Information and Coding Theory (review sheet)

Instructors: Mahdi Cheraghchi, Herbert Wiklicky

Autumn 2017, Imperial College London

30 November 2017

Exercise 1. Let $\mathcal{C}$ be an $[n, k]$ Reed-Solomon code over GF(q) for $q = n > 2$ (that is, the evaluation set consists of all elements in GF(q)). Assume q is prime. Show that $\mathcal{C}^\perp$ is an $[n, n-k]$ Reed-Solomon code over GF(q).

Hint: You may use the fact that

$$\sum_{k=1}^{q} \alpha_k^m = \sum_{k=1}^{q} \alpha_k$$

for all $0 \leq m \leq q-2$, where GF$(q) = \{\alpha_1, \ldots, \alpha_q\}$

Model answer. Recall that the $(i+1)$-th row of the generator matrix of an $[n, k]$ Reed-Solomon code over GF(q) for $q = n$ is $(\alpha_1^i, \alpha_2^i, \ldots, \alpha_n^i)$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the distinct elements of GF(n).

In order to prove the desired statement, it suffices to show that the inner product between $(\alpha_1^i, \alpha_2^i, \ldots, \alpha_n^i)$ and $(\alpha_1^j, \alpha_2^j, \ldots, \alpha_n^j)$ for $0 \leq i \leq k-1$ and $0 \leq j \leq n-k-1$ is 0. We have

$$(\alpha_1^i, \alpha_2^i, \ldots, \alpha_n^i) \cdot (\alpha_1^j, \alpha_2^j, \ldots, \alpha_n^j)^\top = \sum_{k=1}^{n} \alpha_k^{i+j}.$$

Observe that $0 \leq i + j \leq n-2$ always. As a result, we have that

$$\sum_{k=1}^{n} \alpha_k^{i+j} = \sum_{k=1}^{n} \alpha_k.$$

We know that

$$\sum_{k=1}^{n} \alpha_k = \sum_{k=0}^{n-1} k \equiv \frac{n(n+1)}{2} - n.$$

Since $n = q > 2$ is prime, it holds that $n+1$ is even, and so the right hand side is divisible by n. We conclude that $\sum_{k=1}^{q} \alpha_k = 0$ in GF(n), which concludes the proof.

Exercise 2. Show that the RM$(1, m)$ code over GF(2) contains the all-zeros codeword $(0, \ldots, 0)$, the all-ones codeword $(1, \ldots, 1)$, and exactly $2^{m+1} - 2$ codewords of weight exactly 2^{m-1}.

Model answer. Since RM$(1, m)$ is a linear code, it follows that the all-zeros vector is a codeword. The all-ones vector is a codeword because it is the first row of the generator matrix of RM$(1, m)$.

It remains to see that all other $2^{m+1} - 2$ codewords have weight exactly 2^{m-1}. Suppose we wish to encode the message $(a_0, a_1, \ldots, a_m)$, such that $a_i \neq 0$ for some $i \geq 1$, under RM$(1, m)$. Then, the associated codeword consists of the values

$$a_0 + a_1 x_1 + \cdots + a_m x_m$$

for all choices of $x_i \in \{0, 1\}$. We will show that

$$V_b = \{(x_1, \ldots, x_m) : a_0 + a_1 x_1 + \cdots + a_m x_m = b\}$$

satisfies $|V_b| = 2^{m-1}$ for $b \in \{0,1\}$, which leads to the desired result. In order to see this, note that V_0 is a vector subspace. However, V_1 is not necessarily a vector subspace. Nevertheless, it holds that if $x, x' \in V_1$, then $x - x' \in V_0$, and also that if $x \in V_1$ and $x' \in V_0$, then $x + x' \in V_1$. Furthermore, by the choice of $(a_0, a_1, \ldots, a_m)$, we know there exists $x \in V_1$. This means that

$$V_1 = x + V_0 = \{x + x' : x' \in V_0\}.$$

We conclude that $|V_0| = |V_1|$. Since $\text{GF}(2)^m = V_0 \cup V_1$ and V_0 and V_1 are disjoint, it follows that $|V_0| = |V_1| = 2^{m-1}$.

