Exercise 1 (Quizz). Answer the questions. You should justify your answers.

(1) Which of these codes do exist? If they do not, explain why, if they do, explain how they can be constructed.

(a) A $[32, 16, 17]$ Reed–Solomon code over $\mathbb{F}_{32}$;

Answer : Exists. Over $\mathbb{F}_q$, there exists $[n, k, n-k+1]$ RS codes for any $n \leq q$ and any $k \leq n$.

(b) A $[32, 15, 18]$ Generalised Reed-Solomon code over $\mathbb{F}_{19}$;

Answer : Does not exist since the length should be less than or equal to the size of the field.

(c) A $[7, 5, 3]$ binary code;

Answer : Does not exist, since it doesn’t satisfy the Hamming bound.

(d) A $[64, 34, \geq 6]$ alternant code over $\mathbb{F}_2$.


(2) Which of these statements is true?

(a) There is no $[n, k, d]$ code such that $d > n - k + 1$;

Answer : True, Singleton bound.

(b) For all $\epsilon > 0$, for any sequence of binary codes whose relative distance sequence converges to $\delta$ and rate converges to $R$ we have $R \geq 1 - H_2(\delta) - \epsilon$.

Answer : False, not every sequence of codes approaches Gilbert Varshamov bound.

(c) No $[n, k, d]_q$ linear code satisfies $q^k \text{Vol}_q(d, n) \geq q^n$

(where $\text{Vol}_q(d, n)$ denotes the number of elements in a Hamming ball of radius $d$ in $\mathbb{F}_q^n$).

Answer : False, Gilbert Varshamov bound asserts that such a code exists.
(d) There exists an \([n, k, d]\) code over \(\mathbb{F}_q\) such that
\[
d \leq nq^{k-1}\frac{q-1}{q^k-1}.
\]

**Answer**: True, actually, any code does, since it should satisfy Plotkin bound.

(3) How many binary cyclic codes of length 8 do there exist?

**Answer**: We need to compute the number of divisors of \(x^8 - 1 = (x - 1)^8\). This polynomial has 9 divisors : \((x - 1)^i, i \in \{0, \ldots, 8\}\). Hence, there is 9 such codes.

(4) Suppose that one has a list decoding algorithm for any \([32, 20, 11]\) Reed-Solomon code over \(\mathbb{F}_{32}\) correcting up to 10 errors.

(a) Deduce the existence of a list decoder correcting up to 10 errors for any \([32, k]\) Reed-Solomon code with \(k < 20\).

**Answer**: One can apply the decoder to any subcode of the \([32, 20]\) RS code. In particular to any sub–Reed–Solomon code.

(b) For which values of \(k\) can one make sure the decoding is unique?

**Answer**: As soon as 10 is less than half the minimum distance, i.e. as soon as the minimum distance exceeds 21. Equivalently, this decoding is unique for any \(k \leq 12\).

**Exercise 2. Cyclic codes.** You are allowed to skip any question and assume its result to be true in the subsequent questions.

Let \(n\) be an odd integer. Let \(C \subseteq \mathbb{F}_2^n\) be a linear cyclic code of dimension \(k\). Let \(T\) be the corresponding cyclotomic class in \(\mathbb{Z}/n\mathbb{Z}\) and \(g_C\) be the generating polynomial of \(C\).

(1) What is the cardinality of \(T\) ? the degree of \(g_C\)?

**Answer**: \(|T| = \deg g_C = n - k\).

(2) Let \(C'\) be the subset of \(C\) of all words of even weight.

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

**Answer**: It is the intersection of two binary linear codes : the code \(C\) and the parity code.

(b) What is its dimension?

**Answer**: Either \(C' = C\), or \(\dim C' = \dim C - 1\). Indeed, \(C'\) is the kernel of the linear form \(\mathbb{F}_2^n \rightarrow \mathbb{F}_2 \times \mathbb{F}_2 \rightarrow \mathbb{F}_2 \rightarrow \sum_{i=1}^n x_i\). Hence it is either equal to \(C\) or has codimension 1 in \(C\).

(c) Prove that \(C'\) is cyclic.

**Answer**: Both \(C\) and the parity code are cyclic. Hence their intersection is cyclic.
(d) Prove that the following conditions are equivalent:

(i) \( C = C' \);

(ii) \( 0 \in T \);

(iii) \( g_C(1) = 0 \).

**Answer:** Suppose (i); i.e. \( C = C' \), then \( C \) is contained in the parity code, hence for any \( m \in C \), we have \( m_0 + m_1 + \cdots + m_{n-1} = 0 \). Regarding \( m \in C \) as a polynomial, this is equivalent to \( m(1) = 0 \). Thus, \( (x - 1) \) divides any element of \( C \) (viewed as polynomials) and in particular, \( (x - 1) \) divides \( g_C \). Therefore, \( g_C(1) = 0 \). This proves (i) \( \Rightarrow \) (iii).

Clearly if (iii), i.e. if \( g_C(1) = 0 \), then \( 1 = \zeta^0 \) is a root of the code and hence \( 0 \in T \), which proves (iii) \( \Rightarrow \) (ii).

