## MAS309 Coding Theory: Sheet 5

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 3rd March.

1. Prove that there is exactly one $[4,2,3]$-code over $\mathbb{F}_{3}$, up to equivalence.
(Hint: We know that any code is equivalent to a code with a generator matrix $G$ in standard form. There are a limited number of possibilities for the four "free entries" of $G$. Show that the possible choices are equivalent under operations MO4 and MO5.)
2. 

$$
G_{1}=\left(\begin{array}{lllllll}
1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}\right) \quad \text { and } \quad G_{2}=\left(\begin{array}{lllllll}
1 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}\right)
$$

are generator matrices for two binary $[7,3,4]$-codes $\mathcal{C}$ and $\mathcal{D}$ over $\mathbb{F}_{2}$. Prove that $\mathcal{C}$ and $\mathcal{D}$ are are equivalent.
(Hint: one matrix operation suffices!)
3. (a) Suppose $\mathcal{C}$ and $\mathcal{D}$ are two equivalent linear codes of length $n$ over $\mathbb{F}_{q}$. Prove that the maximum weight of any codeword in $\mathcal{C}$ is equal to the maximum weight of any codeword in $\mathcal{D}$, i.e., $\max \{\operatorname{weight}(x): x \in \mathcal{C}\}=\max \{\operatorname{weight}(x): x \in \mathcal{D}\}$, where weight $(x)$ is the Hamming weight of $x$.
(b)

$$
G_{1}=\left(\begin{array}{lllllll}
1 & 0 & 0 & 1 & 1 & 0 & 0
\end{array}\right) \quad \text { and } \quad G_{2}=\left(\begin{array}{lllllll}
1 & 0 & 0 & 1 & 1 & 1 & 0 \tag{3}
\end{array}\right)
$$

are generator matrices for two binary $[8,3,4]$-codes $\mathcal{C}$ and $\mathcal{D}$ over $\mathbb{F}_{2}$. Prove that $\mathcal{C}$ and $\mathcal{D}$ are not equivalent.
4. (a) Construct a Slepian array for the ternary repetition code $\{000,111,222\}$ of length 3 .
(b) Use the array from part (a) to decode the received word 121.
(c) Let us say that two Slepian arrays for a code are equivalent if the first column of the first array is the same as the first column of the second, up to reordering. (Alternatively, the coset leaders are the same in both arrays.) How many distinct Slepian arrays are there, up to equivalence, for the ternary repetition code of length 3? Justify your answer.
(d) Discuss the consequence of non-uniqueness of the Slepian array for decoding a received word $x$. Illustrate your answer with reference to the word $x=012$.

## Solutions

1. Suppose $\mathcal{C}$ is any $[4,2,3]$-code. Consider a generator matrix $G$ in standard form for some code $\mathcal{C}^{\prime}$ that is equivalent to to $\mathcal{C}$. We know such exists by Corollary 4.14. The matrix $G$ looks like this:

$$
G=\binom{10 w x}{01 y z}
$$

Since $\mathcal{C}^{\prime}$ is a linear code with minimum distance 3, all of its codewords have at least 3 non-zero entries. The same goes for the rows of $G$, so $w, x, y, z \in\{1,2\}$.
If $w=2$ then multiply column 3 of $G$ by 2 (MO5); similarly, if $x=2$ then multiply column 4 of $G$ by 2 . We obtain a matrix

$$
G^{\prime}=\left(\begin{array}{ll}
101 & 1 \\
01 & y^{\prime} z^{\prime}
\end{array}\right) .
$$

