TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY
Department of Electrical Engineering

Handout 5 **Codes on Graphs and Iterative Decoding**
Homework 4, **not for submission.** Dr. Igal Sason

Problem 1. This problem refers to a recipe for constructing capacity-achieving sequences of ensemble of LDPC codes where the communications takes place over a binary erasure channel (BEC).

Let $\mathcal{D}$ be the set of functions $\gamma : [0,1) \to \mathbb{R}^+$ which are analytic around zero with a non-negative power series expansion, and let $\mathcal{N}$ be the set of functions $\hat{\gamma} \in \mathcal{D}$ so that $\hat{\gamma}(1) = 1$. As a main ingredient, we need two parameterized functions which depend on a non-negative parameter α: let $\rho_\alpha(\cdot)$ be an element in $\mathcal{N}$, and $\hat{\lambda}_\alpha(\cdot)$ be an element in $\mathcal{D}$. Assume further that the following equality is satisfied

$$\hat{\lambda}_\alpha\Big(1 - \rho_\alpha(1-x)\Big) = x, \quad \forall x \in [0,1). \tag{1}$$

Let $\hat{\lambda}_{\alpha,N}(x)$ denote the function consisting of the first $N+1$ terms in the Taylor series expansion of $\hat{\lambda}_\alpha(x)$ (up to and including the term x^N). Clearly, $\hat{\lambda}_{\alpha,N}(x) \in \mathcal{D}$, and for N sufficiently large $\hat{\lambda}_{\alpha,N}(1) > 0$, so that we can define the *normalized* function

$$\lambda_{\alpha,N}(x) = \frac{\hat{\lambda}_{\alpha,N}(x)}{\hat{\lambda}_{\alpha,N}(1)}$$

where $\lambda_{\alpha,N}(\cdot) \in \mathcal{N}$.

(a) Show that if the threshold of the ensemble of $(n, \lambda_{\alpha,N}, \rho_\alpha)$ LDPC codes under iterative message-passing decoding is equal to $p^{\text{IT}}(\alpha, N)$, then

$$p^{\text{IT}}(\alpha, N) \geq \hat{\lambda}_{\alpha,N}(1).$$

Lets assume that the design rate under iterative message-passing decoding should not be below a certain fraction $1-\varepsilon$ of the capacity of a BEC whose erasure probability is $p^{\text{IT}}(\alpha, N)$ (i.e., we need that the design rate R satisfies the inequality $R \geq (1 - p^{\text{IT}}(\alpha, N))(1-\varepsilon)$).

(b) Show that in order to obtain this requirement, it is sufficient that

$$\frac{\hat{\lambda}_{\alpha,N}(1)}{1 - \hat{\lambda}_{\alpha,N}(1)} \left[\frac{\int_0^1 \rho_\alpha(x)\, \mathrm{d}x}{\int_0^1 \hat{\lambda}_{\alpha,N}(x)\, \mathrm{d}x} - 1 \right] \leq \varepsilon\ . \tag{2}$$

(c) Prove the following strategy for constructing capacity-achieving sequences of ensembles of LDPC codes on a BEC with erasure probability p: given two parameterized functions $\hat{\lambda}_\alpha(x)$ and $\rho_\alpha(x)$ in $\mathcal{D}$ and $\mathcal{N}$, respectively, we need to choose $\alpha = \alpha(N)$ in such a way that

$$\lim_{N\to\infty} \left(1 - \hat{\lambda}_{\alpha,N}(1) \cdot \frac{\int_0^1 \rho_\alpha(x)\, \mathrm{d}x}{\int_0^1 \hat{\lambda}_{\alpha,N}(x)\, \mathrm{d}x}\right) = 1 - p$$

$$\lim_{N\to\infty} \frac{\hat{\lambda}_{\alpha,N}(1)}{1 - \hat{\lambda}_{\alpha,N}(1)} \left[\frac{\int_0^1 \rho_\alpha(x)\, \mathrm{d}x}{\int_0^1 \hat{\lambda}_{\alpha,N}(x)\, \mathrm{d}x} - 1 \right] = 0.$$

Problem 2. This Problem is focused on the asymptotic analysis of the best capacity-achieving sequence of ensembles of LDPC codes which is currently known for the BEC; Surprisingly, it is a sequence of *right-regular ensembles*. The problem relies on the technique which was presented in Problem 1 for constructing capacity-achieving sequences of ensembles of LDPC codes under iterative message-passing decoding, where we assume that the communication takes place over a BEC.

