Mathematics 342. Solutions to Midterm 1

Problem 1. Recall that an \((n, M, d)\)-code is a code of size \(M\), length \(n\) and minimal distance \(d\).

(a) Construct a binary \((3, 4, 2)\) code.

(b) Construct a binary \((5, 4, 3)\) code.

(c) Use parts (a) and (b) to construct a binary \((8, 4, 5)\) code.

(d) Show that \(A_2(8, 5) = 4\).

Solution: (a) Start with the binary code \(F_2^2\) containing every word of length 2:
\[
\{(0, 0), (0, 1), (1, 0), (1, 1)\}.
\]
Now add an overall parity check digit. The resulting code is
\[
C_1 = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}.
\]

(b) Use the code from Example 2.2 in the text
\[
C_2 = \{(0, 0, 0, 0, 0), (0, 1, 1, 0, 1), (1, 0, 1, 1, 0), (1, 1, 0, 1, 1)\}
\]
or create one by trial and error.

(c) Append the code in part (b) to the code in part (a):
\[
C_3 = \{(0, 0, 0, 0, 0, 0, 0, 0), (0, 1, 1, 0, 1, 1, 0, 1), (1, 0, 1, 1, 0, 1, 1, 0), (1, 1, 0, 1, 0, 1, 1, 1)\}
\]
Clearly \(d(C_3) \geq d(C_1) + d(C_2) = 2 + 3 = 5\). On the other hand, the distance between the first two codewords in \(C_3\) is 5. Thus \(d(C_3) = 5\).

Problem 2. Let \(d\) be an even integer, and \(2 \leq d \leq n\). Show that if there is a binary \((n, M, d)\) code \(C\), then there is a binary \((n, M, d)\)-code \(C'\) such that every word in \(C'\) has even weight. Explain how to construct \(C'\) from \(C\). [Recall that the weight of a codeword \(a = (a_1, \ldots, a_n)\) is the number of non-zero entries among \(a_1, \ldots, a_n\).]

Solution: Choose two words \(a\) and \(b\) in \(C\) at distance \(d\). Suppose \(a\) and \(b\) differ in position \(i\). Puncture \(C\) in position \(i\). Denote the resulting code by \(C_1\). As we showed in class, \(C_1\) is a binary \((n-1, M, d-1)\)-code.

Now add a parity check digit to every word in \(C_1\). Denote the resulting code by \(C'\). By construction every word in \(C'\) has even weight. As we showed in class, since \(d-1\) is odd, \(C'\) is a binary \((n, M, d)\)-code.

Problem 3. Find all integers \(x\) between 0 and 46 such that

(a) \(10x \equiv 9 \pmod{47}\),

(b) \(4x^2 \equiv 9 \pmod{47}\).

Solution: (a) Using the Euclidean algorithm and back substitution, we obtain
\[
10 \cdot (-14) + 47 \cdot 3 = 1.
\]
Reduce modulo 47: \((10)^{-1} \equiv -14 \pmod{47}\).

Now multiply both sides of the congruence \(10x \equiv 9 \pmod{47}\) by \((-1)^{-1}\):

\[ x \equiv 9 \cdot (-14) \equiv -126 \equiv -126 + (47 \cdot 3) \equiv 15 \pmod{47}. \]

Alternative solution of part (a): Note that \(10 \cdot 5 \equiv 50 \equiv 3 \pmod{47}\). Multiplying both sides by 3,
we obtain
\[ 10 \cdot 15 \equiv 9 \pmod{47}. \]

Since the congruence \(10x \equiv 9 \pmod{47}\) has a unique solution in \(\{0, 1, 2, \ldots, 46\}\) (why?), we conclude
that \(x = 15\).

(b) Rewrite \(4x^2 \equiv 9 \pmod{47}\) as \(4x^2 - 9 \equiv 0 \pmod{47}\) or equivalently,
\[ (2x - 3)(2x + 3) \equiv 0 \pmod{47}. \]

Since 47 is a prime, this reduces to \(2x \equiv 3 \pmod{47}\) or \(2x \equiv -3 \pmod{47}\). Now observe that \(2^{-1} \equiv 24 \pmod{47}\) (why?). Thus
\[ x \equiv 24 \times (\pm 3) = \pm 72. \] Reducing modulo 47, we obtain:
\[ x = 72 - 47 = 25 \] or
\[ x = -72 + 47 \cdot 2 = 94 - 72 = 22. \]

Problem 4. Let \(q \geq 2\) be a prime integer and let \(C\) be a perfect \(q\)-ary code of length \(n\). Show that
the size of \(C\) (i.e., the number of words in \(C\)) is \(q^k\) for some \(0 \leq k \leq n\).

