UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

4th set - Answers

Exercise 1. For the ternary code $C = \{00122, 12201, 20110, 22000\}$, use the nearest neighbor decoding rule to decode the following words:
(a) 01122, (b) 10021, (c) 22022, (d) 20120.

Answer. Name the codewords as follows: $c_1 = 00122$, $c_2 = 12201$, $c_3 = 20110$ and $c_4 = 22000$. Further, name $w_1 = 01122$, $w_2 = 10021$, $w_3 = 22022$ and $w_4 = 20120$. Notice that

$$d(w_1, c_1) = 1,\ d(w_1, c_2) = 5,\ d(w_1, c_3) = 4,\ d(w_1, c_4) = 5,$$

so, we decode w_1 to c_1. Next, we have that

$$d(w_2, c_1) = 3,\ d(w_2, c_2) = 3,\ d(w_2, c_3) = 4,\ d(w_2, c_4) = 4,$$

so, in the case of complete decoding we can decode w_2 either to c_1 or to c_2, whilst in the case of incomplete decoding we request a re-transmission. Next, we have that

$$d(w_3, c_1) = 3,\ d(w_3, c_2) = 4,\ d(w_3, c_3) = 4,\ d(w_3, c_4) = 2,$$

so, we decode w_3 to c_2. Finally,

$$d(w_4, c_1) = 2,\ d(w_4, c_2) = 5,\ d(w_4, c_3) = 1,\ d(w_4, c_4) = 3,$$

so, we decode w_4 to c_3. □

Exercise 2. Determine the number of binary $(n, 2, n)$-codes, for $n \geq 2$.

Answer. Let $C = \{c_1, c_2\}$ be a binary $(n, 2, n)$-code. By definition, $d(c_1, c_2) = n$, that is, c_1 and c_2 differ in all coordinates. This implies that $c_1 + c_2 = (1, \ldots, 1)$, i.e., c_2 is completely determined by c_1. It follows that we have 2^n choices for the ordered pair (c_1, c_2) and since the pair (c_1, c_2) and (c_2, c_1) yield the same set, we have $2^n/2 = 2^{n-1}$ choices for the code $C = \{c_1, c_2\}$. □

Exercise 3. Determine the number of binary $[n, n-1, 2]$-codes, for $n \geq 2$.

Answer. Let C be a binary $[n, n-1, 2]$-code. Let H be a parity check matrix of C. Because C is a $[n, n-1]$-code, H will be a $1 \times n$ matrix over $\mathbb{F}_2$. Moreover, because $d(C) > 1$, H cannot contain the zero column. It follows that

$$H = (1 \quad 1 \quad \cdots \quad 1),$$

that is, $C = \langle (1, \ldots, 1) \rangle^{\perp}$. In other words, we have exactly one such code. □

Exercise 4. Determine the number of q-ary $[n, k]$-codes, where $k \leq n$.

Answer. Let C be a q-ary $[n, k]$-code. We will first show that C has

$$\frac{1}{k!}\prod_{i=1}^{k}(q^k - q^{i-1})$$

different basis. Indeed, let $(c_1, \ldots, c_k)$ be such that $\{c_1, \ldots, c_k\}$ is a basis of C. Notice that we have $q^k - 1$ options for c_1 (that is, it has to be non-zero). Then, we have $q^k - q$ options for c_2 (that is, it has to be outside $\langle c_1 \rangle$). Similarly, we have $q^k - q^{i-1}$ options for c_i and so on. In total we have

$$\prod_{i=1}^{k}(q^k - q^{i-1})$$

options for $(c_1, \ldots, c_k)$. The result follows, since all the permutations of these items are counted as distinct k-tuples but yield the same basis.

Next, using similar arguments, one can see that we have

$$\frac{1}{k!}\prod_{i=1}^{k}(q^n - q^{i-1})$$

ways of choosing a set of k linearly independent elements of $\mathbb{F}_q^n$. Clearly, each such set produces an $[n, k]$-code, whilst the same code is produced by a number of such sets, as proven above. It follows that there are exactly

$$\frac{\frac{1}{k!}\prod_{i=1}^{k}(q^n - q^{i-1})}{\frac{1}{k!}\prod_{i=1}^{k}(q^k - q^{i-1})} = \prod_{i=0}^{k-1}\frac{q^n - q^i}{q^k - q^i}$$

q-ary $[n, k]$-codes. □

Exercise 5. Let C_i, $i = 1, 2$ be linear codes over $\mathbb{F}_q$ with parameters $[n_i, k_i, d_i]$ respectively. The direct sum $C_1 \oplus C_2$ is a subspace of $\mathbb{F}_q^{n_1+n_2}$. Show that $C_1 \oplus C_2$ is an $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$ linear code over $\mathbb{F}_q$.

