9. Justify that the Hamming codes $\mathrm{Ham}(2, q)$, with redundancy 2, are MDS codes.

6.10. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where α is a root of $1 + t + t^2$. Let C be a linear code over $\mathbb{F}_4$ with generating matrix

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

Write a generating matrix for the dual code $C^\perp$. Show that C and $C^\perp$ are MDS codes.

6.11. Show that the only binary MDS codes are the trivial ones.

6.12. Let C be a q-ary MDS code with parameters $[n, k]$, where $k < n$.
(a) Show that there is a q-ary MDS code with length n and dimention $n - k$.
(b) Show that there is a q-ary MDS code with length $n - 1$ and dimention k.

6.13. In each of the two cases below, show that the linear code C over $\mathbb{F}_q$ with parity-check matrix H is MDS, where $\mathbb{F}_q = \{0, a_1, a_2, \ldots, a_{q-1}\}$ and
(a)

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_{q-1} \\ a_1^2 & a_2^2 & \alpha_3^2 & \cdots & a_{q-1}^2 \\ \vdots & \vdots & \vdots & & \vdots \\ a_1^{r-1} & a_2^{r-1} & a_3^{r-1} & \cdots & a_{q-1}^{r-1} \end{bmatrix} , \quad 1 \le r \le q - 2 ;$$

(b)

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 0 \\ a_1 & a_2 & a_3 & \cdots & a_{q-1} & 0 & 0 \\ a_1^2 & a_2^2 & \alpha_3^2 & \cdots & a_{q-1}^2 & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \vdots & 0 & 0 \\ a_1^{r-1} & a_2^{r-1} & a_3^{r-1} & \cdots & a_{q-1}^{r-1} & 0 & 1 \end{bmatrix} , \quad 1 \le r \le q - 1 .$$

6.14. Let C be the code over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ (where $\alpha^2 = 1 + \alpha$) with parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & 0 & 1 & 0 \\ 1 & \alpha^2 & \alpha & 0 & 0 & 1 \end{bmatrix} .$$

Show that C is a MDS code.
Try to generalize this example, or justify that it can not be done, to obtain a code over an arbitrary field $\mathbb{F}_q$, with length $q + 2$ and redundancy $3 \le r \le q - 1$.

6.15. Let C be an MDS code with parameters $[n, k, d]_q$. Show that
(i) $q^2 - 1$ is the number of code words in C with weight d or $d + 1$ with nonzero entries in $d + 1$ fixed coordinators;
(ii) $\binom{d+1}{d}(q - 1)$ is the number of words with weight d with nonzero entries in $d + 1$ fixed coordinators.
Conclude that the number of code words in C with weight $d + 1$ is

$$A_{d+1} = \binom{n}{d+1}\left((q^2 - 1) - \binom{d+1}{d}(q - 1)\right) .$$

6.16. Find A_d and A_{d+1} for a code C with the following parameters:
(a) $[n, n - 1, 2]_2$;
(b) $[n, n - 1, 2]_3$;
(c) $[4, 2, 3]_3$.
Give an example of a code for each of the previous cases.

6.17. (a) Find all MDS $[n, k, d]_q$-codos with $d = n$.
(b) If $d < n$, show that thare no MDS $[n, k, d]_q$-codes with $d > q$.
Suggestion: use Proposition 6.29.

Chapter 7

7.1. Prove Lemma 7.12: Let $x, y \in \mathbb{F}_q^n$ and show that
(a) $\mathrm{w}(x-y) \geq \mathrm{w}(x) - \mathrm{w}(y)$;
(b) $\mathrm{d}(x,y) = \mathrm{w}(x) - \mathrm{w}(y)$ if and only if x covers y.

7.2. Consider the vector space $V = \mathbb{F}_q^3$.
(a) Show that V contains $\frac{q^3-1}{q-1} = q^2+q+1$ 1-dimentional vector subspaces.
(b) Show that V contains $\frac{q^3-1}{q-1} = q^2+q+1$ 2-dimentional vector subspaces.
(c) Let $\mathcal{P}$ be the set of 1-dimentional vector subspaces and let $\mathcal{B}$ be the set of 2-dimentional vector subspaces. Show that $\mathcal{P}$ (as the set of points) and $\mathcal{B}$ (as the set of blocks), with the relation $P \in \mathcal{P}$ belongs to $B \in \mathcal{B}$ if P is a subspace of B, define a Steiner system $S(2, q+1, q^2+q+1)$.
Remark: Since the number of points and the number of blocks are the same, this Steiner system is called a 2-dimentional projective geometry (or a projective plane) of order q, and it is denoted by $PG(2,q)$ or $PG_2(q)$.

