ENEE739C: Homework 2. Solutions

1. We wish to prove that E contains an information set, or that $\bar{E}$ is contained in a check set (an information set of $\mathcal{C}^{\perp}$).

Let $\mathbf{s} \neq 0$ be the syndrome that corresponds to $\mathbf{x}$. For any check set B there is a vector $\mathbf{e}$ such that

$$\mathbf{H}\mathbf{e}^T = \mathbf{s}, \quad \mathrm{supp}(\mathbf{e}) \subseteq B$$

Hence $|E| \leq n - k$. Moreover, since $\mathbf{x}$ is a vector of minimum weight in its coset, there is no other vector $\mathbf{x}'$ with the same syndrome such that $\mathrm{supp}(\mathbf{x}') \subset \bar{E}$. This implies that $\mathrm{rk}(\mathbf{H}(\bar{E})) = |\bar{E}|$. Hence by Lemma 6a.3

$$0 = |\bar{E}| - \mathrm{rk}(\mathbf{H}(\bar{E})) = k - \mathrm{rk}(\mathbf{G}(E))$$

as required.

2. (a) is obvious. (b) follows from (a) and the equality

$$\sum_{i=1}^{n} \epsilon_{\mathcal{C}}(t) \binom{n}{t} = 2^{n-k}.$$

Indeed,

$$2^{n-k} = \sum_{i=1}^{n} \epsilon_{\mathcal{C}}(t) \binom{n}{t} \geq \sum_{i=0}^{t} \epsilon_{\mathcal{C}}(t) \binom{n}{t} \geq \epsilon_{\mathcal{C}}(t) \sum_{i=0}^{t} \binom{n}{t}.$$

(c) is implied by observing that for $h_2(p) > n - k$ the right-hand side of the inequality in (b) goes to 0, so the fraction of correctable errors of relative weight pn is vanishingly small.

3. Part (a) follows on observing that the outer code corrects $2e + x$ errors, so replacing one error by erasure will not increase its correcting capacity.

(b). Let s be the number of *different* reliability values in the vector W. In particular, assume that the first l_1 coordinates are erased as a result of inner decoding (so their reliability is $w_1 = 1/2$), the next l_2 coordinates all have reliability w_2, and so on up to l_s. Consider s vectors $W_i = ((1/2)^{\sum_{j=1}^{i} l_j} 0^{n_1 - \sum_{j=1}^{i} l_j})$. Let $\omega_0 = 1 - 2w_1, \omega_i = 2(w_{l_i - 1} - w_{l_i}), i = 1, \ldots, s-1, \omega_s = 2w_s$. The rest of the proof is the same.

4. The vector $\mathbf{y}$ is linearly independent of the code $\mathcal{C}$ and therefore is a unique codeword of minimum weight in the code $\mathcal{C}' = \langle \mathcal{C}, \mathbf{y} \rangle$. Therefore running the algorithm on the code $\mathcal{C}'$ finds $\mathbf{y}$, which is the error vector. This solves the decoding task.

5. See the argument in Lecture 8, Remark 2 (on p.8). Essentially the only thing to be proved is that the error exponent $E_0(R, p)$ behaves as $O(\epsilon^2)$ as $\epsilon \to 0$. This is proved by computing the Taylor series (or just by showing that the first derivative $\frac{\partial}{\partial R} D(\delta_{\mathrm{GV}}(R) \| p)$ vanishes for $R = \mathcal{C}$. Write δ for $\delta_{\mathrm{GV}}(R)$.

$$\frac{\partial D(\|p)}{\partial R} = \frac{\log \frac{\delta(1-p)}{(1-\delta)p}}{\log \frac{1-\delta}{\delta}}$$

As $R \to \mathscr{C}$, the value $\delta \to p < \frac{1}{2}$. Then the denominator tends ro a constant $\log \frac{1-p}{p}$ and the numerator to 0.

6. Linear algebra (write out a parity check symbol computed in two ways and convince yourself that the result is the same).