(a) Show that for $0 < \alpha < 1$, the functions

$$\hat{\lambda}_\alpha(x) = 1 - (1-x)^\alpha, \quad \rho_\alpha(x) = x^{\frac{1}{\alpha}}$$

satisfy all the conditions in item (a) of Problem 1. Calculate the truncated polynomial $\lambda_{\alpha,N}(\cdot)$ based on the equality

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k \,, \quad |x| < 1,$$

where

$$\binom{\alpha}{k} \triangleq \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}.$$

(b) Prove that for $N \geq 1$

$$\sum_{k=1}^{N} \frac{(-1)^{k+1}}{k+1} \binom{\alpha}{k} = \frac{\alpha - \binom{\alpha}{N+1}(-1)^N}{\alpha+1} \,, \quad \sum_{k=1}^{N} (-1)^{k+1} \binom{\alpha}{k} = 1 - \frac{N+1}{\alpha} \binom{\alpha}{N+1} (-1)^N$$

(you may use mathematical induction for proving these equalities).

(c) Based on the previous two items, show that the design rate $R(\alpha, N)$ of the ensemble of $(n, \lambda_{\alpha,N}, \rho_\alpha)$ LDPC codes is

$$R(\alpha, N) = \frac{N\binom{\alpha}{N+1}(-1)^N}{\alpha - \binom{\alpha}{N+1}(-1)^N} \,. \tag{3}$$

(d) Based on item (b) in Problem 1, show that a sufficient condition for the ensemble of $(n, \lambda_{\alpha,N}, \rho_\alpha)$ LDPC codes to achieve a fraction $1-\varepsilon$ of the channel capacity whose erasure probability is $p^{\text{IT}}(\alpha, N)$ (so that vanishing bit erasure probability is achieved under iterative message-passing decoding as $n \to \infty$) is to choose α and N to satisfy the inequality

$$\frac{1 - \frac{1}{N+1}}{1 - \frac{1}{\alpha}\binom{\alpha}{N+1}(-1)^N} \geq 1 - \varepsilon. \tag{4}$$

(e) Show that for $0 < \alpha < 1$

$$\ln\left((-1)^N \binom{\alpha}{N+1}\right) = \ln\left(\frac{\alpha}{N+1}\right) + \sum_{k=1}^{N} \ln\left(1 - \frac{\alpha}{k}\right).$$

Based on the equality $\ln(1+x) = \sum_{k=1}^{\infty} \left\{(-1)^{k+1} \, \frac{x^k}{k}\right\}$ for $-1 < x \leq 1$, show that for $0 < \alpha < 1$

$$\ln\left((-1)^N \binom{\alpha}{N+1}\right) = \ln\left(\frac{\alpha}{N+1}\right) - \alpha \sum_{k=1}^{N} \frac{1}{k} - \frac{\alpha^2}{2} \sum_{k=1}^{N} \frac{1}{k^2} - \frac{\alpha^3}{3} \sum_{k=1}^{N} \frac{1}{k^3} - \ldots \,. \tag{5}$$

(f) Prove that the sequence

$$a_n = \sum_{k=1}^{n} \frac{1}{k} - \ln(n) \quad n = 1, 2, \ldots$$

is monotonic decreasing and positive which yields that $\lim_{n\to\infty} a_n$ exists. This limit is called Euler's constant and it is designated by γ. Show that

$$\gamma < a_n < \gamma + \frac{1}{2n}\,, \qquad n = 1, 2, \ldots \tag{6}$$

[*Hint*: a possible way to prove this inequality is to show that for every integer $n \geq 1$

$$a_n = \lim_{k\to\infty} a_k + \sum_{k=1}^{\infty} \left(a_{n+k-1} - a_{n+k}\right),$$

then use the power series of $\ln(1+x)$ to show that

$$0 < a_n - a_{n+1} < \frac{1}{2n(n+1)}\,, \qquad n = 1, 2, \ldots$$

and finally combine the latter two results to obtain this inequality.] We note that the latter inequality enables one to calculate γ in any desired precision; verify that $\gamma \approx 0.5772157$. Inequality (6) can be rewritten alternatively as

$$\ln(N) + \gamma < \sum_{k=1}^{N} \frac{1}{k} < \ln(N) + \gamma + \frac{1}{2N}\,, \quad \forall\, N \geq 1. \tag{7}$$