Solution: By the definition of perfect code, \(M = \frac{q^n}{|B_t|}\), where \(M\) is the size of \(C\). In other words,
\(M \cdot |B_t| = q^n\), and \(M\) divides \(q^n\). Since \(q\) is a prime, the only positive divisors of \(q^n\) are integers of the
form \(q^k\), where \(1 \leq k \leq n\).

Problem 5. Let \(q = 5\) and consider the \(q\)-ary code \(C\) of length 5 consisting of all words \((a_1, a_2, \ldots, a_5)\)
satisfying
\[ a_1 + a_2 + a_3 + a_4 + a_5 \equiv 0 \pmod{5} \quad \text{and} \quad a_2 + 2a_3 + 3a_4 + 4a_5 \equiv 0 \pmod{5}. \]

Here \(a_1, \ldots, a_5\) are elements of the field \(F_5 = \mathbb{Z}_5\).

(a) (1 mark) How many words does \(C\) have?

(b) (2 marks) Prove that the minimal distance \(d(C)\) of this code is \(\leq 3\).

(c) (1 mark) Prove that \(d(C) = 3\).

Solution: (a) Every word \(a = (a_1, a_2, a_3, a_4, a_5)\) in \(C\) is uniquely determined by \(a_3, a_4, a_5\). Moreover,
these three digits can be chosen in an arbitrary manner in \(F_5\). Once \(a_3, a_4\) and \(a_5\) are chosen, \(a_2\) can
be uniquely recovered from the second equation, and then \(a_1\) can be recovered from the first. Thus the
number of words in \(C\) is the same as the number of triples \((a_3, a_4, a_5)\) in \(F_5^3\), i.e., \(5^3 = 125\).

(b) Create two words, \(a = (a_1, a_2, a_3, a_4, a_5)\) and \(b = (b_1, b_2, b_3, b_4, b_5)\) in \(C\) by setting \((a_3, a_4, a_5) = (0, 0, 0)\) and \((b_3, b_4, b_5) = (1, 0, 0)\). Since \(a\) and \(b\) agree in the last two positions, \(d(a, b) \leq 3\). Thus
\(d(C) \leq 3\).

Alternative proof of (b): Assume the contrary: \(d(C) \geq 4\). Then by the Singleton bound, \(|C| \leq 5^{5-4+1} = 25\), contradicting the answer in part (a).
(c) Assume the contrary: $d(\mathbf{a}, \mathbf{b}) \leq 2$ for some distinct words $\mathbf{a} = (a_1, \ldots, a_5)$ and $\mathbf{b} = (b_1, \ldots, b_5)$ in $C$. This means that $b_i = a_i + \epsilon_i$ and $b_j = a_j + \epsilon_j$ for some $i \neq j$ and $\epsilon_i, \epsilon_j \in F_5$, not both 0, while $b_k = a_k$ for every $k$ different from $i$ and $j$. Subtracting
\[ a_1 + a_2 + a_3 + a_4 + a_5 \equiv 0 \pmod{5} \]
from
\[ b_1 + b_2 + b_3 + b_4 + b_5 \equiv 0 \pmod{5} \]
we obtain
\[ \epsilon_i + \epsilon_j \equiv 0 \pmod{5}. \tag{1} \]
Using the second defining equation for $C$ in a similar manner, we obtain
\[ (i - 1)\epsilon_i + (j - 1)\epsilon_j \equiv 0 \pmod{5}. \tag{2} \]
Multiplying (1) by $i - 1$ and subtracting from (2), we obtain $(i - j)\epsilon_j = 0$. Since $i, j = 1, 2, \ldots, 5$ and $i \neq j$, we see that $i - j$ is non-zero, and hence, invertible modulo 5. Thus $\epsilon_j = 0$. Substituting $\epsilon_j = 0$ into (1), we obtain $\epsilon_j = 0$, a contradiction.