Answer. Let $(a_1, b_1),\ (a_2, b_2) \in C_1 \oplus C_2$ and $\kappa, \lambda \in \mathbb{F}_q$, where $a_i \in C_1$ and $b_i \in C_2$. Then $\kappa(a_1, b_1) + \lambda(a_2, b_2) = (\kappa a_1 + \lambda a_2, \kappa b_1 + \lambda b_2) \in C_1 \oplus C_2$, since $\kappa a_1 + \lambda a_2 \in C_1$ and $\kappa b_1 + \lambda b_2 \in C_2$.

Clearly, $C_1 \oplus C_2$ has length $n_1 + n_2$. Also,

$$|C_1 \oplus C_2| = |C_1| \cdot |C_2| = q^{k_1} q^{k_2} = q^{k_1+k_2}.$$

It follows that $\dim(C_1 \oplus C_2) = k_1 + k_2$.

Finally, for the minimum distance, w.l.o.g. assume that $d_1 = \min\{d_1, d_2\}$. Take some $a \in C_1$, such that $\mathrm{wt}(a) = d_1$. Then $(a, \mathbf{0}) \in C_1 \oplus C_2$ (where $\mathbf{0} = (0, \ldots, 0)$) and

$$\mathrm{wt}((a, \mathbf{0})) = \mathrm{wt}(a) + \mathrm{wt}(\mathbf{0}) = d_1 + 0 = d_1,$$

hence $d(C_1 \oplus C_2) \leq d_1$. Also, take some $(a, b) \in C_1 \oplus C_2 \setminus \{\mathbf{0}\}$, then $\mathrm{wt}((a, b)) = \mathrm{wt}(a) + \mathrm{wt}(b)$ and:

- If $b \neq \mathbf{0}$, then $\mathrm{wt}((a, b)) = \mathrm{wt}(a) + \mathrm{wt}(b) \geq \mathrm{wt}(b) \geq d_2 \geq d_1$.
- If $b = \mathbf{0}$, then $a \neq \mathbf{0}$ and $\mathrm{wt}((a, \mathbf{0})) = \mathrm{wt}(a) + \mathrm{wt}(\mathbf{0}) = \mathrm{wt}(a) \geq d_1$.

In any case, $\mathrm{wt}((a, b)) \geq d_1$, which implies $d(C_1 \oplus C_2) \geq d_1$. The result follows. □

Exercise 6. Let C be a binary $[n, k, d]$-code, such that C contains at least one codeword of odd weight. Let

$$C' := \{c \in C \ : \ \mathrm{wt}(c) \text{ even}\}.$$

Show that C' is a binary $[n, k-1, d']$-code, where $d' > d$, if d is odd, and $d' = d$, if d is even.

Answer. First, we will show that C' is, in fact, a linear code. Let $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ be two elements of $\mathbb{F}_2^n$. Define

$$x \star y = (z_1, \dots, z_n), \tag{1}$$

where

$$z_i = \begin{cases} 1, & \text{if } x_i = y_i = 1, \\ 0, & \text{otherwise.} \end{cases}$$

It is now trivial to check that

$$\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\mathrm{wt}(x \star y). \tag{2}$$

The latter implies that C' is closed under addition, hence (since we are over $\mathbb{F}_2$) it is a linear code.

Clearly C' has length n. About the dimension, it suffices to show that C' contains exactly half of the codewords of C. Define

$$C'' = \{c \in C \ : \ \mathrm{wt}(c) \text{ is odd}\}.$$

Clearly $C' \cup C'' = C$ and $C' \cap C'' = \emptyset$, in other words, it suffices to show that $|C'| = |C''|$. The statement implies that $C'' \neq \emptyset$. Take some $w \in C''$ and set

$$\phi : C' \to C'', \ x \mapsto x + w.$$

Equation (2) implies that ϕ is well-defined, while it is trivial to check that it is a bijection. It follows that $|C'| = |C''|$.

