4F5: Advanced Wireless Communications

Handout 5: Low-Density Parity-Check Codes

Jossy Sayir

Signal Processing and Communications Lab Department of Engineering University of Cambridge jossy.sayir@eng.cam.ac.uk

Lent 2012

Linear Block Codes

Definitions

- A binary code C of length n and dimension k is a set of different 2^k binary codewords of length n.
- The rate of the code is $R = \frac{1}{n} \log_2 |\mathcal{C}| = \frac{k}{n}$
- C is a vector subspace of the vector space defined by all possible binary vectors of length *n*, hence the code is linear
- C is the set of codewords **c** satisfying for all $\boldsymbol{b} \in \mathbb{F}_2^k$ (row convention)

 $\boldsymbol{c} = \boldsymbol{b}\boldsymbol{G}, \text{ where } \boldsymbol{G} = \begin{bmatrix} g_{1,1} & \cdots & g_{1,n} \\ g_{2,1} & \cdots & g_{2,n} \\ \vdots & \ddots & \vdots \\ g_{k,1} & \cdots & g_{k,n} \end{bmatrix}$ is the generator matrix

 $\bullet\,$ We can also express the code ${\mathcal C}$ as the set of codewords ${\boldsymbol c}$ such that

 $\boldsymbol{C}\boldsymbol{H}^{T} = \boldsymbol{0}, \text{ where } \boldsymbol{H} = \begin{bmatrix} h_{1,1} & \dots & h_{1,n} \\ h_{2,1} & \dots & h_{2,n} \\ \vdots & \ddots & \vdots \\ h_{n-k,1} & \dots & h_{n-k,n} \end{bmatrix} \text{ is the parity-check matrix}$

• H represents the linear system of equations that every codeword must satisfy

Decoding via the Parity-Check Matrix

	Γ0	1	0	0	0	0	0	0	0	0	0	1	1	0	0	1]
H =	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0
	0	0	1	0	1	0	0	0	1	0	0	0	0	1	0	0
	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0
	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0
	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0
	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0
	0	0	0	0	1	0	0	0	0	1	0	0	1	1	0	0
	[1	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0]
y = [0	ε	ε	ε	ε	1	0	0	0	1	ε	1	ε	ε	ε	1]

イロト イヨト イヨト イヨト

Decoding via the Parity-Check Matrix



— column permutation (2,3,4,5,11,13,14,15,1,6,7,8,9,10,12,16)

< 17 ▶

Permuted Columns (2,3,4,5,11,13,14,15,1,6,7,8,9,10,12,16)

	[1]	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1]
H ′ =	0	0	1	0	0	0	0	0	0	1	1	0	0	1	0	0
	0	1	0	1	0	0	1	0	0	0	0	0	1	0	0	0
	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0
	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	1
	1	0	0	0	1	0	0	1	0	0	1	0	0	0	0	0
	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0
	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0
	0	0	0	1	0	1	1	0	0	0	0	0	0	1	0	0
	6	0	1	0	1	0	0	0	1	0	0	1	0	0	0	0]
y ' =	[ε	ε	ε	ε	ε	ε	ε	ε	0	1	0	0	0	1	1	1]



• □ ▶ • □ ▶ • □ ▶









































< A



— Un-permute columns

< E

< 17 ▶

Permuted Columns (2,3,4,5,11,13,14,15,1,6,7,8,9,10,12,16)



→ Un-permute columns

Image: Image:

x = [0	0	1	0	1	1	0	0	0	1	0	1	0	0	0	1]
y = [0	ε	ε	ε	ε	1	0	0	0	1	ε	1	ε	ε	ε	1	1





































— resolve parity-check equations with 1 erasure

Comparison of Decoder 1 (triangulation) vs. Decoder 2 (resolve parity-check equations of H with 1 erasure)

- Both decoders operate by resolving parity-check equations with 1 erasure
- The second decoder uses only the (N K) parity-check equations in **H**
- The first decoder constructs additional parity-check equations from among the 2^{N-K} 1 non-trivial linear combinations of the parity-check equations of *H* specifically so that it can successively resolve all erasures
- The first decoder is an optimal ML decoder and is superior to the second decoder
- The second decoder has extremely low complexity but you have to be lucky for it to work.
- We will attempt to evaluate the probability of being lucky in terms of the properties of *H* and for a Binary Erasure Channel (BEC) with erasure probability δ.

