E2 205 Error-Control Coding
Homework 7

1. The Fig. 1 shows the junction tree associated with variable node 11 of a certain LDPC code. Identify the associated MPF problem along with the local domains and the local kernels. What is the objective function being computed if messages are passed as indicated by the arrows ?

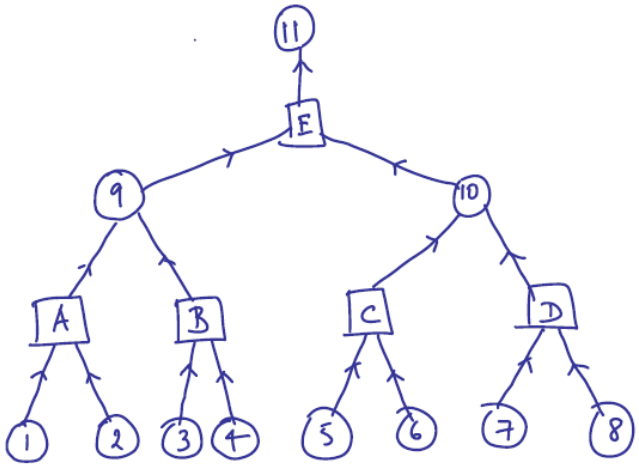

Figure 1: Computational tree associated to node 11.

2. In the density evolution analysis of (d_v, d_c)-regular LDPC codes, where the goal is to determine the evolution of the density of number of incorrect messages passed between variable nodes and check nodes, it is customary to assume that the all-$\underline{1}$ codeword is transmitted. What are the assumptions on the channel and the processing carried out at the variable and check node under which this assumption is valid ? Explain your answer while making clear any notation that you introduce.

3. Consider density evolution associated to Gallager Decoding Algorithm A applied to an LDPC code $\mathscr{C}$. Thus the channel is a BSC with cross-over probability $\varepsilon << 1$ and all messages passed are either 1 or -1. You may assume that the neighborhood of every node in the Tanner graph of $\mathscr{C}$ is tree-like to depth 8. What is the probability $p_{-1}^{(1)}$ that at the end of iteration 1, the message passed from a variable node to check node will be in error?

   (Notation is as in class. Following an initial round of message passing, from the variable nodes to check nodes, based only on channel inputs, each subsequent iteration is composed of two rounds of message passing: from check node to variable node followed by from variable node back to check node. Show all your working clearly. You may use the fact that $\varepsilon << 1$ to simplify calculations. Hence $a\varepsilon^2$ for integer constants $a < 100$ (say) may safely be ignored in comparison with ε, etc.)

4. Show clearly that the check-node symmetry condition holds when LDPC codes are decoded using belief propagation with log-likelihood ratios (LLR) in place of beliefs.

5. Let W be a binary symmetric channel with crossover probability ε. Derive expressions for the following:

   (a) symmetric capacity $I(W)$

   (b) Bhattacharya parameter $Z(W)$

   (c) $I(W^+)$ and $I(W^-)$

6. Prove that for any binary input discrete memoryless channel W, the probability of error for maximum likelihood decoding is upper bounded by Bhattcaharya parameter $Z(W)$. Also, show that $Z(W)$ is upper bounded by 1.

7. Let W be a binary erasure channel with erasure probability ε. Derive expressions for the following:

   (a) $I(W), Z(W)$

   (b) $I(W^+), I(W^-)$

   (c) $Z(W^+), Z(W^-)$

8. Let $q = 2$ and $N = 23$. What is the order m of $q \pmod N$? Let α be a primitive N-th root of unity lying in $GF(2^m)$. Determine the dimension of the binary $q = 2$ cyclic code of length $N = 23$ all of whose codewords $c(t)$ satisfy

$$\hat{c}(\lambda) = 0, \lambda = 1 \ .$$

9. Determine the number of binary sequences $\{a_t\}$ of period $N = 15$ that satisfy the condition

$$\hat{a}_\lambda \ \in \ \{0,1\}, \text{ all } \lambda, \ \ 0 \leq \lambda \leq 14.$$

10. Why are there no interesting linear, cyclic binary codes of length $N = 19$?

11. Design a single-error correcting, double-error detecting binary linear, cyclic code of length 21. Naturally you would like to have dimension k as large as possible.

12. Identify the null spectrum of a Reed-Solomon (RS) code over $GF(9)$ code of length $N = 8$ and designed distance $d_{\min} = 6$.

13. Consider the binary cyclic code $\mathscr{C}$ of length $N = 15$ with null spectrum $\{1,2,3,4,5,6,8,9,10,12\}$. You may assume that transforms are computed using primitive element $\alpha \in GF(16)$ satisfying $\alpha^4 + \alpha + 1 = 0$.

    Does the all-one codeword $(1, \ 1, \ \ldots \ 1, \ 1)$ belong to the cyclic code $\mathscr{C}$? Explain your answer.

14. How many binary cyclic codes of length 23 are there? Design a double-error-correcting cyclic code of length 23 and identify its dimension.

15. Let $\alpha \in GF(16)$ satisfy $\alpha^4 + \alpha + 1 = 0$. Let $\mathscr{C}$ be the binary cyclic BCH code of length $N = 15$ having parameters $m_0 = 1, d = 5$. (Fourier transforms are computed using primitive element α). Find the nearest codeword if the received vector r_t is given by

$$(r_t, t = 0, 1, 2, ..., 14) = (100100000000000).$$

(The answer is clearly, the all-zero codeword. However, go through the decoding procedure provided in class using the extended EDA).