

# TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY

## Department of Electrical Engineering

### Handout 11

### Codes on Graphs and Iterative Decoding

Homework 8, due **July 25, 2004**.

Dr. Igal Sason

**Problem 1 (linearization of the density evolution equation).** This problem refers to the linearization of the density evolution equation. It is performed in order to prove the necessity of the stability condition for the belief propagation decoding algorithm. Let us assume that the bit error probability at a certain iteration is equal to  $\varepsilon$  (where  $\varepsilon > 0$ ). We want to prove that if the stability condition is not satisfied, then the bit error probability is bounded from below by a certain positive number, no matter how many iterations we perform. To this end, we assign a density for the left-to-right outgoing messages at that iteration which is given by

$$Q_0(x) = 2\varepsilon\delta_0(x) + (1 - 2\varepsilon)\delta_\infty(x) \quad (1)$$

where  $\delta_0(x)$  and  $\delta_\infty(x)$  designate the delta of Dirac at zero and infinity, respectively. We note that the resulting bit error probability with this assignment is also  $\varepsilon$ , but according to the erasure decomposition lemma, the actual channel is physically degraded with respect to a BEC whose erasure probability is equal to  $2\varepsilon$ . Based on the density evolution equation, the resulting densities of the outgoing messages from left to right in next iterations are calculated by the recursive equation

$$Q_l = a_0 \otimes \lambda \left( \Gamma^{-1} \left( \rho \left( \Gamma(Q_{l-1}) \right) \right) \right) \quad l = 1, 2, \dots \quad (2)$$

where  $a_0(\cdot)$  is the pdf of the log-likelihood ratio (LLR) of the true channel, given that  $x = 1$  is transmitted. In the continuation, we will do a first order approximation of the density evolution equation (2) for  $\varepsilon \ll 1$ .

- (a) Show that  $\delta_\infty(x)$  is a fixed point of the density evolution equation (2) (i.e., show that if  $Q_{l-1}(x) = \delta_\infty(x)$  then also  $Q_l(x) = \delta_\infty(x)$ ), and explain the meaning of this result in light of the update rule at the variable nodes of the bipartite graph.
- (b) Let  $f$  and  $g$  be two arbitrary functions. Prove the equality

$$(f + g)^{\otimes n} = \sum_{k=0}^n \binom{n}{k} f^{\otimes(n-k)} \otimes g^{\otimes k} \quad (3)$$

which is similar to the binomial formula of Newton (except that multiplications of scalars are replaced by convolutions of functions). We note that  $f^{\otimes 0} \triangleq \delta_0$ , where  $\delta_0(x)$  designates the delta of Dirac at zero.

*Hint:* prove this equality by mathematical induction, relying on the property that the convolution operation is commutative and associative. You may also use the identity  $\binom{n}{m-1} + \binom{n}{m} = \binom{n+1}{m}$  for  $m \leq n$ .

- (c) Prove the equalities

$$\Gamma(\delta_\infty)(s, x) = \chi_{\{s=1\}}\delta_0(x) \quad (4)$$

$$\Gamma(\delta_0)(s, x) = \frac{1}{2} \delta_\infty(x) \chi_{\{s=1\}} + \frac{1}{2} \delta_\infty(x) \chi_{\{s=-1\}}. \quad (5)$$

- (d) Show that  $\Gamma$  and  $\Gamma^{-1}$  are linear operators, and also give an interpretation to the equalities

$$P_0 \otimes \delta_0 = P_0, \quad P_0 \otimes \delta_\infty = \delta_\infty \quad (6)$$

for an arbitrary *pdf*  $P_0$ .

- (e) Let  $P_0$  be an arbitrary *pdf*, and prove the equality

$$(\delta_0(x) \chi_{\{s=1\}}) \otimes \Gamma(P_0) = \Gamma(P_0) \quad (7)$$

and also show that

$$(\delta_0(x) \chi_{\{s=1\}})^{\otimes i} = \delta_0(x) \chi_{\{s=1\}}, \quad i = 1, 2, \dots \quad (8)$$

- (f) Let  $P_0$  be an arbitrary *pdf*, and let us define

$$Q = \epsilon P_0 + (1 - \epsilon) \delta_\infty + O(\epsilon^2) \quad (9)$$

$$R = a_0 \otimes \lambda \left( \Gamma^{-1} \left( \rho(\Gamma(Q)) \right) \right). \quad (10)$$