Exercise 3. Let $\mathcal{C}$ be an $[n,k]_q$ linear code. Show that for each $i \in \{1,\ldots,n\}$ we either have $c_i = 0$ for all $c \in \mathcal{C}$, or there are exactly q^{k-1} codewords $c \in \mathcal{C}$ such that $c_i = \alpha$ for each $\alpha \in \text{GF}(q)$.

Model answer. Fix a linear code $\mathcal{C}$ with parameters $[n,k]_q$ and some $i \in \{1,\ldots,n\}$. If $c_i = 0$ for all $c \in \mathcal{C}$ the desired statement holds, so assume that there exists $c \in \mathcal{C}$ such that $c_i \neq 0$. Since $\mathcal{C}$ is linear, the vector $c' = \alpha \cdot c_i^{-1} \cdot c$ is in $\mathcal{C}$ and satisfies $c'_i = \alpha$. As a result, we conclude that for each $\alpha \in \text{GF}(q)$ there exists $c \in \mathcal{C}$ such that $c_i = \alpha$. Consider the vector subspace V of $\text{GF}(q)^n$ defined as

$$V := \{c \in \mathcal{C} : c_i = 0\},$$

and define also

$$\mathcal{C}_\alpha := \{c \in \mathcal{C} : c_i = \alpha\}.$$

Our goal is to show that $|\mathcal{C}_\alpha| = q^{k-1}$ for all $\alpha \in \text{GF}(q)$. Observe that $\mathcal{C}_0 = V$. However, $\mathcal{C}_\alpha$ for $\alpha \neq 0$ is not a vector subspace. Nevertheless, note that if $c, c' \in \mathcal{C}_\alpha$, then $c - c' \in V$. Moreover, if $c \in \mathcal{C}_\alpha$ and $c' \in V$, then $c + c' \in \mathcal{C}_\alpha$. Therefore, we can conclude that, for fixed $c_\alpha \in \mathcal{C}_\alpha$, we have

$$\mathcal{C}_\alpha = c_\alpha + V = \{c_\alpha + c : c \in V\}.$$

In particular, we have $|\mathcal{C}_\alpha| = |V|$. As a result,

$$q^k = |\mathcal{C}| = \sum_\alpha |\mathcal{C}_\alpha| = q \cdot |V|.$$

Hence, it holds that $|V| = q^{k-1}$, and so $|\mathcal{C}_\alpha| = q^{k-1}$ for all $\alpha \in \text{GF}(q)$, as desired.

Exercise 4. Let $\mathcal{C}$ be a binary linear code with parity-check matrix H such that every column of H is distinct from the others and has odd weight. Show that the minimum distance of $\mathcal{C}$ is at least 4.

Model answer. In order to show that the minimum distance of $\mathcal{C}$ is at least 4, it suffices to prove that every three columns of H are linearly independent. Let L_1, L_2, and L_3 be three distinct columns of H. By hypothesis, we have $L_1 \neq L_2$, $L_1 \neq L_3$, and $L_2 \neq L_3$. Therefore, it suffices to show that we cannot have

$$L_1 + L_2 = L_3.$$

In view of a contradiction, suppose this is the case. Then, we have

$$w(L_3) = w(L_1 + L_2) = w(L_1) + w(L_2) - 2w(L_1 \wedge L_2),$$

where $w(\cdot)$ denotes the Hamming weight, and $L_1 \wedge L_2$ denotes the coordinate-wise AND of the bits of L_1 and L_2. By hypothesis, all of $w(L_1)$, $w(L_2)$, and $w(L_3)$ are odd. However, under this hypothesis, it holds that

$$w(L_1) + w(L_2) - 2w(L_1 \wedge L_2)$$

is even, which contradicts the assumption that $w(L_3)$ is odd.

