

We use Q matrix to construct the parity matrix H to be

$$H = \begin{bmatrix} QP_1 \\ QP_2 \\ \vdots \\ QP_j \end{bmatrix}, \quad (3)$$

where P_i is a uniform random $n \times n$ permutation matrix for $i = 1, \dots, j$.

2.2 Average weight enumerator

To find the average enumerator the Gallager ensemble, first, we compute the average enumerator for more general case. We define the parity matrix H as

$$H = \begin{bmatrix} H_1P_1 \\ H_2P_2 \\ \vdots \\ H_jP_j \end{bmatrix}. \quad (4)$$

Notice that the defined H is a general case of the parity-check matrix of the Gallager ensemble since for the Gallager ensembles all H_i 's are same and equal to Q .

Let C_i denote the code defined by H_i and $A_h^{(i)}$ denote the number of codewords with weight h in C_i . Let C denote the code defined by H . In fact, the code C is simply the result of intersecting permuted versions of the codes C_1, C_2, \dots, C_j . This holds because the code defined by stacking two parity-check matrices is the intersection of the codes.

Since P_1, P_2, \dots, P_j are random permutation matrices, the code C is random as well as its weight enumerator. Therefore, A_h is a random variable which depends on P_1, P_2, \dots, P_j . Let \underline{x} be an arbitrary vector of weight h and P_i be a uniform random $n \times n$ permutation matrix. If $\underline{z}_i = \underline{x}P_i^T$, then \underline{z}_i is a uniform random binary vector of weight h and we have

$$\mathbb{P}(\underline{x}P_i^T H_i^T = \underline{0}) = \mathbb{P}(\underline{z}_i H_i^T = \underline{0}) = \frac{A_h^{(i)}}{\binom{n}{h}} \quad (5)$$

Moreover, since $\{P_i\}_1^j$ are independent random permutation matrices, the random vectors $\{\underline{z}_i = \underline{x}P_i^T\}_1^j$ are independent. Therefore, the probability that the arbitrary vector \underline{x} of weight h belongs to C can be written as

$$\mathbb{P}(\underline{x}H^T = \underline{0}) = \mathbb{P}(\underline{z}_1 H_1^T = 0, \underline{z}_2 H_2^T = 0, \dots, \underline{z}_j H_j^T = 0) \quad (6)$$

$$= \prod_{i=1}^j \mathbb{P}(\underline{z}_i H_i^T = \underline{0}) = \prod_{i=1}^j \frac{A_h^{(i)}}{\binom{n}{h}}. \quad (7)$$

Let \underline{x}_i denote the i -th vector of weight h in some arbitrary order. We can write $\mathbb{E}[A_h]$ as

$$\begin{aligned}\mathbb{E}[A_h] &= \mathbb{E} \left[\sum_{i=1}^{\binom{n}{h}} I(\underline{x}_i \in C) \right] = \binom{n}{h} \mathbb{P}(\underline{x}H^T = 0) \\ &= \binom{n}{h} \prod_{i=1}^j \frac{A_h^{(i)}}{\binom{n}{h}}.\end{aligned}\tag{8}$$

For Gallager code, $H_1 = H_2 = \dots = H_j = Q$. Therefore, the average weight enumerator of Gallager code can be written as

$$\bar{A}_h = \binom{n}{h} \prod_{i=1}^j \frac{A_h^{(Q)}}{\binom{n}{h}} = \frac{\left(A_h^{(Q)}\right)^j}{\binom{n}{h}^{j-1}},\tag{9}$$

where $A_h^{(Q)}$ denotes the number of vectors of weight h such that $\underline{x}Q^T = \underline{0}$.

