Soft-Decision Decoding Algorithm for Low-density Parity-check Codes: Belief Propagation

NGUYEN Trong Cuong

Computer Communication Lab., The University of Aizu, Japan

January 31, 2023



SD Algorithm LDPC

I. Review of LDPC Codes

II. Decoding Algorithm: Belief Propagation

III. An Example of Belief Propagation Over BI-AWGN Channel

Cuong Nguyen (CCL, UoA)

SD Algorithm LDPC

January 31, 2023

イロト イポト イヨト イヨト

Linear Block Code

Linear block code C(N, K) is the set of 2^K vectors of length N

- Each vector in *C* is called a **codeword**
- Any linear combination of codewords is also a codeword
- Linear block codes can be <u>defined</u> through **generator matrix** *G* or **parity check matrix** *H*
- Generator matrix G is a $K \times N$ matrix used to encode a K-bits message vector **m** to a N-bits codeword $\mathbf{c} \in C$

$$\mathbf{c} = \mathbf{m}G = (m_1 \cdots m_K) \begin{pmatrix} g_{1,1} \cdots g_{1,N} \\ \vdots \\ g_{K,1} \cdots g_{K,N} \end{pmatrix}_{K \times N} = (c_1 \cdots c_N)$$

Parity Check Matrix

Parity check matrix *H* is a $(N - K) \times N$ matrix that satisfy

 $GH^T = \mathbf{0}$

Let M = N - K. A codeword $c \in C$ if and only if

$$H\mathbf{c}^{T} = \begin{pmatrix} z_{1,1} \cdots z_{1,N} \\ \vdots & \vdots \\ z_{M,1} \cdots & z_{M,N} \end{pmatrix}_{M \times N} \begin{pmatrix} c_{1} \\ \vdots \\ c_{N} \end{pmatrix} = \begin{pmatrix} \mathbf{z}_{1}\mathbf{c}^{T} \\ \vdots \\ \vdots \\ \mathbf{z}_{M}\mathbf{c}^{T} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

• The product $\mathbf{z}_i \mathbf{c}^T = 0$ is called a **check equation**

In other words, a codeword $c \in C$ if and only if it passes all check equations

Low-density Parity-check Codes

- Low-density parity check (LDPC) codes are <u>linear block codes</u> that have a very sparse parity check matrix
 - A matrix is said to be sparse if more than half of elements are zero
- The parity check matrix of LDPC can be graphically presented by a **Tanner graph**
 - Each variable node represents a bit in the codeword
 - Each check node represent a check equation
 - Each edge connects a variable node to a check node

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} \xrightarrow{z_1 \\ z_2 \\ z_3 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{bmatrix} \xrightarrow{z_2 \\ c_6 \\ c_6$$

Notations

Given a variable node c_n , let denote \mathcal{M}_n is the set of **checks node** connecting to c_n

$$\mathcal{M}_n = \{m : H_{mn} = 1\}$$

Given a check node z_m , let denote N_m is the set of **variable nodes** connecting to z_m

$$\mathcal{N}_m = \{n : H_{mn} = 1\}$$



I. Review of LDPC Codes

II. Decoding Algorithm: Belief Propagation

III. An Example of Belief Propagation Over BI-AWGN Channel

Cuong Nguyen (CCL, UoA)

SD Algorithm LDPC

イロト イヨト イヨト イヨト

э

Hard-decision & Soft-decision Decoder

- Hard-decision decoder operates on data that take on a *fixed set of possible values (commonly 0 and 1)*
- **Soft-decision decoder** takes on a *whole range of values in between*
 - Extra information provides the reliability of each input and thus help the decoder make the decision better



Belief Propagation

- Belief propagation is a soft-decision iterative decoding algorithm for linear block codes.
- The main idea of belief propagation is the **information update** between variable nodes and check nodes in each iteration
 - Each variable node sends a message to each connected check node
 - Each check node sends a message to each connected variable node
- The updated information are log-likelihood ratios (LLRs)



Log Likelihood Ratio

• Let \tilde{x} be the binary-valued random variable taking values on set $\{0, 1\}$. The log-likelihood ratio (LLR) of \tilde{x} is

$$L(\tilde{x}) = \ln \frac{P(\tilde{x}=1)}{P(\tilde{x}=0)}$$

|L (x̃) | measures the reliability of x̃
If P (x̃ = 0) → 0, |L (x̃) | → ∞
If P (x̃ = 0) = P (x̃ = 1) = 1/2, |L (x̃) | = 0



∃ ► < ∃ ►</p>

If $\tilde{x_1}$ and $\tilde{x_2}$ are statistically indepedent

$$L\left(\tilde{x_1} \oplus \tilde{x_2}\right) = \ln \frac{1 + e^{L(\tilde{x_1})} e^{L(\tilde{x_2})}}{e^{L(\tilde{x_1})} + e^{L(\tilde{x_2})}},$$

where \oplus is the addition operation in GF(2).

