Information Theory

Exercise Sheet 7

Exercise 1 (Compute some dimensions and minimum distance)**.** *Let,*

$$(U, U+V) \stackrel{def}{=} \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \ \mathbf{u} \in U \ \textit{and} \ \mathbf{v} \in V\} \ \textit{where } U, V \subseteq \mathbb{F}_q^{n/2} \textit{ are linear codes.}$$

$$\mathrm{RS}_k(\mathbf{x}) = \{(f(x_1), \dots, f(x_n)) : \ f \in \mathbb{F}_q[X] \ \textit{and} \ \deg(f) < k \leq n\} \ \textit{where the } x_i\textit{'s are distinct}$$

1. *Show that* $(U, U+V)$ *and* $\mathrm{RS}_k(\mathbf{x})$ *are linear codes.*
2. *Compute their dimension.*
3. *Compute their minimum distance.*

Exercise 2 (Minimum distance and parity-check matrix)**.** *Let* $\mathcal{C} \subseteq \mathbb{F}_q^n$ *with parity-check matrix* $\mathbf{H}$*. Show that*

$$\mathcal{C} \textit{ has minimum distance} \geq d \iff \textit{every } d-1 \textit{ columns of } \mathbf{H} \textit{ form a free family}$$

Exercise 3 (Minimum distance and syndrome)**.** *Let* $\mathcal{C}$ *be a linear code with minimum distance* d*. Show that the* $\mathbf{He}^\top$ *are distinct when* $|\mathbf{e}| \leq \lfloor (d-1)/2 \rfloor$*.*

Exercise 4 (About large Hamming weight codewords)**.** *Let* $\mathcal{C}$ *be a binary linear code with minimum distance* d*. Let* $t \in (n - d/2, n]$*. Show that there exists at most one codeword with Hamming weight* t*.*

Exercise 5 (About the (non-asymptotic) Gilbert-Varshamov bound)**.** *Show the following statement*

$$q^k \cdot \sum_{i=0}^{d-2} \binom{n}{i} (q-1)^i < q^n \implies \textit{ it exits an } [n,k]_q\textit{-code with minimum distance } d$$

Hint: *use the result of Exercise 2*

Exercise 6 (Poisson summation formula and linear programming bounds)**.** *In this exercise we suppose that q is prime. Let,*

$$\forall \mathbf{x} \in \mathbb{F}_q^n,\ \chi_{\mathbf{x}} : \mathbf{y} \in \mathbb{F}_q^n \mapsto \mathrm{e}^{2i\pi\langle \mathbf{x},\mathbf{y}\rangle/q} \quad \textit{where} \quad \langle \mathbf{x},\mathbf{y}\rangle = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_q$$

1. *Given an $[n,k]_q$-code code $\mathcal{C}$, show that*

$$\sum_{\mathbf{c}\in\mathcal{C}} \chi_{\mathbf{c}}(\mathbf{y}) = \begin{cases} q^k \ \textit{if}\ \mathbf{y} \in \mathcal{C}^{\perp} \\ 0 \ \textit{otherwise} \end{cases}$$

2. *Recall that for $f : \mathbb{F}_q^n \longrightarrow \mathcal{C}$, its Fourier transform is defined as:*

$$\widehat{f}(\mathbf{y}) = \frac{1}{q^n} \sum_{\mathbf{x}\in\mathbb{F}_q^n} f(\mathbf{x})\chi_{\mathbf{y}}(\mathbf{x})$$

   Show the Poisson summation formula, i.e. for all $[n,k]_q$-codes,

$$\sum_{\mathbf{c}\in\mathcal{C}} f(\mathbf{c}) = q^k \cdot \sum_{\mathbf{c}^{\perp}\in\mathcal{C}^{\perp}} \widehat{f}(\mathbf{c}^{\perp})$$

3. *Let $\mathcal{C}$ be an $[n,k]_q$-code and $f : \mathbb{F}_q^n \to \mathbb{C}$ such that*

$$(1) : f(\mathbf{x}) \leq 0 \ \textit{for}\ |x \geq d_{\min}(\mathcal{C}) \quad \textit{and} \quad (2) : \widehat{f}(\mathbf{t}) \geq 0 \ \textit{for all}\ \mathbf{t}.$$

   Then,

$$q^k \leq \frac{f(\mathbf{0})}{\widehat{f}(\mathbf{0})}.$$

4. *Let $f, g : \mathbb{F}_q^n \longrightarrow \mathbb{C}$, show that*

$$\widehat{f \star g} = q^n \ \widehat{f} \cdot \widehat{g}$$

   where $\star$ denotes the convolution product, i.e.

$$f \star g(\mathbf{x}) = \sum_{\mathbf{y}\in\mathbb{F}_q^n} f(\mathbf{y})g(\mathbf{x}-\mathbf{y})$$

5. *Use the result of Question 3 with the following function,*

$$f(\mathbf{x}) = 1_{\left\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \right\rfloor} \star 1_{\left\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \right\rfloor}$$

where $1_{\left\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \right\rfloor}$ *denotes the indicator function of the Hamming ball* $\mathcal{B}\left(\left\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \right\rfloor\right)$ *of radius* $\left\lfloor \frac{d_{\min}(\mathcal{C})-1}{2} \right\rfloor$.

What do you deduce?