ECC HW1 Solutions

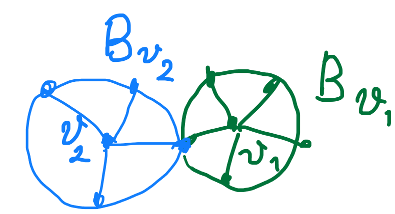
1. ([GRS] Prob. 4.8)

1. Follows by the definitions of $G_{n,d,q}$ and of the independent set.

2. Let $I \subset V$ be an independent set of maximum size

Let $v \in I$; let $B_v := \{u \in V(G) : (u,v) \in E(G)\} \cup \{v\}$

We have $\bigcup_{v \in I} B_v \supseteq V(G)$



because any vertex outside the union of B_v's can be added to I, contradicting maximality.

$$\therefore \quad |I|(\Delta+1) \geq \left|\bigcup_{v \in I} B_v\right| \geq q^n, \quad \text{or} \quad |I| \geq \frac{q^n}{\Delta+1}$$

3. From 1 and 2, there is a code of size

$$\geq \frac{q^n}{\Delta+1} = \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i} = q^{n(1-h_q(\frac{d}{n})-o(1))}$$

as required

2. ([GRS Prob 6.7])

1. $\Pr(rk(G) < k) = \Pr(\text{last row} \in \text{span}(k-1 \text{ rows}))$

$$= \frac{q^{k-1}}{q^n} < q^{k-n}$$

2. $P_{err}(G|J) = P(\geq 2 \text{ codewords agree on } J^c)$ complement $[n] \setminus J$

$$= P\left(\text{rank } G(J^c) < k\right) < q^{k-(n-|J|)}$$

3. Compute the expected P_{err} over the choice of G. For a specific G

$$P_{err}(G) = \sum_{J\subset[n]} \underbrace{Pr(J)}_{|J| \text{ erasures}} \underbrace{P_{err}(G|J)}_{\substack{\text{decoding failure} \\ \text{for this choice of erasures}}}$$

$$\leqslant \sum_{J:|J|<(\alpha+\varepsilon)n} Pr(J)\, P_{err}(G|J) + \sum_{J:|J|\geqslant(\alpha+\varepsilon)n} Pr(J)$$

$$\leqslant \sum_{|J|<(\alpha+\varepsilon)n} Pr(J)\, q^{k-n+(\alpha+\varepsilon)n} + e^{-\Omega(n)}$$

Prob. of the Binomial tail (e.g., Chernoff–Hoeffding)

$$\leqslant q^{n(R-(1-\alpha)+\varepsilon)} + e^{-\Omega(n)} \quad (\text{for any } \varepsilon>0)$$

Since all G in the ensemble are equiprobable, $E_G P_{err}(G) \leqslant q^{n(R-(1-\alpha)+\varepsilon)} + o(n)$.

4. For $R<(1-\alpha)-\varepsilon$ the right-hand side $\downarrow 0$. Thus, there exists a code that supports reliable transmission for all $R<1-\alpha$.

3. (a) Count the total size of the codes $C(E)$, $E\subset\{1,\dots,n\}$:

$$\sum_{|E|=w} C(E) = \sum_{|E|=w} \sum_{\substack{x\in C \\ x_i=0,\, i\notin E}} 1 = \sum_{x\in C} \binom{n-w_H(x)}{n-w} = \sum_{i=0}^{w} A_i \binom{n-i}{n-w}$$

(b) Take a codeword $x=(x_1,\dots,x_w,0,\dots,0)$ all of whose ones are in a subset $E\subset\{1,\dots,n\}$, $|E|=w$ (above $E=\{1,\dots,w\}$ for illustration)
Let $x(E)=(x_1,\dots,x_w)$; clearly