7.3. From the extended Golay code G_{24}, construct a Steiner system $S(5,8,24)$.

7.4. (Generalization of the previous exercise.) Let C be a binary perfect code with length n and minimum distance $2t+1$. Show that there is a Steiner system $S(t+2, 2t+2, n+1)$.

7.5. Show that a q-ary Hamming code $\mathrm{Ham}(r,q)$ contains

$$A_3 = \frac{q(q^r-1)(q^{r-1}-1)}{6}$$

words with weight 3.

7.6. How many words with weight 7 are there in G_{23}?

7.7. How many words with weight 5 are there in G_{11}?

7.8. For any code C, we define *weight enumerator polynomial*[3] by

$$W_C(t) = \sum_{i \geq 0} A_i t^i \ , \quad \text{where} \quad A_i = \#\{x \in C \ : \ \mathrm{w}(x) = i\} \ .$$

If C is a binary code, with length n, show that
(a) $W_{C'}(t) = \frac{1}{2}\big(W_C(t) + W_C(-t)\big)$, where $C' = \{x \in C \ : \ \mathrm{w}(x) \text{ is even}\}$;
(b) $W_{\widehat{C}}(t) = \frac{1}{2}\big((1+t)W_C(t) + (1-t)W_C(-t)\big)$, where $\widehat{C}$ is the parity extension of C.

7.9. Write the wight enumerator polynomial for the code C when
(a) $C = \widehat{\mathrm{Ham}}(3,2)$;
(b) $C = G_{24}$ [suggestion: show that $\vec{1} \in G_{24}$];
(c) $C = G_{23}$.

7.10. (a) Let $C \subset \mathbb{F}_2^8$ be a self-dual linear code. Find all possible weight enumerator polynomials for C. Give an example of a self-dual code for each of the polynomials you found. Suggestion: Exercise 4.4.
(b) Show that, if C and C' are self-dual binary codes with length 8 and have equal weight enumerator polynomials, then C and C' equivalent codes.

7.11. Let p be a prime number and let $\zeta \in \mathbb{C}$ be a primitive p-th root of the identity, i.e., $\zeta^p = 1$ and $\zeta^i \neq 1$ for $1 \leq i \leq p-1$. Given any function $f\colon \mathbb{F}_p^n \to V$, where V is a complex vector space, define $\widehat{f}\colon \mathbb{F}_p^n \to V$ by[4]

$$\widehat{f}(x) = \sum_{y \in \mathbb{F}_p^n} f(y) \zeta^{x \cdot y} \ ,$$

[3]Note that the polynomial $W_C(t)$ is just the generating function of the sequence $\{A_i\}_{i \in \mathbb{N}_0}$

[4]In this exercise, we identify a class in $\mathbb{F}_p = \mathbb{Z}_p$ with the corresponding representative between 0 and $p-1$.

where $x \cdot y$ denots the euclidean inner product in $\mathbb{F}_p^n$. Let $C \subset \mathbb{F}_p^n$ be a linear code.

(a) Define $C_i(y) = \{x \in C \,:\, x \cdot y = i\}$, for $y \in \mathbb{F}_p^n$ and $i \in \mathbb{F}_p$. Show that $C = \cup_{i \in \mathbb{F}_p} C_i(y)$. Show that $C_i(y)$ is a $C_0(y)$-class in C if and only if $y \notin C^\perp$, that is, show that

$$\Big(\forall i \in \mathbb{F}_p \quad \exists c_i \in C \quad \text{s.t.} \quad C_i(y) = c_i + C_0(y)\Big) \Longleftrightarrow y \notin C^\perp \ .$$

(b) Show that

$$\sum_{x \in C} \zeta^{x \cdot y} = \begin{cases} |C| & \text{if } y \in C^\perp, \\ 0 & \text{if } y \notin C^\perp. \end{cases}$$

(c) Show that, for $y \in \mathbb{F}_p^n$,

$$f(y) = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} \widehat{f}(x) \zeta^{-x \cdot y} \ .$$

(d) Show that

$$\sum_{y \in C^\perp} f(y) = \frac{1}{|C|} \sum_{x \in C} \widehat{f}(x) \ .$$

(e) Let $f(y) = t^{\mathrm{w}(y)} \in \mathbb{C}[t]$. Show that, for $x \in \mathbb{F}_p^n$,

$$\widehat{f}(x) = \big(1 + (p-1)t\big)^{n - \mathrm{w}(x)} (1 - t)^{\mathrm{w}(x)} \ .$$

(f) Prove the *MacWilliams' Identity*[5] for the weight enumerator polynomial for C and its dual $C^\perp$:

$$W_{C^\perp}(t) = \frac{1}{|C|} \big(1 + (p-1)t\big)^n W_C\Big(\frac{1 - t}{1 + (p-1)t}\Big) \ .$$

(g) Write the weight enumerator polynomial for $\mathrm{Ham}(r, p)$.
Suggestion: Recall taht $\mathrm{Ham}(r, p) = S(r, p)^\perp$ and write $W_{S(r,p)}(t)$.

