Evaluating the bounds of Wiechman-Sason for our LDPC Ensemble

We first recall the following result from [1].

Theorem 1: Let C be a binary linear block code of length n and rate R transmitted over an MBIOS channel $\mathcal{C}$. Let X and Y designate the transmitted codeword and the received sequence, respectively. For an arbitrary representation of the code C by a full-rank parity-check matrix, let Γ_k designate the fraction of the parity-check equations of degree k, and $\Gamma(x) \triangleq \sum_k \Gamma_k x^k$ be the degree distribution of the parity-check nodes in the corresponding bipartite graph. Then, the conditional entropy of the transmitted codeword given the received sequence satisfies

$$\frac{H(X|Y)}{n} \geq 1 - \text{Cap}(\mathcal{C}) - (1-R)\left(1 - \frac{1}{2\ln 2}\sum_{p=1}^{\infty}\frac{\Gamma(g_p)}{p(2p-1)}\right)$$

where

$$g_p \triangleq \int_0^{\infty} a(\ell)(1+e^{-\ell})\tanh^{2p}\left(\frac{\ell}{2}\right) d\ell,$$

and $a(\cdot)$ denotes the conditional pdf of the LLR given that the channel input is 0.

We consider the ensemble of LDPC codes where each column of the parity check matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ has d ones distributed uniformly at random among its entries. In order to evaluate Γ_j for this ensemble, we need to compute the probability of a row of the parity check matrix having exactly j ones.

The probability of any particular entry of H being a one according to our model is given by

$$P_1 = \left(\frac{1}{n-k}\right)\left(\frac{n-k-1}{n-k}\right)^{d-1} + \left(\frac{1}{n-k}\right)^3\left(\frac{n-k-1}{n-k}\right)^{d-3} + \cdots + \left(\frac{1}{n-k}\right)^d$$

if d is odd, and by

$$P_1 = \left(\frac{1}{n-k}\right)\left(\frac{n-k-1}{n-k}\right)^{d-1} + \left(\frac{1}{n-k}\right)^3\left(\frac{n-k-1}{n-k}\right)^{d-3} + \cdots + \left(\frac{1}{n-k}\right)^{d-1}\left(\frac{n-k-1}{n-k}\right)$$

if d is even. By evaluating the sum of this geometric progression, we obtain that

$$P_1 = \frac{(n-k-1)^{d+1-2\lceil d/2\rceil}}{(n-k)^d} \cdot \frac{(n-k-1)^{2\lceil d/2\rceil}-1}{(n-k-1)^2-1}.$$

Since the columns of H are independent of each other, we have that the probability of a row having exactly j ones is

$$\Gamma_j = \binom{n}{j} P_1^j (1-P_1)^{n-j}.$$

Hence

$$\begin{aligned}\Gamma(x) &= \sum_{j=1}^{n} \binom{n}{j} P_1^j (1-P_1)^{n-j} x^j \\ &= (1 - P_1 + P_1 x)^n .\end{aligned}$$

Hence as $n, k \to \infty$, we have that $\Gamma(x) > 0$ iff $x \geq 1$. Further, since $\tanh(x) < 1 \ \forall \ x$, and from the symmetry property of the pdf of the LLR $a(\cdot)$, we have that

$$\begin{aligned}g_p &= \int_0^\infty a(\ell)(1+e^{-\ell}) \tanh^{2p}\left(\frac{\ell}{2}\right) d\ell \\ &< \int_0^\infty a(\ell)(1+e^{-\ell}) d\ell \\ &= 1.\end{aligned}$$

Hence the bound in Theorem 1 evaluates to

$$\frac{H(X|Y)}{n} \geq R - \text{Cap}(\mathcal{C}),$$

which in turn gives us that $I(X;Y) \leq n$ Cap($\mathcal{C}$).

References

[1] G. Wiechman and I. Sason, "Parity-Check Density Versus Performance of Binary Linear Block Codes: New Bounds and Applications," *IEEE Trans. Inform. Theory*, Vol. 53, No. 2, pp. 550-579, Feb. 2007.