Belief-Propagation Decoding of LDPC Codes

Amir Bennatan,

Princeton University

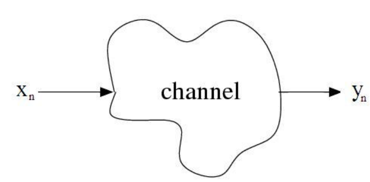
LDPC Codes: Motivation

- **Revolution in coding theory**
- **Reliable transmission, rates approaching capacity.**
  - BIAWGN, Rate = 0.5, Threshold 0.0045 dB of Shannon limit.
  - BIAWGN, Rate = 0.88, Threshold 0.088 dB of Shannon limit.
  - BSC, Rate = 0.5, Threshold 0.005 of maximum crossover.
  - BEC, any rate: achieve capacity!
- **Low-complexity decoding: belief propagation**

History

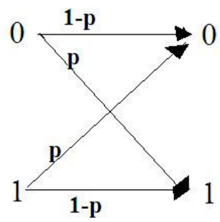
- 1963: **Invented** by Gallager
- 1988: **Belief-propagation**, by Pearl
- 1993: **Turbo-codes**, (Berrou, Glavieux, Thitimajshima)
- 1996: **Rediscovered** (MacKay, Neal, Sipser, Spielman)

Discrete-time, memoryless channel



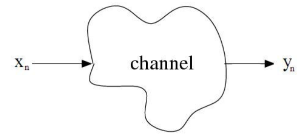
- Discrete time instances, $1, ..., N$.
- Output y_n dependent only on x_n.

Example: Binary Symmertic Channel (BSC)



(assume $p = 1/4$)

Decoding, no code case



- Assume $y_n = 1$.
- Which x_n was transmitted?

Maximum likelihood rule:

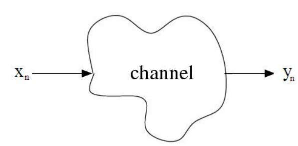
$$\begin{aligned} \Pr[X_n = \mathbf{1} \,|\, Y_n = 1] &= ? \qquad \text{(Assume } p = 1/4\text{)} \\ \Pr[X_n = \mathbf{0} \,|\, Y_n = 1] &= ? \end{aligned}$$

Decoding, no code case

$$\begin{aligned} \Pr[X_n = 1 \,|\, Y_n = 1] &= \\ &= \frac{\Pr[Y_n = 1, X_n = 1]}{\Pr[Y_n = 1]} \\ &= \frac{\Pr[Y_n = 1 \,|\, X_n = 1] \cdot \Pr[X_n = 1]}{\Pr[Y_n = 1]} \\ &= \frac{\Pr[Y_n = 1 \,|\, X_n = 1] \cdot \mathbf{1/2}}{\Pr[Y_n = 1]} \end{aligned}$$

Assumption: equal *a priori* **probabilities:**
$\Pr[X_n = 1] = \Pr[X_n = 0] = 1/2$

Decoding, no code case

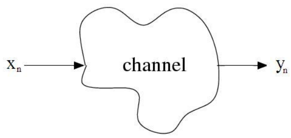


- Assume $y_n = 1$.
- Which x_n was transmitted?

$$\begin{aligned} \Pr[X_n = 1 \,|\, Y_n = 1] &= 0.75 \qquad \text{(Assume } p = 1/4\text{)} \\ \Pr[X_n = 0 \,|\, Y_n = 1] &= 0.25 \end{aligned}$$

Decoder decides: $\hat{x}_n = 1$

Decoding, no code case



Maximum likelihood rule:

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr[X_n = d \mid Y_n = y_n]$$

Decoding, code case

Example:

$$\mathcal{C} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\} \qquad \mathbf{y} = \begin{bmatrix} 0 \\ \mathbf{1} \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Let's focus on x_2.

- Which x_2 was transmitted?

