Mid-term exam, November 28

You have 1h30. Personal lecture notes are authorized.
Computers and phones are forbidden.
The exercises are independent.
You can answer either in French or in English.

Exercise 1. (1) Compute the weight distribution of the $[7,4,3]_2$ Hamming code. Explain in a few words how you computed it.

(2) Deduce that of its dual.

(3) More generally, considering a $[2^\ell - 1, 2^\ell - \ell, 3]$ Hamming code. How many codewords of weight 3 and 4 does it contain ?

Exercise 2. (1) List all the minimal cyclotomic classes for $\mathbb{F}_5^{12}$, i.e. the minimal subsets of $\mathbb{Z}/12\mathbb{Z}$ stable by multiplication by 5.

(2) What is the number of cyclic codes of length 12 over $\mathbb{F}_5$?

(3) What is the number of cyclic codes of length 12 and dimension 9 over $\mathbb{F}_5$?

(4) Prove the existence of a cyclic code of length 12 over $\mathbb{F}_5$ of dimension 5 and minumum distance at least 6.

Exercise 3. Let p denote a prime number and n be a positive integer. The Hamming weight of a vector $\mathbf{y} \in \mathbb{F}_p^n$ is denoted as $w_H(\mathbf{y})$. The *support* of a vector $\mathbf{y} \in \mathbb{F}_p^n$ is the subset $\mathbf{Supp}(\mathbf{y}) \subset \{1, \dots, n\}$ of the indexes of its nonzero entries.

(1) Let $\zeta = e^{\frac{2i\pi}{p}} \in \mathbb{C}$ be a primitive p–th root of unity. Prove that for any integer ℓ prime to p we have

$$\sum_{j \in \mathbb{F}_p \setminus \{0\}} \zeta^{\ell j} = -1.$$

Note. Since, for $t \in \mathbb{Z}$, the number ζ^t depends only on the class of t modulo p, the notation ζ^a for $a \in \mathbb{F}_p$ makes sense.

(2) Let ℓ be a positive integer and $\mathbf{x} = (x_1, \dots, x_\ell, 0, \dots, 0) \in \mathbb{F}_p^n$ where $x_1, \dots, x_\ell$ are all nonzero. Let $0 \leqslant j \leqslant \ell$ and $I \subseteq \{1, \dots, n\}$ be a set such that $|I \cap \{1, \dots, \ell\}| = j$ and $D_I \subseteq \mathbb{F}_p^n$ be the set of vectors whose support equals I. Prove that

$$\sum_{\mathbf{y} \in D_I} \zeta^{\langle \mathbf{x}, \mathbf{y} \rangle} = (-1)^j (p-1)^{|I|-j}.$$

(3) Let t be a positive integer, with $t \geqslant j$ and $\mathbb{S}(0,t) \subseteq \mathbb{F}_p^n$ be the set of vectors of weight t. Deduce from the previous result that

$$\sum_{\mathbf{y} \in \mathbb{S}(0,t)} \zeta^{\langle \mathbf{x}, \mathbf{y} \rangle} = \sum_{j=0}^{t} \binom{\ell}{j} \binom{n-\ell}{t-j} (-1)^j (p-1)^{t-j}. \tag{1}$$

(4) The right hand side of (1) is a polynomial expression in ℓ that we denote by $K_t(\ell)$. Deduce from the previous questions that for any $\mathbf{x} \in \mathbb{F}_p^n$ of weight ℓ,

$$\sum_{\mathbf{y} \in \mathbb{S}(0,t)} \zeta^{\langle \mathbf{x}, \mathbf{y} \rangle} = K_t(\ell).$$

(5) Let $\mathcal{C} \subseteq \mathbb{F}_p^n$ be a code and $P_{\mathcal{C}} = \sum_{\ell=0}^{n} A_\ell z^\ell$ its weight enumerator polynomial. Prove that for any $0 \leqslant t \leqslant n$,

$$\sum_{\ell=0}^{n} A_\ell K_t(\ell) \geqslant 0.$$

Hint. One can use the following fact appearing in your lecture notes. For any $\mathbf{y} \in \mathbb{F}_p^n$,

$$\sum_{\mathbf{c} \in \mathcal{C}} \zeta^{\langle \mathbf{c}, \mathbf{y} \rangle} = \begin{cases} |\mathcal{C}| & \text{if} \quad \mathbf{y} \in \mathcal{C}^\perp \\ 0 & \text{else} \end{cases}$$

(6) Deduce that the coefficients of weight enumerator $P_{\mathcal{C}} = \sum_{\ell=0}^{n} A_\ell z^\ell$ of a code $\mathcal{C} \subseteq \mathbb{F}_p^n$ of minimum distance d and dimension k should satisfy the following equations and inequations
  (i) $A_0 + \cdots + A_n = p^k$;
  (ii) $A_1 = \cdots = A_{d-1} = 0$;
  (iii) $\forall t \geqslant d$, $\sum_{\ell=0}^{n} A_\ell K_t(\ell) \geqslant 0$.

(7) We wish to know the maximum dimension of a linear code over $\mathbb{F}_2$ of length 9 and minimum distance $\geqslant 4$ having only even weight codewords. In this context the inequations of the previous question yield (you can admit that fact) $A_4 \leqslant 18$, $A_6 \leqslant \frac{24}{5}$ and $A_8 \leqslant \frac{9}{5}$. What is the largest possible dimension of a such a code ?

(8) Prove that the previous result is sharper than what one could prove using the Hamming bound.