[5]The MacWilliams' Identity holds for any fieald $\mathbb{F}_q$, with q not necessary a prime numeber. See S. Roman's book for a proof in the general case. R. Hill does only the proof for the binary case.

Chapter 8

8.1. (a) Show that the *cyclic shift* map $\sigma : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ defined by

$$\sigma(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$$

is a bijective linear function.

(b) Show that the code C is cyclic if and only if $\sigma^i(C) = C$ for all $i \in \mathbb{Z}$.

8.2. (a) Show that $\langle 2, t\rangle$ is not a principal ideal in $\mathbb{Z}[t]$.

(b) Show that $\langle x, y\rangle$ is not a principal ideal in the ring of two variable polynomials[6] $\mathbb{F}_q[x, y]$.

8.3. For a fixed $a \in \mathbb{F}_q$, show that the set $I = \{f(t) \in \mathbb{F}_q[t] \ : \ f(a) = 0\}$ is an ideal in $\mathbb{F}_q[t]$. Determine a generator for I.

8.4. The ideals in the following questions are ideals in the ring $R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle$. Assuming that $g(t)|t^n - 1$ in $\mathbb{F}_q[t]$, show that

(a) $\langle f_1(t)\rangle \subset \langle f_2(t)\rangle$ if and only if $f_2(t)$ divides $f_1(t)$ in R_n;

(b) $\langle f(t)\rangle = \langle g(t)\rangle$ if and only if there exists $a(t) \in \mathbb{F}_q[t]$ such that $f(t) \equiv a(t)g(t) \pmod{t^n - 1}$ and $\gcd(a(t), h(t)) = 1$, where $h(t)g(t) = t^n - 1$;

8.5. Factor $t^7 - 1$ in $\mathbb{F}_2[t]$ and identify all cyclic binary codes with length 7.

8.6. Classify all cyclic codes with length 4 over $\mathbb{F}_3$. Conclude that the ternary Hamming code $\mathrm{Ham}(2, 3)$ is not equivalent to a cyclic code.

8.7. (a) Write $t^{12} - 1$ as a product of irredduble polynomials in $\mathbb{F}_2[t]$.

(b) How many binary cyclic codes of length 12 are there?

(c) Determine the integers k for wihch there is a binary $[12, k]$ cyclic code.

(d) How many binary $[12, 9]$ cyclic codes are there?

(e) Determine all binary self-dual cyclic codes with length 12, write the generator polynomial for those codes.

8.8. Let C be a binary cyclic code with generator polynomial $g(t)$.

(a) Show that, if $t - 1$ divides $g(t)$, then all code words have even weight.

(b) Assuming that C has odd length, show that C contains a word with odd weight if and only if the vector $\vec{1} = (1, \ldots, 1)$ is a code word.

8.9. (a) Determine the generator polynomial and the dimention of the smallest binary cyclic code which contains the word $c = 1110010 \in \mathbb{F}_2^7$.

(b) Write a generating matrix, the check polinomial and the parity-check matrix for the code your code in part (a).

8.10. Determine the generator polynomial and the dimention of the smallest ternary cyclic code which contains the word $c = 220211010000 \in \mathbb{F}_3^{12}$.

8.11. Let C be a cyclic code, with length n, with generator polynomial $g(t)$. Show that, if $C = \langle f(t)\rangle$, i.e., if $f(t)$ is a generator for the ideal C, then $g(t) = \gcd(f(t), t^n - 1)$. In particular, conclude that the generator polynomial of the smallest cyclic code, with length n, containing $f(t)$ is $g(t) = \gcd(f(t), t^n - 1)$.

8.12. If $g(t)$ is the generator polynomial of a cyclic code, show that $\langle g(t)\rangle$ and $\langle \bar{g}(t)\rangle$ are equivalent codes. Conclude that the code generated by the check polynomial of a cyclic code C is equivalent to the dual code $C^{\perp}$.

8.13. Suppose that, in $\mathbb{F}_2[t]$,

$$t^n - 1 = (t - 1)g_1(t)g_2(t)$$

and that $\langle g_1(t)\rangle$ and $\langle g_2(t)\rangle$ are equivalent codes. Show that:

(a) If $c(t)$ is a code word in $\langle g_1(t)\rangle$ with odd weight w, then

(i) $w^2 \geq n$;

(ii) If, moreover, $g_2(t) = \overline{g}_1(t)$, then $w^2 - w + 1 \geq n$.

[6]This holds in $\mathbb{K}[x, y]$, with $\mathbb{K}$ any field.