Decoding, code case

Example:

$$\mathcal{C} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\} \qquad \mathbf{y} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{aligned} \Pr[X_2 = 1 \mid \mathbf{Y_2 = 1}] &= \mathbf{0.75} \\ \Pr[X_2 = 0 \mid \mathbf{Y_2 = 1}] &= \mathbf{0.25} \end{aligned}$$

Decoder decides: $\hat{x}_2 = 1$
Bad!!!!!

Decoding, code case

Old decoding rule,

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{\, X_n = d \mid Y_n = y_n \,\}$$

Better decoding rule,

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{\, X_n = d \mid Y_1 = y_1, ..., Y_N = y_N, \; [X_1, ..., X_N] \text{ is a codeword} \,\}$$

Decoding, code case

Example:

$$\mathcal{C} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\} \qquad \mathbf{y} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

- With **new** decoding rule,

$$\begin{aligned} \Pr[X_2 = 1 \mid \mathbf{Y} = \mathbf{y}, \mathbf{X} \text{ is a codeword}] &= \cancel{0.75}\ \mathbf{0.0357} \\ \Pr[X_2 = 0 \mid \mathbf{Y} = \mathbf{y}, \mathbf{X} \text{ is a codeword}] &= \cancel{0.25}\ \mathbf{0.9643} \end{aligned}$$

Decoder decides: $\cancel{\hat{x}_2 = 1}$ $\hat{x}_2 = 0$

Word error vs. bit error

- **Possibility 1:** Minimize probability of **word error**.

$$\Pr[\text{error}] \triangleq \Pr[\hat{\mathbf{x}} \neq \mathbf{x}]$$

- **Possibility 2:** At each bit n, minimize probability of **bit error**.

$$\Pr[\text{error in bit } n] \triangleq \Pr[\hat{x}_n \neq x_n]$$

Our focus: bit error

Decoding, code case

Old decoding rule,

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{\ X_n = d \quad | \quad Y_n = y_n\ \}$$

Better decoding rule,

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{\ X_n = d \quad | \quad Y_1 = y_1, ..., Y_N = y_N, \ [X_1, ..., X_N] \text{ is a codeword}\ \}$$

Complexity $\Theta(\mathbf{2^{RN}})$

($R > 0$ is rate of code)

Decoding, code case

Status:

- **Old decoding rule,**

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{X_n = d \mid Y_n = y_n\}$$

Bad performance, **excellent** complexity.

- **New decoding rule,**

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{X_n = d \mid \mathbf{Y} = \mathbf{y}, \mathbf{X} \text{ is a codeword}\}$$

Excellent performance, **terrible** complexity.

Any compromise?

Linear binary block codes

Parity check matrix. A binary matrix $\mathbf{H}$. e.g.

$$\mathbf{H} \cdot \mathbf{x} = \mathbf{0}$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 1 & 1 & \dots & 0 \\ & & & \dots & & & \\ 0 & 1 & 1 & 0 & 1 & \dots & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_N \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}$$

$$\mathbf{x} \text{ is a codeword} \iff \mathbf{H} \cdot \mathbf{x} = \mathbf{0}$$

Linear binary block codes

Parity check matrix. A binary matrix $\mathbf{H}$. e.g.

$$\mathbf{H} \cdot \mathbf{x} = \mathbf{0}$$

$$\begin{bmatrix} \longleftarrow \mathbf{h}_1 \longrightarrow \\ \longleftarrow \mathbf{h}_2 \longrightarrow \\ \dots \\ \longleftarrow \mathbf{h}_M \longrightarrow \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_N \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}$$

$$\begin{aligned} \mathbf{x} \text{ is a codeword} &\iff \mathbf{H} \cdot \mathbf{x} = \mathbf{0} \\ &\iff \mathbf{h}_m \cdot \mathbf{x} = 0, \quad m = 1, \dots, M \end{aligned}$$

Each equation $\mathbf{h_m} \cdot \mathbf{x} = 0$ called a **parity check**.