• Let define the operator \blacksquare as

$$L(\tilde{x_1}) \boxplus L(\tilde{x_2}) \stackrel{\Delta}{=} L(\tilde{x_1} \oplus \tilde{x_2})$$

A Posteriori Probability

- Target of the algorithm: Evaluate the probability of a bit c_n given the receiver vector **r** and the parity constraints in each iteration
- The probability is called a posterior probability (APP)

$$L_{\text{APP}}(n) = \ln \frac{P(c_n = 1 | \{z_m = 0 \text{ for all } m \in \mathcal{M}_n\}, \mathbf{r})}{P(c_n = 0 | \{z_m = 0 \text{ for all } m \in \mathcal{M}_n\}, \mathbf{r})}$$



Intrinsic

Applying Bayes' rule, the APP can be expressed as

$$L_{\text{APP}}(n) = \underbrace{\ln \frac{P(c_n = 1|r_n)}{P(c_n = 0|r_n)}}_{\text{intrinsic}} + \underbrace{\ln \frac{P(\{z_m = 0 \text{ for all } m \in \mathcal{M}_n\}|c_n = 1, \mathbf{r})}{P(\{z_m = 0 \text{ for all } m \in \mathcal{M}_n\}|c_n = 0, \mathbf{r})}_{\text{extrinsic}}$$

J

Intrinsic Term

• The intrinsic term represents the reliability of the received bit based on channel output

$$L_{\rm ch}(n) \stackrel{\Delta}{=} \ln \frac{P(c_n = 1 | r_n)}{P(c_n = 0 | r_n)}$$

- **The intrinsic term** depends on channel model
- E.g., binary-input additive white Gaussian noise (BI-AWGN) where the channel input belong to the set $\{-A, A\}$, the noise variance is σ^2

$$L_{\rm ch}(n) = \ln \frac{\exp\left[-\frac{1}{2\sigma^2}(r_n - A)^2\right]}{\exp\left[-\frac{1}{2\sigma^2}(r_n + A)^2\right]} = \frac{2r_n A}{\sigma^2}$$

Extrinsic Term (1)

• The extrinsic term represents the reliability of received bits given the observation of the code structure

$$L_{E_{\nu}}(m,n) \stackrel{\Delta}{=} \ln \frac{P(\{z_m = 0 \text{ for all } m \in \mathcal{M}_n\} | c_n = 1, \mathbf{r})}{P(\{z_m = 0 \text{ for all } m \in \mathcal{M}_n\} | c_n = 0, \mathbf{r})}$$

• Let denote $z_{m,n}$ as the computation of *m*-th parity check excluding bit c_n

$$z_{m,n} = \bigoplus_{j \in \mathcal{N}_m \setminus n} c_j$$

If c_n = 1, z_{m,n} = 1 for all check m ∈ M_n
 If c_n = 0, z_{m,n} = 0 for all check m ∈ M_n



Extrinsic Term (2)

The extrinsic term can be rewritten as

$$L_{E_{v}}(m,n) = \ln \frac{P\left(\{z_{m} = 0 \text{ for all } m \in \mathcal{M}_{n}\} | c_{n} = 1, \mathbf{r}\right)}{P\left(\{z_{m} = 0 \text{ for all } m \in \mathcal{M}_{n}\} | c_{n} = 0, \mathbf{r}\right)}$$
$$= \ln \frac{P\left(z_{m,n} = 1 \text{ for all } m \in \mathcal{M}_{n} | \mathbf{r}\right)}{P\left(z_{m,n} = 0 \text{ for all } m \in \mathcal{M}_{n} | \mathbf{r}\right)}$$
$$= \ln \frac{\prod_{m \in \mathcal{M}_{n}} P\left(z_{m,n} = 1 | \mathbf{r}\right)}{\prod_{m \in \mathcal{M}_{n}} P\left(z_{m,n} = 0 | \mathbf{r}\right)}$$
$$= \sum_{m \in \mathcal{M}_{n}} \ln \frac{P\left(z_{m,n} = 1 | \mathbf{r}\right)}{P\left(z_{m,n} = 0 | \mathbf{r}\right)}$$
$$= \left[\sum_{m \in \mathcal{M}_{n}} L\left(z_{m,n} | \mathbf{r}\right)\right]$$

The LLR terms are messages from check nodes to variable nodes

Cuong Nguyen (CCL, UoA)

SD Algorithm LDPC

January 31, 2023

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

э

15/36

A Posteriori Probability (cont.)

