Sílvio A. Abrantes
DEEC/FEUP
2006

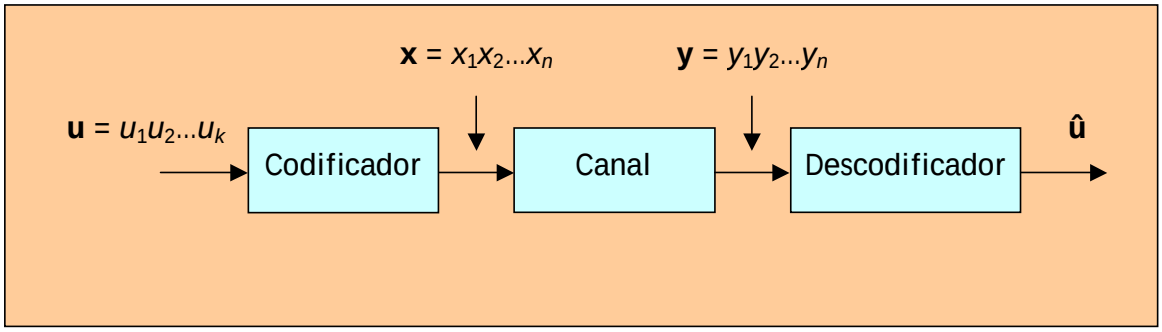
Descodificação iterativa

2

Descodificação de códigos LDPC por transferência de mensagens em grafos de Tanner

Introdução

Diagrama de blocos de um sistema genérico de codificação e descodificação:



Exemplo de matriz H de um código LDPC regular:

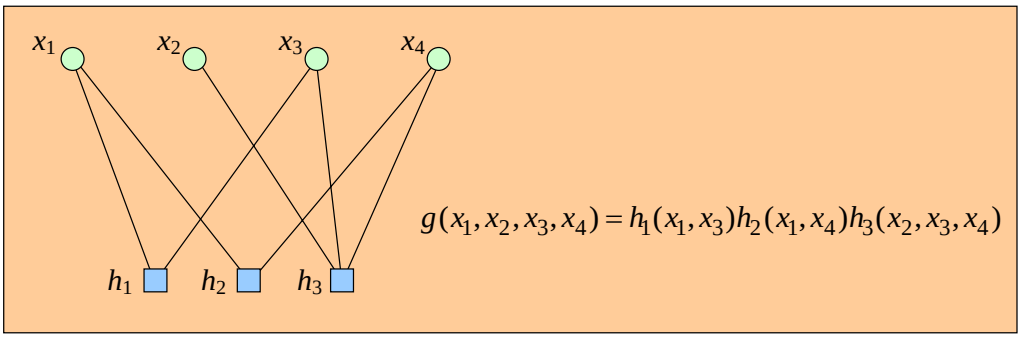
$$\mathbf{H} = \begin{bmatrix} 0&0&1&0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&1&0 \\ 0&1&0&0&1&0&1&0&0&1&0&0&1&0&0&0&0&1&0&0 \\ 1&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&1&1&0 \\ 0&1&0&0&0&0&0&1&0&0&1&1&0&0&0&1&0&0&0&1 \\ 1&0&0&1&0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0 \\ 0&0&1&1&0&0&1&0&1&0&0&0&1&0&0&0&0&0&0&1 \\ 0&0&0&0&1&1&0&1&0&1&0&1&0&0&1&0&0&0&0&0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

Seis bits "1" por linha

Três bits "1" por coluna

Código LDPC (3, 6)

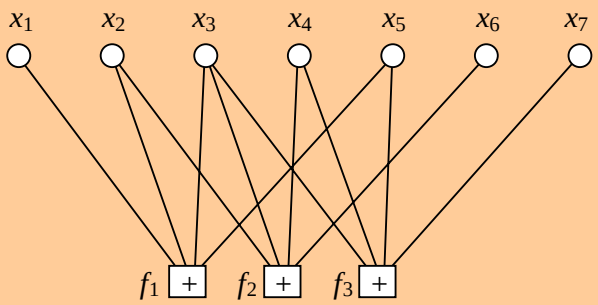
Um grafo de factores:



Introdução aos grafos de factores

Código de Hamming (7,4)

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



Equações de paridade:

$$x_1 \oplus x_2 \oplus x_3 \oplus x_5 = 0$$
$$x_2 \oplus x_3 \oplus x_4 \oplus x_6 = 0$$
$$x_3 \oplus x_4 \oplus x_5 \oplus x_7 = 0$$

Grafo de factores e funções identificadoras de pertença binárias:

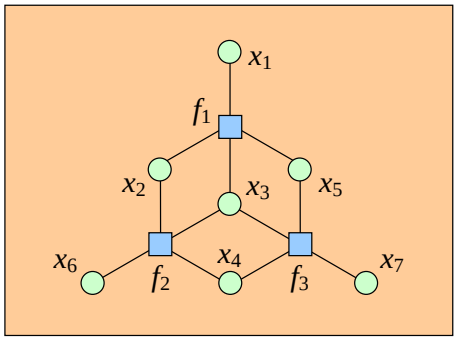
$$f_1(x_1, x_2, x_3, x_5) = \delta(x_1 \oplus x_2 \oplus x_3 \oplus x_5) = \begin{cases} 1 & x_1 \oplus x_2 \oplus x_3 \oplus x_5 = 0 \\ 0 & x_1 \oplus x_2 \oplus x_3 \oplus x_5 \neq 0 \end{cases}$$

$$f_2(x_2, x_3, x_4, x_6) = \delta(x_2 \oplus x_3 \oplus x_4 \oplus x_6)$$

$$f_3(x_3, x_4, x_5, x_7) = \delta(x_3 \oplus x_4 \oplus x_5 \oplus x_7)$$

em que $\delta(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}$ (delta de Kronecker)

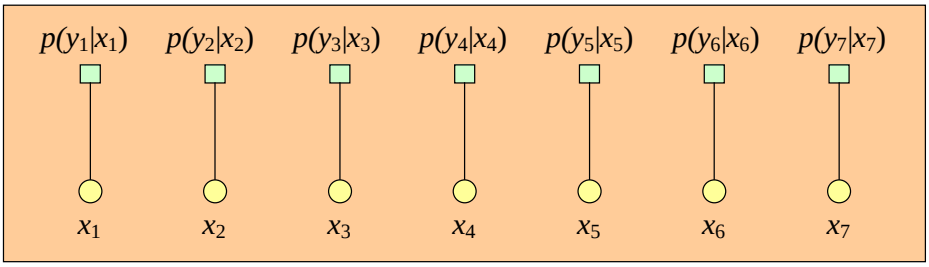
Grafo de Tanner desenhado como um grafo de factores:



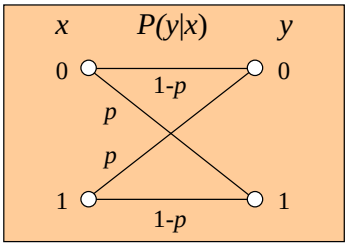
Grafos de factores de canais sem memória (BSC e AWGN)

Num canal sem memória as n transmissões de símbolos são independentes $\Rightarrow$ probabilidade condicional conjunta a priori $p(\mathbf{y}|\mathbf{x})$ é igual ao produto das probabilidades condicionais individuais $p(y_i|x_i)$:

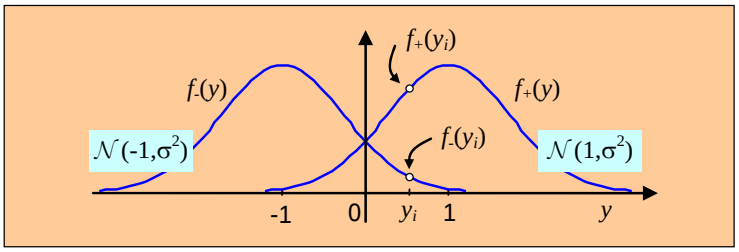
$$p(\mathbf{y}\,|\,\mathbf{x}) = p(y_1, y_2, \ldots, y_n \,|\, x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} p(y_i \,|\, x_i)$$



Canal BSC:



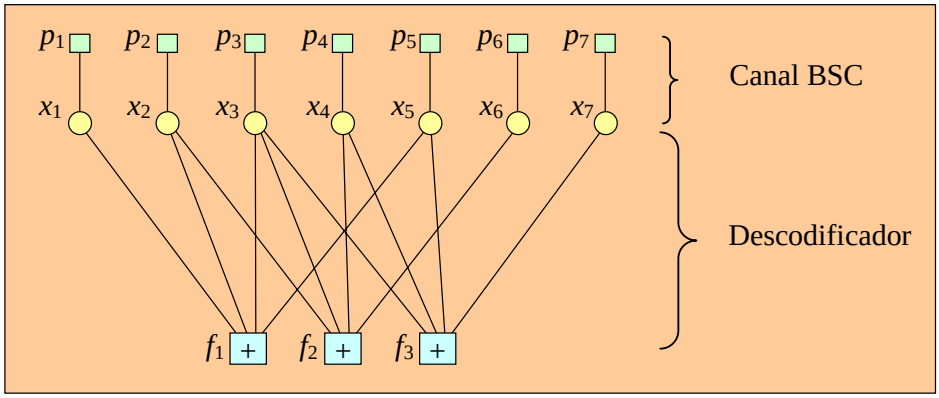
Canal AWGN:



$$p(y_i|x_i=-1) = \frac{f_-(y_i)}{f_-(y_i)+f_+(y_i)} = \frac{1}{1+\exp\left(2y_i/\sigma^2\right)}$$

$$p(y_i|x_i=+1) = \frac{f_+(y_i)}{f_-(y_i)+f_+(y_i)} = \frac{1}{1+\exp\left(-2y_i/\sigma^2\right)}$$

Grafo de factores de um canal em série com um descodificador de canal binário



$$p(y_i \mid x_i = 1) = p_i$$

- variável x_i **q**uestiona f_j sobre as "opiniões" que os outros x_i têm dela e f_j **r**esponde-lhe com as "opiniões" que conhece:

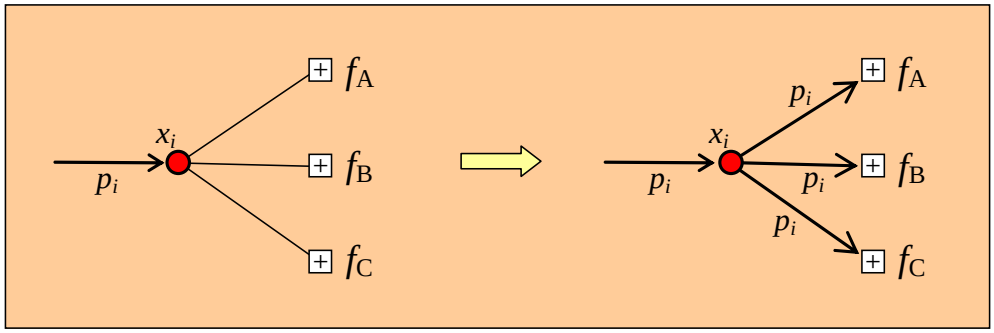
  $q_{ij} = p(x_i = 1 \mid \sim\{f_j\}, \mathbf{y})$ – mensagem do nó de variável x_i para o nó de paridade f_j

  - é a probabilidade de x_i ter um certo valor, dado o valor observado dessa variável (a quantidade $p(y_i|x_i)$) e dados os valores que recebeu dos outros nós de paridade

  $r_{ji} = p(x_i = 1, f_j(\,) = 1 \mid \mathbf{y})$ – mensagem do nó de paridade f_j para o nó de variável x_i

  - é a probabilidade de x_i ter um certo valor e a equação de paridade f_j ser satisfeita, dado que se recebeu **y**

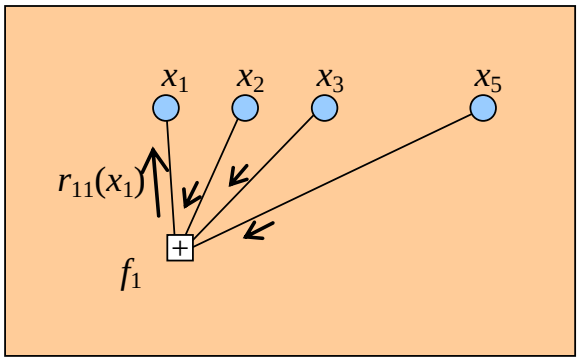
Início da difusão de mensagens dos nós de variáveis para os nós de paridade:



Transferência de mensagens entre nós de grafos bipartidos

Significado das mensagens

Exemplo com a mensagem r_{11}



$$r_{11} = r_{11}(1) = p(x_1 = 1,\, f_1(x_1, x_2, x_3, x_5) = 1 \,|\, \mathbf{y})$$

Mas $\quad f_1(x_1, x_2, x_3, x_5) = 1 \quad \Rightarrow \quad x_1 \oplus x_2 \oplus x_3 \oplus x_5 = 0$

$$\Downarrow$$

$$r_{11} = p(x_1 = 1, x_1 \oplus x_2 \oplus x_3 \oplus x_5 = 0 \,|\, \mathbf{y}) =$$
$$= p(x_2 \oplus x_3 \oplus x_5 = 1 \,|\, \mathbf{y})$$

A soma dos três bits x_2, x_3 e x_5 é igual a 1 em quatro situações mutuamente exclusivas:

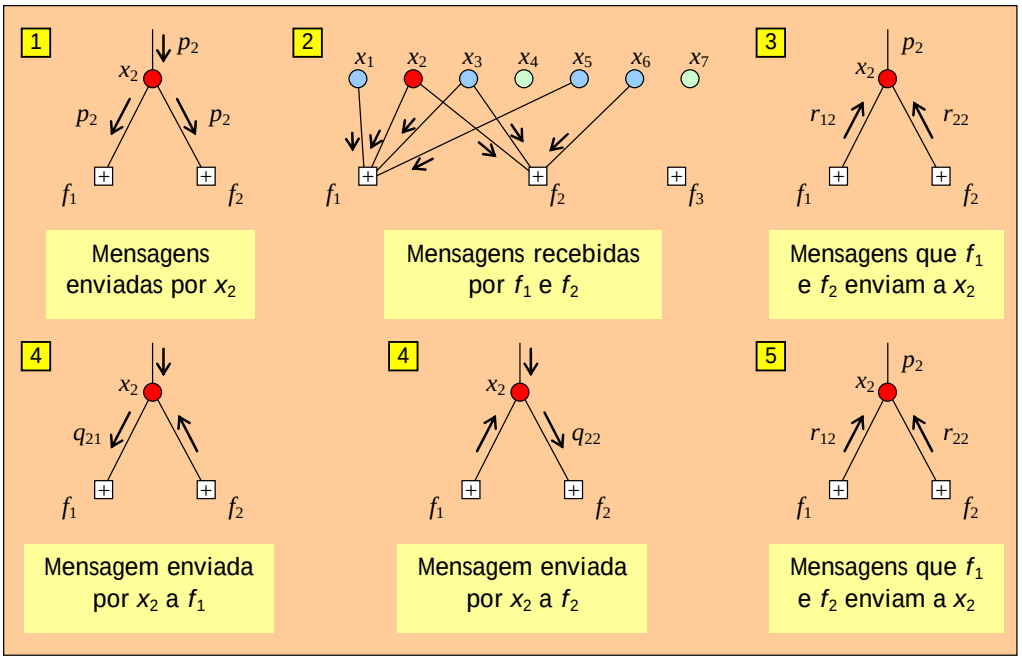
Soma igual a 1
$x_2 = 0,\ x_3 = 0,\ x_5 = 1$
$x_2 = 0,\ x_3 = 1,\ x_5 = 0$
$x_2 = 1,\ x_3 = 0,\ x_5 = 0$
$x_2 = 1,\ x_3 = 1,\ x_5 = 1$

$$\Downarrow$$

$$r_{11} = p(x_2 = 0, x_3 = 0, x_5 = 1 \,|\, \mathbf{y}) + p(x_2 = 0, x_3 = 1, x_5 = 0 \,|\, \mathbf{y}) +$$
$$+ p(x_2 = 1, x_3 = 0, x_5 = 0 \,|\, \mathbf{y}) + p(x_2 = 1, x_3 = 1, x_5 = 1 \,|\, \mathbf{y})$$

Transferência de mensagens entre nós de grafos

Exemplo de transferência de mensagens entre nós de grafos bipartidos



1. No início a variável x_2 espalha pelos nós de paridade f_1 e f_2 a mensagem a priori (isto é, a estimativa de probabilidade) que recebeu do canal, p_2.

2. Mas o nó f_1 também recebeu estimativas de x_1, x_3 e x_5 e o nó f_2 também recebeu estimativas de x_3 e x_6.

3. Cada um dos nós f_1 e f_2 processa as mensagens que **não** vieram de x_2 e envia a esta o resultado (r_{12} e r_{22}, respectivamente).

4. O processo agora repete-se com as mensagens a circular das variáveis para os nós de paridade e destes para as variáveis: por exemplo e voltando à variável x_2, esta envia a f_1 uma mensagem q_{21} baseada no que **os outros** nós de paridade, p_2 e f_2, lhe enviaram[1], e envia a f_2 uma outra mensagem, q_{22}, esta baseada no que recebeu de p_2 e f_1.

5. Os nós f_1 e f_2 enviam a x_2 novas mensagens mais refinadas.

[1] Note-se que cada nó de paridade do canal envia a x_i sempre a mesma mensagem p_i em todas as iterações.