Linear binary block codes

$$\begin{aligned} \mathbf{X} \text{ is a codeword} &\iff \mathbf{H} \cdot \mathbf{X} = \mathbf{0} \\ &\iff \mathbf{h}_m \cdot \mathbf{X} = 0, \quad m = 1, \dots, M \end{aligned}$$

$$\begin{aligned} \hat{x}_n &= \operatorname*{argmax}_{d=0,1} \Pr\{X_n = d \,|\, \mathbf{Y} = \mathbf{y},\ \mathbf{X} \text{ is a codeword}\} \\ &= \operatorname*{argmax}_{d=0,1} \Pr\{X_n = d \,|\, \mathbf{Y} = \mathbf{y},\ \mathbf{H} \cdot \mathbf{X} = \mathbf{0}\} \\ &= \operatorname*{argmax}_{d=0,1} \Pr\{X_n = d \,|\, Y_1 = y_1, Y_2 = y_2, \dots, Y_N = y_N \\ &\qquad\qquad \mathbf{h}_1\mathbf{X} = 0, \mathbf{h}_2\mathbf{X} = 0, \dots, \mathbf{h}_M\mathbf{X} = 0\} \end{aligned}$$

Decoding, code case

- **Old decoding rule,**

$$\hat{x}_n = \operatorname*{argmax}_{d=0,1} \Pr\{X_n = d \,|\, Y_n = y_n\}$$

- **New decoding rule,**

$$\begin{aligned} \hat{x}_n = \operatorname*{argmax}_{d=0,1} \Pr\{X_n = d \,|\, & Y_1 = y_1, Y_2 = y_2, \dots, Y_N = y_N \\ & \mathbf{h}_1\mathbf{X} = 0, \mathbf{h}_2\mathbf{X} = 0, \dots, \mathbf{h}_M\mathbf{X} = 0\} \end{aligned}$$

- **Compromise: Use some $\{y_n\}$, some parity checks!**

$$\begin{aligned} \hat{x}_n = \operatorname*{argmax}_{d=0,1} \Pr\{X_n = d \,|\, & Y_{\mathrm{l_1}} = y_{\mathrm{l_1}}, \dots, Y_{\mathrm{l_L}} = y_{\mathrm{l_L}} \\ & \mathbf{h}_{\mathrm{m_1}}\mathbf{X} = 0, \dots, \mathbf{h}_{\mathrm{m_K}}\mathbf{X} = 0\} \end{aligned}$$

Compromise: Iterative Decoding

1. **Start with old decoding rule,**

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{X_n = d \mid Y_n = y_n\}$$

2. **Iteratively add more h's and y's,**

$$\hat{x}_n = \underset{d=0,1}{\operatorname{argmax}} \Pr\{X_n = d \mid Y_{l_1} = y_{l_1}, ..., Y_{l_L} = y_{l_L}$$
$$\mathbf{h}_{m_1}\mathbf{X} = 0, ..., \mathbf{h}_{m_K}\mathbf{X} = 0\}$$

How? Belief propagation

Some formal stuff...

- Let $\mathbf{w} = [w_1, ..., w_N]$, assume $\mathbf{w} \notin \mathcal{C}$,

$$\Pr[\mathbf{X} = \mathbf{w}] = 0?$$

- Answer:

$$\Pr[\mathbf{X} = \mathbf{w}] = \left(\frac{1}{2}\right)^N$$

$$\Pr[\mathbf{X} = \mathbf{w} \mid \mathbf{X} \text{ is a codeword}] = 0$$

Formal probability model

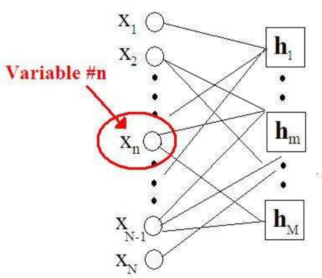
Properties of formal probability model

1. Assumes no code
2. Valid mathematically
3. Non-restrictive
4. We can express other useful values.

Concepts of belief-propagation

1. **Graph based**
2. Beliefs
3. Iterative message passing
4. Extrinsic information rule
5. Ignore loops

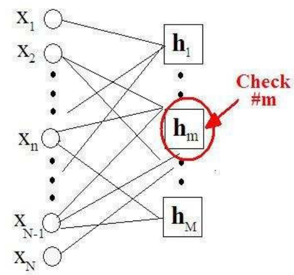
Graph based



Variable node $\#n$, corresponds to time slot

- to unknown code bit X_n.
- to received channel output y_n.

