

TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY

Department of Electrical Engineering

Handout 7

Codes on Graphs and Iterative Decoding

Homework 5, due date May 30, 2004.

Dr. Igal Sason

---

**Problem 1.** [Information-theoretic bounds on the block/ bit error probability] Consider a binary linear code  $\mathcal{C}$  of length  $n$  and rate  $R$ , and let us first assume (for the sake of simplicity) that the transmission takes place over a binary symmetric channel (BSC) with crossover probability  $p$ . Assume that the codewords of the code  $\mathcal{C}$  are equiprobable.

Let  $\mathbf{x}$  be the transmitted codeword, and let  $\mathbf{y}$  be the received sequence at the output of the channel. Let  $\mathcal{G}$  be an arbitrary bipartite graph which represents the code  $\mathcal{C}$ , and let  $d_{\text{avg}}$  designate the average degree of the parity-check nodes of  $\mathcal{G}$ .

- (a) The normalized mutual information between the input and the output of the BSC is expressed in two ways

$$\frac{I(\mathbf{x}; \mathbf{y})}{n} = \frac{H(\mathbf{x})}{n} - \frac{H(\mathbf{x}|\mathbf{y})}{n} = \frac{H(\mathbf{y})}{n} - \frac{H(\mathbf{y}|\mathbf{x})}{n}.$$

Calculate the normalized entropies  $\frac{H(\mathbf{x})}{n}$  and  $\frac{H(\mathbf{y}|\mathbf{x})}{n}$ .

- (b) Show that the entropy of a parity-check node of an arbitrary degree  $k$  is equal to  $h(p_k)$  where  $h(\cdot)$  designates the binary entropy function (on base 2), and

$$p_k = \frac{1 - (1 - 2p)^k}{2}. \tag{1}$$

- (c) Let us specify the received sequence  $\mathbf{y}$  at the output of the BSC by specifying its syndrome (i.e.,  $\mathbf{y}H^T$  where  $H$  is a parity-check matrix of the code), and then by specifying the appropriate sequence in the coset corresponding to the same syndrome vector. Based on item (b), show that the normalized entropy of the received sequence at the output of the BSC satisfies the inequality

$$\frac{H(\mathbf{y})}{n} \leq (1 - R) \sum_k \left\{ d_k h(p_k) \right\} + R \tag{2}$$

where  $d_k$  designates the fraction of the parity-check nodes in the bipartite graph  $\mathcal{G}$  whose degree is equal to  $k$ , and  $p_k$  is introduced in Eq. (1).

- (d) Conclude from item (c) that

$$\frac{H(\mathbf{y})}{n} \leq (1 - R) h\left(\frac{1 - (1 - 2p)^{d_{\text{avg}}}}{2}\right) + R. \tag{3}$$

*Hint:* Show that the function

$$f(x) \triangleq h\left(\frac{1 - (1 - 2p)^x}{2}\right), \quad 0 < p < \frac{1}{2}$$

is a concave function in the interval  $x \in [0, \infty)$ , and invoke Jensen's inequality to obtain Eq. (3) from Eq. (2).

(e) Derive the following lower bound on the conditional entropy

$$\frac{H(\mathbf{x}|\mathbf{y})}{n} \geq h(p) - (1 - R) h\left(\frac{1 - (1 - 2p)^{d_{\text{avg}}}}{2}\right). \quad (4)$$

*Hint:* Rely on your results from item (a) and Eq. (3).

(f) Show the following upper bound on the conditional entropy

$$\frac{H(\mathbf{x}|\mathbf{y})}{n} \leq \frac{h(P_B)}{n} + RP_B, \quad \frac{H(\mathbf{x}|\mathbf{y})}{n} \leq R h(P_b) \quad (5)$$

where  $P_B$  and  $P_b$  designate the block and the bit error probability of the code  $\mathcal{C}$ , respectively, and combine the bounds in Eqs. (4) and (5) to obtain lower bounds on the block and the bit error probability.

(g) We wish here to generalize the previous result for a general memoryless, binary-input and output-symmetric channel, whose probability density function is  $p(y|x)$ . To this end, let us introduce a physically degraded channel which is a BSC whose output only depends on the sign of the log-likelihood ratio of the original channel (in case that the log-likelihood ratio is equal to zero, the output of the latter channel will be either zero or one with equal probability.) Let  $\mathbf{z} = (z_1, z_2, \dots, z_n)$  designate the received sequence at the output of the degraded BSC.

