Model answers

11.1 General codes

From the 2013 Coding Theory exam paper — medium difficulty:

A4. Consider the following binary code of length 6: $C = \{000111, 110001, 011100\}$.

(a) Is C a linear code? Give a reason for your answer.

(b) Find $d(C)$.

(c) Show that there does not exist a vector $\underline{y} \in \mathbb{F}_2^6$ such that $d(\underline{y}, \underline{c}) = 1$ for all $\underline{c} \in C$.

Solution.

(a) C is not linear, e.g. because C does not contain 000000. (*There are other reasons.*)

(b) All pairwise distances between codewords are 4 so $d(C) = 4$.

(c) By the Triangle Inequality, $d(000111, 110001) \leq d(000111, \underline{y}) + d(\underline{y}, 110001)$. The left-hand side of this inequality is 4 so the right-hand side cannot be $1 + 1$.

11.2 Bounds

From the 2013 Coding Theory exam paper, question A3 — medium difficulty:

(e) Prove:

1. The sphere $S_{10}(\underline{0})$ in $\mathbb{F}_3^{2013}$ consists of an odd number of elements.
2. Any perfect code in $\mathbb{F}_3^{2013}$ consists of an odd number of codewords.

Solution.

1. The formula for the number of elements in a Hamming sphere $S_r(\underline{y})$ tells us that $\#S_{10}(\underline{0}) = \binom{2013}{0} + \binom{2013}{1}2^1 + \cdots + \binom{2013}{10}2^{10}$. The first summand $\binom{2013}{0} = 1$ is odd, the rest contain powers of 2 so are even. Therefore, the sum is odd.

2. A perfect code C attains the Hamming bound, which can be written in the form $M(\#S_t(\underline{0})) = 3^{2013}$. So $M = \#C$ is a divisor of the odd integer 3^{2013}, so M is odd.

Challenging: A3g from the 2015 Coding Theory exam paper, also used in coursework in later years:

(g) You are given that $C \subseteq D \subseteq \mathbb{F}_q^n$ where $|C| < |D|$ and C is a perfect code. $d(C) > 2d(D)$. You may quote any result from the course without proof.

Solution.

The assumptions mean that $D \not\subseteq C$, so there is a codeword $\underline{x}$ of D such that $\underline{x} \notin C$. Since C is perfect, by a result from the course, $\underline{x}$ has a unique nearest neighbour $\underline{c}$ in C with $d(\underline{x}, \underline{c}) \le t$, where $t = [(d(C) - 1)/2]$. Note that $t < d(C)/2$. Both $\underline{x}$ and $\underline{c}$ are in D, and $\underline{x} \neq \underline{c}$ (one word is not in C, the other is in C). So $d(D) \le d(\underline{x}, \underline{c}) < d(C)/2$, and so $2d(D) < d(C)$ as claimed.

11.3 Linear codes I

From 2019/20 coursework: fairly difficult

D. An interesting weight enumerator [20 marks] Show that there is no linear code over $\mathbb{F}_8$ with weight enumerator $x^9 + 16x^5y^4 + 16x^4y^5 + 256y^9$. Does a linear code with such weight enumerator exist over any other field? Justify your answer.

Solution.

Suppose a linear code has weight enumerator $x^9 + 16x^5y^4 + 16x^4y^5 + 256y^9$. This means that the code contains one codevector of weight 0, sixteen codevectors of weight 4, sixteen codevectors of weight 5 and 256 codevectors of weight 9. The total number of codevectors is then $1 + 16 + 16 + 256 = 289$. Since 289 is not a power of 8, the code cannot be a linear code over $\mathbb{F}_8$: such codes always contain 8^k elements where $k = \dim C$ is an integer.