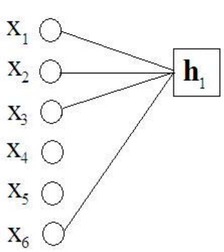
Graph based



Check node $\#m$, corresponds:

- to parity-check $\mathbf{h}_m$.

Parity check



$$\mathbf{h}_1 \cdot \mathbf{X} = X_1 + X_2 + X_3 + X_6 = 0$$

Check node connected to **participating variables**.

Concepts of belief-propagation

1. Graph based
2. **Beliefs**
3. Iterative message passing
4. Extrinsic information rule
5. Ignore loops

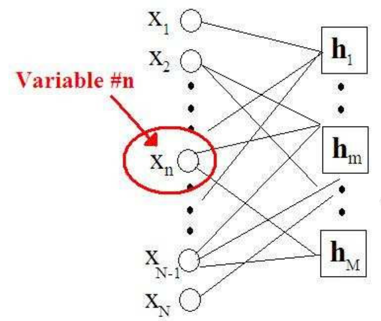
Belief Propagation

- The knowledge ("beliefs") we have:

$$Y_1 = y_1, Y_2 = y_2, ..., Y_N = y_N$$
$$\mathbf{h}_1\mathbf{X} = 0, \mathbf{h}_2\mathbf{X} = 0, ..., \mathbf{h}_M\mathbf{X} = 0$$

- Divide it between the nodes.

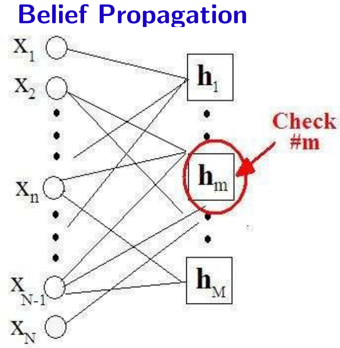
Belief Propagation



Variable nodes know channel outputs.

- Variable n knows value of y_n.

Belief Propagation



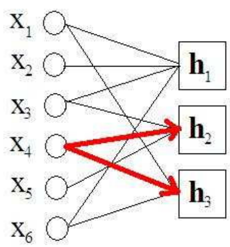
Check nodes known parity checks.

- Check m knows that $\mathbf{h}_m\mathbf{X} = 0$.

Concepts of belief-propagation

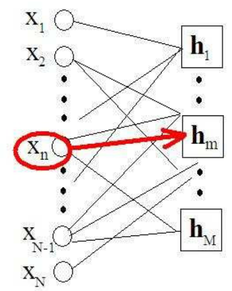
1. Graph based
2. Beliefs
3. **Iterative message passing**
4. Extrinsic information rule
5. Ignore loops

Iterative message passing



- Nodes communicate using messages.
- Messages are sent through edges to neighboring nodes.
- Each message is a number $m \in [0, 1]$.

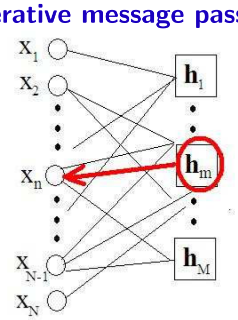
Iterative message passing



- Message from variable n to check m:

$$V_{n\to m} = \Pr[\mathbf{X_n} = \mathbf{1} \mid \text{some } h\text{'s and some } y\text{'s}]$$

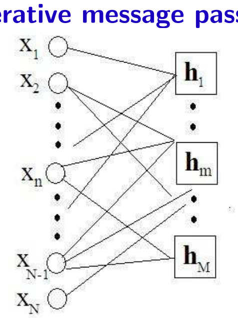
Iterative message passing



- Message from check m to check n:

$$C_{m\to n} = \Pr[\mathbf{X_n} = \mathbf{1} \mid \text{other } h\text{'s and other } y\text{'s}]$$

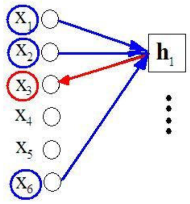
Iterative message passing



Rightbound and leftbound iterations.