(b) If n is an odd prime number, $g_2(t) = \overline{g}_1(t)$ and $c(t)$ is a code word in $\langle g_1(t) \rangle$ with even weight w, then
   (i) $w \equiv 0 \pmod 4$;
   (ii) $n \neq 7 \Rightarrow w \neq 4$.

(c) Show that the binary cyclic code with length 23 generated by the polynomial $g(t) = 1 + t^2 + t^4 + t^5 + t^6 + t^{10} + t^{11}$ is a perfect code $[23, 12, 7]$ – *the binary Golay Code*.

8.14. (a) Let $g(t)$ be the generator polynomial of a binary Hamming code $\text{Ham}(r, 2)$, with $r \geq 3$. Show that the parameter of $C = \langle (t-1)g(t) \rangle$ are $[2^r - 1, 2^r - r - 2, 4]$.
Suggestion: apply exercise 8.8.
(b) Show that the code C can be used to correct all adjacent double errors.
(c) (Generalization of the previous part.) Let $C = \langle (t+1)f(t) \rangle$ be a binary cyclic code with length n, where $f(t) \mid t^n - 1$, but $f(t) \nmid t^k - 1$, for $1 \leq k \leq n-1$. Show that C corrects all simple errors and also the adjacent double errors.

8.15. Consider binary cyclic code with length $n = 15$ generated by the polynomial

$$g(t) = 1 + t^4 + t^6 + t^7 + t^8 \ .$$

(a) Justify that $g(t)$ is indeed the generator polynomial of this code.
(b) Write a generator matrix, the check polynomial and a parity-check matrix for this code.
(c) Write a generator matrix in the form $G = \begin{bmatrix} R & I \end{bmatrix}$ for this code and the corresponding parity-check matrix.
Suggestion: use equation (8.5) (and Theorem 8.37) to determine the rows of R.
(d) Use systematic coding to encode the message vector $m = 1001001$.
(e) Given that this code has minimum distance $d(C) = 5$, decode the received vectors

$$y = 000101011110000 \qquad \text{and} \qquad z = 011001001001111 \ .$$

8.16. (a) Verify that $g(t) = 2 + t^2 + 2t^3 + t^4 + t^5$ divides $t^{11} - 1$ in $\mathbb{F}_3[t]$.
(b) Let C be the ternary cyclic code generated by $g(t)$. Knowing that it is a $[11, 6, 5]_3$ code, use the Error Trapping Algorithm to decode the received vector $y = 20121020112$.
(c) What is the proportion of errors with weight 2 which are corrected by this algorithm?

8.17. Consider again the binary cyclic with length $n = 15$ with generator polynomial $g(t) = 1 + t^4 + t^6 + t^7 + t^8$ as in Exercise 8.15.
(a) Verify that, althougth this is a code with minimum distance 5, it corrects up to burst 3-errors.
(b) Decode the received vector $y = 100000110111110$ using the Burst-Error Trapping Algorithm.

8.18. (a) Let C be a cyclic $[n, k, d]_q$-code qith generator polynomial $g(t)$. Since C is also a linear code, the number of linearly independent columns in a parity-check matrix guarantees that syndrome decoding, for C, corrects all erasure errors up to $d - 1$ symbols. Using now the cyclic property of the code and the Error Trapping Algorithm, what type of erasure errors can C correct? Consider not only the number of deleted symbols but also its distribution in the received word.
(b) Considere again the binary cyclic code with length $n = 15$ and with generator polynomial $g(t) = 1 + t^4 + t^6 + t^7 + t^8$ as in Exercise 8.15. The minimum distance of this code is $d = 5$. Decode, if possible, the following received vectors

$$y = 000??????111000 \qquad \text{and} \qquad z = ?0101?0101?0000 \ .$$

8.19. Let C be the cyclic code over $\mathbb{F}_5$ with length 15 and with the following generator polynomial

$$g(t) = 1 + 3t + t^2 + 2t^3 + t^4 + 3t^5 + t^6 \in \mathbb{F}_5[t] \ .$$

(a) How many cyclic codes, over $\mathbb{F}_5$, with length 15 and with the same dimension as C are there? Write the generator polynomial for those codes.

(b) Given that C corrects all l-burst errors with $l \leq 3$, decode the received vector

$$y = 042201213100000 \in \mathbb{F}_5^{15} \ ,$$

using the Burst Error Trapping Algorithm.

(c) Given that only erasure errors occured, correct, if possible, the following received vectors

$$z = ?20?04031000000 \qquad \text{and} \qquad w = 0000?0000?0000?$$

Suggestion: check that the syndrome of $S(t^{10}) = 4t^5 + 4$ is t^{10} .