(g) Based on the equality $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$ (which yields that $\sum_{k=1}^{N} \frac{1}{k^p} < \frac{\pi^2}{6}$ for any $p \geq 2$ and $N \geq 1$) and on Eqs. (5) and (7), show that

$$\frac{\alpha \cdot c(\alpha)}{(N+1)^{\alpha+1}} < (-1)^N \binom{\alpha}{N+1} < \frac{\alpha}{(N+1)^{\alpha+1}}\,, \qquad \forall\, 0 < \alpha < 1,\; N \geq 1 \text{ integer}$$

where $c(\alpha) \triangleq (1-\alpha)^{\frac{\pi^2}{6}} \cdot e^{\alpha\left(\frac{\pi^2}{6} - \gamma\right)}$ for $\alpha \in [0, 1]$.

Consider a BEC whose erasure probability is p ($0 < p < 1$).

(h) Show that the function $c(\cdot)$ is monotonic decreasing in the interval $[0, 1]$, so that $c(\alpha) \geq c(p)$ for $0 \leq \alpha \leq p$.

(i) Choose N and α to satisfy the equality $\frac{1}{(N+1)^\alpha} = 1 - p$.
Based on items (c) and (g), show that for $0 < \alpha < 1$

$$\frac{N}{N+1} \cdot \frac{(1-p)\, c(\alpha)}{1 - \frac{1-p}{N+1}} < R(\alpha, N) < \frac{1-p}{1 - \frac{(1-p)\, c(\alpha)}{N+1}}$$

and

$$\lim_{N\to\infty} R(\alpha, N) = 1 - p$$

which implies that when $N \to \infty$, the design rate of the LDPC ensemble $(n, \lambda_{\alpha,N}, \rho_\alpha)$ is equal to the capacity of a BEC whose erasure probability is p.

(j) Based on items (d), (g) and (h), show that Eq. (4) is satisfied for

$$N = \max\left(\left\lfloor \frac{1 - c(p)\cdot(1-p)(1-\varepsilon)}{\varepsilon} \right\rfloor, \left\lfloor (1-p)^{-\frac{1}{p}} \right\rfloor\right) .$$

(k) Show that the right degree of the considered ensemble of $(n, \lambda_{\alpha,N}, \rho_\alpha)$ LDPC codes behaves similarly to the lower bound on the average right degree which was derived in class (i.e., show that in both cases, the coefficients of $\ln\left(\frac{1}{\varepsilon}\right)$ coincide). Discuss the implication of your result with respect to the decoding complexity of this LDPC ensemble under iterative message-passing decoding.

(l) Derive the stability condition for the ensemble of $(n, \lambda_{\alpha,N}, \rho_\alpha)$ LDPC codes in item (a) for a BEC whose erasure probability is p, and verify that the choice of the parameters α and N above satisfies the stability condition.

(m) Design an ensemble of right-regular LDPC codes with a design rate of $R = 0.650$ and a fixed right degree of $a_\mathrm{R} = 12$. Calculate the threshold of this ensemble and the multiplicative gap to capacity under iterative message-passing decoding, where the communications takes place over a BEC. Plot the left degree distribution of this ensemble.
Hint: Write a computer program which first computes the parameters α and N in order to achieve the desired right degree and the design rate (note that the expression of $R(\alpha, N)$ in Eq. (3) is a monotonic decreasing function of N, so choose N to be as close as possible to the design rate R). Then calculate the exact design rate and the left degree distribution $\lambda(\cdot)$. Finally, calculate the threshold of this ensemble on the BEC, and the resulting gap to capacity under iterative message-passing decoding.