Since $289 = 17^2$, such a code could in principle exist over $\mathbb{F}_{17}$ or over $\mathbb{F}_{289}$. But saying that a code *could* exist is not a proof that it exists — we need to construct the code. Consider the 17-ary code generated by $G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$. It has 16 codevectors of weight 4 and of the form $\lambda\lambda\lambda\lambda 00000$ with $\lambda \in \mathbb{F}_{17} \setminus \{0\}$; 16 codevectors of weight 5 of the form $0000\mu\mu\mu\mu\mu$ with $\mu \in \mathbb{F}_{17} \setminus \{0\}$; and the rest of its 289 codevectors are of the form $\lambda\lambda\lambda\lambda\mu\mu\mu\mu\mu$, of weight 9. Hence the code has the required weight enumerator.

11.4 Linear codes II: encoding and decoding

11.5 Dual codes

From the 2020/21 exam: medium difficulty

A1. Let C be the linear code over the field $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ generated by the matrix

$$G = \begin{bmatrix} 1 & 0 & 2 & 3 & 0 & 1 \\ 0 & 1 & 3 & 1 & 0 & 2 \\ 2 & 0 & 4 & 0 & 0 & 4 \end{bmatrix}.$$

For each of the statements about the code C, given below, determine if the statement is true and justify your answer. Marks will not be given for true/false answers without any justification.

(c) $d(C^\perp) = 2$.

(e) $\sum_{\underline{c} \in C} w(\underline{c}) = 600$.

Solution.

False: since the fifth column of G is zero, the dual code $C^\perp$ contains the vector 000010 of weight 1, so $d(C^\perp) = w(C^\perp) = 1$.

False: by the Average Weight Equation, the average weight of a codevector of C is $(n-z)(1-q^{-1})$ where $n - z$ is the number of non-zero columns of G and $q = 5$. This gives $5 \times (1 - 1/5) = 4$. The number of codevectors is $5^3 = 125$ so the sum of weights is $125 \times 4 = 500 \neq 600$.

11.6 Hamming codes and simplex codes

From the 2013 exam, question B6 — medium difficulty:

(e) Let q be given. Describe all values of s such that $\mathrm{Ham}(s, q)$ is an MDS code. You may quote any result from the course without proof.

(f) Write down a generator matrix for $\mathrm{Ham}(3, 2)$ in standard form.

(g) Find $\max\{d(\underline{x}, \underline{y}) : \underline{x}, \underline{y} \in \mathrm{Ham}(3, 2)\}$, that is, the *maximum* distance between two codewords in $\mathrm{Ham}(3, 2)$. Justify your answer.

Solution.

(e) $k = \dim \mathrm{Ham}(s, q) = n - s$, and the code is MDS iff $k = n - d + 1$. Since $d = 3$ for Hamming codes, the MDS condition rewrites as $n - s = n - 3 + 1$. Therefore, the answer is: $s = 2$.

(f) Start with a check matrix for $\mathrm{Ham}(3, 2)$, *writing the three identity columns on the right*: for example, $H = \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right] = \left[A \mid I_3 \right]$. No need to do any row operations! Then a generator matrix in standard form is $G = \left[\, I_4 \mid -A^T \right] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$. The answer is not unique, but all possible answers are obtained from this one by permuting the 3-bit rows of the rightmost 4×3 block $\left|\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right.$.

(g) $d(\underline{x}, \underline{y})$ is the weight $w(\underline{x} - \underline{y})$ of the vector $\underline{x} - \underline{y}$ which is a codevector (because the Hamming code is linear). We do have the codevector 1111111 of weight 7, for example the sum of the rows of G above. Alternatively, $1111111H^T = 0$ so the vector is in the code, no matter the order of columns of H. Hence the answer is 7, e.g., by taking $\underline{x} = 1111111$, $\underline{y} = \underline{0}$.

11.7 Cyclic codes

From the 2011 exam, question B7 — medium difficulty:

Given that, over $\mathbb{F}_3$,

$$x^8 - 1 = (x^5 + x^4 + x^3 - x^2 + 1)(x^3 - x^2 - 1):$$

4. Write down a generator polynomial and a check polynomial for a ternary cyclic code of length 8 and dimension 5.
5. Write down a generator matrix and a parity check matrix for this code.
6. Find the minimum distance of this code.
7. Are either of the vectors 11000000 or 11102000 in this code?
8. The repetition code in $\mathbb{F}_p^{(n)}$ is always a cyclic code. Write down a generator matrix and a check polynomial for the repetition code.