8.20. Show that the interleaved code of degree s, $C^{(s)}$, is equivalent to the sum code $C \oplus \cdots \oplus C$ of s copies of C. Conclude that $\mathrm{d}(C^{(s)}) = \mathrm{d}(C)$.

8.21. Finish the proof of Theorem 8.57 (a): Let C be a q-ary linear code and let $x^{(s)}$ and $y^{(s)}$ be the vectors obtained by interleaving $x_1, \ldots, x_s \in C$ and $y_1, \ldots, y_s \in C$, respectively. Show that

(i) $x^{(s)} + y^{(s)}$ is the result of interleaving the vectors $x_1 + y_1, \ldots, x_s + y_s$;

(ii) $ax^{(s)}$ is the result of interleaving the vectors $ax_1, \ldots, ax_s$, where $a \in \mathbb{F}_q$.

8.22. Let $C = \mathrm{Ham}(3, 2)$ be the binary Hamming code with redundancy 3 and generator polynomial $g(t) = 1 + t + t^3$.

(a) Find the parameters $[n, k, d]$ of $C^{(3)}$.

(b) Find the generator polynomial and the parity-check polynomial of $C^{(3)}$.

(c) Show that $C^{(3)}$ corrects all m-burst errors with $m \leq 3$, but it does not correct all 4-burst errors.

(d) Using the Burst Error Trapping Algorithm, decode the following received vector

$$y(t) = t + t^3 + t^4 + t^9 + t^{13} \ .$$

8.23. A q-ary cyclic code, with length n, is called *degenerate* if there is $r \in \mathbb{N}$ such that r divides n and each code word is of the form $c = c'c' \cdots c'$ with $c' \in \mathbb{F}_q^r$, i.e., each code word consists of n/r identical copies of a sequence c' with length r.

(a) Show that the interleaved code $C^{(s)}$ of a repetition code C is degenerate.

(b) Show that the generator polynomial of a degenerate cyclic code with lenth n is of the form

$$g(t) = a(t)(1 + t^r + t^{2r} + \cdots + t^{n-r}) \ .$$

(c) Show that a cyclic code with lenght n and check polymonial $h(t)$ is degenerate if and only if there is $r \in \mathbb{N}$ such that r divides n and $h(t)$ divides $t^r - 1$.

8.24. Let C be the binary linear code with the following parity-check matrix

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

(a) Find the minimum distance $\mathrm{d}(C)$, and determine the code capacity for detecting and correcting random errors.

(b) Show that C detects all m-burst errors with $m \leq 3$.
Remark: In this exercise, we consider only m-burst errors in the "strict sense", i.e., vectors in the form $(0, \ldots, 0, 1, *, \ldots, *, 1, 0, \ldots, 0)$ where all nonzero coordenates have indices between $i \geq 1$ and $i + m - 1 \leq n$.

(c) Let C' be the punctured code, in the last coordinate, of the dual code $C^\perp$. Show that C' is a degenerate cyclic code, and determine its generator polynomial.

8.25. Determine all degenerate, cyclic and binary codes with length 9, writing the generator polynomials and the corresponding r-sequences.

8.26. Consider the linear code $A = \langle (1, \alpha^2, 0), (\alpha, 0, 1) \rangle$ over $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, where $\alpha^2 = 1 + \alpha$, and the binary linear code $B = \langle 1010, 0101 \rangle$. Let A^* be the concatenation of A and B with respect to the linear function $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^4$ defined by $\phi(1) = 1010$ and $\phi(\alpha) = 1111$.

(a) Write a basis for the code A^*.

(b) Find the parameters $[n, k, d]$ for the code A^*.

8.27. Let $C = \langle(0, \alpha, \alpha^2, 1), (1, 1, 1, 1)\rangle \subset \mathbb{F}_4^4$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 = 1 + \alpha$.

(a) Find a generating matrix and the parameters for the concatenation code $C^* = \phi^*(C)$, where $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^2$ is the linear map over $\mathbb{F}_2$ defined by $\phi(1) = 10$ and $\phi(\alpha) = 01$.

(b) Justify that the code C^* is equivalent to $\widehat{\text{Ham}}(3, 2)^\perp$.

8.28. Let $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where α is a root of $1 + t^2 + t^3 \in \mathbb{F}_2[t]$, and consider the linear code over $\mathbb{F}_8$

$$A = \langle(\alpha + 1, \alpha^2 + 1, 1)\rangle \ .$$

(a) Consider the map $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ defined by $\phi(a_1 + a_2\alpha + a_3\alpha^2) = (a_1, a_2, a_3)$, where $a_1, a_2, a_3 \in \mathbb{F}_2$. What are the parameters of $A^*\phi^*(A)$?

