This assignment consists of two pages.

1. The International Standard Book Number (ISBN) system, used to uniquely identify books, is a non-binary code defined over the 11-letter alphabet \( \{0, 1, 2, \ldots, 9, X\} \), where \( X \) represents the number 10. An ISBN codeword, \( c_1c_2 \ldots c_{10} \), is ten digits in length. The first nine digits are “information digits” that record data such as publisher, title and edition. The tenth digit is a check digit, chosen so that

\[
\sum_{i=1}^{10} i \cdot c_i \equiv 0 \pmod{11}
\]

(a) In this application, the common types of error are digits being wrong, and transpositions, in which some two digits, \( c_i \) and \( c_j \), are interchanged. Analyze the error detection/correction capability of the ISBN code against these types of errors.

(b) Does the ISBN code \( \mathcal{C} = \{ (c_2, c_2, \ldots, c_{10}) \in \mathbb{F}_{11}^{10} : \sum_{i=1}^{10} i c_i \equiv 0 \pmod{11} \} \) form a vector space over \( \mathbb{F}_{11} \)? Justify your answer.

2. A \( k \)-bit message is to be transmitted across a memoryless binary symmetric channel with probability of error \( p = 0.1 \). The error-protection scheme used is an \( r \)-fold repetition code, in which each message bit is repeated \( r \) times before transmission, and a majority rule is used for decoding at the channel output. Given a value of \( k \), let \( r(k) \) denote the minimum value of \( r \) for which the probability that the entire \( k \)-bit message will be received and decoded correctly is at least 0.999.

(a) Determine \( r(1) \), \( r(2) \) and \( r(3) \).

(b) Show that \( r(k) \) is a non-decreasing function of \( k \), i.e., \( k_1 \leq k_2 \Rightarrow r(k_1) \leq r(k_2) \).

(c) Show that \( r(k) \) is unbounded, i.e., there is no real number \( R \) such that \( r(k) \leq R \) for all \( k \).

This problem shows that repetition codes are poor coding schemes. Note that \( \frac{1}{r(k)} \) denotes the coding rate required to ensure a 99.9\% chance of successful transmission of a \( k \)-bit message using a repetition code. Parts (b) and (c) of the problem show that \( \lim_{k \to \infty} r(k) = \infty \). Thus, the coding rate must go to zero as the length of the message increases, to maintain reliable transmission.

3. Let \( \mathcal{C} \) be a block code with minimum distance \( d \), and let \( \rho, \tau \) be non-negative integers such that \( 2\tau + \rho \leq d - 1 \). Specify a decoder for \( \mathcal{C} \) that can correct every error-cum-erasure pattern that contains at most \( \tau \) errors along with at most \( \rho \) erasures.

4. Let \( \overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\} \), where \( \mathbb{R} \) denotes the set of real numbers, and let \( \min \) denote the minimum operation: \( \min(a, b) \) is the minimum of \( a \) and \( b \) for all \( a, b \in \overline{\mathbb{R}} \), with the convention that \( \min(a, \infty) = \min(\infty, a) = a \) for all \( a \in \mathbb{R} \). Also, let \( + \) denote the usual addition operation in \( \mathbb{R} \), extended to \( \overline{\mathbb{R}} \) by defining \( a + \infty = \infty + a = \infty \) for all \( a \in \mathbb{R} \).
(a) Recall that an operation ‘·’ is said to be distributive over an operation ‘+’ if 
\(a \cdot (b + c) = a \cdot b + a \cdot c\) and 
\((b + c) \cdot a = b \cdot a + c \cdot a\) hold for all \(a, b, c\). Verify that in \(\mathbb{R}\), the ‘+’ operation is distributive over min.

(b) Is \((\mathbb{R}, \text{min}, +)\) a commutative ring?
[Note that with respect to our usual ring notation of \((R, +, \cdot)\), the role of the ‘+’ operation on \(R\) is played by the min operation on \(\mathbb{R}\), and the role of the ‘·’ operation on \(R\) is played by the ‘+’ operation on \(\mathbb{R}\).]

5. Find the multiplicative inverse of 200 in the field \(\mathbb{F}_{2011}\). [Yes, 2011 is prime.]

6. (a) Let \((\mathbb{F}, +, \cdot)\) be a field. Show that if \(a \cdot b = 0\) for some \(a, b \in \mathbb{F}\), then either \(a = 0\) or \(b = 0\) (or both).

(b) Let us equip \(\mathbb{R}^2\) with the following addition and multiplication operations:
\[
(a, b) + (c, d) = (a + c, b + d) \quad \text{and} \quad (a, b) \cdot (c, d) = (ac, bd),
\]
where \(a + b, ab\) etc. are the usual addition and multiplication operations in \(\mathbb{R}\). Verify that \(\mathbb{R}^2\) equipped with these operations is a commutative ring with unity. Is it a field?