TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY

Department of Electrical Engineering

Handout 10 **Codes on Graphs and Iterative Decoding**

Homework 7, due **July 11, 2004.** Dr. Igal Sason

Problem 1. [Parity-check nodes update equation for belief propagation]. In this problem, we refer to the belief propagation algorithm, and prove the processing rule at the parity-check nodes of a binary linear code. Recall that the messages in this case are log-likelihood ratios of the observations.

(a) Let $(\alpha_1, \alpha_2, \ldots, \alpha_K)$ be a sequence of K real numbers, and let $(x_1, x_2, \ldots, x_K)$ be an arbitrary sequence of numbers which get the values ± 1. Prove that

$$\sum_{x_1,x_2,\ldots,x_K:\, \prod_{i=1}^K x_i = 1} \left\{ \prod_{i=1}^K \alpha_i^{\frac{1+x_i}{2}} \right\} = \frac{1}{2} \left[\prod_{i=1}^K (\alpha_i + 1) + \prod_{i=1}^K (\alpha_i - 1) \right],$$

$$\sum_{x_1,x_2,\ldots,x_K:\, \prod_{i=1}^K x_i = -1} \left\{ \prod_{i=1}^K \alpha_i^{\frac{1+x_i}{2}} \right\} = \frac{1}{2} \left[\prod_{i=1}^K (\alpha_i + 1) - \prod_{i=1}^K (\alpha_i - 1) \right].$$

(b) Assume that we are given K i.i.d. random variables X_i which take on the values ± 1 with equal probability. Define $X = \prod_{i=1}^K X_i$. Let Y_i denote the result of passing X_i through a noisy channel, where we assume that all observations are conditionally statistically independent. Define the map $\phi : [-\infty, \infty] \to [-\infty, \infty]$, $\phi(x) = \frac{x+1}{x-1}$. Let

$$\alpha \triangleq \frac{p_{Y_1,Y_2,\ldots,Y_K|X}(y_1, y_2, \ldots, y_K|1)}{p_{Y_1,Y_2,\ldots,Y_K|X}(y_1, y_2, \ldots, y_K|-1)}, \quad \alpha_i \triangleq \frac{p_{Y_i|X_i}(y_i|1)}{p_{Y_i|X_i}(y_i|-1)}, \quad \forall\, i = 1, 2, \ldots, K.$$

be the corresponding likelihood ratios. Prove that $\phi(\alpha) = \prod_{i=1}^K \phi(\alpha_i)$.
Hint: Rely on the equalities in item (a), and verify that the function ϕ is its own inverse.

(c) Let

$$L(y_1, y_2, \ldots, y_K) = \ln \alpha, \quad L(y_i) = \ln \alpha_i, \quad \forall i = 1, 2, \ldots, K.$$

Based on Eq. (1), prove that

$$\tanh\left(\frac{L(y_1, y_2, \ldots, y_K)}{2}\right) = \prod_{i=1}^K \tanh\left(\frac{L(y_i)}{2}\right). \tag{1}$$

and therefore

$$\ln\coth\left(\frac{|L(y_1, y_2, \ldots, y_K)|}{2}\right) = \sum_{i=1}^K \ln\coth\left(\frac{|L(y_i)|}{2}\right). \tag{2}$$

(d) Show that the $f(x) = \ln\coth\left(\frac{x}{2}\right)$ is an inverse function of itself, i.e.,

$$y = \ln\coth\left(\frac{x}{2}\right) \Leftrightarrow x = \ln\coth\left(\frac{y}{2}\right)$$

which yields from Eq. (2) that

$$|L(y_1, y_2, \ldots, y_K)| = \ln\coth\left(\frac{1}{2}\sum_{i=1}^{K}\ln\coth\left(\frac{|L(y_i)|}{2}\right)\right). \tag{3}$$

and

$$\text{sign}\Big(L(y_1, y_2, \ldots, y_K)\Big) = \prod_{i=1}^{K}\text{sign}\Big(L(y_i)\Big) \tag{4}$$

For the belief propagation iterative decoding algorithm, Eq. (1) gives the non-linear equation which relates the outgoing message from a parity-check node of degree d_c to the $K = d_c - 1$ incoming messages through the *other edges* which are connected to this parity-check node (where the messages designate the log-likelihood ratios of the corresponding observations).

Problem 2. [Density evolution] In this problem, we derive the density evolution equations for belief propagation when the communications takes place over a binary-input output-symmetric memoryless channel.

