MAS309 Coding Theory: Sheet 1

Please send comments and corrections to `M.Jerrum@qmul.ac.uk`.
Put solutions in the orange box on the ground floor by 17:00 on Monday, 21st January.

1. Consider the following ternary code (i.e., code over the alphabet $\mathbb{A} = \{\mathtt{0}, \mathtt{1}, \mathtt{2}\}$) of length 7:

   $$\mathcal{C} = \{\mathtt{0000000}, \mathtt{0111112}, \mathtt{1012221}, \mathtt{1220111}, \mathtt{2122012}, \mathtt{2201210}\}.$$

   The code $\mathcal{C}$ has minimum distance 4.

   (a) Suppose $x \in \mathcal{C}$ is a codeword, and $z \in \mathbb{A}^7$ a word obtained from x by changing 4 symbols. Demonstrate that $\mathcal{C}$ is not 4-error-detecting by finding x and z as above, such that a recipient of z cannot tell from examining z that errors have been introduced. [2]

   (b) Now suppose $x \in \mathcal{C}$ is a codeword, and $z \in \mathbb{A}^7$ a word obtained from x by changing 2 symbols. Demonstrate that $\mathcal{C}$ is not 2-error-correcting by finding x and z as above, such that a recipient of z cannot with certainty determine the codeword x just from examining z. Exhibit two possible decodings of z. [3]

2. Given q, let A be the alphabet $\{\mathtt{0}, \mathtt{1}, \ldots, q-1\}$. In each of the following cases find three words a, b, c in $\mathbb{A}^n$ satisfying $d(a,b) = d_1$, $d(a,c) = d_2$, $d(b,c) = d_3$, or prove that no such words exist. For example, with $q = 2$, $n = 3$, $d_1 = d_2 = d_3 = 2$, we could take $a = \mathtt{000}$, $b = \mathtt{011}$, $c = \mathtt{110}$.

   (a) $q = 3$, $n = 5$, $d_1 = 3$, $d_2 = 4$, $d_3 = 4$. [1]

   (b) $q = 3$, $n = 9$, $d_1 = 3$, $d_2 = 4$, $d_3 = 4$. [1]

   (c) $q = 2$, $n = 9$, $d_1 = 3$, $d_2 = 4$, $d_3 = 4$. [2]

   (d) $q = 2$, $n = 6$, $d_1 = 4$, $d_2 = 4$, $d_3 = 4$. [1]

   (e) $q = 3$, $n = 6$, $d_1 = 2$, $d_2 = 1$, $d_3 = 4$. [2]

   (f) $q = 2$, $n = 5$, $d_1 = 4$, $d_2 = 4$, $d_3 = 4$. [2]

   [9]

3. Let $\mathbb{A} = \{\mathtt{A}, \mathtt{B}, \mathtt{C}\}$, and let

   $$\mathcal{C} = \{\mathtt{AAC}, \mathtt{ABC}, \mathtt{ACB}, \mathtt{BCB}\}$$

   and

   $$\mathcal{D} = \{\mathtt{AAB}, \mathtt{ABB}, \mathtt{BAA}, \mathtt{BAC}\}.$$

   Show that the codes $\mathcal{C}$ and $\mathcal{D}$ are equivalent.

   (Hint: Find the right permutation of positions first. It is unique!) [6]

   Find the minimum distances of $\mathcal{C}$ and $\mathcal{D}$ and verify that they are equal. [1]

4. Suppose $\mathbb{A} = \{\mathtt{0}, \mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}\}$, and that v and w are words of length 3 over $\mathbb{A}$ with $d(v,w) = 2$. Let $\mathcal{C} = \{v, w\}$. Prove that $\mathcal{C}$ is equivalent to the code $\{\mathtt{000}, \mathtt{011}\}$. [4]

Solutions

1. (a) By inspection we find that codewords 0111112 and 2122012 are distance 4 apart. (They are the unique such pair.) So choose $x = \texttt{0111112}$ and $z = \texttt{2122012}$ (or vice versa). We cannot tell from looking at z whether it is a corrupted version of 0111112 or an uncorrupted 2122012.

   (b) Let $x = \texttt{0111112}$ as before, and let z be one of the six words that are distance 2 from both 0111112 and 2122012, say, $z = \texttt{0112012}$. We cannot tell from looking at z whether it is a corrupted version of 0111112 or of 2122012.

2. (a) Yes. E.g., $a = \texttt{00000}, b = \texttt{00111}, c = \texttt{02222}$.

   (b) Yes. E.g., just pad out (a): $a = \texttt{000000000}, b = \texttt{000000111}, c = \texttt{000002222}$.

