

TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY
Department of Electrical Engineering

Handout 3

Codes on Graphs and Iterative Decoding

Homework 2, due **May 2, 2004**.

Dr. Igal Sason

Problem 1. The purpose of this problem is to show that almost all binary linear codes do not have a low-density representation.

- (a) Prove that for any positive integer n and $0 < \delta < \frac{1}{2}$

$$\binom{n}{n\delta} \leq 2^{nh(\delta)}, \quad \sum_{k=0}^{n\delta} \binom{n}{k} \leq \binom{n}{n\delta} \frac{1-\delta}{1-2\delta}.$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ ($0 < x < 1$) designates the binary entropy function.

- (b) 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.
- (c) Conclude from items (a) and (b) that if we pick randomly (with uniform distribution) a binary linear code of length n and rate $R = \frac{k}{n}$, then the probability that one of its parity-check matrices has a number of ones which is at most an (where a is an arbitrary positive constant) is upper bounded by an expression which decays exponentially to zero. In particular, show that for large values of n , this probability does not exceed $2^{-\alpha n^2}$ where α is a positive constant for $0 < R < 1$ (calculate α).

Problem 2. Consider an ensemble of (n, λ, ρ) LDPC codes. According to our notations $\lambda(x) = \sum_i \lambda_i x^{i-1}$ and $\rho(x) = \sum_i \rho_i x^{i-1}$, where λ_i and ρ_i designate the probabilities that if we pick an edge at random (with uniform distribution), then this edge is connected to a variable node or a parity-check node of degree i .

Define also two degree polynomials from a node perspective

$$\Lambda(x) = \sum_i \Lambda_i x^i \quad \Omega(x) = \sum_i \Omega_i x^i$$

where Λ_i and Ω_i designate the probabilities that a variable (left) node or parity-check (right) node (which are chosen randomly with uniform distribution) have degree i , respectively. To conclude, $\lambda(\cdot)$ and $\rho(\cdot)$ are two polynomials which refer to ensembles of LDPC codes from an *edge* perspective, and $\Lambda(\cdot)$ and $\Omega(\cdot)$ are degree polynomials which refer to these ensembles from a *node* perspective.

- (a) Show that

$$\Lambda(x) = \frac{\int_0^x \lambda(t) dt}{\int_0^1 \lambda(t) dt} \quad \Omega(x) = \frac{\int_0^x \rho(t) dt}{\int_0^1 \rho(t) dt}.$$

- (b) Show that

$$\lambda(x) = \frac{\Lambda'(x)}{\Lambda'(1)} \quad \rho(x) = \frac{\Omega'(x)}{\Omega'(1)}.$$

(c) Show that the design rate R of the LDPC ensemble is given by

$$R = 1 - \frac{\int_0^1 \rho(x) dx}{\int_0^1 \lambda(x) dx} = 1 - \frac{\Lambda'(1)}{\Omega'(1)}.$$

Problem 3. Consider the ensemble of LDPC codes with left degree distribution $(\lambda_2, \lambda_3, \dots)$, and with constant right degree a (i.e., the degree of the check nodes is equal to a).

- (a) If the ensemble rate is $R = 0.95$, what is the *smallest* possible value of a ? For which left degree distribution it is achieved?
- (b) Assume that the left degree distribution of the *edges* is

$$\lambda_i = c i 0.5^i, \quad i = 2, 3, \dots$$

Calculate the value of c , and then find what is the required value of a , so that the design rate will be equal to $R = 0.95$? (compare your result with the one you got in item (a)).

Rely here on the equalities $\sum_{n=1}^{\infty} x^n = \frac{x}{1-x}$ and $\sum_{n=1}^{\infty} nx^n = \frac{x}{(1-x)^2}$ for $|x| < 1$.

Problem 4. Consider an ensemble of (n, λ, ρ) LDPC codes where

$$\lambda(x) = \frac{613}{1500} x + \frac{303}{1500} x^2 + \frac{114}{1500} x^3 + \frac{294}{1500} x^6 + \frac{176}{1500} x^7, \quad \rho(x) = x^5.$$

- (a) Calculate the degree distributions of the variables (left) nodes and the parity-check (right) nodes.
- (b) Calculate the average left degree (a_L) and the right degree (a_R) of the bipartite graph.
- (c) Calculate the design rate of this ensemble.

Problem 5. Consider the ensemble of regular LDPC codes of block length n where the degrees of the variable nodes and the parity-check nodes are d_v and d_c , respectively.

- (a) Prove that the number of distinct codes from the ensemble of regular LDPC codes is equal to $\frac{(nd_v)!}{m! (d_c!)^m}$ where $m = \frac{nd_v}{d_c}$ designates the number of parity-check nodes.
- (b) Show that the number of distinct codes from the considered ensemble of regular LDPC codes is approximately

$$\sqrt{d_c} \left\{ \frac{1}{(d_c - 1)!} \left(\frac{nd_v}{e} \right)^{d_c - 1} \right\}^{\frac{nd_v}{d_c}}.$$

Hint: Use Stirling's approximation $n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.

- (c) Compare the results in items (a) and (b) in case that $n = 100$, $d_v = 3$ and $d_c = 6$.

Problem 6. Consider a regular LDPC code of length n where the degree of the variable nodes is d_v , and the degree of the parity-check nodes is d_c . Assume that iterative message-passing decoding is performed to decode the code.

- (a) Consider the mild condition where $n - 1 > d_v(d_c - 1)$ (we note that d_v and d_c are typically rather small positive integers while n is typically at least few hundreds of bits, so in practice, our assumption is automatically satisfied). Show that the maximal number of decoding iterations (m) which can be achieved before the assumption on the statistical independence of the messages in the message-passing iterative decoder becomes invalid is upper bounded by

$$m < \frac{\log\left(\frac{(d_v-1)n}{d_v}\right)}{\log((d_v-1)(d_c-1))}.$$

The latter inequality implies that the number of independent iterations grows at most like the log of the block length of the code.

- (b) Let L designate the *girth* of the Tanner graph representing the code (i.e., the shortest cycle in the graph). We note that the girth of the graph affects the performance of the code especially in the error floor region, and in general, for reducing the decoding error probability in the error floor region, one wishes to construct LDPC codes with large girth. Show that the girth (L) is related to the number of independent decoding iterations (m) via the inequality

$$m < \frac{L}{4} \leq m + 1.$$

- (c) Consider an arbitrary regular LDPC code where the degrees of the variable nodes and the parity-check nodes are $d_v = 3$ and $d_c = 6$, respectively.
1. What is the design rate of the code ?
 2. Calculate an upper bound on the maximal possible girth of the corresponding Tanner graph if the block length of the code is $n = 1000$.
 3. Calculate a lower bound on the block length of the code so that the girth of the Tanner graph representing the code will be equal to 12.

Tentative reading:

Read the paper of G. Miller and G. Cohen, "The rate of regular LDPC codes," *IEEE Trans. on Information Theory*, vol. 49, pp. 2989–2993, November 2003.

It is demonstrated there that the rate of a code from the ensemble of regular LDPC codes converges asymptotically (as we let the block length tend to infinity) to the design rate. The proof refers to a convergence in the sense of quadratic mean and also almost surely. It gives an operational meaning to the design rate of LDPC ensembles; apart of a lower bound on the code rate, it is also in high probability the asymptotic rate of these codes.