MPRI 2.13.2 - Error-correcting codes and applications to cryptography

Exercises
15/11/2023

Exercise 1. *Weight distribution of some self-dual code*
Let $\mathcal{C} \subseteq \mathbf{F}_q^n$ be a *self-dual* code, i.e., $\mathcal{C} = \mathcal{C}^\perp$.

1. Show that the length n of $\mathcal{C}$ is even and that its dimension equals $\frac{n}{2}$.
2. Show that all codewords in a binary self-dual code have an even Hamming weight.
3. Let $\mathcal{C}$ be a binary self-dual code of length 6. Show that its weight enumerator has the following form
$$P_{\mathcal{C}}(x, y) = y^6 + a_2x^2y^4 + a_4x^4y^2 + a_6x^6$$
with $a_6 \in \{0, 1\}$ and $1 + a_2 + a_4 + a_6 = 8$.
4. Deduce from MacWilliams' formula that such a code contains the all-one word.
5. Deduce that $a_2 = a_4$.
6. Compute the weight distribution of a binary self-dual code of length 6.

Exercise 2. *Cyclic codes*
We want to study the cyclic codes included in $\mathbf{F}_3^{13}$. We recall that the q-ary cyclotomic cosets modulo 13 are the subsets of $\mathbb{Z}/13\mathbb{Z}$ invariant under multiplication by q.

1. Give the list of all cyclotomic cosets modulo 13 which are minimal for inclusion.
2. Deduce the existence of a cyclic code included in $\mathbf{F}_3^{13}$, of dimension 7 and minimum distance at least 5.
3. We now consider $\mathbf{F}_{27}$. What are the cyclotomic classes modulo 13, i.e. the subsets of $\mathbb{Z}/13\mathbb{Z}$ invariant under multiplication by 27?
4. Prove that there exist MDS cyclic codes included in $\mathbf{F}_{27}^{13}$.

Exercise 3. *Griesmer bound*
Let $\mathcal{C}$ be a linear binary code of length n, dimension k and minimum distance d. W.l.o.g. we assume that the word $c = (1 \cdots 1 \ 0 \cdots\cdots 0)$ of weight d defined by $c_1 = \cdots = c_d = 1$ and $c_{d+1} = \cdots = c_n = 0$ belongs to $\mathcal{C}$ (otherwise, the coordinates of the code can be permuted, since it does not influence the weight distribution). Let p be the mapping defined by

$$p : \begin{array}{ccc} \mathbf{F}_2^n & \to & \mathbf{F}_2^{n-d} \\ (x_1, \ldots, x_n) & \mapsto & (x_{d+1}, \ldots, x_n). \end{array}$$

1. Prove that c is the unique word in $\mathcal{C} \setminus \{0\}$ such that $p(c) = 0$.
2. Prove that the image $\mathcal{C}'$ of $\mathcal{C}$ by p has dimension $k - 1$.
3. Let d' be the minimum distance of $\mathcal{C}'$. Let $v \in \mathcal{C}$ be a word such that $p(v) \in \mathcal{C}'$ has weight d'. Let $a = w_H(v) - d'$. Prove that

(i) $a + d' \geq d$;

(ii) $d - a + d' \geq d$.

4. Deduce that $d' \geq \frac{d}{2}$.

5. Show that, for any binary code $\mathcal{C}$ with parameters $[n, k, d]$, we have

$$n \geq \sum_{i=0}^{k-1} \frac{d}{2^i}. \tag{1}$$

6. Exhibit a generator matrix of a binary $[6, 2, 4]$-code, and a generator matrix of a binary $[9, 2, 6]$-code. More generally, prove that the Griesmer bound (1) is optimal for $k = 2$ and n multiple of 3.

7. Let $(\mathcal{C}_\ell)_{\ell \in \mathbb{N}}$ be a sequence of codes with parameters $[n_\ell, k_\ell, d_\ell]$ such that $(n_\ell)_\ell$ and $(k_\ell)_\ell$ tend to infinity and $(d_\ell/n_\ell)_\ell$ converges to some integer δ. Prove that $\delta \leq \frac{1}{2}$.

8. Is this result more or less accurate that the asymptotic Plotkin bound?