- **Rightbound iteration.** Variables send messages to checks.
- **Leftbound iteration.** Checks send messages to variables.

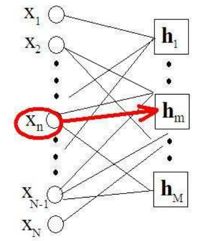
Iterative message passing



At node n,

1. Collect all incoming messages, **previous iteration**
2. Add "**my knowledge**"
3. Compute new (better?) message

Iterative message passing

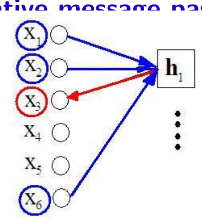


Rightbound iteration #1: At variable n,

1. Collect all incoming messages, previous iteration (none)
2. Add "my knowledge" (channel output y_n)
3. Compute new (better?) message

$$V_{n\to m} = \Pr[X_n = 1 \mid Y_n = y_n]$$

Iterative message passing

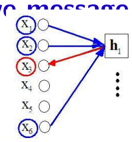


Leftbound iteration #1: At check node 1, to variable 3

1. Collect all incoming messages $(V_{1\to 1}, V_{2\to 1}, V_{3\to 1}, V_{6\to 1})$
2. Add "my knowledge" (parity check $X_1 + X_2 + X_3 + X_6 = 0$)
3. Compute new (better?) message

$$C_{1\to 3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, \\ Y_1 = y_1, Y_2 = y_2, \cancel{Y_3 = y_3}, Y_6 = y_6]$$

Iterative message passing



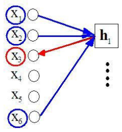
Leftbound iteration #1: At check node 1, to variable 3

1. Collect all incoming messages $(V_{1\to 1}, V_{2\to 1}, V_{3\to 1}, V_{6\to 1})$
2. Add "my knowledge" (parity check $X_1 + X_2 + X_3 + X_6 = 0$)
3. Compute new (better?) message

$$C_{1\to 3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, \\ Y_1 = y_1, Y_2 = y_2, \cancel{Y_3 = y_3}, Y_6 = y_6]$$

Extrinsic information rule:
Message to node never function of message from node.

Iterative message passing



Leftbound iteration #1: At check node 1, to variable 3

1. Collect all incoming messages $(V_{1\to 1}, V_{2\to 1}, V_{6\to 1})$
2. Add "my knowledge" (parity check $X_1 + X_2 + X_3 + X_6 = 0$)
3. Compute new (better?) message

$$C_{1\to 3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, \\ Y_1 = y_1, Y_2 = y_2, Y_6 = y_6] = ?$$

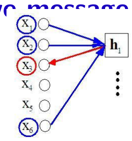
Some formal stuff...

$$\Pr[X_1 = 0, X_2 = 1] = \Pr[X_1 = 0] \cdot \Pr[X_2 = 1]$$

$$\Pr[X_1 = 0, Y_2 = 1, X_2 = 1] = \Pr[X_1 = 0] \cdot \Pr[Y_2 = 1, X_2 = 1]$$

$$\Pr[X_1 + X_3 = 0, Y_3 = 1, X_2 + X_4 = 0, Y_4 = 1] = \\ \Pr[X_1 + X_3 = 0, Y_3 = 1] \cdot \Pr[X_2 + X_4 = 0, Y_4 = 1]$$