(b) Consider the map $\psi : \mathbb{F}_8 \to \mathbb{F}_2^4$ defined by $\phi(a_1 + a_2\alpha + a_3\alpha^2) = (a_1, a_2, a_3, a_1 + a_2 + a_3)$, where $a_1, a_2, a_3 \in \mathbb{F}_2$. What are the parameters of $A' = \psi^*(A)$? Suggestion: A' is the concatenation of A with a binary code B; identify B.

(c) What can you conclude about the capacity of A^* e de A' for correcting randon and/or burst errors?

8.29. Let C be the repetition code with length n over $\mathbb{F}_{q^m}$ and let C^* be the concatenation of C with the q-ary trivial code $(\mathbb{F}_q)^m$. Show that C^* is a cyclic q-ary code and find its parameters $[N, K, D]$.

Chapter 9

9.1. Write a generator matrix and a parity-check matrix for a Reed-Solomon code $[6, 4]$, and determine its minimum distance.

9.2. Determine the generator polynomial of a Reed-Solomon over $\mathbb{F}_{16}$ with dimention 11. Write a parity-check matrix for that code.

9.3. Show that the dual of a Reed-Solomon code is a Reed-Solomon code.

9.4. Let C be the Reed-Solomon code over $\mathbb{F}_8$ with generator polynomial $g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)$, where $\alpha \in \mathbb{F}_8$ is a root of $1 + t + t^3$.
(a) Justify that α is a primitive element in $\mathbb{F}_8$.
(b) Find the parameters of C.
(c) Find the parameters of the dual code $C^\perp$.
(d) Find the parameters of the extended code $\widehat{C}$.
(e) Find the parameters of the concatenation code $C^* = \phi^*(C)$, where $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ is the linear map defined by $\phi(1) = 100$, $\phi(\alpha) = 010$ and $\phi(\alpha^2) = 101$.

9.5. Consider the Reed-Solomon code C over $\mathbb{F}_8$ with the following generator polynomial:

$$g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)(t-\alpha^4) = \alpha^3 + \alpha t + t^2 + \alpha^3 t^3 + t^4 \ ,$$

where we identify $\mathbb{F}_8$ with the quotient $\mathbb{F}_2[t]/\langle 1 + t + t^3 \rangle$, and $\alpha \in \mathbb{F}_8$ is a root of $1 + t + t^3$.
(a) Find the parameters $[n, k, d]$ of C.
(b) Apply the Error Trapping Algorithm to decode the following received vectors

$$y = (0, 1, 0, \alpha^2, 0, 0, 0) \quad \text{and} \quad z = (0, \alpha^3, 0, 1, \alpha^3, 1, 1).$$

(c) Let $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ be a linear isomorphism over $\mathbb{F}_2$. What can you say about the capacity of the concatenation code $C^* = \phi^*(C)$ for correcting burst errors?

9.6. Consider the linear code over $\mathbb{F}_{11}$ with gerating matrix

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

(a) Show that this code is equivalent to a cyclic code C.
(b) Determine the generator polymonial and conclude that C is a Reed-Solomon code.

9.7. (Generalization of the previous exercise.) Let C be a $[q-1, k]$ code, over $\mathbb{F}_q$, with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \alpha^{3(k-1)} & \cdots & \alpha^{(q-2)(k-1)} \end{bmatrix} ,$$

where α is a primitive element in $\mathbb{F}_q$ and $1 \leq k \leq q-2$.
(a) Show that C is a cyclic code.
(b) Determine the generator polynomial and conclude that C is a Reed-Solomon code.

9.8. Let $C \subset \mathbb{F}_5^4$ be the cyclic code with generator polynomial $g(t) = (t-2)(t-4)$.
(a) Justify that C is a Reed-Solomon code and find its parameters.
(b) Find the parameters and a generating matrix for the extension $\widehat{C}$.
(c) Let $\widetilde{C}$ be a cyclic code with length 5 and dimension 2. Write a generating matrix for $\widetilde{C}$ and show that this code is linearly equivalent to $\widehat{C}$.
(d) Conclude that any nonzero cyclic code with length 5 over $\mathbb{F}_5$ is MDS.

9.9. Recall that a linear code C is *self-orthogonal* if $C \subset C^\perp$. Determine the generator polynomial of all self-orthogonal Reed-Solomon codes over $\mathbb{F}_{16}$. Which of these codes are self-dual?

Appendix A

A.1. Prove the Inclusion-Exclusion Principle by induction on the number of the sets E_i, $1 \leq i \leq r$.

A.2. How many integers between 1 and 1000 are not divisible by 2, 3 or 5, but are divisible by 7?

A.3. How many permutations of $\{a, b, c, \ldots, x, y, z\}$ do not contain the words *sim*, *riso*, *mal* and *cabe*?