Let denote the message from *m*-th check node to *n*-th variable node as

$$L_{\mathbf{c}}(m,n) \stackrel{\Delta}{=} L\left(z_{m,n}|\mathbf{r}\right)$$

The APP of variable nodes is

$$L_{\text{APP}}(n) = L_{\text{ch}}(n) + \sum_{m \in \mathcal{M}_n} L_{\text{c}}(m, n).$$



• Next question: How to compute the LLR messages from check nodes to variable nodes?

Message From Check Node

The LLR message from *m*-th check node to *n*-th variable node is obtained from *all variable nodes* of the check node, excluding *n*-th variable node

$$L_{c}(m, n) = L(z_{m,n}|\mathbf{r})$$
$$= L\left(\bigoplus_{j \in \mathcal{N}_{m,n}} c_{j}|\mathbf{r}\right)$$
$$= \underbrace{[+]}_{j \in \mathcal{N}_{m} \setminus n} L(c_{j}|\mathbf{r})$$



■ The LLR terms are messages from variable nodes to check nodes

- The message from a variable node to a check node is computed by taking into account of other check nodes
- Let denote the message from *n*-th variable node to *m*-th check node as

$$L_{v}(m,n) \stackrel{\Delta}{=} L(c_{n}|\{z_{m'}=0 \text{ for all } m' \in \mathcal{M}_{n}\backslash m\}, \mathbf{r})$$

= $L_{ch}(n) + \sum_{m' \in \mathcal{M}_{n}\backslash m} L_{c}(m',n)$
$$L_{ch}(n)$$

$$z_{m'}, m' \in \mathcal{M}_n \setminus m$$

$$z_m$$

$$u_c(m, n)$$

$$L_{ch}(n)$$

18/36

Summary: Belief Propagation

Input: The # of iterations *L*, set $L_v(m, n) = L_{ch}(n)$ for all (m, n) with H(m, n) = 1, **decoding** = False

for each iteration do

end

for each (m, n) with H(m, n) = 1 do variable node update $L_{v}(m, n) = L_{ch}(n) + \sum_{i \in \mathcal{M}_{n,m}} L_{c}(i, n)$

end

for each n do

$$L_{\text{APP}}(n) = L_{\text{ch}}(n) + \sum_{i \in \mathcal{M}_n} L_{\text{c}}(i,n)$$

if $L_{\text{APP}}(n) < 0$ **then** set $\tilde{c_n} = 0$;
else set $\tilde{c_n} = 1$;

end

if
$$H\tilde{c}^T = \theta$$
 then set decoding = True and break;

end

I. Review of LDPC Codes

II. Decoding Algorithm: Belief Propagation

III. An Example of Belief Propagation Over BI-AWGN Channel

Cuong Nguyen (CCL, UoA)

SD Algorithm LDPC

January 31, 2023

イロト イロト イヨト イヨト

э

An Example



Consider a transmission model with signal amplitude A = 1, noise variance of AWGN channel $\sigma^2 = 1$

$$\mathbf{c} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \mathbf{t} = \begin{pmatrix} -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ \mathbf{r} = \begin{pmatrix} -0.63 & -0.83 & -0.73 & -0.04 & 0.1 & 0.95 & -0.76 & 0.66 & -0.55 & 0.58 \end{pmatrix}$$

$$\mathbf{\hat{c}} = \begin{pmatrix} 0 & 0 & 0 & \underline{0} & \underline{1} & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Initialization

January 31, 2023

(日)(四)(日)(日)(日)(日)

Initialization





Cuong Nguyen (CCL, UoA)

SD Algorithm LDPC

January 31, 2023

23/36



イロト イポト イヨト イヨト



イロト イポト イヨト イヨト



イロト イポト イヨト イヨト



イロト イポト イヨト イヨト

Check Node Update - Finish



< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >



January 31, 2023

イロト イポト イヨト イヨト



January 31, 2023

<ロト < 四ト < 三ト < 三ト



<ロト < 四ト < 三ト < 三ト



<ロト < 四ト < 三ト < 三ト

Variable Node Update - Finish



イロト イポト イヨト イヨト

Computing the APP



January 31, 2023

<ロト < 四ト < 三ト < 三ト

Computing the APP



January 31, 2023

イロト イロト イヨト イヨト

Parity Check

- The estimated codeword after the first iteration is
- $\tilde{\mathbf{c}} = \begin{pmatrix} 0 & 0 & 0 & 1 & \underline{1} & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$
- The estimated codeword is **failed** the parity check. The procedure is repeated in the next iteration

Iteration 2:

 $\tilde{\mathbf{c}} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ **Iteration 3:** $\tilde{\mathbf{c}} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

After two more iterations, the codeword is corrected