MPRI **Year 2017–18**

Module 2.13.2 : Error correcting codes and applications to cryptography

Mid-term exam, November 23

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

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

(1) Which of these codes do exist ? If they do not, explain why, if they do, explain how they can be constructed.

  (a) A $[32, 16, 17]$ Reed–Solomon code over $\mathbb{F}_{32}$;
  (b) A $[32, 15, 18]$ Generalised Reed-Solomon code over $\mathbb{F}_{19}$;
  (c) A $[7, 5, 3]$ binary code ;
  (d) A $[64, 34, \geqslant 6]$ alternant code over $\mathbb{F}_2$.

(2) Which of these statements is true ?

  (a) There is no $[n, k, d]$ code such that $d > n - k + 1$;
  (b) For all $\epsilon > 0$, for any sequence of binary codes whose relative distance sequence converges to δ and rate converges to R we have $R \geqslant 1 - H_2(\delta) - \epsilon$.
  (c) No $[n, k, d]_q$ linear code satisfies
$$q^k Vol_q(d, n) \geqslant q^n$$
(where $Vol_q(d, n)$ denotes the number of elements in a Hamming ball of radius d in $\mathbb{F}_q^n$).
  (d) There exists an $[n, k, d]$ code over $\mathbb{F}_q$ such that
$$d \leqslant nq^{k-1} \frac{q-1}{q^k - 1}.$$

(3) How many binary cyclic codes of length 8 do there exist ?

(4) Suppose that one has a list decoding algorithm for any $[32, 20, 11]$ Reed-Solomon code over $\mathbb{F}_{32}$ correcting up to 10 errors.

  (a) Deduce the existence of a list decoder correcting up to 10 errors for any $[32, k]$ Reed-Solomon code with $k < 20$.
  (b) For which values of k can one make sure the decoding is unique ?

Turn the page please.

Exercise 2. Cyclic codes. *You are allowed to skip any question and assume its result to be true in the subsequent questions.*

Let n be an odd integer. Let $C \subseteq \mathbb{F}_2^n$ be a linear cyclic code of dimension k. Let T be the corresponding cyclotomic class in $\mathbb{Z}/n\mathbb{Z}$ and g_C be the generating polynomial of C.

(1) What is the cardinality of T ? the degree of g_C ?

(2) Let C' be the subset of C of all words of even weight.
  (a) Prove that C' is a linear code.
  (b) What is its dimension ?
  (c) Prove that C' is cyclic.
  (d) Prove that the following conditions are equivalent :
    (i) $C = C'$;
    (ii) $0 \in T$;
    (iii) $g_C(1) = 0$.
  (e) If $C \neq C'$ describe the generating polynomial of C' and its cyclotomic class.

(3) Prove that C contains the all-one codeword $(1, 1, \ldots, 1)$ if and only if $0 \notin T$.

(4) List the minimal 2 cyclotomic classes in $\mathbb{Z}/21\mathbb{Z}$ (i.e. the smallest subsets stable by multiplication by 2).

(5) How many binary cyclic codes of length 21 do there exist ?

(6) Prove the existence of a $[21, 12, \geqslant 5]$ binary cyclic code which contains the all-one codeword (you can use Question 3).

Let

$$P_C(X, Y) = \sum_{i=0}^{21} p_i X^i Y^{n-i}$$

be the weight enumerator of C. That is, p_i is the number of words of weight i in C.

(7) Prove that the weight enumerator of such a $[21, 12, \geqslant 5]$ binary cyclic code is self reciprocal, i.e. $P_C(X, Y) = P_C(Y, X)$. In particular, prove that there is no codeword of weight $w \in \{17, \ldots, 20\}$.

(8) Let

$$\sigma : \left\{ \begin{array}{ccc} \mathbb{F}_q^{21} & \longrightarrow & \mathbb{F}_q^{21} \\ (x_1, \ldots, x_n) & \longmapsto & (x_n, x_1, \ldots, x_{n-1}) \end{array} \right.$$

be the cyclic shift. Prove that if $c \in \mathbb{F}_q^{21}$ satisfies $\sigma^\ell(c) = c$ for some $\ell > 1$ and $\sigma^j(c) \neq c$ for all $1 \leqslant j < \ell$, then :
  (a) ℓ divides 21 ;
  σ^ℓ generates a subgroup of the group generated by σ, namely, the *stabilizer* of c. By Lagrange Theorem, ℓ divides the order of σ.
  (b) $\frac{21}{\ell}$ divides the weight of c.

(9) Prove that
  (a) $p_8, p_{10}, p_{11}, p_{13}$ are divisible by 21 ;
  (b) p_6, p_9, p_{12}, p_{15} are divisible by 3 ;
  (c) p_7, p_{14} are divisible by 7.