MPRI **Year 2016–17**

Module 2.13.2 : Error correcting codes and applications to cryptography

Mid-term exam, November 24

You have 1h30. Any document including personal lecture notes is authorized.
The three exercises are independent.
You can answer either in French or in English.

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

(1) Does there exist :
   (a) A $[7, 4, 3]$ Reed Solomon code over $\mathbb{F}_8$?
   (b) A $[9, 6, 4]$ Reed Solomon code over $\mathbb{F}_9$?
   (c) A $[11, 9, 3]$ Reed Solomon code over $\mathbb{F}_7$?

(2) Let C be a Reed Solomon code of length 25 and minimum distance 6 over $\mathbb{F}_{25}$. Give a lower bound for the dimension of its subfield subcode $C_{|\mathbb{F}_5}$ over $\mathbb{F}_5$. (Remind that, this code is defined as $C_{|\mathbb{F}_5} := C \cap \mathbb{F}_5^{25}$).

(3) (a) What is the largest number of errors one can correct using the repetition code of length 10 over $\mathbb{F}_2$?
   (b) What is the largest number of erasures one can correct using the repetition code of length 10 over $\mathbb{F}_2$?

(4) What is the largest number of errors one can correct using the $[7, 4, 3]$ Hamming code ?

(5) What is the dimension of a self dual code of length 10 ?

(6) Can one have a sequence of codes $(C_s)_{s \geqslant 0}$ over $\mathbb{F}_5$ with parameters $[n_s, k_s, d_s]$ such that $n_s \to +\infty$, $\frac{k_s}{n_s} \to 0.1$ and $\frac{d_s}{n_s} \to 0.9$?

(7) Which one of these problems is the most difficult to solve ?
   (a) Given a generator matrix G of a code C, compute a parity-check matrix of C ;
   (b) Given a generator matrix G of a code C, compute the minimum distance of C ;
   (c) Given a basis of a code C, compute a basis of $C^\perp$;
   (d) Given a code C and its weight enumerator polynomial P, compute the weight enumerator polynomial of $C^\perp$.

(8) Denote by $\mathrm{Vol}_q(r, n)$ the volume of a Hamming ball of radius r in $\mathbb{F}_q^n$. Which one of these three statements is true ?
   (a) For any $[n, k, d]$ code over $\mathbb{F}_q$, $q^k.\mathrm{Vol}_q(d, n) < q^n$;
   (b) For any $[n, k, d]$ code over $\mathbb{F}_q$, $q^k.\mathrm{Vol}_q(d, n) \geqslant q^n$;
   (c) There exists an $[n, k, d]$ code over $\mathbb{F}_q$ such that $q^k.\mathrm{Vol}_q(d, n) \geqslant q^n$;

(9) Given a code C with a generator matrix G, which one of these operations on G provides another generator matrix of C ?
   (a) Swapping two rows of G ;
   (b) Swapping two columns of G.

(10) Let C be a Reed Solomon code of length n and minimum distance d. Is it possible to correct d errors using Guruswami Sudan algorithm ?

Please turn the page.

Exercise 2. Let C be the binary code with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Note that any column of H has weight 3.

(1) Prove that the code has minimum distance > 3.

(2) Give a codeword of weight 4 of C.

(3) Prove that any word of C has an even weight.

(4) We denote the homogeneous weight enumerator polynomial of C by $P_C(x, y)$. Prove that

$$P_C(x, y) = P_C(y, x).$$

(5) Assuming that C has 16 words of weight 6, give the complete weight distribution of C without enumerating it.

Exercise 3 (Concatenated codes). Let $m > 2$ be an integer. Let C_o be an $[N, K, D]$ code over $\mathbb{F}_{2^m}$ and C_i be an $[n, m, d]$ code over $\mathbb{F}_2$. Finally, let $\phi : \mathbb{F}_{2^m} \to C_i$ be an injective $\mathbb{F}_2$–linear map. We define the binary code

$$C_o \square C_i := \{(\phi(c_1), \ldots, \phi(c_N)) \mid (c_1, \ldots, c_N) \in C_o\}.$$

(1) Prove that $C_o \square C_i$ has parameters $[Nn, Km, \geqslant Dd]_2$.

(2) Prove that the minimum distance of $(C_o \square C_i)^\perp$ is bounded from above by the minimum distance of $C_i^\perp$.

Bonus questions. *If you did everything well up to here, you'll have 20/20. The remaining questions are bonus.*

(3) Suppose that C_o is a Reed Solomon code of length $N = 2^m$ and dimension $K = 2^{m-1} + 1$ over $\mathbb{F}_{2^m}$. Let $\epsilon > 0$ such that $\epsilon < 1 - H_2(1/4)$ and C_i be a random binary code of length n and dimension m such that

$$m = \lfloor (1 - H_2(1/4) - \epsilon) n \rfloor,$$

where $H_2(\cdot)$ denotes the binary entropy function : $H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$. Prove that the probability that the code $C_o \square C_i$ has parameters :

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

tends to 1 when m tends to infinity.

(4) If C_o is replaced by a Reed Solomon code of length 2^m and dimension $K = R \cdot 2^m$ for some $R \in]0, 1[$, which asymptotic parameters can one expect for the code $C_o \square C_i$?