Problems to Hand In:

1. Let $X_1, \ldots, X_n$ be $n$ independent (but not necessarily identically distributed) binary (i.e., 0 or 1) valued random variables, and let $S$ denote their mod 2 sum:

$$S = X_1 + X_2 + \cdots + X_n.$$  

This problem considers methods of computing the pdf of $S$ from those of the $X_i$’s, which is closely related to the problem of updating the messages at the check nodes of a message-passing decoder like the one discussed in class on May 15.

(a) For any binary random variable $Y$, define

$$\Delta(Y) = \Pr\{Y = 0\} - \Pr\{Y = 1\}.$$  

Show that if $S$ is defined as in (1),

$$\Delta(S) = \prod_{i=1}^{n} \Delta(Y_i).$$

(b) For any binary random variable $Y$, define

$$L(Y) = \log \frac{\Pr\{Y = 0\}}{\Pr\{Y = 1\}}.$$  

(The logarithm is “natural.”) Using the result from part(a), find a formula expressing $L(S)$ in terms of $L(X_1), \ldots, L(X_n)$. (You may wish to use the identity

$$
\frac{e^x - 1}{e^x + 1} = \tanh \frac{x}{2}
$$

to simplify your answer.)

2. In class on May 15, Prof. McEliece discussed (Tanner) graph-based “belief propagation” decoding of the $(7, 4)$ binary linear code defined by the parity-check matrix

$$H = \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1
\end{pmatrix}. $$

Suppose that an unknown codeword $(x_1, x_2, \ldots, x_n)$ from this code is transmitted over a binary-input memoryless channel and received as $(y_1^*, \ldots, y_n^*)$. Use the BP decoding algorithm to compute the *a posteriori* probabilities

$$\Pr\{X_i = x_i| (y_1^*, \ldots, y_n^*)\} \quad i = 1, \ldots, 7$$

in the following two cases.
(a) Binary symmetric channel, crossover probability $p = .2$,

\[(y_1^*, \ldots, y_n^*) = (1000111).\]

(b) Additive gaussian noise channel (inputs are $\pm 1$ rather than $\{0, 1\}$), noise variance $\sigma^2 = 0.2$,

\[(y_1^*, \ldots, y_n^*) = (-0.9, -1.1, 0, 1.1, -0.9, -1.2, -1.1).\]