Mid term exam, November 24 — Solutions

Exercise 1 (**Quizz).** Answer the questions. **You should justify your answers.**

(1) (a) A $[7, 4, 3]$ Reed Solomon code over $\mathbb{F}_8$ does not exist since a Reed-Solomon is MDS, hence with this length and dimension it should have minimum distance 4.

(b) A $[9, 6, 4]$ Reed Solomon code over $\mathbb{F}_9$ exists since for any $n \leqslant 9$ and any $k \leqslant n$ there exists an $[n, k, n-k+1]$ code.

(c) A $[11, 9, 3]$ Reed Solomon code over $\mathbb{F}_7$ does not exist since the length of a Reed Solomon code over $\mathbb{F}_7$ is upper bounded by 7.

(2) Such a Reed Solomon code has dimension 20 since a Reed Solomon code is MDS. Since $\mathbb{F}_{25}$ is an extension of $\mathbb{F}_5$ of degree $m = 2$. The dimension of the subfield subcode is at least $n - m(n-k)$ which gives a subfield subcode of dimension at least 15.

(3) (a) Using a majority voting algorithm one can correct up to 4 errors.

(b) One can correct up to 9 erasures : as soon as we have one non erased digit we can recover the complete codeword by copying the non erased digit.

(4) The algorithm presented in the lecture notes which is nothing but the syndrome decoder permits to correct one error. It is not possible to correct 2 errors : the code is perfect and hence if one receives $y = c + e$ where c is in the Hamming code and e has weight 2, then there is a codeword c' different from c in the Hamming code which is at distance 1 from y.

(5) Since the code is self dual, its dimension k satisfies :

$$k = \dim C = \dim C^{\perp} = 10 - \dim C.$$

Therefore, $k = 5$.

(6) No, the asymptotic Plotkin bound shows that sequence of codes whose asymptotic rate is nonzero have an asymptotic $\delta < 0.8$.

(7) The most difficult problem is (b) which has been proved to be NP-Hard. (a) and (c) can be solved by Gaussian elimination and (d) can be solved using McWilliams identity.

(8) Answer (c), according to the lecture notes, there exists a code reaching or exceeding Gilbert Varshamov bound

(9) Swapping to rows does not change the code since the code is the vector space spanned by the rows. The way rows are sorted is not worth. Swapping columns may change the code (the obtained code is isometric to C).

(10) No, correcting $d = n - k + 1$ errors is far beyond Johnson bound. In particular, given a word $y \in \mathbb{F}_q^n$, then, one can check that the number of codewords at distance less than $n - k + 1$ is exponential in k.

Exercise 2. (1) Since there is no zero column, the minimum distance is > 1. Since there is no two column which are equal, the minimum distance is > 2. Finally, any column has weight 3. Thus the sum of two distinct columns has weight either 2 (if the columns match at two positions) or 4 or 6. Thus the sum of 3 distinct columns is always nonzero and hence, the minimum distance is > 3.

(2) (1 1 0 0 0 0 0 0 0 0 0 0 1 1).

(3) It suffices to check that the sum of r distinct columns of H with r odd is never 0. For this sake we will prove that the sum of an odd number of columns is odd. Note that the weight of a word of $\mathbb{F}_2^6$ modulo 2 equals the inner product of the word with $u := (1\ 1\ 1\ 1\ 1\ 1)$. Any column of H has odd weight and hence an inner product 1 with u. By linearity, the sum of an odd number of columns of H has also inner product 1 with u and hence has odd weight.

According to the lecture notes, codewords are in correspondence with tuples of columns of a parity–check matrix which sum to zero. Therefore, the code C has only even weights.

(4) Since $v = (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \in C$, for any codeword $c \in C$ of weight a there exists $v - c$ which has weight $12 - a$. Thus the number of codewords of weight a equals that of codewords of weight $12 - a$. This is translated by the identity $P(x, y) = P(y, x)$.

(5) Since C has dimension 6, it has $2^6 = 64$ codewords, It contains the codewords $(0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$ and $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$. Since $P(x, y) = P(y, x)$ and since there is no codeword of weight 2 (the minimum distance is 4), there is no codeword of weight 10 either. Then, the possible weights are $0, 4, 6, 8$ and 12. Using again the property $P(x, y) = P(y, x)$ we get that

$$P(x, y) = y^{12} + ax^4y^8 + bx^6y^6 + ax^8y^4 + x^{12}.$$

Finally, since we know that $b = 16$ and that the code has 64 codewords we conclude that $a = 23$. That is :

$$P(x, y) = y^{12} + 23x^4y^8 + 16x^6y^6 + 23x^8y^4 + x^{12}.$$

Exercise 3 (Concatenated codes). (1) Each $\mathbb{F}_{2^m}$–digit is represented by an n–tuple of elements of $\mathbb{F}_2$, hence the new length is Nn.

For the dimension, consider the map

$$\left\{ \begin{array}{ccc} C_0 & \longrightarrow & \mathbb{F}_2^{Nn} \\ (c_1, \ldots, c_N) & \longmapsto & (\phi(c_1), \ldots, \phi_{C_N}) \end{array} \right. .$$

Since ϕ is $\mathbb{F}_2$–linear and injective, then so is the above map and $C_o \square C_i$ is the image of the above map. Therefore, the dimension of $C_o \square C_i$ equals the dimension of C_o **regarded as an $\mathbb{F}_2$–vector space**. Thus the dimension equals Km.

Finally, let $a \in C_o \square C_i \setminus \{0\}$. Then, there exists $c \in C_o \setminus \{0\}$ such that $a = (\phi(c_1), \ldots, \phi(c_n))$. There are at least D of the c_j's which are nonzero. By definition of C_i for j such that $c_j \neq 0$, the weight of $\phi(c_j)$ is at least d. Thus, the minimum distance is at least equal to Dd.

(2) Let $a \in C_i^\perp \setminus \{0\}$ be a minimum weight codeword. Then, the word, $(a, \phi(0), \ldots, \phi(0))$ is nonzero and is in $(C_o \square C_i)^\perp$.

(3) According to the course, since random code are close to Gilbert Varshamov bound with a probability tending to 1 when m tends to infinity, the code C_i has distance $\geqslant n/4$ with a probability tending to 1 when m tends to infinity. According to question (1), the parameters of the code $C_o \square C_i$ are

$$\left[Nn, Km, \geqslant \frac{Nn}{8} \right]_2$$

with a probability which tends to 1 when m tends to infinity.

(4) With the very same reasoning, let $\delta \in [0, 1/2]$ be such that $R = 1 - H_2(\delta)$, i.e.

$$\delta = H_2^{-1}(1 - R)$$

we get asymptotic parameters

$$\left[Nn, Km, \geqslant \frac{\delta Nn}{2} \right]_2$$