Exercise 5. Let $\mathcal{C}_1$ be an $[n, k_1, d_1]_2$ linear code, and let $\mathcal{C}_2$ be an $[n, k_2, d_2]_2$ linear code. Consider the code

$$\mathcal{C}_1 \ominus \mathcal{C}_2 = \{(c_1, c_1 + c_2) : c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2\}.$$

1. Give a generator matrix for $\mathcal{C}_1 \ominus \mathcal{C}_2$ as a function of the generator matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$.
2. Show that $\mathcal{C}_1 \ominus \mathcal{C}_2$ is a $[2n, k_1 + k_2, \min(2d_1, d_2)]_2$ linear code.

Model answer.

1. Suppose the generator matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$ are G_1 and G_2, respectively. Then, consider the following $2n \times (k_1 + k_2)$ matrix

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}.$$

   We show that G is a generator matrix for $\mathcal{C}_1 \ominus \mathcal{C}_2$. First, the fact that G is full-rank follows from the fact that both G_1 and G_2 are full-rank. To see this, let r_{1i} be the i-th row of G_1, and r_{2i} the i-th row of G_2. Suppose that there exist c_{1i} and c_{2j} for $i = 1, \ldots, k_1$ and $j = 1, \ldots, k_2$, not all zero, such that

$$\sum_{i=1}^{k_1} c_{1i} \cdot (r_{1i}, r_{1i}) + \sum_{j=1} c_{2j} \cdot (0, r_{2j}) = 0.$$

   Then, we must have $\sum_{i=1}^{k_1} c_{1i} \cdot r_{1i} = 0$. By the linear independence of the rows of G_1, it follows that $c_{1i} = 0$ for all $i = 1, \ldots, k_1$. This implies that we must have $\sum_{j=1} c_{2j} \cdot r_{2j} = 0$. By the linear independence of the rows of G_2, it must be the case that $c_{2j} = 0$ for all $j = 1, \ldots, k_2$. We can then conclude that the rows of G are linearly independent, and hence G has rank $k_1 + k_2$.

   Now, it suffices to see that the rows of G span $\mathcal{C}_1 \ominus \mathcal{C}_2$. Suppose m_1 and m_2 are such that $m_1 G_1 = c_1$ and $m_2 G_2 = m_2$. Then, we have

$$[m_1, m_2]G = (m_1 G_1, m_1 G_1 + m_2 G_2) = (c_1, c_1 + c_2).$$

   This yields the desired result.

2. The length and alphabet size of $\mathcal{C}_1 \ominus \mathcal{C}_2$ follow trivially from those of $\mathcal{C}_1$ and $\mathcal{C}_2$. The dimension follows immediately from the previous item. It remains to see that the minimum distance d satisfies $d = \min(2d_1, d_2)$.

   First, we show that $d \leq \min(2d_1, d_2)$. Indeed, let $c_1 \in \mathcal{C}_1$ and $c_2 \in \mathcal{C}_2$ be such that $w(c_1) = d_1$ and $w(c_2) = d_2$. Then, the desired inequality follows from the fact that both (c_1, c_1) and $(0, c_2)$ are in $\mathcal{C}_1 \ominus \mathcal{C}_2$.

   Second, we show that $d \geq \min(2d_1, d_2)$. Fix any codeword $(c_1, c_1 + c_2) \in \mathcal{C}_1 \ominus \mathcal{C}_2$. If $c_2 = 0$, we have

$$w(c_1, c_1 + c_2) = w(c_1, c_1) = 2w(c_1) \geq 2d_1.$$

   On the other hand, in general we have

$$w(c_1, c_1 + c_2) = w(c_1) + w(c_1 + c_2) = 2w(c_1) + w(c_2) - 2w(c_1 \wedge c_2) \geq w(c_2).$$

   Therefore, we conclude that $w(c_1, c_1 + c_2) \geq w(c_2) \geq d_2$ whenever $c_2 \neq 0$. Combining the two cases above shows that $d \geq \min(2d_1, d_2)$, as desired.