Solution.

4. Since $\dim C = n - \deg g(x)$, we have $\deg g(x) = 8 - 5 = 3$. An obvious choice is $g(x) = x^3 - x^2 - 1$.

5. $G = \begin{bmatrix} 2 & 0 & 2 & 1 & & & & \\ & 2 & 0 & 2 & 1 & & & \\ & & 2 & 0 & 2 & 1 & & \\ & & & 2 & 0 & 2 & 1 & \\ & & & & 2 & 0 & 2 & 1 \end{bmatrix}$, $H = \begin{bmatrix} 1 & 1 & 1 & 2 & 0 & 1 & & \\ & 1 & 1 & 1 & 2 & 0 & 1 & \\ & & 1 & 1 & 1 & 2 & 0 & 1 \end{bmatrix}$. Blanks mean zeros (and are used for emphasis), and it is acceptable to write -1 instead of 2 in $\mathbb{F}_3$. Note the order in which the coefficients of $g(x) = 2 + 0x + 2x^2 + 1x^3$ are used in the rows of G, and the order in which the coefficients of $h(x) = x^5 + x^4 + x^3 + 2x^2 + 0x + 1$ are used in H.

6. Note that $d(C) = w(C) \leq 3$ because $\underline{g} = 2021000 \in C$ is a vector of weight 3. On the other hand, H has no zero columns so by the distance theorem $d(C) \geq 2$, and no two columns of H are proportional so by the distance theorem $d(C) \geq 3$. Hence $d(C) = 3$.

7. 11000000 is of weight 2 so is not in the code — the minimum weight in the code is 3.

$11102000H^T = 000$ so 11110200 is in the code. *Alternatively,* $2x^4 + x^2 + x + 1 = (2x+2)(x^3 + 2x^2 + 2) = (2x+2)g(x)$, e.g., by long division, so $2x^4 + x^2 + x + 1$ is a code polynomial.

8. $G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \end{bmatrix}$ and so the generator polynomial is $g(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$. The check polynomial is $h(x) = x - 1$ since $(x-1)g(x) = x^n - 1$.

11.8 Classification of perfect codes

From the 2016 exam, question B4 — difficult:

(f) Given that C is a perfect linear $[n,k,d]_q$-code with weight enumerator $W_C(x,y) = Ax^n + Bx^{n-2}y^2 + nx^{n-3}y^3 + nx^{n-4}y^4 + y^n$, find n, k, d, q, A and B.

Solution.

- $A = 1$, because there is exactly 1 vector of weight 0 in a linear code.
- If $B \neq 0$, then $d(C) = 2$ (even) which is impossible for a perfect code. So $B = 0$.
- The term y^n shows that there is exactly one vector of weight n in C, say $\underline{v}$. Yet if $\lambda \in \mathbb{F}_q$, $\lambda \neq 0, 1$, then $\lambda\underline{v}$ would be another vector of weight n. Hence $\mathbb{F}_q$ contains only 0 and 1, and $q = 2$.
- If $\underline{a} \in C$ is of weight 3, then $\underline{v} - \underline{a} = 111\dots1 - \underline{a}$ has weight $n-3$. So C must contain n vectors of weight $n-3$, and (similarly) n vectors of weight $n-4$. From the weight enumerator, $\{n-4, n-3\}$ must be $\{3,4\}$, and so $n = 7$.
- Thus $W_C(x,y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7$. One has $\#C = 1 + 7 + 7 + 1 = 16$ and so $k = \log_2 16 = 4$.

We discover that C is parameter equivalent to $\mathrm{Ham}(3,2)$. There are alternative ways to solve this problem which use classification of perfect codes.

11.9 Reed-Muller codes