Comparison of Decoder 1 (triangulation) vs. Decoder 2 (resolve parity-check equations of H with 1 erasure)

- Both decoders operate by resolving parity-check equations with 1 erasure
- The second decoder uses only the (N K) parity-check equations in **H**
- The first decoder constructs additional parity-check equations from among the 2^{N-K} 1 non-trivial linear combinations of the parity-check equations of *H* specifically so that it can successively resolve all erasures
- The first decoder is an optimal ML decoder and is superior to the second decoder
- The second decoder has extremely low complexity but you have to be lucky for it to work.
- We will attempt to evaluate the probability of being lucky in terms of the properties of *H* and for a Binary Erasure Channel (BEC) with erasure probability δ.

Comparison of Decoder 1 (triangulation) vs. Decoder 2 (resolve parity-check equations of H with 1 erasure)

- Both decoders operate by resolving parity-check equations with 1 erasure
- The second decoder uses only the (N K) parity-check equations in **H**
- The first decoder constructs additional parity-check equations from among the 2^{N-K} 1 non-trivial linear combinations of the parity-check equations of *H* specifically so that it can successively resolve all erasures
- The first decoder is an optimal ML decoder and is superior to the second decoder
- The second decoder has extremely low complexity but you have to be lucky for it to work.
- We will attempt to evaluate the probability of being lucky in terms of the properties of *H* and for a Binary Erasure Channel (BEC) with erasure probability δ.

Comparison of Decoder 1 (triangulation) vs. Decoder 2 (resolve parity-check equations of H with 1 erasure)

- Both decoders operate by resolving parity-check equations with 1 erasure
- The second decoder uses only the (N K) parity-check equations in **H**
- The first decoder constructs additional parity-check equations from among the 2^{N-K} 1 non-trivial linear combinations of the parity-check equations of *H* specifically so that it can successively resolve all erasures
- The first decoder is an optimal ML decoder and is superior to the second decoder
- The second decoder has extremely low complexity but you have to be lucky for it to work.
- We will attempt to evaluate the probability of being lucky in terms of the properties of *H* and for a Binary Erasure Channel (BEC) with erasure probability δ.

Comparison of Decoder 1 (triangulation) vs. Decoder 2 (resolve parity-check equations of H with 1 erasure)

- Both decoders operate by resolving parity-check equations with 1 erasure
- The second decoder uses only the (N K) parity-check equations in **H**
- The first decoder constructs additional parity-check equations from among the 2^{N-K} 1 non-trivial linear combinations of the parity-check equations of *H* specifically so that it can successively resolve all erasures
- The first decoder is an optimal ML decoder and is superior to the second decoder
- The second decoder has extremely low complexity but you have to be lucky for it to work.
- We will attempt to evaluate the probability of being lucky in terms of the properties of *H* and for a Binary Erasure Channel (BEC) with erasure probability δ.

・ロン ・回 と ・ 回 と

Comparison of Decoder 1 (triangulation) vs. Decoder 2 (resolve parity-check equations of H with 1 erasure)

- Both decoders operate by resolving parity-check equations with 1 erasure
- The second decoder uses only the (N K) parity-check equations in **H**
- The first decoder constructs additional parity-check equations from among the 2^{N-K} 1 non-trivial linear combinations of the parity-check equations of *H* specifically so that it can successively resolve all erasures
- The first decoder is an optimal ML decoder and is superior to the second decoder
- The second decoder has extremely low complexity but you have to be lucky for it to work.
- We will attempt to evaluate the probability of being lucky in terms of the properties of *H* and for a Binary Erasure Channel (BEC) with erasure probability δ .

