Homework 4

Due date: November 16, 2016

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

1. Show that the linear \([n, k, d]\) code \(C\) over \(\mathbb{F}\) is MDS if and only if every set of \(k\) columns in its generator matrix is linearly independent.

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

2. 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.

3. Let \(H_{GRS}\) be a parity-check matrix of the \([4, 2, 3]\) GRS code \(C\) over \(\mathbb{F}_5\) given by

\[
H_{GRS} = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4
\end{pmatrix}
\]

Find a generator matrix \(G_{GRS}\) of \(C\) in the canonical form, i.e.

\[
G_{GRS} = \begin{pmatrix}
v_1 & v_2 & \ldots & v_n \\
v_1 \alpha_1 & v_2 \alpha_2 & \ldots & v_n \alpha_n \\
\vdots & \vdots & \ddots & \vdots \\
v_1 \alpha_1^{k-1} & v_2 \alpha_2^{k-1} & \ldots & v_n \alpha_n^{k-1}
\end{pmatrix}
\]

Conclude that dual code \(C^\perp\) is also GRS.

**Hint.** It can be helpful to note that dual code of GRS code can be described with the same code locators as the original code but perhaps different column multipliers.

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

\[
d(\vec{y}, C) = \min_{\vec{c} \in C} d(\vec{y}, \vec{c})
\]

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

\[
R = \max_{\vec{y} \in \mathbb{F}^n} d(\vec{y}, C)
\]

(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

\[ M \cdot S_{R,n} \geq q^n, \]

where \( S_{R,n} = S_{R,n}(\bar{x}) \) is the volume of the sphere of radius \( R \) in \( \mathbb{F}^n \) around any \( \bar{x} \in \mathbb{F}^n \).

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

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

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