Information Theory

Exercise Sheet 8

Exercise 1 (Fundamental equality for random codes)**.** *Let* $\mathbf{H}$ *be a matrix picked uniformly at random among* $\mathbb{F}_q^{(n-k)\times n}$*. Show that,*

$$\forall \mathbf{s} \in \mathbb{F}_q^{n-k},\ \forall \mathbf{x} \in \mathbb{F}_q^{n}\backslash\{\mathbf{0}\},\ \ \mathbb{P}_{\mathbf{H}}\left(\mathbf{H}\mathbf{x}^\top = \mathbf{s}^\top\right) = \frac{1}{q^{n-k}}$$

Exercise 2 (Estimating the weight distribution of random linear codes)**.** *Let* $\mathcal{C} \subseteq \mathbb{F}_q^n$ *be a linear code and,*

$$N_t(\mathcal{C}) = \sharp\{\mathbf{c} \in \mathcal{C} :\ |\mathbf{c}| = t\}$$

Show that

$$\forall t \in [1, n], \quad \mathbb{E}_{\mathcal{C}}\left(N_t(\mathcal{C})\right) = \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$

when $\mathcal{C}$ *is a random* $[n,k]_q$*-code, i.e.,*

$$\mathcal{C} = \left\{\mathbf{c} \in \mathbb{F}_q^n :\ \mathbf{H}\mathbf{c}^\top = \mathbf{0}\right\}$$

with $\mathbf{H}$ *being picked uniformly at random among* $\mathbb{F}_q^{(n-k)\times n}$*.*

Exercise 3 (Almost all codes have minimum distance the Gilbert-Varshamov bound)**.** *In the previous exercise we have shown that the expected number of codewords of weight* $t > 0$ *in a random* $[n,k]_q$*-code is given by*

$$\frac{\binom{n}{t}(q-1)^t}{q^{n-k}}$$

We therefore expect that the minimum distance of a random code is roughly given by the minimum t_0 *such that*

$$\binom{n}{t_0}(q-1)^{t_0} \geq q^{n-k}$$

Our aim is to prove this (at least asymptotically). Let us admit that

$$\frac{t_0}{n} \xrightarrow[n\to+\infty]{} \delta_{\mathrm{GV}} \overset{def}{=} h_q^{-1}(1-R)$$

where $R \stackrel{def}{=} k/n$ *and* $h_q(x) = -(1-x)\log_2(1-x) - x\log_q(x/(q-1))$ *is the* q*-ary entropy. Let us also admit that,*

$$x \in [0, \delta_{\mathrm{GV}}] \mapsto h_q(x) \text{ is an increasing function and } \binom{n}{t}(q-1)^t = q^{nh_q(t/n)(1+o(1))}$$

Our aim in this exercise is to show that,

$$\mathbb{P}_{\mathcal{C}}\left((1-\varepsilon)\delta_{\mathrm{GV}} < \frac{d_{\min}(\mathcal{C})}{n} < (1+\varepsilon)\delta_{\mathrm{GV}}\right) \geq 1 - q^{-\alpha n(1+o(1))}$$

where $\alpha \stackrel{def}{=} \min\left((1-R) - h_q\left((1+\varepsilon)\delta_{\mathrm{GV}}\right), h_q\left((1-\varepsilon)\delta_{\mathrm{GV}}\right) - (1-R)\right) > 0$ *and* $\mathcal{C}$ *is a random* $[n, Rn]_q$*-code as defined in the previous exercise (via a uniform parity-check matrix).*

1. *Let* $k \stackrel{def}{=} Rn$*. Show that,*

$$\mathbb{P}_{\mathcal{C}}\left(\frac{d_{\min}(\mathcal{C})}{n} \leq (1-\varepsilon)\delta_{\mathrm{GV}}\right) \leq \sum_{\ell=0}^{(1-\varepsilon)n\delta_{\mathrm{GV}}} \frac{\binom{n}{\ell}(q-1)^\ell}{q^{n-k}}$$

Deduce that,

$$\mathbb{P}_{\mathcal{C}}\left(\frac{d_{\min}(\mathcal{C})}{n} \leq (1-\varepsilon)\delta_{\mathrm{GV}}\right) \leq q^{-\alpha n(1+o(1))}$$

Let $\mathbb{1}_{\mathbf{x}}$ *be the indicator function of the event* $\mathbf{H}\mathbf{x} = \mathbf{0}$ *(recall that* $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ *is supposed uniform) and*

$$N_t(\mathcal{C}) = \sharp\left\{\mathbf{c} \in \mathcal{C} : |\mathbf{c}| = t\right\}$$

2. *Show that for all* $a > 0$*,*

$$\mathbb{P}_{\mathcal{C}}\left(\left|N_t(\mathcal{C}) - \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}\right| \geq a\right) \leq \frac{1}{a^2}\left(\frac{\binom{n}{t}(q-1)^t}{q^{n-k}} + \sum_{\substack{\mathbf{x},\mathbf{y}:|\mathbf{x}|=|\mathbf{y}|=t \\ \mathbf{x}\neq\mathbf{y}}} \mathbb{E}_{\mathcal{C}}(\mathbb{1}_{\mathbf{x}}\mathbb{1}_{\mathbf{y}}) - \mathbb{E}_{\mathcal{C}}(\mathbb{1}_{\mathbf{x}})\mathbb{E}_{\mathcal{C}}(\mathbb{1}_{\mathbf{y}})\right)$$

3. *Show that,*

$$\mathbb{E}_{\mathbf{H}}(\mathbb{1}_{\mathbf{x}}\mathbb{1}_{\mathbf{y}}) \leq \begin{cases} \frac{1}{q^{n-k}} & \text{if } \mathbf{x} \text{ and } \mathbf{y} \text{ are colinear} \\ \frac{1}{q^{2(n-k)}} & \text{otherwise.} \end{cases}$$

4. *Deduce that,*

$$\mathbb{P}_{\mathcal{C}}\left(\left|N_t(\mathcal{C}) - \frac{\binom{n}{t}(q-1)^t}{q^{n-k}}\right| \geq a\right) \leq \frac{(q-2)\binom{n}{t}(q-1)^t}{q^{n-k}}$$

5. *By using the previous question, show that*

$$\mathbb{P}_{\mathcal{C}}\left(\frac{d_{\min}(\mathcal{C})}{n} \geq (1+\varepsilon)\delta_{\mathrm{GV}}\right) \leq (q-1)\frac{q^{n-k}}{\binom{n}{u}(q-1)^u}$$

   for some well chosen u.

6. *Conclude.*