ENEE739C: Homework 1. Solutions

1. Let $\begin{bmatrix} n \\ k \end{bmatrix}$ be the Gaussian binomial. Consider the ensemble of all $[n,k]$ linear binary codes (there are $\begin{bmatrix} n \\ k \end{bmatrix}$ of them). A vector $\mathbf{x} \neq 0$ is contained in $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ codes. The probability that $\mathbf{x}$ is a vector in a random code from the ensemble is then

$$\Pr[\mathbf{x} \in \mathcal{C}] = \frac{\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}}{\begin{bmatrix} n \\ k \end{bmatrix}} = \frac{2^k - 1}{2^n - 1}.$$

The expected number of vectors of weight w in a code is

$$\mathsf{E}\, A_w = \binom{n}{w} \frac{2^k - 1}{2^n - 1}.$$

By the Markov inequality,

$$\Pr[A_w \geq n\binom{n}{w} 2^{k-n}] \leq \frac{\mathsf{E}\, A_w}{n\binom{n}{w}2^{k-n}} = \frac{1}{n} 2^{n-k} \frac{2^k - 1}{2^n - 1} < \frac{1}{n}$$

Hence there exists a code in the ensemble in which the number of vectors of weight w satisfies

$$A_w \leq n\binom{n}{w} 2^{k-n}$$

simultaneously for all $w = 1, 2, \ldots, n$.

2. Consider the subset $X' \subset X$ formed by all the points $\mathbf{y} \in X$ such that $\mathrm{vol}(\mathcal{B}_{d-1}(\mathbf{y})) \geq 2\langle B_{d-1} \rangle$. Clearly, $|X'| \leq |X|/2$. Consider the subset $Y = X \backslash X'$. Next perform the Gilbert procedure on Y. We see that there exists a code $\mathcal{C}$ of distance d and size M satisfying

$$M \geq \frac{|Y|}{\max_{\mathbf{y} \in Y} \mathrm{vol}(\mathcal{B}_{d-1}(\mathbf{y}))} \geq \frac{|X|}{2} \frac{1}{2\langle B_{d-1} \rangle}$$

as claimed.

3. Part (a) is obvious by considering the supports of two distinct vectors in $\mathscr{J}^{n,w}$. For part (b) let us compute the volume of the ball of radius $d - 2 = 2(\delta n - 1)$ in $\mathscr{J}^{n,w}$:

$$\mathrm{vol}(\mathcal{B}_{d-2}) = \sum_{i=0}^{\delta n - 1} \binom{w}{i} \binom{n-w}{i}.$$

To find the maximum on i take 2 vectors $\mathbf{x}, \mathbf{y} \in \mathscr{J}^{n,w}$. If $\mathbf{x}$ is fixed, the maximum is attained when $\mathbf{y}$ is a "typical random vector" of weight w. Then $i \approx w(1 - \frac{w}{n})$. Thus if $\delta \leq \omega(1-\omega)$, volume of the ball has the same exponential order as the last term in the sum. Substituting this into the Gilbert inequality and putting $w = \omega n$ we obtain

$$M = 2^{Rn} \geq \frac{|\mathscr{J}^{n,w}|}{\mathrm{vol}(\mathcal{B}_{d-2})} \gtrsim \frac{\binom{n}{w}}{\binom{w}{\delta n - 1}\binom{n-w}{\delta n - 1}}.$$

Computing logarithms and dividing by n we obtain the bound claimed.

4. We have (with t the covering radius)

$$P_e \leq 2^{-n(1-R)} \sum_{w=d}^{2t} \binom{n}{w} \sum_{r=\lceil w/2 \rceil}^{t} \Big[\sum_{i=w/2}^{w} \binom{w}{i} \binom{n-w}{r-i} \Big] p^r (1-p)^{n-r} + \sum_{r=t+1}^{n} \binom{n}{r} p^r (1-p)^{n-r}.$$

The first term on the right i a growing and the second a falling function of p as long as $pn < t$. Hence the minimum, which is attained when the two terms are (roughly) equal, is attained for the smallest t that satisfies

$$2^{-n(1-R)} \sum_{w=d}^{2t} \binom{n}{w} \sum_{i=w/2}^{w} \binom{w}{i} \binom{n-w}{t-i} \geq \binom{n}{t}.$$

As we have seen, for large i we can replace the sum on i with the first summand, obtaining

$$2^{-n(1-R)} \sum_{w=d}^{2t} \binom{n}{w} \binom{w}{w/2} \binom{n-w}{t-w/2} = \binom{n}{t}.$$

To maximize on w on the left we can employ the Covering Lemma which says that the maximum is attained for $w = 2t(1 - \frac{t}{n})$. Putting $t = \tau n$ and recalling that the left-hand side behaves as $2^{-n(1-R)}\binom{n}{t}^2$, we find the equation for t

$$2^{-n(1-R)} \binom{n}{t}^2 = \binom{n}{t}$$

or

$$h_2(\tau) = 1 - R = h_2(\delta_{\mathrm{GV}}),$$

whence $\tau = \delta_{\mathrm{GV}}(R)$.

5. Observe that $\mathbf{G}\mathbf{G}^T = 0$, so $\mathcal{C} = \mathcal{C}^\perp$. Hence one possibility for the parity-check patrix is $\mathbf{H} = \mathbf{G}$. Further, by inspection, every triple of columns in $\mathbf{G}$ has rank 3, so $d(\mathcal{C}) = 4$. Thus, $\mathcal{C}$ is a $[8, 4, 4]$ code. Therefore, $\mathcal{C}_E$ has the parameters $[3, 3, 1]$, $\mathcal{C}^E$ is a $[3, 0]$ code. Finally, $(\mathcal{C}^\perp)_E = \mathcal{C}_E$, $(\mathcal{C}^\perp)^E = \mathcal{C}^E$.

6. Let $\mathbf{G}$ be a generator matrix of $\mathcal{C}$. Every $k \times k$ submatrix of $\mathbf{G}$ has full rank. For suppose not. Then there are two distinct vectors which are equal in some k coordinates. Their difference gives a vector of weight $n - k < d$ which is impossible.

The distance of the dual code is then $d^\perp \geq k+1$. Hence $C^\perp$ is MDS since $n-k^\perp+1 = n-(n-k)+1 = k+1$. (Note that $d^\perp > k + 1$ is impossible by the Singleton bound).