We note that  $\epsilon$  in (9) and  $\varepsilon$  in (1) are not the same. Based on items (a)–(e), prove the following equalities

$$\begin{aligned} \Gamma(Q) &= \epsilon \Gamma(P_0) + (1 - \epsilon) \delta_0(x) \chi_{\{s=1\}} + O(\epsilon^2) \\ \Rightarrow (\Gamma(Q))^{\otimes i-1} &= (i-1)\epsilon \Gamma(P_0) + (1 - (i-1)\epsilon) \delta_0(x) \chi_{\{s=1\}} + O(\epsilon^2), \quad i \geq 2 \\ \Rightarrow \rho(\Gamma(Q)) &\triangleq \sum_{i \geq 2} \rho_i (\Gamma(Q))^{\otimes i-1} = (1 - \epsilon \rho'(1)) \delta_0(x) \chi_{\{s=1\}} + \rho'(1)\epsilon \Gamma(P_0) \\ \Rightarrow \Gamma^{-1} \left( \rho(\Gamma(Q)) \right) &= (1 - \epsilon \rho'(1)) \delta_\infty(x) + \epsilon \rho'(1) P_0 \end{aligned}$$

- (g) Show that for  $k \geq 2$

$$\left[ (1 - \epsilon \rho'(1)) \delta_\infty(x) + \epsilon \rho'(1) P_0 \right]^{\otimes k} = \delta_\infty(x) + O(\epsilon^2)$$

and hence, conclude from items (d) and (f) that

$$\begin{aligned} \lambda \left( \Gamma^{-1} \left( \rho(\Gamma(Q)) \right) \right) &= (1 - \lambda'(0) \rho'(1) \epsilon) \delta_\infty(x) + \lambda'(0) \rho'(1) \epsilon P_0 + O(\epsilon^2) \\ \Rightarrow R &= a_0 \otimes \lambda \left( \Gamma^{-1} \left( \rho(\Gamma(Q)) \right) \right) \\ &\quad (1 - \lambda'(0) \rho'(1) \epsilon) \delta_\infty(x) + \lambda'(0) \rho'(1) \epsilon (a_0 \otimes P_0) + O(\epsilon^2). \end{aligned}$$

- (h) Based on your result in item (g), the initial *pdf*  $Q_0$  in (1), and the density evolution equation (2), prove that

$$Q_l(x) = 2\varepsilon (\lambda'(0) \rho'(1))^l (a_0^{\otimes l})(x) + (1 - 2\varepsilon (\lambda'(0) \rho'(1))^l) \delta_\infty(x) + O(\varepsilon^2). \quad (11)$$

*Hint:* By comparing (1) and (2) with equations (9) and (10), respectively, set the initial  $\epsilon$  in (9) to be  $2\varepsilon$ , and apply your result from item (g) in a recursive manner  $l$  times.

**Problem 2 (upper and lower bounds on the error probability  $P_e(a_0^{\otimes l})$ ).** In the proof of the necessity part of the stability condition, we needed to obtain the exponential growth rate of the error probability which is associated with the pdf  $a_0^{\otimes l}$ , given that one is transmitted. The error probability is given by the equality

$$P_e(a_0^{\otimes l}) = \int_{-\infty}^{0^-} a_0^{\otimes l}(x) dx + \frac{1}{2} \int_{0^-}^{0^+} a_0^{\otimes l}(x) dx .$$

Let  $Z_1, Z_2, \dots, Z_l$  be  $l$  i.i.d. random variables which are distributed according to the pdf  $a_0$ , and define the random variable  $Z$  to be their sum ( $Z \triangleq \sum_{i=1}^l Z_i$ ). Since  $Z \sim a_0^{\otimes l}$ , then

$$P_e(a_0^{\otimes l}) = \text{Prob}(Z \leq 0).$$

(a) Based on the Chernof bound, show that

$$\text{Prob}(Z \leq 0) \leq (E[e^{sZ_1}])^l, \quad \forall s < 0. \quad (12)$$

(b) In order to obtain the tightest Chernof bound, we need to calculate the infimum of  $E[e^{sZ_1}]$  over the interval  $s \in (-\infty, 0)$ . We rely here on the symmetry of the pdf  $a_0$  of the LLR given that one is transmitted (which follows from the symmetry of the considered binary-input memoryless channel). Show that the infimum is achieved at  $s = -\frac{1}{2}$ , and

$$\inf_{s < 0} E[e^{sZ_1}] = \int_{-\infty}^{+\infty} a_0(x) e^{-\frac{x}{2}} dx \triangleq \mathcal{B}(a_0).$$

Show that it is the well known constant which appears in the Bhattacharyya bound. We therefore conclude from items (a) and (b) that

$$P_e(a_0^{\otimes l}) \leq \mathcal{B}(a_0)^l. \quad (13)$$

We want to derive now a lower bound on the error probability  $P_e(a_0^{\otimes l})$  which will have the *same exponential growth rate* as the upper bound above.

(c) Let us define

$$\hat{A}_0(\omega) \triangleq \int_{-\infty}^{\infty} e^{-i\omega x} e^{-\frac{x}{2}} a_0(x) dx. \quad (14)$$

We note that it is the Fourier transform evaluated at  $\omega - \frac{i}{2}$ . Show that  $\hat{A}_0$  is real and even  $\hat{A}_0(\omega) = \hat{A}_0(-\omega)$ , and  $\hat{A}_0'(0) = 0$ .