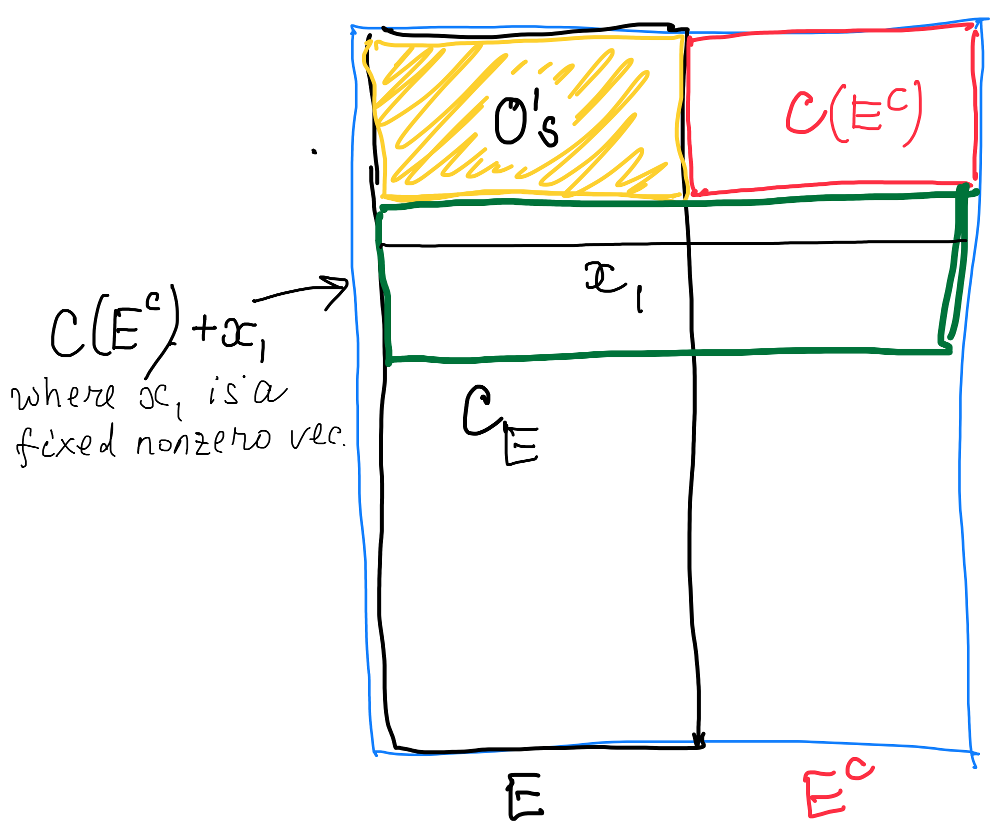
$$H(E)\,(x(E))^T = 0 \qquad (1)$$

The solutions of the linear system (1) form a linear space of dimension $|E| - \mathrm{rk}\, H(E) = w - \mathrm{rk}\, H(E)$, as required.

(c) Consider the code $C_E = \mathrm{proj}_E(C)$, i.e. a linear code obtained by discarding from every vector $x \in C$ the coordinates outside the subset E.

The dimension $\dim(C_E) = \mathrm{rk}(G(E))$ by def of C_E

Now consider the figure below: the code C_E splits into cosets of the code $C(E^c)$, which has 0's in E.



$C_E = C/C(E^c)$

$$\dim C_E = \dim C - \dim C(E^c)$$

$$\mathrm{rk}(G(E)) = K - (w - \mathrm{rk}\, H(E^c)) \quad (*)$$

(part (b))

This relation is what we wanted to prove once we switch the roles of E and E^c

(d) Finally, use parts (a), (c), and (a) in succession:

$$\sum_{i=0}^{n-u} A_i^\perp \binom{n-i}{u} \overset{(a)}{=} \sum_{|E|=n-u} |C^\perp(E)| = \sum_{|E|=u} |C^\perp(E^c)|$$

$$= \sum_{|E|=u} 2^{\mathrm{rk}(H(E^c))} = \sum_{|E|=u} 2^{n-u-K+\mathrm{rk}(G(E))}$$

Pt(c), Eq. (*): $\mathrm{rk}(H(E^c)) = (n-u) - K + \mathrm{rk}(G(E))$

$$= 2^{n-K-u} \sum_{|E|=u} |C(E)| = 2^{n-K-u} \sum_{i=0}^{u} \binom{n-i}{n-u} A_i \quad //$$

Remark: It is instructive to convince yourself that the relation we just proved is actually equivalent to the Mac Williams theorem proved in the lectures. See e.g., Roth's Book.

4. (a) Take a random $(n-k)\times n$ parity-check matrix H. For any $x \in \{0,1\}^n \setminus 0^n$ the probability that a random parity check is satisfied, equals $\frac{1}{2}$

Thus $$\Pr(Hx^T = 0) = 2^{k-n}$$

Then for any $w \geq 1$, $EA_w = \binom{n}{w} 2^{k-n}$

$$EA_w^2 = E\Big[\sum_{i=1}^{\binom{n}{w}} \mathbb{1}(x_i \in \underbrace{\ker(H)}_{\text{code } C})\Big]^2 = E\sum_{i=1}^{\binom{n}{w}} \mathbb{1}(x_i \in C)$$

$$+ E\sum_{\substack{i,j=1 \\ i\neq j}}^{\binom{n}{w}} \underbrace{\mathbb{1}(x_i \in C)\,\mathbb{1}(x_j \in C)}_{\text{independent RVs}} = \binom{n}{w} 2^{k-n} + \binom{n}{w}\Big[\binom{n}{w}-1\Big] 2^{k-n} \quad (E^2)$$

(b) Now consider the Generator matrix ensemble. Below G is a random matrix and C is an $\mathbb{F}_2$-linear space that it spans.

Let $w=0$. The vector 0^n is in C, and if $\mathrm{rk}(G) < k$, then some nonzero vectors $m \in \{0,1\}^k$ satisfy $mG = 0$.

Let $g_1, \dots, g_k$ be the rows of G, then

$$mG = 0 \iff \sum_{i=1}^{k-1} m_i g_i = m_k g_k. \quad (**)$$

The vector g_k has n independent random coord's; thus $(**)$ holds true if n independent events take place, each with prob. $1/2$. Altogether

$$EA_0 = 1 + E\sum_{m \neq 0^k} \mathbb{1}(mG=0) = 1 + \frac{2^k - 1}{2^n}.$$

Now take $w \geq 1$. For any specific vector $c \in \{0,1\}^n$, $w(c) = w$

$$P(mG = c) = \frac{1}{2^n} \qquad \text{(assuming that } m \neq 0\text{)}$$

Thus $$EA_w = \binom{n}{w} \frac{2^k - 1}{2^n}$$

Similarly to Eq.(E^2) above, we write EA_w^2 as a sum of the indicators, argue that the events $m_1 G = c$ and $m_2 G = c$ are independent, isolate the "diagonal" terms and obtain the claimed equality.