# TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY

**Department of Electrical Engineering**

**Handout 8** — **Codes on Graphs and Iterative Decoding**

Homework 6, due **June 13, 2004.** — Dr. Igal Sason

---

**Problem 1.** Consider a binary-input, output-symmetric and memoryless channel with input $x \in \{-1, 1\}$ and output $y \in Y$ defined by its transition probability density function (*pdf*) $p_{Y|X}(y|x)$. Let $L(Y)$ designate the log-likelihood ratio of the observation $y$ at the channel output given $x = 1$ was transmitted, i.e., $L(y) = \ln\left(\frac{p_{Y|X}(y|1)}{p_{Y|X}(y|-1)}\right)$.

(a) Show that

$$p_{Y|X}(y|x) = p_Y(y) \cdot \frac{e^{xL(y)}}{p_X(-x) + p_X(x)e^{xL(y)}}$$

and conclude that the optimal decoder can be based on the log-likelihood ratio instead of the observation $y$.

(b) We have shown in class that the *pdf* of the log-likelihood ratio $L(Y)$, conditioned on $X = 1$, is symmetric, i.e., $p_L(l) = e^l \, p_L(-l)$. Let

$$D(y) = \tanh\left(\frac{L(y)}{2}\right).$$

Show that if $X = \pm 1$ are a priori equally probable, then

$$D(y) = \text{Prob}(1|y) - \text{Prob}(-1|y),$$

and prove that the *pdf* of $D$ satisfies the equality

$$\frac{p_D(u)}{p_D(-u)} = \frac{1+u}{1-u}\,, \quad \forall\, u \in (-1, 1].$$

(c) Let $p_L^+(\cdot)$ designate the *pdf* of the absolute value of the log-likelihood ratio (i.e., $|L(Y)|$), conditioned on $X = 1$. Similarly, let $p_D^+(\cdot)$ be the *pdf* of $|D(y)|$, conditioned on $X = 1$. Prove that the capacity of the channel can be expressed in three equivalent ways as

$$\begin{aligned} C &= \int_{-\infty}^{\infty} p_L(y)\ \left(1 - \log_2(1 + e^{-y})\right)\ \mathrm{d}y \\ &= \int_0^{\infty} p_L^+(y)\ \left(1 - h\left(\frac{1}{1 + e^{-y}}\right)\right)\ \mathrm{d}y \\ &= \int_0^1 p_D^+(y)\ \left(1 - h\left(\frac{1 - y}{2}\right)\right)\ \mathrm{d}y \end{aligned}$$

where $C$ is given in bits per channel use, and $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ designates the binary entropy function on base 2.

**Problem 2.** Consider the binary-input additive white Gaussian noise (BIAWGN) channel where $E_s$ designates the energy per transmitted symbol, and $N_0$ is the one-sided spectral density of the additive white Gaussian noise.

(a) Show that the capacity of the BIAWGN channel can be expressed as

$$C = 1 - \frac{1}{\sqrt{2\pi}\,\ln(2)} \int_{-\infty}^{\infty} e^{-\frac{(y-\beta)^2}{2}} \ln\bigl(1 + e^{-2\beta y}\bigr)\, dy \quad \text{bits per channel use}$$

where $\beta \triangleq \sqrt{\frac{2E_s}{N_0}}$.

(b) Based on item (a), show that the capacity can be rewritten in the form

$$C = 1 - \frac{1}{\ln(2)} \left[ \frac{2\beta e^{-\frac{\beta^2}{2}}}{\sqrt{2\pi}} - (2\beta^2 - 1)Q(\beta) + \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k(k+1)} \cdot e^{2k(k+1)\beta^2} Q\bigl((2k+1)\beta\bigr) \right].$$

Hint: Write the integral in item (a) as a sum of two integrals from 0 to $\infty$, and use the power series expansion of the logarithmic function

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1} x^k}{k}, \qquad -1 < x \leq 1.$$

(c) The Euler transform converts a convergent alternating series $\sum_{k=0}^{\infty} (-1)^k a_k$ to another series which converges to the same value more rapidly. The transformed series is

$$\sum_{k=0}^{\infty} \frac{(-1)^k \Delta^k a_0}{2^{k+1}}$$

where

$$\Delta^k a_0 \triangleq \sum_{m=0}^{k} (-1)^m \binom{k}{m} a_{k-m}\,, \qquad k = 1, 2, \ldots$$