(d) Prove that the second derivative of  $\hat{A}_0(\omega)$  is lower bounded by

$$\frac{d^2}{d\omega^2} \hat{A}_0(\omega) \geq -32e^{-2}. \quad (15)$$

*Hint:* Calculate the maximal value of  $g(x) = x^2 e^{-\frac{x}{2}}$  over the interval  $x \in [0, \infty)$ .

(e) Prove the inequality

$$\hat{A}_0(\omega) \geq \mathcal{B}(a_0) \left( 1 - \frac{1}{\mathcal{B}(a_0)} 16e^{-2} \omega^2 \right). \quad (16)$$

*Hint:* rely on items (c), (d), and use the Taylor series expansion of the second order for  $\hat{A}_0(\cdot)$ .

(f) Based on the symmetry of  $a_0$ , show that  $a_0^{\otimes l}$  is symmetric, and

$$P_e(a_0^{\otimes l}) = \frac{1}{2} \int_{-\infty}^{\infty} e^{-|\frac{x}{2}|} e^{-\frac{x}{2}} a_0^{\otimes l}(x) dx \quad (17)$$

and then use Parseval's theorem to obtain the equality

$$P_e(a_0^{\otimes l}) = \frac{2}{\pi} \int_0^{\infty} \frac{1}{1+4\omega^2} \hat{A}_0(\omega)^l d\omega \quad (18)$$

(g) Let  $l$  be even. Based on item (e), show that

$$\hat{A}_0^l(\omega) \geq \mathcal{B}(a_0)^l \left( 1 - \frac{l}{\mathcal{B}(a_0)} 16e^{-2\omega^2} \right)^+ \quad (19)$$

where  $x^+ \triangleq \max(0, x)$ , and then prove that for every non-negative and even  $l$

$$P_e(a_0^{\otimes l}) \geq \mathcal{B}(a_0)^l \frac{1}{1 + \frac{e^2 \mathcal{B}(a_0)}{4l}} \frac{e}{3\pi} \sqrt{\frac{\mathcal{B}(a_0)}{l}} \quad (20)$$

(h) Based on item (g) and the inequality  $\hat{A}_0(\omega) \leq \mathcal{B}(a_0)$ , show that for every non-negative and odd  $l$

$$P_e(a_0^{\otimes l}) \geq \mathcal{B}(a_0)^l \frac{1}{1 + \frac{e^2 \mathcal{B}(a_0)}{4(l+1)}} \frac{e}{3\pi} \sqrt{\frac{\mathcal{B}(a_0)}{l+1}} \quad (21)$$

(i) Combine the lower bounds (20) and (21) for even and odd numbers, respectively, and show that the resulting lower bound has the same exponential growth rate in  $l$  as the upper bound (13).

The results in items (b) and (i) yield the equality

$$P_e(a_0^{\otimes l}) \doteq e^{-rl}$$

where

$$r \triangleq -\ln \mathcal{B}(a_0) = -\ln \left( \int_{-\infty}^{\infty} e^{-\frac{x}{2}} a_0(x) dx \right).$$

**Problem 3 (stability condition for binary-input Cauchy and Laplace channels).** Solve item (c) in Problem 3 of homework assignment no. 6.

**Problem 4 (stability condition for fully-interleaved fading channels).** Consider a fully-interleaved Rayleigh fading channel which is a memoryless channel (due to a perfect channel interleaver which makes the fading samples i.i.d.). We have

$$y_t = \alpha_t x_t + n_t$$

where  $x_t \in \{\pm 1\}$ ,  $n_t \sim N(0, \sigma^2)$ , and  $\alpha_t$  is Rayleigh distributed, i.e., its probability density function is  $a_\alpha(x) = 2\alpha e^{-\alpha^2 x^2}$ ,  $\alpha \geq 0$ . We further assume that  $\{\alpha_t\}_t$  and  $\{n_t\}_t$  form i.i.d. sequences of random variables, and they are independent of each other. We consider the case where there is *perfect side information* about the fading samples, so the channel output at time  $t$  is  $(y_t, \alpha_t)$ .

- (a) Calculate the log-likelihood ratio, and its conditional probability density function (*pdf*) given that  $x = 1$  is transmitted. Is the resulting *pdf* symmetric? explain.
- (b) Consider the transmission of codes from an ensemble of LDPC codes whose pair of degree distributions is  $(\lambda, \rho)$ . The communication takes place over a fully interleaved Rayleigh fading channel as above. Show that under belief propagation decoding, the stability condition gets the form

$$\lambda'(0) \rho'(1) < 1 + \frac{1}{2\sigma^2}.$$

- (c) Let us assume the more realistic case where the side information about the fading is not perfect. How would you expect  $e^r$  in the stability condition to vary as a function of the correlation between the real fading samples and their estimates? explain.