・ロ・ ・ 日・ ・ ヨ・



Analysis of successful decoding

- X₂ can be resolved if Y₂ is not an erasure OR if Equations E₁ or E₆ can be resolved
- Supposing Y₂ is an erasure, Equation E₁ can be resolved if X₁₂ AND X₁₃ AND X₁₆ can be resolved
- Supposing Y_2 is an erasure, Equation E_6 can be resolved if X_7 AND X_{11} AND X_{15} can be resolved

 $Y_2 \rightarrow X_2$

• etc.



Analysis of successful decoding

- X_2 can be resolved if Y_2 is not an erasure OR if Equations E_1 or E_6 can be resolved
- Supposing Y_2 is an erasure, Equation
- Supposing Y_2 is an erasure, Equation





Analysis of successful decoding

- X_2 can be resolved if Y_2 is not an erasure OR if Equations E_1 or E_6 can be resolved
- Supposing Y_2 is an erasure, Equation E_1 can be resolved if X_{12} AND X_{13} AND X_{16} can be resolved
- Supposing Y_2 is an erasure, Equation





Analysis of successful decoding

- X_2 can be resolved if Y_2 is not an erasure OR if Equations E_1 or E_6 can be resolved
- Supposing Y_2 is an erasure, Equation E_1 can be resolved if X_{12} AND X_{13} AND X_{16} can be resolved
- Supposing Y_2 is an erasure, Equation E_6 can be resolved if X_7 AND X_{11} AND X_{15} can be resolved





Analysis of successful decoding

- X₂ can be resolved if Y₂ is not an erasure OR if Equations E₁ or E₆ can be resolved
- Supposing Y_2 is an erasure, Equation E_1 can be resolved if X_{12} AND X_{13} AND X_{16} can be resolved
- Supposing Y_2 is an erasure, Equation E_6 can be resolved if X_7 AND X_{11} AND X_{15} can be resolved



etc.



Analysis of successful decoding

- X₂ can be resolved if Y₂ is not an erasure OR if Equations E₁ or E₆ can be resolved
- Supposing Y_2 is an erasure, Equation E_1 can be resolved if X_{12} AND X_{13} AND X_{16} can be resolved
- Supposing Y_2 is an erasure, Equation E_6 can be resolved if X_7 AND X_{11} AND X_{15} can be resolved



etc.



Lent 2012 9 / 20



Lent 2012 9 / 20



Lent 2012 9 / 20



Binary Erasure Channel (BEC)



	F٥	1	0	0	0	0	0	0	0	0	0	1	1	0	0	17
H =	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0
	0	0	1	0	1	0	0	0	1	0	0	0	0	1	0	0
	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0
	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0
	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0
	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0
	0	0	0	0	1	0	0	0	0	1	0	0	1	1	0	0
	L1	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0

イロト イヨト イヨト イヨ

Linear Block Codes Definitions

• Hamming (7, 4) code of rate $R = \frac{4}{7}$, parity-check matrix given by

	[1	1	0	1	1	0	0]
H =	1	0	1	1	0	1	0
	0	1	1	1	0	0	1

• The parity-check matrix implies that all codewords satisfy $\boldsymbol{cH}^T = 0$

$$c_1 + c_2 + c_4 + c_5 = 0$$

$$c_1 + c_3 + c_4 + c_6 = 0$$

 $c_2 + c_3 + c_4 + c_7 = 0$

● Factor graph representation: bit nodes (), check nodes (), edges if there is a '1')



(I)

LDPC Basics

LDPC Basics

- A bit node has degree *d* if it is connected to *d* check nodes (influences *d* parity-check equations)
- A check node has degree *d* if it is connected to *d* bit nodes (the parity-check equation has *d* variables)
- Regular LDPC: all bit nodes have the same degree, all check nodes have the same degree
- Irregular LDPC: different bit (check) nodes can have different degrees
- The (7,4) Hamming code has 3 bit nodes of degree 1, 3 bit nodes of degree 2 and 1 bit node of degree 3. All 3 check nodes have degree 4.
- Typically degree distributions are represented by polynomials