(a) Consider a variable node of degree l. By definition of the belief propagation algorithm, an outgoing left-to-right message from a variable node of degree d_v is equal to the sum of the received message from the channel, which has density a_0, and $(d_v - 1)$ right-to-left messages whose average probability density function is b_{l-1} where l is the iteration number. Since in the asymptotic case where the block length tends to infinity, all the LLR messages are statistically independent, then the density of the outgoing message is the convolution of the densities of all summands, i.e., $\mathrm{a}_0 \otimes \mathrm{b}_{l-1}^{\otimes(d_v-1)}$. By averaging over the edge degree distribution, show that the outgoing density is equal to

$$\mathrm{a}_l = \mathrm{a}_0 \otimes \lambda(\mathrm{b}_{l-1}) \tag{5}$$

and define how λ operates on log-likelihood densities.

(b) Let Z be a random variable over $(-\infty, +\infty]$ with probability distribution $A(\cdot)$. We wish to calculate the distribution of the dual representation $\gamma(Z) \triangleq (\gamma_1(Z), \gamma_2(Z))$ where $\gamma_1(Z) = \text{sign}(Z)$, and $\gamma_2(Z) = \ln\coth\frac{|Z|}{2}$. This problem is approached by assigning two distributions associated to $\gamma_2(z)$ under the conditions $\gamma_1(z) = 1$ and $\gamma_1(z) = -1$, respectively. The "distribution" of $\gamma(Z)$ is defined as

$$\Gamma(A)(s, x) = \chi_{\{s=1\}}\,\Gamma_1(A)(x) + \chi_{\{s=-1\}}\,\Gamma_{-1}(A)(x) \tag{6}$$

where $\chi_{\{s=a\}}$ denotes the characteristic function of the set $\{s = a\}$, i.e., $\chi_{\{s=a\}} = 1$ if $s = a$, and $\chi_{\{s=a\}} = 0$ otherwise, and

$$\Gamma_1(A)(x) = \Pr\{\gamma_1(Z) = 1, \gamma_2(Z) \le x\}, \quad \Gamma_{-1}(A)(x) = \Pr\{\gamma_1(Z) = -1, \gamma_2(Z) \le x\}.$$

Show that

$$\Gamma_1(A)(x) = \Pr\{Z \ge \ln\coth\frac{x}{2}\} = 1 - A^-\left(\ln\coth\frac{x}{2}\right) \tag{7}$$

where $A^-(x) \triangleq \lim_{y\to x^-} A(y)$ is left continuous, and

$$\Gamma_{-1}(A)(x) = \Pr\{Z \le -\ln\coth\frac{x}{2}\} = A\left(-\ln\coth\frac{x}{2}\right). \tag{8}$$

In particular, show that

$$\lim_{x\to+\infty} \Gamma_1(A)(x) = \Pr(Z > 0), \quad \lim_{x\to+\infty} \Gamma_{-1}(A)(x) = \Pr(Z < 0)$$

and

$$\lim_{x\to 0^+} \Gamma_1(A)(x) = \Pr(Z = +\infty), \quad \lim_{x\to 0^+} \Gamma_{-1}(A)(x) = 0.$$

(c) Based on item (d) of Problem 1 where you show that the function $f(x) = \ln\coth\left(\frac{x}{2}\right)$ is the inverse function of itself, show that the function Γ has a well-defined inverse. Given the distribution $G = \chi_{\{s=1\}}\, G_1 + \chi_{\{s=-1\}}\, G_{-1}$ as in item (b), show that

$$\Gamma^{-1}(G)(x) = \chi_{\{x>0\}} \left(1 - G_1\left(\ln\coth\frac{x}{2}\right)\right) + \chi_{\{x<0\}}\, G_{-1}\left(\ln\coth\frac{-x}{2}\right) \tag{9}$$

and $\Gamma^{-1}(G)(0) = 1 - \lim_{x\to+\infty} G_1(x)$.

(d) Let us speak of densities over $\{\pm 1\} \times [0, +\infty]$

$$g(s, x) = \chi_{\{s=1\}} g_1(x) + \chi_{\{s=-1\}} g_{-1}(x)$$

by substituting for G_1 and G_{-1} their associated densities. By differentiating the equalities in item (b), show that given a random variable Z with probability density $a(\cdot)$, then

$$\Gamma(a)(s, x) = \chi_{\{s=1\}}\; g_1(x) + \chi_{\{s=-1\}}\; g_{-1}(x)$$

where

$$g_1(x) = \frac{1}{\sinh(x)} \cdot a\left(\ln\coth\frac{x}{2}\right), \quad g_{-1}(x) = \frac{1}{\sinh(x)} \cdot a\left(\ln\tanh\frac{x}{2}\right). \tag{10}$$