A.4. How many integer solutions to $x_1 + x_2 + x_3 + x_4 = 21$ are there if:
(a) $x_i \geq 0$, $i = 1, 2, 3, 4$;
(b) $0 \leq x_i \leq 8$, $i = 1, 2, 3, 4$;
(c) $0 \leq x_1 \leq 5$, $0 \leq x_2 \leq 6$, $3 \leq x_3 \leq 8$, $4 \leq x_4 \leq 9$.

A.5. Determine the number of monic polynomials of degree n in $\mathbb{F}_q[t]$ without roots in $\mathbb{F}_q$, where $\mathbb{F}_q$ is a field with q elements.

A.6. (a) How many integers n between 1 and 15000 satisfy $\gcd(n, 15000) = 1$?
(b) How many integers n between 1 and 15000 have a common prime divisor with 15000?

A.7. Compute $\phi(n)$ and $\mu(n)$ for: (i) 51, (ii) 82, (iii) 200, (iv) 420 and (v) 21000.

A.8. Find all positive integers $n \in \mathbb{N}$ such that
(a) $\phi(n)$ is odd;
(b) $\phi(n)$ is a power of 2;
(c) $\phi(n)$ is a multiple of 4.

A.9. Show that $\phi(n^m) = n^{m-1}\phi(n)$, for $n, m \in \mathbb{N}$.

A.10. Prove the following properties of the Euler function:
(i) if p is prime, then $\phi(p) = p - 1$ and $\phi(p^k) = p^k - p^{k-1}$;
(ii) if $n = ab$ with $\gcd(a, b) = 1$, then $\phi(n) = \phi(a)\phi(b)$.
And use them to show that

$$\phi(n) = n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} + \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right),$$

where $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, with $p_1, \ldots, p_r$ distinct prime numbers and $e_i \geq 1$.

A.11. Write the power series for $\dfrac{1}{1 - ax}$, $a \neq 0$, that is, compute the inverse of $1 - ax$ in the ring $\mathbb{Z}[[x]]$ (or in $\mathbb{R}[[x]]$).

A.12. Use formal derivatives and induction to show that

$$\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{k-1+n}{n} x^n, \qquad \text{for all } k \in \mathbb{N}.$$

A.13. A die is rolled 12 times. What is the probability that the sum is 30?

A.14. Zé wants to buy n blue, red or white marbles (the shop has a large stock in each color). In how many ways can Zé choose n marbles so that he buys an even number in blue?

A.15. Ana, Bernardo, Carla and David organized a barbeque and bought 12 steaks and 16 sardines. In how many ways can they share the steaks and sardines if:
(a) Each of them gets at least a steak and two sardines.
(b) Bernardo gets at least a steak and three sardines, and each of the other friends gets at least two steaks but no more than five sardines.

A.16. Let $f_0(x)$ be the generating function for the sequence $1, 1, 1, \ldots$ and, for $k \geq 1$, let $f_k(x)$ be the generating function for $0^k, 1^k, 2^k, 3^k, \ldots$. We have already shown that $f_0(x) = \frac{1}{1-x}$. Now show that

$$f_k(x) = x\big(f_{k-1}(x)\big)' \qquad \text{for } k \geq 1.$$

Write the functions f_1, f_2 and f_3 explicitly.

A.17. Show that $\log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \frac{x^n}{n}$.

A.18. Using generating functions, solve the following recurrence relation:

$$\begin{cases} a_0 = 1, \\ a_1 = 2, \\ a_n = 2a_{n-2}, \quad n \geq 2. \end{cases}$$

A.19. Using generating function, find the general term of the Fibonacci sequence

$$\begin{cases} a_0 = a_1 = 1, \\ a_n = a_{n-1} + a_{n-2}, \quad \text{for } n \geq 2 \ . \end{cases}$$

A.20. Let d_n be the determinant of the following $n \times n$ $(n \geq 1)$ matrix

$$A_n = \begin{bmatrix} 2 & -1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 2 & -1 & 0 & & & 0 \\ 0 & -1 & 2 & \ddots & \ddots & & \vdots \\ 0 & 0 & \ddots & \ddots & \ddots & 0 & 0 \\ \vdots & & \ddots & \ddots & 2 & -1 & 0 \\ 0 & & & 0 & -1 & 2 & -1 \\ 0 & 0 & \cdots & 0 & 0 & -1 & 2 \end{bmatrix} .$$

Find a recurrence relation for d_n and solve it.

A.21. Repeat the previous exercise for the matrix obtained from A_n
(a) replacing 2 by 3, and -1 by $\sqrt{2}$;
(b) replacing 2 by 0 and keeping the -1 entries.

A.22. Find a recurrence relation for $s_n = \sum_{i=0}^{n} i^2$ and solve it.