Based on item (b), show that

$$C = 1 - \frac{1}{\ln(2)} \left[ \frac{2\beta e^{-\frac{\beta^2}{2}}}{\sqrt{2\pi}} - (2\beta^2 - 1)Q(\beta) + \sum_{k=0}^{\infty} \frac{(-1)^k \cdot \Delta^k a_0}{2^{k+1}} \right]. \tag{1}$$

where

$$\Delta^k a_0 = \frac{1}{2}\, e^{-\frac{\beta^2}{2}} \sum_{m=0}^{k} \left\{ \frac{(-1)^m}{(k-m+1)(k-m+2)} \binom{k}{m} \operatorname{erfcx}\left( \frac{(2k-2m+3)\beta}{\sqrt{2}} \right) \right\}$$

and $\operatorname{erfcx}(x) \triangleq 2e^{x^2} Q(\sqrt{2}x)$ (we note that $\operatorname{erfcx}(x) \approx \frac{1}{\sqrt{\pi}} \cdot \frac{1}{x}$ for large values of $x$).

(d) Let us assume that the information bits are encoded by a binary linear code of rate $R$, BPSK modulated, and transmitted over a BIAWGN channel. Let the energy per channel symbol be equal to $E_s = RE_b$ where $R$ and $E_b$ designate the code rate and the energy per information bit, respectively. Based on Eq. (1), find numerically the minimal value of the energy per information bit to spectral noise density $\left(\frac{E_b}{N_0}\right)$ which is required to achieve reliable communication if the code rate is equal to $R = \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}$ and 0.95 bits per channel use. For numerical calculations, we note that the results are very accurate by taking into account the first 20 terms of the alternating series in item (c).

(e) Compare your numerical results in item (d) with the corresponding values of $\frac{E_b}{N_0}$ which correspond to an AWGN channel with continuous input. Note that in this case, capacity of the AWGN channel is achieved for a Gaussian distributed input, and show that in the latter case, the minimal required value of $\frac{E_b}{N_0}$ is equal to $\frac{2^{2R}-1}{2R}$.

**Problem 3.** The binary-input Cauchy channel (BCC) and binary-input Laplace channel (BLC) are modeled by $y_t = x_t + z_t$, where the input $x_t$ gets the values $\pm 1$, and $\{z_t\}$ is a sequence of i.i.d. random variables whose *pdfs* are equal to

$$p_{\mathrm{BCC}(\lambda)}(z) = \frac{\lambda}{\pi(\lambda^2 + z^2)}\,, \quad p_{\mathrm{BLC}(\lambda)}(z) = \frac{1}{2\lambda}\, e^{-\frac{|z|}{\lambda}}, \quad -\infty < z < +\infty,$$

respectively (where $\lambda > 0$).

(a) Prove that these two families of channels are ordered by physical degradation.

*Hint:* Use the following identity for the continuous Fourier transform

$$\mathcal{F}\left(\frac{1}{a^2 + t^2}\right) = \frac{\pi e^{-a|f|}}{a}, \quad \mathrm{Re}(a) > 0$$

and show that a serial concatenation of BCC($\lambda_1$) with a channel whose additive noise is Cauchy distributed with parameter $\lambda_2$ (where $\lambda_1, \lambda_2 > 0$) gives the binary-input Cuachy channel BCC($\lambda_1 + \lambda_2$). For the physical degradation of the BLC, show that a serial concatenation of a BLC with parameter $\lambda'$ and a memoryless channel whose additive noise has the *pdf*

$$p(z) = \left(\frac{\lambda'}{\lambda}\right)^2 \delta(z) + \left(1 - \left(\frac{\lambda'}{\lambda}\right)^2\right) \frac{1}{2\lambda}\, e^{-\frac{|z|}{\lambda}}\,, \quad \lambda > \lambda'$$

where $\delta(\cdot)$ denotes the Dirac delta function, gives a BLC with parameter $\lambda$.

(b) Prove that the capacity of the BLC is equal to

$$C_{\mathrm{BLC}} = \frac{-\pi + 4\arctan(e^{-\frac{1}{\lambda}})}{2e^{\frac{1}{\lambda}}\,\ln 2} - \log_2\left(\frac{1 + e^{-\frac{2}{\lambda}}}{2}\right) \quad \text{bit per channel use.}$$

(c) Derive the stability condition for the BCC and the BLC.

