Advanced Quantum Information and Computing

Exercise Sheet 1

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

$(U, U+V) \stackrel{def}{=} \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \mathbf{u} \in U \text{ and } \mathbf{v} \in V\}$ *where* $U, V \subseteq \mathbb{F}_2^{n/2}$ *are linear codes.*

1. *Show that* $(U, U+V)$ *is a linear code.*
2. *Compute its dimension.*
3. *Compute its minimum distance.*

Exercise 2 (From one representation to the other)**.** *Show how from a generator matrix of an* $[n, k]$*-code we can compute a parity-check matrix in time* $O(n^3)$ *(and reciprocally).*

Exercise 3 (Minimum distance out of 2 for linear codes)**.** *Let* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *be a linear code. Recall that its minimum distance* d *is defined as*

$$d \stackrel{def}{=} \min\left(|\mathbf{c}| \ : \ \mathbf{c} \in \mathcal{C} \backslash \{\mathbf{0}\}\right)$$

where $|\cdot|$ *denotes the Hamming weight, namely*

$$\forall \mathbf{x} \in \mathbb{F}_2^n, \quad |\mathbf{x}| = \sharp\left\{i \in [\![1, n]\!], \ x_i \neq 0\right\}.$$

Let $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$ *be a parity-check matrix of* $\mathcal{C}$*, namely* $\mathcal{C} = \left\{\mathbf{c} \in \mathbb{F}_2^n \ : \ \mathbf{H}\mathbf{c}^\top = \mathbf{0}\right\}$*. Show that*

$$\forall \mathbf{e}_1, \mathbf{e}_2 \in \mathbb{F}_2^n : \ \mathbf{e}_1 \neq \mathbf{e}_2 \ \text{ and } \ |\mathbf{e}_1|, |\mathbf{e}_2| < \frac{d}{2} \implies \mathbf{H}\mathbf{e}_1^\top \neq \mathbf{H}\mathbf{e}_2^\top$$

Deduce an algorithm to decode linear codes via syndromes. Under which condition over the error is your algorithm successful? Is your algorithm efficient?

Exercise 4 (About large Hamming weight codewords)**.** *Let* $\mathcal{C}$ *be a 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 (Gilbert-Varshamov' bound for linear error correcting codes)**.** *We assume here that a linear code $\mathcal{C}$ of length n is drawn at random by choosing an $(n-k)\times n$ parity-check matrix $\mathbf{H}$ for it uniformly at random.*

1. *Let $\mathbf{x}\in\mathbb{F}_2^n\backslash\{\mathbf{0}\}$. Compute $\mathbb{P}(\mathbf{x}\in\mathcal{C})$.*
2. *Compute $\mathbb{E}(n_t)$ where n_t denotes the number of codewords in $\mathcal{C}$ of weight t.*
3. *What is $\mathbb{E}(n_{\leq t})$ where $n_{\leq t}$ denotes the number of non-zero codewords of weight $\leq t$?*
4. *What can you say when $\mathbb{E}(n_{\leq t})<1$?*
5. *Let $h(x)\stackrel{def}{=}-x\log_2(x)-(1-x)\log_2(1-x)$. By using*

$$\sum_{i=1}^{t-1}\binom{n}{i}\leq 2^{nh(t/n)} \tag{1}$$

which holds whenever $t/n\leq 1/2$, prove that there exists a code of minimum distance $\geq t$ and dimension $\geq k$ as soon as

$$1-h(t/n)>k/n$$

Comment: it turns out that *almost all* codes of dimension k have minimum distance t as soon as the above inequality is an equality.