A.23. An *order k homogeneous linear recurrence relation with constant coeficients* is of the form

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0 \quad (n \geq k) \ ,$$

where $c_0, c_1, \ldots, c_k \in \mathbb{R}$ are constants, and $c_0 \neq 0$. The *characteristic polynomial* of the recurrence relation is defined by

$$p(x) = c_0 x^k + c_1 x^{k-1} + \cdots + c_{k-1} x + c_k \ \in \mathbb{R}[x],$$

and its roots are called *characteristic roots*. Assume that $c_k \neq 0$, i.e., 0 is not a characteristic root.

(a) Show that the general solution of a first order recurrence relation is $a_n = a_0 r^n$, $n \geq 0$, where $r = -\frac{c_1}{c_0}$, i.e., r is the root of the associated characteristic polynomial.

(b) Study the homogeneous quadratic (of second order) case by proving the following statements:

(i) If the characteristic roots r_1 and r_2 are real and distinct, then the general solution is

$$a_n = A(r_1)^n + B(r_2)^n \ ,$$

where $A, B \in \mathbb{R}$ are constants, i.e., $(r_1)^n$ and $(r_2)^n$ are two linearly independent solutions.

(ii) If there is only one characteristic root $r \in \mathbb{R}$ (of multiplicity 2), then the general solution is

$$a_n = Ar^n + Bnr^n \ ,$$

where $A, B \in \mathbb{R}$ are constants.

(iii) If there are two complex roots $r_1, r_2 \in \mathbb{C}$, then r_1 and r_2 are complex conjugates and the general solution is

$$a_n = A(r_1)^n + B(r_2)^n \ ,$$

where $A, B \in \mathbb{C}$ are constants (as in the real case). Show also that, if $a_0, a_1 \in \mathbb{R}$, then A and B are complex conjugates and $a_n \in \mathbb{R}$, for all $n \geq 0$.
[Sugestion: recall that any $z \in \mathbb{C} \setminus \{0\}$ can be written as $z = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta))$ and $(\cos(\theta) + i\,\mathrm{sen}(\theta))^n = \cos(n\theta) + i\,\mathrm{sen}(n\theta)$.]

(c) Generalize part (b) for relations of order k:

(i) Show that, if $r \in \mathbb{R}$ is a characteristic root with multiplicity m, then it contributes with

$$a_n^{(r)} = A_0 r^n + A_1 n r^n + A_2 n^2 r^n + \cdots + A_{m-1} n^{m-1} r^n \ ,$$

for the general solution, where $A_0, A_1, \ldots, A_{m-1} \in \mathbb{R}$ are constants.

(ii) If $r \in \mathbb{C}$ is a complex characteristic root with multiplicity m, what is the contribution of r and of its conjugate $\bar{r}$ to the general solution?

A.24. Using the previous exercise, solve the following recurrence relations:

(a) $a_n = 2a_{n-1} + 3a_{n-2}$, $n \geq 2$, and $a_0 = 3$, $a_1 = 5$;
(b) $4a_n - 4a_{n-1} + a_{n-2} = 0$, $n \geq 2$, and $a_0 = 5$, $a_1 = 4$;
(c) $a_n - 2a_{n-1} + 2a_{n-2} = 0$, $n \geq 2$, and $a_0 = a_1 = 4$;
(d) $a_n = a_{n-1} + 5a_{n-2} + 3a_{n-3}$, $n \geq 3$, and $a_0 = a_1 = 3$, $a_2 = 7$.

A.25. Show that the expression (A.9) obtained for $I(q, n)$ is always positive, that is, show that for $q \geq 2$ and $n \geq 1$, we have

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d > 0 \ .$$

(We don't need the existence of a finite field with q elements.)

Appendix B

B.1. Determine the q-cyclotomic classes modulo n in the following cases:
(a) $q = 2$, $n = 9$;
(b) $q = 3$, $n = 13$.

B.2. Given $n \in \mathbb{N}$ such that $\gcd(n, q) = 1$, show that there exists $m \in \mathbb{N}$ such that $n \mid q^m - 1$.

B.3. Find the irreducible polymonial factorization of $t^n - 1$ in the following cases:
(a) $t^{q-1} - 1$ in $\mathbb{F}_q[t]$;
(b) $t^q - 1$ in $\mathbb{F}_q[t]$;
(c) $t^8 - 1$ in $\mathbb{F}_3[t]$;
(d) $t^{13} - 1$ in $\mathbb{F}_3[t]$.

B.4. Show that $t^{q^n-1} - 1$ divides $t^{q^m-1} - 1$ in $\mathbb{F}_q[t]$ if and only if $n \mid m$.
Suggestion: Solve fisrt Exercise 3.15.

B.5. (a) Determine the 9-cyclotomic classes modulo 10.
(b) Find the number of cyclic codes over $\mathbb{F}_9$, with length 10 and dimension 7.