$$\Lambda(x) = \sum_{i}^{d_{\text{max}}^{\ell}} \Lambda_{i} x^{i} = 3x + 3x^{2} + x^{3}, \quad P(x) = \sum_{i}^{d_{\text{max}}^{r}} P_{i} x^{i} = 3x^{4} \text{ (total number of nodes)}$$

$$L(x) = \sum_{i}^{d_{\text{max}}^{\ell}} L_{i} x^{i} = \frac{3}{7}x + \frac{3}{7}x^{2} + \frac{1}{7}x^{3}, \quad R(x) = \sum_{i}^{d_{\text{max}}^{r}} R_{i} x^{i} = \frac{3}{3}x^{4} \text{ (fraction of nodes)}$$

$$\lambda(x) = \sum_{i}^{d_{\text{max}}^{\ell}} \lambda_{i} x^{i-1} = \frac{3}{12} + \frac{6}{12}x + \frac{3}{12}x^{2}, \quad \rho(x) = \sum_{i}^{d_{\text{max}}^{r}} \rho_{i} x^{i-1} = \frac{12}{12}x^{3} \text{ (edge fraction)}$$

LDPC Basics

LDPC Basics

- Let *N_e* denote the number of edges in the graph (an edge corresponds to a '1' in the parity check matrix)
- Then, $\sum_{i} i\Lambda_i = \sum_{i} iP_i = N_e$, $\Lambda(1) = n$ and P(1) = n(1 R)
- Average degrees are $\bar{d}^{\ell} = L'(1) = \frac{1}{\int_0^1 \lambda(x) dx}$ and $\bar{d}^r = R'(1) = \frac{1}{\int_0^1 \rho(x) dx}$

• Hence
$$R = 1 - \frac{P(1)}{\Lambda(1)} = 1 - \frac{L'(1)}{R'(1)} = 1 - \frac{\overline{d}^{\ell}}{\overline{d}^{r}} = 1 - \frac{\int_{0}^{1} \rho(x) dx}{\int_{0}^{1} \lambda(x) dx} = 1 - \frac{3}{7} = \frac{4}{7}$$

Define LDPC(n, λ, ρ) as the ensemble of all possible LDPC codes of length n generated according to λ(x), ρ(x), i.e., the probability that a randomly selected edge is connected to a bit (check) node of degree i is λ_i (ρ_i)

• Regular LDPC, $\lambda(x)$, $\rho(x)$ monomials

LDPC Basics

Example

LDPC(10, x^2 , x^5) is also known as the (3, 6)-Gallager code of length 10. The rate is $R = 1 - \frac{3}{6} = \frac{1}{2}$ and a possible parity-check matrix is given below

$$\boldsymbol{H} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$



© Jossy Sayir (CUED)

Advanced Wireless Communications

Message Passing Algorithm

- Initialisation
 - Set all check-to-bit node messages $m^{c \rightarrow b} = ?$
- Bit-to-check node messages (1/2 iteration)
 - For all erased bit nodes $m^{b \rightarrow c} = \begin{cases} ? & \text{if all incoming messages are '?'} \\ m^{c \rightarrow b} & \text{if one or more incoming messages } \neq ? \end{cases}$

Oheck-to-bit node messages (1/2 iteration)

For all check nodes $m^{c \to b} = \begin{cases} ? & \text{if one or more incoming messages are } ? \\ \sum_{i} m_{i}^{b \to c} & \text{if all incoming messages } \neq ? \end{cases}$

Note that outgoing messages do not depend on the incoming message to that node



Error Probability Analysis

- It is not difficult to see that the error probability of the iterative decoder does not depend on the transmitted codeword, hence we assume the all-zero codeword
- We will analyse how the error probability of the iterative decoder evolves through the iterations
- Directed neighbourhood of an edge $e = b \rightarrow c$, of depth *d* denoted by $\mathcal{N}_e^{(d)}$ is the subgraph including all paths of length *d* starting from bit node b and not including the edge *e*
- $\mathcal{N}_{e}^{(d)}$ is a tree if all nodes are distinct: no cycles, closed paths