   (c) No. Let S be the set of positions where a and b differ, and let T be the set of positions where a and c differ. Then b and c differ in positions $S \oplus T$, where $\oplus$ denotes symmetric difference. But $|S \oplus T| = |S| + |T| - 2|S \cap T|$ is odd, since $|S|$ is odd and $|T|$ is even. Contradiction.

   (d) Yes. E.g., double up the illustrative example from the question: $a = \texttt{000000}, b = \texttt{001111}, c = \texttt{111100}$.

   (e) No. Violates the triangle inequality, since $4 = d(b, c) > d(b, a) + d(a, c) = 3$.

   (f) No. Let S and T be as before. Then (since there are only two symbols available) b and c agree on positions in $S \cap T$. Now $|S \cup T| \leqslant |\{1, 2, 3, 4, 5\}| = 5$, so

$$|S \cap T| = |S| + |T| - |S \cup T| \geqslant 4 + 4 - 5 = 3.$$

   Thus b and c agree in at least 3 places, and $d(b, c) \leqslant 5 - 3 = 2$.

3. Following the hint, we find first the appropriate permutation of positions, which is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

   This is forced by simple considerations: (a) the 1st position of $\mathcal{C}$ and the 2nd of $\mathcal{D}$ are the only ones in which two symbols spit $3 : 1$ (in both cases, there are three As and one Bs) so $\sigma(2) = 1$; (b) the 2nd position of $\mathcal{C}$ and the 3rd of $\mathcal{D}$ are the only ones in which all three symbols occur, so $\sigma(3) = 2$; (c) then necessarily $\sigma(1) = 3$. Observe that

$$\mathcal{C}_\sigma = \{\texttt{CAA}, \texttt{CAB}, \texttt{BAC}, \texttt{BBC}\}.$$

   For the permutations of alphabet symbols it is easiest to begin with the 1st position. The singleton B must map to the singleton B, and A to A so the permutation we need to apply in the 2nd position is the identity.

Consider the word $\mathtt{BBC}$ in $\mathcal{C}_\sigma$. It must map to some word of the form $*\mathtt{B}*$ in $\mathcal{D}$, and $\mathtt{ABB}$ is the only possibility. Thus the permutation we need to apply to the 1st position of $\mathcal{C}_\sigma$ must map $\mathtt{B}$ to $\mathtt{A}$ and hence, by elimination, $\mathtt{C}$ to $\mathtt{B}$. I.e., we need to apply the permutation

$$f = \begin{pmatrix} \mathtt{A} & \mathtt{B} & \mathtt{C} \\ \mathtt{C} & \mathtt{A} & \mathtt{B} \end{pmatrix}.$$

Finally, it is now easy to check that two permutations are possible for 3rd position: either

$$g = \begin{pmatrix} \mathtt{A} & \mathtt{B} & \mathtt{C} \\ \mathtt{A} & \mathtt{C} & \mathtt{B} \end{pmatrix} \qquad \text{or} \qquad g = \begin{pmatrix} \mathtt{A} & \mathtt{B} & \mathtt{C} \\ \mathtt{C} & \mathtt{A} & \mathtt{B} \end{pmatrix}.$$

So $\mathcal{C}$ and $\mathcal{D}$ are equivalent, and, explicitly, $\mathcal{D} = ((\mathcal{C}_\sigma)_{f,1})_{g,3}$.

By inspection, the minimum distance of both $\mathcal{C}$ and $\mathcal{D}$ is 2.

4. From lecture notes, we know that $\mathcal{C}$ is equivalent to a code $\mathcal{C}'$ containing the word $\mathtt{000}$, and since equivalence preserves size and minimum distance of codes, we have

$$\mathcal{C}' = \{\mathtt{000}, v\}$$

where $v = \mathtt{0}ab$, $a\mathtt{0}b$ or $ab\mathtt{0}$. for some $a, b \neq \mathtt{0}$. In the second case, set

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

and replace $\mathcal{C}'$ with $\mathcal{C}'_\sigma = \{\mathtt{000}, \mathtt{0}ab\}$. In the third case, do the same with

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

So in any case, $\mathcal{C}$ is equivalent to the code $\mathcal{C}'' = \{\mathtt{000}, \mathtt{0}ab\}$. Now take a permutation f of A such that $f(\mathtt{0}) = \mathtt{0}$ and $f(a) = \mathtt{1}$ (for example, $f(a) = 1, f(\mathtt{1}) = a, f(x) = x$ for all other x). Also take a permutation g that treats b analogously. Then $\mathcal{C}$ is equivalent to $(\{\mathtt{000}, \mathtt{0}ab\}_{f,2})_{g,3} = \{\mathtt{000}, \mathtt{011}\}$.