Calculate the crossover probability ( $w$ ) of the degraded BSC in terms of the conditional probability density function  $p(y|x)$  of the original channel. Justify the following chain of equalities and inequalities:

$$H(\mathbf{x}) = nR,$$

$$H(\mathbf{y}) = H(\mathbf{z}) - nH(z|y) + H(\mathbf{y}|\mathbf{z}),$$

$$H(\mathbf{y}|\mathbf{z}) \leq nH(y|z) = n[H(y) - H(z) + H(z|y)],$$

$$\begin{aligned} H(\mathbf{x}|\mathbf{y}) &= nR - H(\mathbf{y}) + nH(y|x) \\ &\geq nR + nH(z) - H(\mathbf{z}) - nI(x; y) \\ &\geq nR + nH(z) - H(\mathbf{z}) - nC, \end{aligned}$$

$$H(z) = 1,$$

$$H(\mathbf{z}) \leq nR + n(1 - R) h\left(\frac{1 - (1 - 2w)^{d_{\text{avg}}}}{2}\right),$$

and finally obtain that

$$\frac{H(\mathbf{x}|\mathbf{y})}{n} \geq 1 - C - (1 - R) h\left(\frac{1 - (1 - 2w)^{d_{\text{avg}}}}{2}\right). \quad (6)$$

which generalizes Eq. (4). By combining Eq. (6) with the results in item (f), obtain lower bounds on the block and the bit error probability of the code  $\mathcal{C}$  whose validity is extended for all memoryless binary-input, output-symmetric channels.

**Problem 2.** [Information-theoretic lower bounds on the parity-check density] In this problem, we intend to derive information-theoretic lower bounds on the density of parity-check matrices which correspond to a sequence of binary linear block codes that achieve a fraction  $1 - \varepsilon$  of the capacity of an arbitrary memoryless binary-input output-symmetric channel (where  $\varepsilon$  is an arbitrary number between zero and one.) Under iterative message-passing decoding, the density of the parity-check matrix is directly related to the decoding complexity per information bit during a single iteration (and for the BEC, since we can modify the iterative message-passing decoding algorithm, so that we use every edge of the bipartite graph only once, the density is linked to the decoding complexity per information bit.) As we defined in class, let  $H$  be an arbitrary parity-check matrix of a binary linear block code  $\mathcal{C}$  of length  $n$  and rate  $R$ . The density  $\Delta$  of the matrix  $H$  is defined as the normalized number of ones in  $H$  per information bit of the linear code (i.e., the density of  $H$  is equal to number of ones in  $H$  divided by  $nR$ ).

- (a) Show that the parity-check density ( $\Delta$ ) and the average degree of the parity-check nodes ( $a_{\text{avg}}$ ) in the corresponding bipartite graph are related according to the equation

$$\Delta = \left( \frac{1 - R}{R} \right) a_{\text{avg}}. \quad (7)$$

- (b) Show that the binary entropy function satisfies the inequality

$$h(x) \leq 1 - \frac{2}{\ln 2} \cdot \left( \frac{1}{2} - x \right)^2 \quad 0 \leq x \leq \frac{1}{2}. \quad (8)$$

- (c) Let  $\{\mathcal{C}_m\}$  be a sequence of binary linear codes achieving a fraction  $1 - \varepsilon$  of the capacity of a memoryless binary-input output-symmetric channel with vanishing *bit error probability*. Show that the asymptotic density of their parity-check matrices satisfies the inequality

$$\liminf_{m \rightarrow \infty} \Delta_m > \frac{K_1 + K_2 \ln \frac{1}{\varepsilon}}{1 - \varepsilon}, \quad (9)$$

where

$$K_1 = \frac{(1 - C) \cdot \ln \left( \frac{1}{2 \ln 2} \cdot \frac{1 - C}{C} \right)}{2C \cdot \ln \left( \frac{1}{1 - 2w} \right)}, \quad K_2 = \frac{1 - C}{2C \cdot \ln \left( \frac{1}{1 - 2w} \right)}.$$

Here  $C$  stands for the channel capacity, and  $w$  was introduced in item (g) of Problem 1. *Hint:* Rely on Eqs. (6), (7) and (8).

The result in (9) tells us that the parity-check density grows *at least* like  $\ln \left( \frac{1}{\varepsilon} \right)$  where the asymptotic rate is  $1 - \varepsilon$  of the channel capacity (so, it also tends to infinity as  $\varepsilon \rightarrow 0$ .) Under the assumption of ML decoding, it can be shown that the logarithmic behavior of the above lower bound is indeed achievable (up to a scaling).

**Problem 3.** [Information-theoretic upper bounds on the achievable rates of LDPC codes under ML decoding] Let  $\{\mathcal{C}_m\}$  be a sequence of binary linear codes with an asymptotic rate  $R$ , and assume that their transmission takes place over a memoryless binary-input output-symmetric channel with capacity  $C$ .

- (a) Prove that a necessary condition for reliable communication with vanishing bit error probability is

$$R \leq 1 - \frac{1 - C}{h\left(\frac{1 - (1 - 2w)^{d_{\text{avg}}}}{2}\right)} \quad (10)$$

where  $d_{\text{avg}}$  and  $w$  designate the asymptotic average degree of the parity-check nodes, and the crossover probability of the degraded BSC introduced in item g of Problem 1, respectively.

- (b) Assume that the transmission of the LDPC codes takes place over a BSC with crossover probability  $p$ . Then, based on item (g) of Problem 1, show that

$$w = \min(p, 1 - p).$$

Calculate upper bounds on the threshold  $p$  for the ensembles of (3, 6), (4, 8) and (5, 10) regular LDPC codes under ML decoding (to this end, rely on (10)).