Final Exam of Error-Correcting Codes

Jan. 14, 2021

1. Consider an (n, k) BCH code over $GF(q)$ which can correct t errors.
   (a) (4%) Let $n = 31$, $q = 2$ and $t = 3$. Find the value of k.
   (b) (4%) Let $n = 63$, $q = 2$ and $t = 5$. Find the value of k.
   (c) (4%) Let $n = 15$, $q = 4$ and $t = 3$. Find the value of k.

2. (8%) Describe the procedure of Peterson-Gorenstein-Zierler decoder in the decoding of BCH code.

3. (6%) What is the key equation in the decoding of BCH codes?

4. Let $\alpha \in \mathrm{GF}(q)$ be an element of order n. Let $A(X)$ be a polynomial over $\mathrm{GF}(q)$. The (n, k) Reed-Solomon code over $\mathrm{GF}(q)$ can be defined as the set $C = \{\mathbf{a} = (a_0, a_1, ..., a_{n-1}) | a_i = A(\alpha^i), i = 0, 1, ..., n-1, deg(A(X)) < k\}$.
   (a) (6%) Prove that the minimum distance of C is $n - k + 1$.
   (b) (8%) Prove that this C is a nonbinary cyclic code over $\mathrm{GF}(q)$ of length n for which its code polynomial contains $n - k$ consecutive roots.

5. (3%) What is a catastrophic convolutional code?
   (4%) Describe the condition of checking whether a convolutional code is catastrophic by its state diagram.

6. (8%) Prove that the final survivor in the Viterbi algorithm is the maximum likelihood path.

7. (a) (6%) Convert the nonsystematic convolutional (NSC) code with generator sequences $\bar{g}_1 = (111)$ and $\bar{g}_2 = (101)$ into a recursive systematic convolutional (RSC) code.
   (b) (6%) Draw the state diagram of the RSC code describe above.

8. (7%) Consider a Gaussian channel with input $X \in \{+1, -1\}$ and output $y \in R$, where $p(y|x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(y-x)^2/2\sigma^2}$. Let $L(x|y) = \ln\frac{P(x=+1|y)}{P(x=-1|y)}$. Please express $L(x|y)$ in the form of $L_c y + L(x)$.

9. (8%) Use the transfer characteristics of the EXIT chart to explain the pinch-off region, bottleneck region and the wide-open region in the BER curves of turbo codes.

10. (5%) In the iterative decoding of message passing for an LDPC code, what is the definition of a cycle? What is the major problem regarding the cycle length?

11. Consider a irregular LDPC code. The degree-distribution polynomial for the variable node is $\lambda(X) = \sum_{i=1}^{d_v} \lambda_i X^{i-1}$ where λ_i denotes the fraction of all edges connected to degree-i variable nodes. The degree-distribution polynomial for the check node is $\rho(X) = \sum_{i=1}^{d_c} \rho_i X^{i-1}$ where ρ denotes the fraction of all edges connected to degree-i check nodes. Let m, n, E and R be the number of check nodes, the number of variable nodes, the total number of edges in the graph and code rate respectively.
    (a) (5%) Express E as a function of n and $\lambda(X)$.
    (b) (5%) Express R as a function of $\rho(X)$ and $\lambda(X)$.

(Continued on the reverse side)

12. Let W be a symmetric binary-input discrete-memoryless channel (B-DMC) W with input $x \in \{0, 1\}$, output y and transition probability $W(y|x)$.

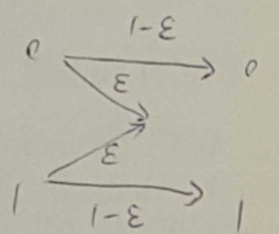
Consider the basic component of a polar code by combining two W channels, where each W has input x_i and output y_i, $i = 1, 2$ into W_2, for which the two input bits u_1 and u_2 are related to x_1 and x_2 such that $x_1 = u_1 \oplus u_2$ and $x_2 = u_2$.

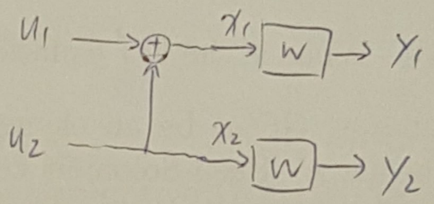
We then have two polarized channels $W_2^{(1)}$ and $W_2^{(1)}$. Define the Bhattacharyya parameter by

$Z(W) = \sum_y \sqrt{W(y|0)W(y|1)}$.

(a) (3%) Let W be a binary erasure channel with erasure rate ϵ. Find $Z(W)$.

(b) (3%) What are the values of $Z(W_2^{(1)}) = 2Z(W) - Z(W)^2$ and $Z(W_2^{(2)}) = Z(W)^2$?





$\cancel{1-\varepsilon}$

$W_N^{(2i-1)}$

$W_N^{(2i)}$