MATH 8560 - Spring 2016

Homework 3

Due: Mar. 3rd (Thursday)

QUESTION 1. *Erasure correctability.*

Let e be an erasure pattern, i.e., $e \subseteq [n]$ (an index set for the erased positions of a received word). Let $P_e : \mathbb{F}_q^n \to \mathbb{F}_q^n$ denote the projection map defined by $P_e(v) = w$ where

$$w_i = \begin{cases} 0 & \text{if } i \in e \\ v_i & \text{otherwise} \end{cases}$$

In other words, P_e substitutes zeros for the symbols that would have been erased by e.
Let $\mathcal{C}$ be an $[n, k]$ linear code. Prove that the following are equivalent:

1. The erasure pattern e is correctable by $\mathcal{C}$.
2. No nonzero codeword $c \in \mathcal{C}$ has $\mathrm{supp}(v) \subseteq e$.
3. $\dim \ker P_e\restriction_{\mathcal{C}} = 0$.
4. $\dim P_e(\mathcal{C}) = \dim \mathcal{C}$.

Now, let $P(v) = \{X \subseteq [n] \mid \mathrm{supp}(v) \subseteq X\}$ be the set of erasure patterns that contain the support of v. The set $U(\mathcal{C})$ of uncorrectable erasure patterns associated with $\mathcal{C}$ is then $U(\mathcal{C}) = \bigcup_{c \in \mathcal{C} \setminus \{0\}} P(v)$. Note that if $|e| < d_{min}(\mathcal{C})$, then $e \notin U(\mathcal{C})$.

QUESTION 2. *Perfect codes.*

A code is called perfect if it attains the sphere-packing bound.

1. Show that the minimum distance of a perfect code must be odd.
2. Let $\mathcal{C}$ be a perfect $(n, M, d = 2t + 1)$ code over $\mathbb{F}_q$ and suppose that $0 \in \mathcal{C}$. Show that the cardinality of

$$|\{c \in \mathcal{C} \mid \mathrm{wt}(c) = 2t + 1\}| = \frac{\binom{n}{t+1}(q-1)^{t+1}}{\binom{2t+1}{t}}.$$

QUESTION 3. *Constant weight codes.*

Let $\mathcal{C}$ be a $(n, M, d; w)$ constant-weight code, i.e., a code having only codewords of weight w.

- Prove or disprove: there exists a linear constant-weight code.
- If $\mathcal{C}$ has parameters $(n, M, 2t + 1; 2t + 1)$, prove that

$$M \leq \frac{\binom{n}{t+1}(q-1)^{t+1}}{\binom{2t+1}{t}}.$$

- When is the bound attained?

QUESTION 4. *Doubly-extended GRS codes.*

A $[n, n - r, d]$ code $\mathcal{C}$ over $\mathbb{F}$ is a doubly-extended GRS code if it is defined by a parity check matrix

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{r-2} & \alpha_2^{r-2} & \cdots & \alpha_{n-1}^{r-2} & 0 \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_{n-1}^{r-1} & 1 \end{pmatrix} \begin{pmatrix} v_1 & 0 & \cdots & 0 \\ 0 & v_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & v_n \end{pmatrix}$$

where $\alpha_1, \ldots, \alpha_{n-1}$ are distinct elements and $v_1, \ldots, v_n$ are nonzero elements of $\mathbb{F}_q$.

- Show that $\mathcal{C}$ is MDS.
- Show that $\mathcal{C}^\perp$ is also a doubly-extended GRS code.