Finally, we move our attention to the minimum distance. Since C' is a subcode of C, $d' \geq d$. However, by definition, the codewords of C of weight d are codewords of C' if and only if d is even. The desired result follows. □

Exercise 7.
1. Show that every codeword in a self-orthogonal binary code has even weight.
2. Show that every codeword in a self-orthogonal ternary code has weight divisible by 3.
3. Let x, y be codewords of a self-orthogonal binary code, such that both $\mathrm{wt}(x)$ and $\mathrm{wt}(y)$ are divisible by 4. Show that $4 \mid \mathrm{wt}(x+y)$.

Answer.
1. Take $w = (w_1, \dots, w_n)$ be a codeword of a self-orthogonal binary code. The *support* of some $x \in \mathbb{F}_{q^n}$ consists of the non-zero coordinates of x and is denoted as $\mathrm{supp}(x)$. Assume that $\mathrm{supp}(w) = \{w_{s_1}, \dots, w_{s_\ell}\}$. Clearly, $\mathrm{wt}(w) = |\mathrm{supp}(w)| = \ell$ and $w_{s_j} = 1$ for $1 \le j \le \ell$. We have that

$$w \cdot w = 0 \iff \sum_{i=1}^{n} w_i^2 = 0 \iff \sum_{j=1}^{\ell} w_{s_j}^2 = 0 \iff \ell = 0 \text{ (in } \mathbb{F}_2).$$

   The result follows.

2. Take $w = (w_1, \dots, w_n)$ be a codeword of a self-orthogonal ternary code. Assume that $\mathrm{supp}(w) = \{w_{s_1}, \dots, w_{s_\ell}\}$. Clearly, $\mathrm{wt}(w) = |\mathrm{supp}(w)| = \ell$ and $w_{s_j} = \pm 1 \iff w_{s_j}^2 = 1$ for $1 \le j \le \ell$. We have that

$$w \cdot w = 0 \iff \sum_{i=1}^{n} w_i^2 = 0 \iff \sum_{j=1}^{\ell} w_{s_j}^2 = 0 \iff \ell = 0 \text{ (in } \mathbb{F}_3).$$

   The result follows.

3. Since the code is self-orthogonal, we have that

$$x \cdot y = 0 \iff \mathrm{wt}(x \star y) = 0 \text{ (in } \mathbb{F}_2),$$

   where $x \star y$ as defined in (1). It follows that $\mathrm{wt}(x \star y)$ is even. Now, (2) implies that $4 \mid \mathrm{wt}(x+y)$. □

Exercise 8. Let C be a self-dual binary $[n, k, d]$-code.

1. Show that $(1, 1, \dots, 1) \in C$.
2. Show that either all the codewords of C have weight divisible by 4, or exactly half of them have weight divisible by 4.
3. Suppose $n = 6$. Determine d.

Answer.
1. For every $w \in C$, we have that

$$(1, \dots, 1) \cdot w = w \cdot w = 0,$$

   that is $(1 \dots, 1) \in C^{\perp}$. The result follows from the fact that $C = C^{\perp}$.

2. Suppose that C contains some $w \in C$, such that $4 \nmid \mathrm{wt}(w)$. Set

$$C' = \{c \in C \ : \ 4 \mid \mathrm{wt}(c)\} \text{ and } C'' = \{c \in C \ : \ 4 \nmid \mathrm{wt}(c)\}.$$

   For our purposes, since clearly $C' \cup C'' = C$ and $C' \cap C'' = \emptyset$, it suffices to show that $|C'| = |C''|$. Let

$$\phi : C' \to C'',\ x \mapsto x + w.$$

   Equation (2) implies that ϕ is well-defined and it is clearly a bijection. The result follows.

3. From the previous items, we have that d has to be even, i.e., $d = 2, 4$ or 6. Moreover, since C is a binary self-dual code of length 6, we have that $k = \dim(C) = 6/2 = 3$, that is, C has $q^k = 8$ codewords.

   Clearly, $d \neq 6$, since in this case C can only contain the all-zero and all-one words. Next, assume that $d = 4$. Then C contains some c of weight 4. Also, from the first item, $(1, \ldots, 1) \in C$, that is, $c' = (1, \ldots, 1) + c \in C$. However, $\mathrm{wt}(c') = 2$, a contradiction. It follows that $d = 2$. □