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.

Answer : The code is the right kernel of the matrix :

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

One first observes that the code contains the vector $\mathbf{1} = (1\ 1\ 1\ 1\ 1\ 1\ 1)$ since the rows of $\mathbf{H}$ have all even weight. Therefore, the number of words of weight i equals that of words of weight $7 - i$ du to the bijection $\mathbf{x} \mapsto \mathbf{x} + \mathbf{1}$.
Set $P_C(z) := \sum_{i=0}^{7} P_i z^i$. One knows that $P_0 = P_7 = 1$ since the code contains the vector 0 and $\mathbf{1}$. Since the code has minimum distance 2 we deduce that $P_1 = P_2 = 0$ and then, by symmetry : $P_5 = P_6 = 0$.
Let us compute P_3. It corresponds to number the triples of distinct columns of $\mathbf{H}$ that sum up to 0. For any non ordered pair $\{\mathbf{u}, \mathbf{v}\}$ of distinct columns, we get the non ordered triple $\{\mathbf{u}, \mathbf{v}, \mathbf{u}+\mathbf{v}\}$. On the other hand any such triple can be obtained from 3 distinct pairs, namely $\{\mathbf{u}, \mathbf{v}\}$, $\{\mathbf{u}, \mathbf{u}+\mathbf{v}\}$ and $\{\mathbf{v}, \mathbf{u}+\mathbf{v}\}$. This yields $\frac{1}{3}\binom{7}{2} = 14$ such triples. In summary, we get

$$P_C(z) = 1 + 7z^3 + 7z^4 + z^7.$$

(2) Deduce that of its dual.

Answer : Using McWilliams identity, or computing the weight if any codeword, we get :

$$P_{C^\perp}(z) = 1 + 7z^4$$

(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 ?

Answer : For the number of codewords of weight 3 one uses the same approach and get :

$$P_3 = \frac{1}{3}\binom{2^\ell - 1}{2}.$$

Then, to count 4-tuples of columns that sum up to 0, we count any possible triple excluding the triples that sum up to 0. This gives :

$$P_4 = \frac{1}{4}\left(\binom{2^\ell - 1}{3} - P_3\right).$$

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.

Answer :

$$\{0\},\ \{1,5\},\ \{2,10\},\ \{3\},\ \{4,8\},\ \{6\},\ \{7,11\},\ \{9\}$$

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

Answer : There are 8 minimal cyclotomic classes, thus $2^8 = 256$ manner to combine them. Hence 256 such codes.

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

Answer : We have to count the number of cyclotomic classes of cardinality 3. For this sake we need to combine a minimal class of cardinality 2 and one of cardinality 1 or combine three classes of cardinality 1. This yields $4 \times 4 + \binom{4}{3} = 20$ possibilities.

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

Answer : Apply the BCH bound to the code associated to the cyclotomic class of $\{1,2,3,4,5,8,10\}$ It contains the sequence $(1,2,3,4,5)$ and hence has minimum 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.

Answer :

$$\begin{aligned}\sum_{j=1}^{p-1} \zeta^{\ell j} &= -1 + \sum_{i=0}^{p-1} \zeta^{\ell j} \\ &= -1 + \frac{(\zeta^\ell)^p - 1}{\zeta^\ell - 1} \\ &= -1 + 0,\end{aligned}$$

where the last equality comes from the fact that ζ is a p–th root of unity and hence so is ζ^ℓ.

(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

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

Answer : Set $t = |I|$. Denote by $I = \{i_1, \ldots, i_j, \ldots, i_t\}$. The set $\{1, \ldots, \ell\} \cap I$ equals $\{i_1, \ldots, i_j\}$.

$$\begin{aligned}
\sum_{\mathbf{y} \in D_I} \zeta^{\langle \mathbf{x}, \mathbf{y} \rangle} &= \sum_{\mathbf{y} \in D_I} \zeta^{x_{i_1} y_{i_1} + \cdots + x_{i_t} y_{i_t}} \\
&= \prod_{s=1}^{t} \left(\sum_{y_{i_s} \in \mathbb{F}_p \setminus \{0\}} \zeta^{x_{i_s} y_{i_s}} \right) \\
&= \prod_{s=1}^{j} \left(\sum_{y_{i_s} \in \mathbb{F}_p \setminus \{0\}} \zeta^{x_{i_s} y_{i_s}} \right) \cdot \prod_{s=j+1}^{t} \left(\sum_{y_{i_s} \in \mathbb{F}_p \setminus \{0\}} 1 \right),
\end{aligned}$$

where the last equality comes from the fact that for $s > j$, we have $x_s = 0$. Finally, using the previous question, we get the result.

(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

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

Answer : It suffices to count the number of possible sets I of cardinality t that meet $\{1, \ldots, \ell\}$ at j elements, which is

$$\binom{\ell}{j} \binom{n-\ell}{t-j}.$$

Then, it is a direct consequence of the previous question.

(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,

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

Answer : Up to a permutation of the entries, one can suppose that $\mathbf{x} = (x_1, \ldots, x_\ell, 0, \ldots, 0)$ where $x_1, \ldots, x_\ell$ are all nonzero. Then it is a direct consequence of the previous results.

(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 $\mathbf{y} \in \mathbb{F}_p^n$,

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

Answer :

$$\begin{aligned}\sum_{\ell=0}^{n} A_\ell K_t(\ell) &= \sum_{\ell=0}^{n}\sum_{\mathbf{c}\in\mathcal{C}} K_t(\ell)\\ &= \sum_{\ell=0}^{n}\sum_{\mathbf{c}\in\mathcal{C}}\sum_{\mathbf{y}\in\mathbb{S}(0,t)} \zeta^{\langle \mathbf{y},\mathbf{c}\rangle}\\ &= \sum_{\ell=0}^{n}\sum_{\mathbf{y}\in\mathbb{S}(0,t)\cap\mathcal{C}^\perp} |\mathcal{C}|\\ &\geqslant 0\end{aligned}$$

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

Answer : (6i) is due to the fact that $A_0 + \cdots + A_n = |\mathcal{C}|$. (6ii) is due to the assumption that the minimum distance is d and hence there are no nonzero codewords of weight less than d. (6iii) is a direct consequence of the previous question.

(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 ?

Answer : Clearly $A_0 = 1$ since the code is linear and hence contains the zero codeword. Then applying (6i), we get

$$2^k \leqslant 1 + 18 + \frac{24}{5} + \frac{9}{5} = 128/5 = 25.6.$$

Therefore, the dimension is at most 4.

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

Answer : Using the Hamming bound, we should find the largest possible k such that

$$2^k \mathrm{Vol}_2(9,1) \leqslant 2^9.$$

That is

$$2^k \leqslant \frac{2^9}{9} \leqslant \frac{2^9}{2^4} = 2^5,$$

which yields $k \leqslant 5$. Hence the upper bound obtained in the previous question is sharper.