MTAT.05.082: Introduction to Coding Theory **University of Tartu**

Homework Assignment 4

Due date: November 30, 2018

It is possible to collect up to 110 points in this homework.

1. Show that the minimum distance of a perfect code must be odd.

   Reminder. *Perfect* code is a code that achieves the sphere-packing bound with equality.

2. Let $\mathcal{C}$ be a Hamming code of length $n = (q^m - 1)/(q - 1)$ over the finite field $\mathbb{F} = \mathbb{F}_q$. For $i = 0, 1, \cdots, n$, denote by W_i the number of codewords in $\mathcal{C}$ of Hamming weight i.

   (a) Let $\mathcal{D}$ be a nearest-codeword decoder for $\mathcal{C}$ and let $\boldsymbol{c}$ be a codeword of Hamming weight t in $\mathcal{C}$. For each of the following values of i, find the number of words of Hamming weight i in $\mathbb{F}^n$ that will be decoded by $\mathcal{D}$ into $\boldsymbol{c}$:

   (a) $i = t - 1$;
   (b) $i = t + 1$;
   (c) $i = t$.

   Hint: recall that Hamming code is a perfect code.

   (b) Show that for $0 < i < n$,

   $$(i+1) \cdot W_{i+1} + (i(q-2)+1) \cdot W_i + (n-i+1)(q-1)W_{i-1} = \binom{n}{i}(q-1)^i \,,$$

   where $W_0 = 1$ and $W_1 = 0$.

   (c) Show that $W_3 = \frac{1}{6} \cdot n(n-1)(q-1)^2$.

3. Let $G = [\ I \mid A\ ]$ be a systematic generator matrix of a linear $[n, k, d]$ code $\mathcal{C}$ over $\mathbb{F}$. Show that $\mathcal{C}$ is MDS if and only if every square sub-matrix of A is invertible.

   Reminder. *Maximum distance separable (MDS)* code is a code that achieves the Singleton bound with equality.

4. Let $\mathcal{C}$ be an (n, M, d) code over an alphabet $\mathbb{F}$ of size q. The Hamming distance from $\mathcal{C}$ of a word $\bar{\boldsymbol{y}} \in \mathbb{F}^n$, denoted by $\mathsf{d}(\bar{\boldsymbol{y}}, \mathcal{C})$, is defined as the Hamming distance between $\bar{\boldsymbol{y}}$ and a nearest to $\bar{\boldsymbol{y}}$ codeword in $\mathcal{C}$, i.e.

   $$\mathsf{d}(\bar{\boldsymbol{y}}, \mathcal{C}) = \min_{\bar{\boldsymbol{c}} \in \mathcal{C}} \mathsf{d}(\bar{\boldsymbol{y}}, \bar{\boldsymbol{c}}) \,.$$

   The *covering radius* of $\mathcal{C}$, denoted by R, is the largest distance of any word in $\mathbb{F}^n$ from $\mathcal{C}$, i.e.

   $$\mathsf{R} = \max_{\bar{\boldsymbol{y}} \in \mathbb{F}^n} \mathsf{d}(\bar{\boldsymbol{y}}, \mathcal{C}) \,.$$

   (a) Find the covering radius of the $[n, 1, n]$ repetition code over $\mathbb{F}$.

(b) Find the covering radius of the Hamming $[n, n-m, 3]$ code over $\mathbb{F}$, where

$$n = (q^m - 1)/(q-1) \ .$$

(c) (The sphere-covering bound.) Show that

$$M \cdot \mathcal{S}_{\mathsf{R},n} \geq q^n \ ,$$

where $\mathcal{S}_{\mathsf{R},n} = \mathcal{S}_{\mathsf{R},n}(\bar{\boldsymbol{x}})$ is the volume of the sphere of radius R in $\mathbb{F}^n$ around any $\bar{\boldsymbol{x}} \in \mathbb{F}^n$.

(d) Show that $\mathsf{R} \geq (d-1)/2$ and that equality holds if and only if $\mathcal{C}$ is perfect.

(e) Show that if $\mathcal{C}$ is a linear $[n, k, d]$ code over a finite field $\mathbb{F}_q$, then $\mathsf{R} \leq n - k$.

(f) An (n, M, d) code is called *maximal* if the addition of any new codeword to $\mathcal{C}$ reduces its minimum distance. Show that if $\mathcal{C}$ is maximal then $\mathsf{R} < d$.