# MATH 8560 - Spring 2014

# Homework 3

Due: Feb. 27th (Thursday)

**Question 1.** **(3 marks)**

*(Log likelihood ratio)*

Let $S = (\mathbb{F}_2, p(y \mid x), \mathcal{Y})$ be a binary memoryless channel such that $p(y \mid x) \geq 0$ for any $y \in \mathcal{Y}$ and $x \in \mathbb{F}_2$. The *log likelihood ratio* for a $y \in \mathcal{Y}$ is

$$\mu(y) := \log_2 \left( \frac{p(y \mid 0)}{p(y \mid 1)} \right).$$

Let $\mathcal{C}$ be a $(n, M)$ code over $\mathbb{F}_2$, and define the decoder $\mathcal{D} : \mathcal{Y}^n \to \mathcal{C}$ such that for any $y = (y_1, \ldots, y_n) \in \mathcal{Y}^n$

$$\mathcal{D}(y) = \mathrm{argmax}_{c \in \mathcal{C}} \sum_{i=1}^{n} (-1)^{c_i} \mu(y_i).$$

Show that $\mathcal{D}$ is a maximum-likelihood decoder for $\mathcal{C}$ with respect to $S$.

**Question 2.** **(3 marks)**

*(Decoding failure)*

Show that for every $(n, M, d)$ codes $\mathcal{C}$ over $\mathcal{X}$ and for every decoder $\mathcal{D} : \mathcal{X}^n \to \mathcal{C}$, there is a codeword $c \in \mathcal{C}$ and a vector $y \in \mathcal{X}^n$ such that $d(y, c) \leq \lfloor (d+1)/2 \rfloor$ and $\mathcal{D}(y) \neq c$.

**Question 3.** **(6 marks)**

*(Some properties of linear codes)*

Let $\mathcal{C} \subset \mathbb{F}_2^n$ be a $[n, k]$ linear code.

1. Show that either any codeword has even weight, or exactly half of them have even weight.
2. If $\mathcal{C}$ has a codeword of odd weight, then show that the even weight codewords of $\mathcal{C}$ form an $[n, k-1]$ linear code.
3. Show that either all codewords in $\mathcal{C}$ begin with 0, or exactly half of them begin with zero.
4. Show that the sum of the weights of all codewords in $\mathcal{C}$ is at most $n2^{k-1}$.

**Question 3.** **(3 marks)**

*(Puncturing a linear code)*

Let $\mathcal{C}$ be a linear $[n, k, d]$ code over a field $\mathbb{F}$. For $i = 1, \ldots, n$ denotes with $\mathcal{C}_i$ the code

$$\mathcal{C}_i := \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \mid (c_1, \ldots, c_n) \in \mathbb{F}_n\}.$$

The code $\mathcal{C}_i$ is said to be obtained by puncturing $\mathcal{C}$ at the $i$-th coordinate.

- Show that $\mathcal{C}_i$ is a linear $[n-1, k_i, d_i]$ code over $\mathbb{F}$ where $k_i \geq k - 1$ and $d_i \geq d - 1$.
- Show that there are at least $n - k$ indices $i$ for which $k_i = k$.