Iterative message passing

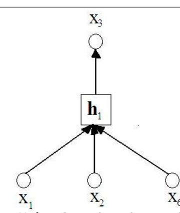


Leftbound iteration #1: At check node 1, to variable 3

1. Collect all incoming messages $(V_{1\to 1}, V_{2\to 1}, V_{6\to 1})$
2. Add "my knowledge" (parity check $X_1 + X_2 + X_3 + X_6 = 0$)
3. Compute new (better?) message

$$C_{1\to 3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, \\ Y_1 = y_1, Y_2 = y_2, Y_6 = y_6]$$

$$= \frac{1}{2} \cdot \left[1 - \prod_{i=1,2,6} (1 - 2V_{i\to 1}) \right]$$



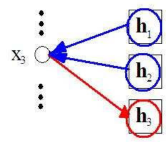
Leftbound iteration #1: At check node 1, to variable 3

1. Collect all incoming messages $(V_{1\to 1}, V_{2\to 1}, V_{3\to 1}, V_{6\to 1})$
2. Add "my knowledge" (parity check $X_1 + X_2 + X_3 + X_6 = 0$)
3. Compute new (better?) message

$$C_{1\to 3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, \\ Y_1 = y_1, Y_2 = y_2, Y_6 = y_6]$$

$$= \frac{1}{2} \cdot \left[1 - \prod_{i=1,2,6} (1 - 2V_{i\to 1}) \right]$$

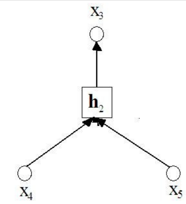
Iterative message passing



Rightbound iteration #2: From variable 3, to check node 3

1. Collect all incoming messages $(C_{1\to3}, C_{2\to3})$
2. Add "my knowledge" (channel output y_3)
3. Compute new (better?) message

$$V_{3\to3} = \Pr[\mathbf{X_3 = 1} \mid \text{some knowledge}]$$

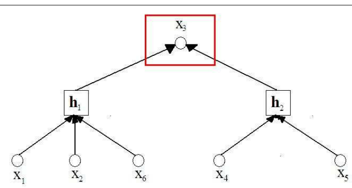


Leftbound iteration #1: At check node 1, to variable 3

1. Collect all incoming messages $(V_{4\to2}, V_{3\to2}, V_{5\to2})$
2. Add "my knowledge" (parity check $X_3 + X_4 + X_5 = 0$)
3. Compute new (better?) message

$$\mathbf{C_{2\to3}} = \Pr[X_3 = 1 \mid X_3 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_6]$$

$$= \frac{1}{2} \cdot \left[1 - \prod_{i=4,5} (1 - 2V_{i\to2})\right]$$



$$C_{1\to3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6]$$
$$C_{2\to3} = \Pr[X_3 = 1 \mid X_3 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5]$$

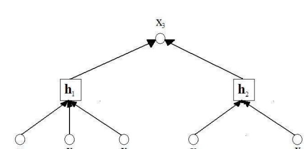
Therefore,

$$V_{3\to3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, X_3 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5, Y_3 = y_3]$$

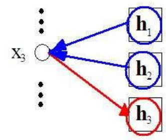
Notation:

$$V_{3\to3} = \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, X_3 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5, Y_3 = y_3]$$

$$V_{3\to3} = \Pr[X_3 = 1 \mid \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3]$$



Iterative message passing



Rightbound iteration #2: From variable 3, to check node 3

1. Collect all incoming messages $(C_{1\to 3}, C_{2\to 3})$
2. Add "my knowledge" (channel output y_3)
3. Compute new (better?) message

$$V_{3\to 3} = \Pr[X_3 = 1 \mid \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3]$$

$$\Pr[X_3 = 1 \mid \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3] =$$
$$= \frac{\Pr[X_3 = 1, \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3]}{\Pr[\mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3]}$$