Exercise 6. Let $\mathcal{C}$ be a linear code over GF(q) such that $\mathcal{C}^\perp$ has minimum distance $d^\perp$. Show that, for every set $\mathcal{I} \subseteq \{1, \ldots, n\}$ with $|\mathcal{I}| = t \leq d^\perp - 1$, we have $\mathcal{C}_\mathcal{I} = \text{GF}(q)^t$, where $\mathcal{C}_\mathcal{I}$ denotes the restriction of $\mathcal{C}$ to the entries in $\mathcal{I}$.

Model answer. Let G be the generator matrix of $\mathcal{C}$. Since G is the parity-check matrix of $\mathcal{C}^\perp$, we know that

$$d^\perp = 1 + \max\{t : \text{every set of } t \text{ columns of } G \text{ are linearly independent}\}.$$

Fix a set $\mathcal{I} \subseteq \{1, \ldots, n\}$ of size $|\mathcal{I}| = t \leq d^\perp - 1$, and let $G_\mathcal{I}$ denote the submatrix of the generator matrix G which contains the i-th column of G whenever $i \in \mathcal{I}$. By the equality for $d^\perp$ above and the fact that $t \leq d^\perp - 1$, we know that all columns of $G_\mathcal{I}$ are linearly independent, and hence $G_\mathcal{I}$ has rank t. Since each row of $G_\mathcal{I}$ has length t, this means that the rows of $G_\mathcal{I}$ span $\mathrm{GF}(q)^t$. The result now follows by noting that $\mathcal{C}_\mathcal{I}$ is spanned by the rows of $G_\mathcal{I}$, and hence $\mathcal{C}_\mathcal{I} = \mathrm{GF}(q)^t$.

Exercise 7. Let $\mathcal{C}$ be an $[n, k, d]_q$ linear MDS code over $\mathrm{GF}(q)$. Show that there are exactly $\binom{n}{d}(q-1)$ codewords of weight d in $\mathcal{C}$.

Model answer. We show that for every set of d coordinates $\mathcal{I} = \{i_1, \ldots, i_d\}$ there exist $q - 1$ codewords $c \in \mathcal{C}$ of weight d such that $c_i \neq 0$ only if $i \in \mathcal{I}$. This yields the desired result as there are $\binom{n}{d}$ possible choices for $\mathcal{I}$.

Since $\mathcal{C}$ is an MDS code, we have $d = n - k + 1$. Let H denote its parity-check matrix. Recall that we have

$$d = 1 + \max\{t : \text{every set of } t \text{ columns of } H \text{ are linearly independent}\}.$$

Combining the previous two statements, we conclude that every $n - k$ columns of H are linearly independent. Moreover, since H has rank $n - k$, every set of $n - k + 1$ columns of H is linearly dependent. Given a set $\mathcal{I}$, let $H_\mathcal{I}$ denote the sub-matrix of H containing the columns indexed by $\mathcal{I}$. In our case, it holds that $|\mathcal{I}| = n - k + 1$. The previous observations imply that $H_\mathcal{I}$ has $n - k + 1$ columns and rank $n - k$. As a result, we conclude that the kernel of $H_\mathcal{I}$ has dimension 1. This means there are $q - 1$ nonzero vectors c' of length $n - k + 1 = d$ such that $H_\mathcal{I} \cdot c' = 0$. Because of this, each such vector c' can be uniquely extended to a codeword $c \in \mathcal{C}$ by setting $c_i = 0$ for $i \notin \mathcal{I}$ and $c_i = c'_i$ for $i \in \mathcal{I}$. In particular, we have $w(c) = w(c')$. On the one hand, it must be the case that $w(c) \geq d$ since $\mathcal{C}$ has minimum distance d. On the other hand, we have $w(c) = w(c') \leq d$ since c' has length d. This implies that all such vectors c' yield distinct minimum weight codewords of $\mathcal{C}$, and so we conclude the proof.