Similarly, based on item (c), show that

$$\Gamma^{-1}\left(\chi_{\{s=1\}}\; g_1(x) + \chi_{\{s=-1\}}\; g_{-1}(x)\right) = a(x)$$

where for $x > 0$,

$$a(x) = \frac{1}{\sinh(x)} \cdot g_1\left(\ln\coth\frac{x}{2}\right) \tag{11}$$

and for $x < 0$,

$$a(x) = \frac{1}{\sinh(-x)} \cdot g_{-1}\left(\ln\coth\frac{-x}{2}\right). \tag{12}$$

Verify algebraically that it follows from Eqs. (10), (11) and (12) that $\Gamma^{-1}(\Gamma(a)) = a$. *Hint*: Show that

$$\sinh\left(\ln\coth\frac{x}{2}\right) = \operatorname{csch}(x), \quad x > 0$$

and also rely on the fact that the function $f(x) = \ln\coth\frac{x}{2}$ (where $x > 0$) is an inverse function of itself, so $f\big(f(x)\big) = x$ for all $x > 0$.

(e) Define the convolution of two density functions

$$\chi_{\{s=1\}} g_1(x) + \chi_{\{s=-1\}} g_{-1}(x)$$

and

$$\chi_{\{s=1\}} h_1(x) + \chi_{\{s=-1\}} h_{-1}(x)$$

to be the density function

$$\chi_{\{s=1\}}\big((g_1 \otimes h_1) + (g_{-1} \otimes h_{-1})\big) + \chi_{\{s=-1\}}\big((g_1 \otimes h_{-1}) + (g_{-1} \otimes h_1)\big)$$

where $\otimes$ denotes the convolution operator. If Z_1 and Z_2 are independent random variables over $\{\pm 1\} \times [0, +\infty)$ with densities g_{Z_1} and g_{Z_2} respectively, show that the density of $Z_1 + Z_2$ is $g_{Z_1} \otimes g_{Z_2}$.

(f) Consider a parity-check node of degree d_{c}. The outgoing message from such a parity-check node is the sum of the $(d_{\text{c}}-1)$ independent left-to-right messages whose average probability density function is $\Gamma(a_{l-1})$, assuming that the messages are expressed in the dual representation. Averaging over the right edge degree distribution $\rho(\cdot)$ therefore gives that the density of the right-to-left message in the lth iteration is

$$\rho\big(\Gamma(\mathrm{a}_{l-1})\big) \triangleq \sum_i \rho_i \left((\Gamma(a_{l-1}))^{\otimes(i-1)}\right).$$

Converting right away back into the log-likelihood domain, it follows that the average probability density function of the right-to-left message is

$$\mathrm{b}_{l-1} = \Gamma^{-1}\Big(\rho\big(\Gamma(\mathrm{a}_{l-1})\big)\Big). \tag{13}$$

We note that the computation of the convolution can be simplified with the aid of the Fourier transform (since the Fourier transform of a convolution of signals is equal to the multiplication of their Fourier transforms, so one can calculate the Fourier transform of $\Gamma(a_{l-1})$, raise it to the $(i-1)$th power, and then calculate the inverse Fourier transform in order to obtain $(\Gamma(a_{l-1}))^{\otimes(i-1)}$).

(g) Combine Eqs. (5) and (13) to obtain the recursive equation for the log-likelihood densities of the left-to-right messages

$$\mathrm{a}_l = \mathrm{a}_0 \otimes \lambda\bigg(\Gamma^{-1}\Big(\rho\big(\Gamma(\mathrm{a}_{l-1})\big)\Big)\bigg), \quad l = 1, 2, \ldots \tag{14}$$

where a_0 designates the log-likelihood density of the channel output.

(h) Derive the density evolution equation for the BEC as a particular case of the general density evolution equation in Eq. (14), i.e., show that for a BEC whose erasure probability is p

$$x_l = p\,\lambda\big(1 - \rho(1 - x_{l-1})\big)$$

where x_l designates the bit erasure probability at iteration no. l.

Problem 3. [Symmetry is preserved under density evolution]

(a) If two functions f and g are symmetric, prove that the convolution $f \otimes g$ is also a symmetric function.

(b) Assume $\Gamma(f)(s,x) = \chi_{\{s=1\}} f_1(x) + \chi_{\{s=-1\}} f_{-1}(x)$. We define the function $\Gamma(s,x)$ to be symmetric if and only if

$$\frac{f_1(x)}{f_2(x)} = \coth\left(\frac{x}{2}\right)\ , \ x > 0.$$

Show that f is symmetric (i.e., $f(x) = e^x\ f(-x)$) if and only if $\Gamma(f)(s,x)$ is a symmetric function.

(c) Explain from (14) why for belief propagation which is performed over a memoryless, binary-input and output-symmetric channel, the symmetry of $a_l(\cdot)$ is insured for every non-negative integer l (i.e., for all iterations).