$$\begin{aligned}
&\Pr[X_3 = 1, \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3] = \\
&\quad = \Pr[X_3 = 1, Y_3 = y_3, \\
&\qquad X_1 + X_2 + X_3 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, \\
&\qquad X_3 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5] \\
&\quad = \Pr[X_3 = 1, Y_3 = y_3, \\
&\qquad X_1 + X_2 + 1 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, \\
&\qquad 1 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5] \\
&\quad = ?
\end{aligned}$$

$$\begin{aligned}
&\Pr[X_3 = 1, \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3] = \\
&\quad = \Pr[X_3 = 1, Y_3 = y_3, \\
&\qquad X_1 + X_2 + X_3 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, \\
&\qquad X_3 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5] \\
&\quad = \Pr[X_3 = 1, Y_3 = y_3, \\
&\qquad X_1 + X_2 + 1 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, \\
&\qquad 1 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5] \\
&\quad = \Pr[X_3 = 1, Y_3 = y_3] \times \\
&\qquad \times \Pr[X_1 + X_2 + 1 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6] \\
&\qquad \times \Pr[1 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5]
\end{aligned}$$

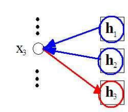
$$\Pr[X_3 = 1, \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,] =$$
$$= \Pr[X_3 = 1, Y_3 = y_3] \times$$
$$\times \Pr[X_1 + X_2 + 1 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6]$$
$$\times \Pr[1 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5\,]$$
$$\ldots$$
$$= \Pr[X_3 = 1 \mid Y_3 = y_3] \times$$
$$\times \Pr[X_3 = 1 \mid X_1 + X_2 + X_3 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6]$$
$$\times \Pr[X_3 = 1 \mid X_3 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5\,]$$
$$\times \mathrm{fun}(y_1, y_2, y_6, y_4, y_5)$$

$$\Pr[X_3 = 1, \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,] =$$
$$= \Pr[X_3 = 1, Y_3 = y_3] \times$$
$$\times \Pr[X_1 + X_2 + 1 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6]$$
$$\times \Pr[1 + X_4 + X_5 = 0, Y_4 = y_4, Y_5 = y_5\,]$$
$$\ldots$$
$$= P_3 \times$$
$$\times C_{1\to 3}$$
$$\times C_{2\to 3}$$
$$\times \mathrm{fun}(y_1, y_2, y_6, y_4, y_5)$$

$$\boxed{P_3 \triangleq \Pr[X_3 = 1 \mid Y_3 = y_3]}$$

$$\Pr[X_3 = 1 \mid \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,] =$$
$$= \frac{\Pr[X_3 = 1, \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,]}{\Pr[\mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,]}$$
$$= \frac{P_3 \cdot C_{1\to 3} \cdot C_{2\to 3} \cdot \mathrm{fun}(y_1, y_2, y_6, y_4, y_5)}{\Pr[\mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,]}$$
$$\ldots$$
$$= \frac{P_3 \cdot \prod_{i=1,2} C_{i\to 3}}{P_3 \cdot \prod_{i=1,2} C_{i\to 3} + (1 - P_3) \cdot \prod_{i=1,2}(1 - C_{i\to 3})}$$

Iterative message passing

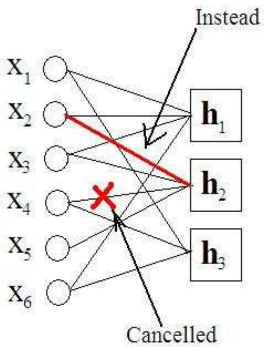


Rightbound iteration #2: From variable 3, to check 3

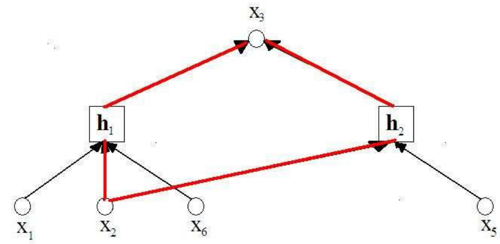
1. Collect all incoming messages ($C_{1\to 3}, C_{2\to 3}$)
2. Add "my knowledge" (channel output y_3)
3. Compute new (better?) message

$$V_{3\to 3} = \frac{P_3 \cdot \prod_{i=1,2} C_{i\to 3}}{P_3 \cdot \prod_{i=1,2} C_{i\to 3} + (1 - P_3) \cdot \prod_{i=1,2}(1 - C_{i\to 3})}$$

Let's change the problem...