**Problem 4 (Physical degradation of symmetric channels).** Let $p_{Y|X}(y|x)$ and $q_{Y|X}(y|x)$ be two output-symmetric channels, and assume that $q$ is physically degraded with respect to $p$. Show that there exists a *symmetric* channel which certifies the physical degradation.

**Problem 5 (Erasure decomposition lemma).** Let $a(y)$ be a symmetric *pdf*. Associate to $a(y)$ the binary-input, output-symmetric, and memoryless channel $p(y|x = 1) = a(y)$. Prove that $P(y|x)$ is physically degraded with respect to the binary erasure channel (BEC) whose erasure probability is equal to $p = 2\varepsilon$ where

$$\varepsilon = \mathrm{P_e}(a) \triangleq \int_{-\infty}^{0^-} a(y)\;\mathrm{d}y + \frac{1}{2}\int_{0^-}^{0^+} a(y)\;\mathrm{d}y.$$

Give an explicit ternary-input channel which certifies the physical degradation with respect to the BEC.

**Problem 6.** We have seen in class that because of the symmetry of the message-passing iterative algorithm, the decoding error probability of a binary linear code is independent of the transmitted codeword in the symmetric channel setting. Thus, without loss of generality, we can assume that the all-zero codeword was transmitted. Show that for asymmetric channels, this simplification of the analysis by restricting to the all-zero codeword is not valid in general. Give a concrete example.

**Problem 7 (Gallager A decoding algorithm).** Consider an ensemble of $(n, \lambda, \rho)$ LDPC codes, and let the block length ($n$) tend to infinity. Assume that the codes are transmitted over a binary symmetric channel (BSC) whose crossover probability is equal to $p$, and that the codes are iteratively decoded by the Gallager A algorithm.

(a) Show that in the $l$-th iteration, the expected fraction of errors ($x_l$) at the variable nodes is given by the recursion

$$x_l = x_0 \left(1 - p^+(x_{l-1})\right) + (1 - x_0)p^-(x_{l-1}), \quad l = 1, 2, \cdots \tag{2}$$

where $x_0 = p$, and

$$p^+(x) \triangleq \lambda\left(\frac{1 + \rho(1 - 2x)}{2}\right), \quad p^-(x) \triangleq \lambda\left(\frac{1 - \rho(1 - 2x)}{2}\right).$$

(b) Derive a stability condition for the recursion in Eq. (2), and show that if

$$\lambda_2 \rho'(1) < 1, \tag{3}$$

then the threshold is upper bounded by $\frac{1-\lambda_2\rho'(1)}{\lambda'(1)\rho'(1)-\lambda_2\rho'(1)}$.
*Hint:* Let us define the function

$$f(x, y) \triangleq x(1 - p^+(y)) + (1 - x)p^-(y), \quad x, y \in [0, 0.5].$$

Show that for small enough values of $y$

$$f(x, y) = c_1 xy + c_2 y + O(y^2)$$

where $c_1$ and $c_2$ are appropriate constants which depend on the pair of degree distributions $\lambda(\cdot)$ and $\rho(\cdot)$ (calculate $c_1, c_2$). Finally show that if the condition in (3) holds, then by setting

$$x = \frac{1 - \lambda_2\rho'(1)}{\lambda'(1)\rho'(1) - \lambda_2\rho'(1)} - \varepsilon, \quad \varepsilon > 0$$

we obtain that

$$f(x, y) < \alpha y + O(y^2)$$

where $0 < \alpha < 1$ (calculate $\alpha$), and explain why it proves the statement.

(c) Let $\tau$ denote the smallest positive real zero of the polynomial

$$p(x) \triangleq xp^+(x) + (x - 1)p^-(x).$$

Show that if (3) holds, then the threshold under Gallager A decoding algorithm is upper bounded by

$$\min\left\{\frac{1 - \lambda_2\rho'(1)}{\lambda'(1)\rho'(1) - \lambda_2\rho'(1)}, \tau\right\}. \tag{4}$$

(d) Calculate the upper bound (4) on the threshold of the $(3, 6)$ Gallager ensemble of regular-LDPC codes under the Gallager A decoding algorithm, and compare your result to the threshold of the same ensemble under belief propagation (which is equal to 0.084).