Finally, suppose (ii). Then \( 1 \) is a root of the code, hence any element \( m \) of \( C \) satisfies \( m(1) = m_0 + \cdots + m_{n-1} = 0 \). That is, \( m \) has even weight, which entails (i).

(e) If \( C \neq C' \) describe the generating polynomial of \( C' \) and its cyclotomic class.

**Answer:** \( g'_C = (x - 1)g_C \) and \( T_{C'} = T_C \cup \{0\} \).

(3) Prove that \( C \) contains the all-one codeword \((1, 1, \ldots, 1)\) if and only if \( 0 \notin T \).

**Answer:** First note that

\[
1 + x + \cdots + x^{n-1} = \prod_{i \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}} (x - \zeta^i).
\]

Therefore, if \( 0 \notin T \), then \( g_C(x) = \prod_{i \in T}(x - \zeta^i) \) divides \( 1 + x + \cdots + x^{n-1} \). Conversely, if \( 1 + x + \cdots + x^{n-1} \in C \), then \( 0 \) cannot be in \( T \).

(4) List the minimal 2 cyclotomic classes in \( \mathbb{Z}/21\mathbb{Z} \) (i.e. the smallest subsets stable by multiplication by 2).

**Answer:** \{0\}, \{1, 2, 4, 8, 16, 11\}, \{3, 6, 12\}, \{5, 10, 20, 19, 17, 13\}, \{7, 14\}, \{9, 18, 15\}.

(5) How many binary cyclic codes of length 21 do there exist?

**Answer:** There are 6 minimal cyclotomic classes, hence \( 2^6 = 64 \) cyclic codes.

(6) Prove the existence of a \([21, 12, \geq 5]\) binary cyclic code which contains the all-one codeword (you can use Question 3).

**Answer:** The BCH code associated to the cyclotomic class \( \{1, 2, 3, 4, 6, 8, 11, 12, 16\} \).

Let

\[
P_C(X, Y) = \sum_{i=0}^{21} p_i X^i Y^{n-i}
\]

be the weight enumerator of \( C \). That is, \( p_i \) is the number of words of weight \( i \) in \( C \).
(7) Prove that the weight enumerator of such a \([21, 12, 5]\) binary cyclic code is self reciprocal, i.e. \(P_C(X, Y) = P_C(Y, X)\). In particular, prove that there is no codeword of weight \(w \in \{17, \ldots, 20\}\).

**Answer:** Since the code contains the all-one codeword and is linear, it contains the complement of any code. Thus for any codeword \(c\) of weight \(w\) the code also contains the word \(c + (1 \ 1 \ldots \ 1)\) of weight \(21 - w\). Therefore, for any nonnegative integer \(w\), the number of codewords of weight \(w\) equals that of codewords of weight \(21 - w\). Hence the weight enumerator is self reciprocal. Finally, since, the minimum distance is at least 5 there is no codeword of weight 1, 2, 3, 4 and, by self-reciprocity, no codeword of weight 20, 19, 18, 17.

(8) Let
\[
\sigma : \begin{cases}
\mathbb{F}_q^{21} \\ (x_1, \ldots, x_n)
\end{cases} \rightarrow \begin{cases}
\mathbb{F}_q^{21} \\ (x_n, x_1, \ldots, x_{n-1})
\end{cases}
\]
be the cyclic shift. Prove that if \(c \in \mathbb{F}_q^{21}\) satisfies \(\sigma^\ell(c) = c\) for some \(\ell > 1\) and \(\sigma^j(c) \neq c\) for all \(1 \leq j < \ell\), then:

(a) \(\ell\) divides 21;

**Answer:** \(\sigma^\ell\) generates a subgroup of the group generated by \(\sigma\), namely, the stabilizer of \(c\). By Lagrange Theorem, \(\ell\) divides the order of \(\sigma\).

(b) \(\frac{21}{\ell}\) divides the weight of \(c\).

**Answer:** Let \(A \subseteq \{0, \ldots, 20\}\), be the support of \(c\), i.e. the set of indexes \(i\) such that \(c_i = 1\). The group generated by \(\sigma^\ell\) acts freely on \(A\), hence \(A\) is a disjoint union of orbits of this group and each orbit has cardinality the order of \(\sigma^\ell\) i.e. \(\ell\). Thus \(\ell\) divides the cardinality of \(A\), which equals the weight of \(c\).

(9) Prove that
(a) \(p_8, p_{10}, p_{11}, p_{13}\) are divisible by 21;

**Answer:** 8, 10, 11, 13 are prime to 21, hence no words of such weight have non trivial stabilizers. Thus, for any such word, its orbit under the action of \(\sigma\) has cardinality 21. Since the set of words of fixed weight is a disjoint union of orbits, we get the result.

(b) \(p_6, p_9, p_{12}, p_{15}\) are divisible by 3;

**Answer:** Such words may be stabilized by \(\sigma^7\), hence their orbit has cardinality either 21 or 3. Thus, any orbit has cardinality divisible by 3.

(c) \(p_7, p_{14}\) are divisible by 7.

**Answer:** Same reasoning.