**Problem 5 (Z channel).** The  $Z$  channel is binary-input, binary-output and memoryless, but the channel is *asymmetric*. The channel is specified by the following transition probabilities

$$\begin{aligned} p_{Y|X}(y = 1|x = 1) &= 1 - \varepsilon, & p_{Y|X}(y = -1|x = 1) &= \varepsilon, \\ p_{Y|X}(y = 1|x = -1) &= 0, & p_{Y|X}(y = -1|x = -1) &= 1. \end{aligned}$$

Let us assume that the input distribution is  $p_x(0) = p$ ,  $p_x(1) = 1 - p$  (since the channel is memoryless, the capacity-achieving input distribution is not uniform).

- (a) Calculate the average mutual information between the input and the output of the  $Z$  channel, and show that

$$I(X; Y) = h_2(p) - (1 - p + \varepsilon p) h_2\left(\frac{\varepsilon p}{1 - p + \varepsilon p}\right)$$

where  $h_2(\cdot)$  is the binary entropy function on base 2.

- (b) By maximizing the mutual information above for a fixed value of  $\varepsilon$  (i.e., the probability transition of the  $Z$  channel), show that the optimal value of  $p$  is given by

$$p_{\text{optimal}} = \frac{1}{1 - \varepsilon + \varepsilon^{-\frac{\varepsilon}{1-\varepsilon}}}, \quad 0 < \varepsilon < 1.$$

- (c) Plot the value of  $p_{\text{optimal}}$  as a function of  $\varepsilon$ , and show that it is a monotonic decreasing function of  $\varepsilon$  which varies between  $\frac{1}{2}$  and  $\frac{1}{e}$ .
- (d) Let us assume that the input distribution to the channel is symmetric. Prove that the average mutual information for the case of uniform input distribution is at least equal to a fraction  $\frac{\varepsilon}{2} \ln(2) = 94.2\%$  of capacity over the whole range of  $\varepsilon$  (with equality when  $\varepsilon$  approaches 1). Obtain the exact values of this fraction for  $\varepsilon = 0.1, 0.5, 0.8$ .

For further reading, please see the recently published paper:

N. Shulman and Feder, "The uniform distribution as a universal prior," *IEEE Transactions on Information Theory*, vol. 50, pp. 1365–1362, June 2004.

From item (d), we see that because of the marginal loss in the achievable rate in case of a uniform distribution (as compared to the capacity-achieving distribution), there is a hope to achieve rates which are very close to capacity with binary LDPC codes (or other ensembles of codes on graphs). Fortunately, it is indeed the case.

We note that the stability condition for LDPC codes over arbitrary discrete-memoryless channels was presented in the paper:

A. Bennatan and D. Burshtein, "Iterative decoding of LDPC codes over arbitrary discrete-memoryless channels," *Proceedings of the Forty-First Annual Allerton Conference on Communication, Control and Computing*, pp. 1416–1425, October 2003.

In general, for a discrete memoryless channel, one can replace the  $e^r$  in the stability condition for the binary-input output-symmetric channel with the constant which appears in the Bhattacharyya bound (but here the *pdf* of the LLR is not necessarily symmetric).

- (e) Consider the transmission of codes from an ensemble of binary LDPC codes whose pair of degree distributions is  $(\lambda, \rho)$ . The transmission of these codes takes place over a Z channel, and the codes are decoded with the belief propagation algorithm. Show that (under the uniform input distribution, i.e.,  $p_X(1) = p_X(-1) = \frac{1}{2}$ ), the stability condition for this channel reads

$$\lambda'(0) \rho'(1) < \frac{1}{\sqrt{\epsilon}}.$$

**Problem 6 (Gaussian approximation).** Consider the transmission of an ensemble of  $(n, \lambda, \rho)$  LDPC codes over a binary-input AWGN channel, and assume that the codes are iteratively decoded with the sum-product algorithm. The additive Gaussian noise has a zero mean and variance  $\sigma^2$ , and let the block length ( $n$ ) tend to infinity.

- (a) Under the Gaussian approximation which was presented in class, derive a recursive equation for the probability of error at the  $l$ -th iteration, i.e., obtain a recursive equation of the form

$$P_e^{(l+1)}(\sigma) = f(P_e^{(l)}(\sigma), \sigma)$$

where  $f(\cdot, \cdot)$  is an appropriate deterministic function, and  $P_e^{(l)}(\sigma)$  designates the probability of error at the  $l$ -th iteration. Calculate the initial value  $P_e^{(0)}(\sigma)$ .

- (b) Show that the stability condition stays consistent under the Gaussian approximation.
- (c) Show that the symmetry property of the message densities is preserved also under the Gaussian approximation.