In the following, we calculate $A_h^{(Q)}$. Since every row of Q has k successive ones, we need to calculate the weight enumerator polynomial of vectors with length k and even weight.

$$A(x) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2i} x^{2i} = \frac{1}{2} [(1+x)^k + (1-x)^k].\tag{10}$$

Also, there are $\frac{n}{k}$ independent choices of even weight vectors. Therefore, the weight enumerator for the codewords satisfying the parity matrix Q can be written

$$A^{(Q)}(x) = A(x)^{\frac{n}{k}} = \left[\frac{1}{2} [(1+x)^k + (1-x)^k] \right]^{\frac{n}{k}}.\tag{11}$$

Let $A^{(Q)}(x) = A(x)^{\frac{n}{k}} = \sum_{i=0}^n A_i^{(Q)} x^i$. For any $x \geq 0$, we have

$$A_h^{(Q)} x^h \leq \sum_{i=0}^n A_i^{(Q)} x^i\tag{12}$$

Therefore, we can write

$$A_h^{(Q)} \leq x^{-h} \sum_{i=0}^n A_i^{(Q)} x^i = x^{-h} A(x)^{\frac{n}{k}}\tag{13}$$

Replacing x by e^s , we can write

$$A_h^{(Q)} \leq e^{-sh} A(e^s)^{\frac{n}{k}}.\tag{14}$$

Since both sides of the above inequality are positive, if we apply the natural logarithm function to both sides, we have

$$\ln A_h^{(Q)} \leq -sh + \frac{n}{k} \ln A(e^s).\tag{15}$$

To obtain the tightest upper bound for $A_h^{(Q)}$, we have

$$\ln A_h^{(Q)} \leq \inf_{s \in \mathbb{R}} -sh + \frac{n}{k} \ln A(e^s)\tag{16}$$

To find an implicit upper bound, we find h such that $\frac{\partial}{\partial s}(-sh + \frac{n}{k} \ln A(e^s)) = 0$.

$$\begin{aligned}\frac{\partial}{\partial s}(-sh + \frac{n}{k} \ln A(e^s)) &= -h + \frac{n}{k} \frac{e^s A'(e^s)}{A(e^s)} = 0, \\ h &= \frac{n}{k} \frac{e^s A'(e^s)}{A(e^s)}.\end{aligned}\tag{17}$$

Let $\delta(s) = \frac{1}{k} \frac{e^s A'(e^s)}{A(e^s)}$. Therefore, $h = n\delta(s)$ and we can write

$$\ln A_{n\delta(s)}^{(Q)} \leq -sn\delta(s) + \frac{n}{k} \ln A(e^s).\tag{18}$$

Then, we can write

$$\frac{1}{n} \ln A_{n\delta(s)}^{(Q)} \leq -s\delta(s) + \frac{1}{k} \ln A(e^s)\tag{19}$$

Let $q(s) = \frac{1}{k} \ln A(e^s) - s\delta(s)$, where $A(e^s) = \frac{1}{2}[(1+e^s)^k + (1-e^s)^k]$. Therefore, for (j, k) Gallager ensemble, we have

$$\begin{aligned}\bar{A}_{n\delta(s)} &= \frac{(A_{n\delta(s)}^{(Q)})^j}{\binom{n}{n\delta(s)}^{j-1}}, \\ \ln \bar{A}_{n\delta(s)} &= j \ln A_{n\delta(s)}^{(Q)} - (j-1) \ln \binom{n}{n\delta(s)}, \\ \frac{1}{n} \ln \bar{A}_{n\delta(s)} &= j \frac{1}{n} \ln A_{n\delta(s)}^{(Q)} - (j-1) \frac{1}{n} \ln \binom{n}{n\delta(s)}.\end{aligned}\tag{20}$$

Using (19), we can calculate an upper bound for $\frac{1}{n} \ln \bar{A}_{n\delta(s)}$ as

$$\frac{1}{n} \ln \bar{A}_{n\delta(s)} \leq jq(s) - (j-1) \frac{1}{n} \ln \binom{n}{n\delta(s)}\tag{21}$$

Since $\lim_{n \rightarrow \infty} \frac{1}{n} \ln \binom{n}{n\delta(s)} = H(\delta(s))$, where H is binary entropy function in nats (i.e., 1 bit is $\ln 2$ nats), we have

$$\lim_{n \rightarrow \infty} \frac{1}{n} \ln \bar{A}_{n\delta(s)} \leq jq(s) - (j-1)H(\delta(s)).\tag{22}$$