Error Probability Analysis

- Assume $\mathcal{N}_e^{(d)}$ cycle free ($n \to \infty$ case). Then input messages independent.
- A message sent by bit node b along edge e at iteration ℓ is a function of the messages propagated through N_e^(2ℓ)
- The error probability at iteration ℓ is given by

$$P_{b}^{(\ell)} = \sum_{\boldsymbol{y}} \Pr\left\{\mathsf{m}_{e}^{\mathsf{b} \to \mathsf{c}} = ? \mid \mathcal{N}_{e}^{(2\ell)} \mathsf{cycle free}, \mathsf{LDPC}(\lambda, \rho), \boldsymbol{y}\right\} \Pr\{\mathsf{LDPC}(\lambda, \rho)\} P_{\boldsymbol{y}}(\boldsymbol{y})$$

- Assume $P_b^{(\ell-1)}$ is known and $P_b^{(0)} = p$
 - ▶ $m^{c \rightarrow b} = ?$ for a degree-*j* check node if some of the *j* − 1 incoming $m^{b \rightarrow c} = ?$

$$q_j = \mathsf{Pr}\{\mathsf{m}^{\mathsf{c} o \mathsf{b}} = ? | \mathsf{check node of degree } j\} = 1 - \left(1 - \mathcal{P}_{b}^{(\ell-1)}\right)^{j-1}$$

Averaging over all possible check node degrees

$$q = \sum_{j} \rho_{j} q_{j} = 1 - \rho \left(1 - P_{b}^{(\ell-1)} \right)$$

 $m^{b \rightarrow c} = ?$ for a degree-*i* bit node if all *i* – 1 incoming messages are erasures

 $p_i = \Pr\{\mathsf{m}^{\mathsf{b}\to\mathsf{c}} = ?|\mathsf{bit} \text{ node of degree } i\} = p q^{i-1}$

Averaging over all possible bit node degrees

$$P_{b}^{(\ell)} = \sum_{i} \lambda_{i} p_{i} = p\lambda \left(1 - \rho \left(1 - P_{b}^{(\ell-1)} \right) \right)$$

• Remember $\lambda(x) = \sum_{i} \lambda_i x^{i-1}$, $\rho(x) = \sum_{j} \rho_j x^{j-1}$

Error Probability Analysis

- The figure below (left) shows the recursion $P_b^{(\ell)}$ vs. $P_b^{(\ell-1)}$ for LDPC(3,6). $P_b^{(0)} = p$ Threshold: $p^* = \sup \left\{ p \in [0, 1] : \lim_{\ell \to \infty} P_b^{(\ell)} = 0 \right\}$
- - for $p < p^*$ then $\lim_{\ell \to \infty} P_b^{(\ell)} = 0$ (single fixed point at zero)
 - for $p > p^*$ then $\lim_{\ell \to \infty} P_b^{(\ell)} > 0$ (multiple fixed point)
- LDPC codes (degree distributions) can be optimised such that the P_b recursion is closest to y = x



Message Passing and General Channels

Message Passing

- The iterative decoder for the BEC is an example of message passing decoders
- For other channels like AWGN, the decoder is different from the BEC one
- Since variables are binary, we can consider log-likelihood ratios

$$L_i^{ch} = \log rac{P_{Y|X}(y_i|+1)}{P_{Y|X}(y_i|-1)}$$

Bit-to-check node messages (1/2 iteration)

$$L_{e}^{b \to c} = L_{i}^{ch} + \sum_{e' \neq e} L_{e'}^{c \to b}$$

Check-to-bit node messages (1/2 iteration)

$$e^{\mathbf{L}_{e}^{\mathbf{D} \to \mathbf{b}}} = 2 \operatorname{tanh}^{-1} \left(\prod_{e' \neq e} \operatorname{tanh} \left(\frac{L_{e'}^{\mathbf{b} \to \mathbf{c}}}{2} \right) \right)$$

Similar decision $\hat{x}_i = \operatorname{sign} \left(L_i^{\operatorname{ch}} + \sum_e L_e^{\operatorname{c} \to \mathrm{b}} \right)$



Lent 2012 19 / 20

Message Passing and General Channels



© Jossy Sayir (CUED)

Lent 2012 20 / 20