Information flow graph,



A loop!

$$
\begin{aligned}
&\Pr[X_3 = 1, \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,] = \\
&\quad = \Pr[X_3 = 1, Y_3 = y_3, \\
&\qquad X_1 + X_2 + X_3 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, \\
&\qquad X_3 + X_2 + X_5 = 0, Y_2 = y_2, Y_5 = y_5\,] \\
&\quad = \Pr[X_3 = 1, Y_3 = y_3, \\
&\qquad X_1 + X_2 + 1 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6, \\
&\qquad 1 + X_2 + X_5 = 0, Y_2 = y_2, Y_5 = y_5\,] \\
&\quad \neq \Pr[X_3 = 1, Y_3 = y_3] \times \\
&\qquad \times \Pr[X_1 + X_2 + 1 + X_6 = 0, Y_1 = y_1, Y_2 = y_2, Y_6 = y_6] \\
&\qquad \times \Pr[1 + X_2 + X_5 = 0, Y_2 = y_2, Y_5 = y_5\,]
\end{aligned}
$$

$$
\Pr[X_3 = 1 \mid \mathbf{h}_1\mathbf{X} = 0, \mathbf{Y}_1 = \mathbf{y}_1, \mathbf{h}_2\mathbf{X} = 0, \mathbf{Y}_2 = \mathbf{y}_2, Y_3 = y_3\,]
$$

$$
\neq \frac{P_3 \cdot \prod_{i=1,2} C_{i\to 3}}{P_3 \cdot \prod_{i=1,2} C_{i\to 3} + (1 - P_3) \cdot \prod_{i=1,2}(1 - C_{i\to 3})}
$$

What to do?

Iterative message passing

Rightbound iteration #2: From variable 3, to check 3

1. Collect all incoming messages $(C_{1\to 3}, C_{2\to 3})$
2. Add "my knowledge" (channel output y_3)
3. Compute new (better?) message

$$V_{3\to 3} = \frac{P_3 \cdot \prod_{i=1,2} C_{i\to 3}}{P_3 \cdot \prod_{i=1,2} C_{i\to 3} + (1-P_3)\cdot \prod_{i=1,2}(1-C_{i\to 3})}$$

Ignore loop: Compute $V_{3\to 3}$ as if no loop!

Ignoring loops

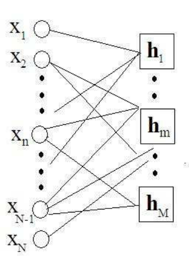
Why is ignoring loops okay?

- Number of loops small.
- Simulation results okay even when some loops.

- **Low-density** parity checks: $d << N$,

$$\begin{aligned} d &\triangleq \text{average check degree} \\ N &\triangleq \text{block length} \end{aligned}$$

- Graph randomly generated.



Belief Propagation Algorithm

Rightbound iteration $\#t$: At variable node n,

$$V_{n\to m} = \frac{P_n \cdot \prod_{i\in\mathcal{A}(n)\setminus\{m\}} C_{i\to n}}{P_n \cdot \prod_{i\in\mathcal{A}(n)\setminus\{m\}} C_{i\to n} + (1-P_n)\cdot \prod_{i\in\mathcal{A}(n)\setminus\{m\}}(1-C_{i\to n})}$$

Leftbound iteration $\#t$: At check node m,

$$C_{m\to n} = \frac{1}{2}\cdot\left[1 - \prod_{i\in\mathcal{A}(m)\setminus\{n\}}(1-2V_{i\to m})\right]$$

where $\mathcal{A}(n)$, $\mathcal{A}(m)$ are the sets of adjacent nodes to n and m.