Mathematics 342 Midterm 1 solutions

February, 2018. Instructor: Z. Reichstein.

Problem 1 Prove that $A_q(3n, 3d) \geq A_q(n, d)$ for any positive integers q, n, d, where $q \geq 2$ and $n \geq d \geq 1$.

Solution: Let C be the largest q-ary code of length n and minimal distance d. By the definition of $A_q(n, d)$, C has $M = A_q(n, d)$ words.

Our goal is to construct a q-ary $(3n, M, 3d)$-code C'. This will show that $A_q(n, d) \geq M$, as desired.

To construct C', for each word $\mathbf{a} = (a_1, \dots, a_n)$, create a word

$$\mathbf{a}' = (a_1, \dots, a_n, a_1, \dots, a_n, a_1, \dots, a_n)\,.$$

Denote the resulting code of length $3n$ and size M by C'. It remains to show that $d(C') = 3d$.

Suppose $\mathbf{b} = (b_1, \dots, b_n)$ is another word in C, different from $\mathbf{a}$, and

$$\mathbf{b}' = (b_1, \dots, b_n, b_1, \dots, b_n, b_1, \dots, b_n)$$

is the word in C' obtained by repeating $\mathbf{b}$ three times. Then

$$d(\mathbf{a}', \mathbf{b}') = 3d(\mathbf{a}, \mathbf{b}).$$

Taking the minimum over all pairs $\mathbf{a}'$, $\mathbf{b}'$, we see that the minimal distance $d(C')$ of C' is $3d$, as desired.

Problem 2. Is there a **perfect** q-ary code C of length n and minimal distance d in the following cases? If the answer is "yes", how many codewords does C have? Explain your answer in each part.

(a) $q = 2$, $n = 5$, $d = 5$.

(b) $q = 2$, $n = 7$, $d = 4$.

(c) $q = 2$, $n = 7$, $d = 3$.

(d) $q = 3$, $n = 8$, $d = 3$.

Solution: (a) Yes. The binary repetition code $\{(0,0,0,0,0), (1,1,1,1,1)\}$ is a perfect code of length 5 and minimal distance 5. Indeed, it meets the Hamming bound $\dfrac{2^5}{1 + 5 + \binom{5}{2}} = 2$.

(b) No. The minimal distance of a perfect code has to be odd.

(c) Yes, we constructed a $(7, 16, 3)$-code in class. It is perfect because it meets the Hamming bound, $\dfrac{2^6}{1+7} = 2^4 = 16$.

(d) No, because the right side of the Hamming bound, $\dfrac{3^3}{1 + 2 \cdot 8} = \dfrac{3^8}{17}$ is not an integer.

Problem 3. (a) Evaluate 2^{100} in $\mathbb{Z}_7$. Your answer should be an integer between 0 and 6.

(b) Evaluate $\dfrac{4}{5}$ in $\mathbb{Z}_{17}$. Your answer should be an integer between 0 and 16.

Solution: (a) Since $2^3 \equiv 1 \pmod 7$, we have $2^{99} = (2^3)^{33} \equiv 1 \pmod 7$, and

$$2^{100} \equiv 2 \cdot 2^{99} \equiv 2 \cdot 1 \equiv 2 \pmod 7.$$

(b) Apply the Euclidean algorithm to 17 and 5 to find 5^{-1}:

$17 - 5 \cdot 3 = 2$

$5 - 2 \cdot 2 = 1.$

Back substitution: $1 = 5 - 2 \cdot 2 = 5 - (17 - 5 \cdot 3) \cdot 2 = 5 \cdot 7 - 17 \cdot 2$. Reducing both sides modulo 17, we obtain $1 = 5 \cdot 7 \pmod{17}$. Thus $5^{-1} \equiv 7 \pmod{17}$ and

$$\frac{4}{5} = 4 \cdot 5^{-1} = 4 \cdot 7 = 28 = 17 + 11 = 11$$

in $\mathbb{Z}_{17}$.

Problem 4 Find the missing ISBN digit: 111?201111.

Solution: Denote the missing digit by x. Then we have to solve

$$1 \cdot 1 + 1 \cdot 2 + 1 \cdot 3 + x \cdot 4 + 2 \cdot 5 + 0 \cdot 6 + 1 \cdot 7 + 1 \cdot 8 + 1 \cdot 9 + 1 \cdot 10 \equiv 0 \pmod{11}.$$

The first three digits and the last three cancel out, because $1 + 10 = 2 + 9 = 3 + 8 \equiv 0 \pmod{11}$, and we are left with $4x + 17 \equiv 0 \pmod{11}$ or, equivalently, $4x + 6 \equiv 0 \pmod{11}$. Since 11 is a prime, we can divide both sides by 2 to obtain $2x + 3 \equiv 0 \pmod{11}$ and thus

$$x \equiv -3 \cdot 2^{-1} \equiv 8 \cdot 6 \equiv 48 \equiv 4 \pmod{11}.$$

Thus the missing digit is 4.

Problem 5. Consider the code C in $(\mathbb{Z}_{11})^{10}$ consisting of words $(a_1, a_2, \ldots, a_{10})$ which satisfy both $a_1 + 2a_2 + 3a_3 + \cdots + 10a_{10} \equiv 0 \pmod{11}$ (same as for the ISBN code) and $a_1 + a_2 + a_3 + \cdots + a_{10} \equiv 0 \pmod{11}$.

(a) How many words does C have?

(b) Prove that the minimal distance $d(C)$ of this code is ≤ 3.

Solution: (a) The last eight digits $a_3, \ldots, a_{10}$ can be specified in an arbitrary manner in $\mathbb{Z}_{11}$. The first two digits, a_1 and a_2 can then be recovered uniquely from the last 8 by solving the system

$a_1 + a_2 = b_1,$

$a_1 + 2a_2 = b_2.$

Here $b_1 = -a_3 - \cdots - 10a_{10}$ and $b_2 = -3a_3 - \cdots - 10a_{10}$. The solution to this system is $a_2 = b_2 - b_1$, $a_1 = 2b_1 - b_2$.

Thus the number of words in C is the number of ways to choose $a_3, \ldots, a_{10}$ in $\mathbb{Z}_{11}$, i.e., 11^8.

(b) Solution 1. Since the all-zero word $(0, \ldots, 0)$ is in C, we only need to show that C contains a word of weight ≤ 3. Indeed, choose $a_3 = 1$ and $a_4 = \cdots = a_{10} = 0$, then solve for a_1 and a_2, as in part (a). The resulting word $(a_1, a_2, 1, 0, \ldots, 0)$ will be in C and will be of weight ≤ 3.

Specifically (even though we do not need these specifics for the solution), in this case $b_1 = -1$, $b_2 = -3$, and $a_2 = b_2 - b_1 = -2 = 9$ and $a_1 = 2b_1 - b_2 = 1$. The resulting word, $(1, 9, 1, 0, \ldots, 0)$ is of weight 3 and lies in C.

Solution 2. Assume the contrary: $d(C) \geq 4$. The $A_{11}(10, 4) \geq |C| = 11^8$ by part (a). The contradicts the Singleton bound: $A_{11}(10, 4) \leq 11^{10-4+1} = 11^7$.