TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY

Department of Electrical Engineering

Handout 2 **Codes on Graphs and Iterative Decoding**

Homework 1, due **April 18, 2004.** Dr. Igal Sason

Problem 1 (One code, many parity-check matrices). Prove that the parity-check matrix H of a binary linear block code of length n and dimension k has $2^{\binom{n-k}{2}} \prod_{i=1}^{n-k} (2^i - 1)$ different representations.

Problem 2. Consider a binary linear block code $\mathcal{C}$ whose generator matrix is given by

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(a) Find a generator matrix for $\mathcal{C}$ in systematic form.

(b) Find a parity-check matrix for $\mathcal{C}$.

(c) Find the minimum distance of $\mathcal{C}$.

Problem 3 (Comparison of hard and soft decision schemes). A binary input channel uses the two input levels A and $-A$. The output of the channel is the sum of the input and the an additive white Gaussian noise with mean 0 and variance σ^2. This channel is used under two different conditions. In one case, the output of the channel is used directly without quantization (i.e., soft decision), and in the other case, an optimal decision is made on each input level (hard decision). Prove the following:

(a) The channel capacity with soft decision is equal to $C_{\text{soft}} = f\left(\frac{A}{\sigma}\right)$ where

$$f(a) = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}}\, e^{-\frac{(u-a)^2}{2}} \log_2\left(\frac{2}{1+e^{-2au}}\right) \mathrm{d}u\,, \quad -\infty < a < \infty.$$

Hint: Show that the capacity-achieving distribution of the input to the channel is uniform, then calculate the resulting mutual information $I(X;Y)$, and finally show that the above function $f(\cdot)$ is even (i.e., $f(a) = f(-a)$).

(b) The channel capacity with hard decision is equal to $C_{\text{hard}} = 1 - h\left(Q\left(\frac{A}{\sigma}\right)\right)$ where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function to the base 2, and $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-\frac{x^2}{2}}\, \mathrm{d}x$ is the complementary Gaussian cumulative function.

(c) Plot the capacities in items (a) and (b) as a function of $\frac{A}{\sigma}$ where $\frac{A}{\sigma}$ varies between 0.1 and 10 (plot the parameter $\frac{A}{\sigma}$ in logarithmic axis). Compare the two results in terms of the gain in $\frac{A}{\sigma}$ (expressed in dB) for achieving a capacity of $\frac{1}{2}\ \frac{\text{bits}}{\text{channel use}}$.

Problem 4 (Puncturing). Let $\mathcal{C}$ be a linear block code of length n and dimension k. In general, puncturing of $\mathcal{C}$ consists of the removal of parity-check symbols. Assume that p parity-check symbols of the code $\mathcal{C}$ are punctured, and let $\mathcal{C}_p$ be the new code.

(a) Is the new block code $\mathcal{C}_p$ linear ?

(b) What are the block length and dimension of the code $\mathcal{C}_p$? What is its code rate ? Does its rate increase or decrease as compared to the rate of the original code $\mathcal{C}$?

(c) Explain how to obtain a parity-check matrix H_p of the punctured code $\mathcal{C}_p$, given the parity-check matrix H of the original code $\mathcal{C}$.

(d) Exemplify your answer in items (b) and (c) for the $(7,4)$ Hamming code when the first and the third parity-check symbols of the code are punctured. Assume that the code $\mathcal{C}$ is represented by a systematic generator matrix.

Problem 5 (Product codes). Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two linear block codes of length n_i, dimension k_i, minimum distance d_i, and code rate $R_i = \frac{k_i}{n_i}$ $(i = 1, 2)$. The *product code* $\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2$ is defined as the block code which includes all the codewords $c \in \mathcal{C}$ in the form of a two-dimensional array such that its rows and columns are the codewords of the code $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively.

(a) Does the product code form a linear block code ?

(b) Express the block length, dimension, code rate and minimum distance of the product code $\mathcal{C}$ in terms of the corresponding parameters of the component codes $\mathcal{C}_1$ and $\mathcal{C}_2$.

(c) Give numerical results to the question in item (b) for the product code which includes the $(7,4)$ and $(15,11)$ Hamming codes as its component codes.

Problem 6 (Convolutional codes). Consider a recursive systematic convolutional (RSC) code $\mathcal{C}$ with the generator matrix $G(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$.

(a) Draw an encoder circuit for $\mathcal{C}$.

(b) Draw a trellis section for the trellis diagram of the code.

(c) Compute the extended weight enumerator $T(D, L, I)$ of the convolutional code $\mathcal{C}$, and expand it into a power series, i.e., a series of the form $T(D, L, I) = \sum_{d,l,i} a_{d,l,i} D^d L^l I^i$.

(d) What is the free distance of the convolutional code ? What is the corresponding path in its trellis diagram and what is the weight of the corresponding input sequence ?

(e) What are the rates of the punctured convolutional codes which are constructed from the above RSC codes with the following puncturing matrices:

$$P_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

(f) A family of punctured convolutional (PC) codes are called *rate-compatible punctured convolutional* (RCPC) codes if all the PC codes within this family have the same puncturing period, and also the branch outputs of every (PC) code are used by the lower rates PC codes in this family.
Do the family of PC codes which are constructed from the above RSC code with the puncturing matrices defined in item (e) form a family of RCPC codes ? Explain.

(g) Let the original RSC code be used over a binary symmetric channel (BSC) with crossover probability p. Calculate a union bound on the bit error probability of the decoded sequence of information bits (i.e., the Viterbi bound), and evaluate it for $p = 0.001$.