It is easily checked that $y^{\prime}=z^{\prime}=1$ or $y^{\prime}=z^{\prime}=2$ would lead to a code of minimum distance at most 2 , so these possibilities can be eliminated. The only remaining possibilities are $y^{\prime}=1$ and $z^{\prime}=2$, or $y^{\prime}=2$ and $z^{\prime}=1$. In the latter case, transpose columns 3 and 4 . In either case, we reach the matrix

$$
G^{\prime \prime}=\binom{1011}{0112}
$$

But $\mathcal{C}$ was an arbitrary ternary $[4,2,3]$-code. So any ternary $[4,2,3]$-code is equivalent to the code generated by matrix $G^{\prime \prime}$, and hence to any other $[4,2,3]$-code.
2. Let $\sigma$ be the permutation

$$
\sigma=\left(\begin{array}{lllllll}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
1 & 2 & 4 & 7 & 3 & 5 & 6
\end{array}\right)
$$

Then $\mathcal{D}=\mathcal{C}_{\sigma}$.
3. (a) Let $w=\max \{\operatorname{weight}(x): x \in \mathcal{C}\}$ and suppose $v \in \mathcal{C}$ is a codeword with weight $(v)=$ $w$. Suppose $\sigma$ is a permutation of positions $\{1,2, \ldots, n\}, a \in \mathbb{F}_{q} \backslash\{0\}$ a non-zero field element, and $i \in\{1,2, \ldots, n\}$ a position. I claim that both OP1 $\left(v \mapsto v_{\sigma}\right)$ and OP2 ${ }^{\prime}\left(v \mapsto v_{a, i}\right)$ preserve Hamming weight.
For OP1,

$$
\operatorname{weight}\left(v_{\sigma}\right)=\left|\left\{i: v_{\sigma(i)} \neq 0\right\}\right|=\left|\left\{i: v_{i} \neq 0\right\}\right|=\operatorname{weight}(v),
$$

since $\sigma$ is a permutation. And for $\mathrm{OP}^{\prime}$,

$$
\text { weight } \begin{aligned}
\left(v_{a, i}\right) & =\left|\left\{j:\left(v_{j} \neq 0 \wedge j \neq i\right) \vee\left(a v_{j} \neq 0 \wedge j=i\right)\right\}\right| \\
& =\left|\left\{j: v_{j} \neq 0\right\}\right|=\operatorname{weight}(v),
\end{aligned}
$$

since $a \neq 0$. Thus any code obtained from $\mathcal{C}$ by any sequence of OP1 and OP2' will contain a codeword of Hamming weight $w$. A similar argument with the roles of $\mathcal{C}$ and $\mathcal{D}$ reversed completes the proof.
(b) Adding the three rows of $G_{1}$ we see that $11111111 \in \mathcal{C}$. So the maximum weight codeword in $\mathcal{C}$ has weight 8 . On the other hand, $11111111 \notin \mathcal{D}$, so the maximum weight codeword in $\mathcal{D}$ has weight strictly less that 8 (in fact 6 ). (This is easy to see, as $G_{2}$ has been presented in standard form.)
4. (a)

$$
\left(\begin{array}{lll}
000 & 111 & 222 \\
001 & 112 & 220 \\
002 & 110 & 221 \\
010 & 121 & 202 \\
020 & 101 & 212 \\
100 & 211 & 022 \\
200 & 011 & 122 \\
012 & 120 & 201 \\
021 & 102 & 210
\end{array}\right) .
$$

(The first row is the code, and is fixed, apart from the order of 111 and 222. The first column contains the coset leaders; these are uniquely defined apart from the last two, 012 and 021. In the final two cosets, any element can be chosen as the leader.)
(b) Find 121 in the table: it is in the fourth row and second column. Travel up the column to find the codeword 111: this is the required decoding.
(c) See the parenthetical remark at the end of the solution to Part (a). All coset leaders are uniquely defined except the last two. In these two cosets the coset leader can be chosen arbitrarily. The two choices are independent, yielding $3 \times 3=9$ distinct Slepian arrays.
(d) Each choice of coset leader yields a different decoding: 012 (as in the Slepian array as given) yields 000, 120 yields 222, and 201 yields 111 . Each of these is nearestneighbour, and hence equally good.