Regras de actualização de mensagens probabilísticas com o algoritmo da soma-e-produto

Regras de actualização de mensagens com variáveis binárias

- **Do nó de variável x_i para o nó de paridade f_j:**

$$q_{ij} = K_{ij}\, p_i \prod_{j' \neq j} r_{j'i} \quad (\text{com } K_{ij} = \frac{1}{p_i \prod_{j' \neq j} r_{j'i} + (1-p_i) \prod_{j' \neq j} (1-r_{j'i})})$$

- **Do nó de paridade f_j para o nó de variável binária x_i:**

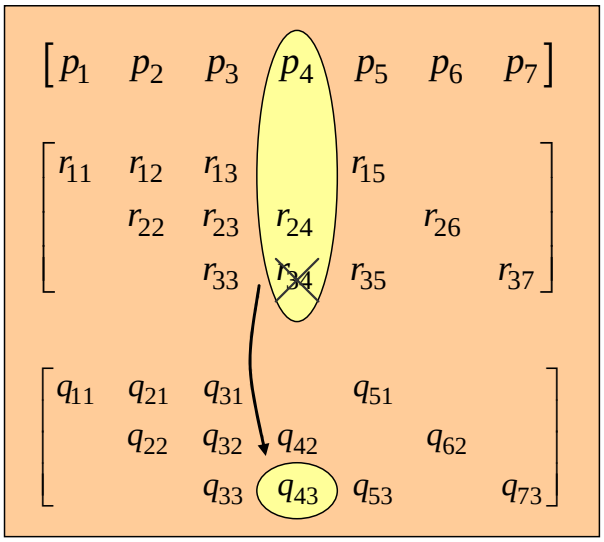
$$1 - 2r_{ji} = \prod_{i' \neq i} (1 - 2q_{i'j}) \quad \text{ou} \quad r_{ji} = \frac{1}{2}\left[1 - \prod_{i' \neq i} (1 - 2q_{i'j})\right]$$

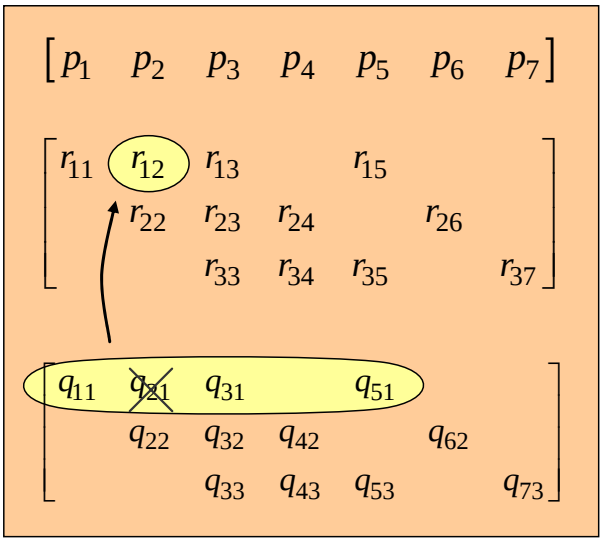
K_{ij} – factor de normalização

No fim das iterações: $p(x_i \mid \mathbf{y}) = q_i = K_{ij}\, p_i \prod_{j'} r_{j'i}$ (limiar de decisão: 0,5)

(produto de todas as mensagens confluentes na variável x_i)

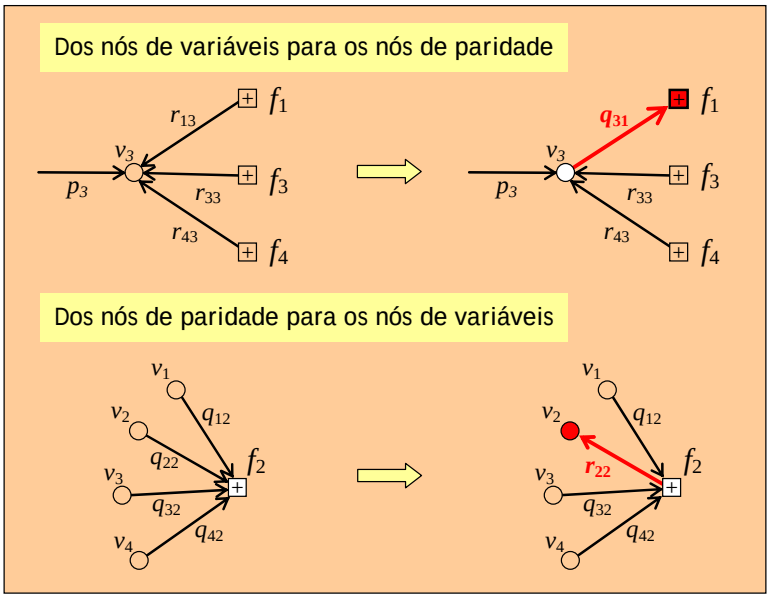
Indicação das mensagens envolvidas nos cálculos através da adaptação da matriz H (exemplo do código de Hamming (7,4)):





Regras de actualização de mensagens probabilísticas: um exemplo

Como calcular as mensagens enviadas pelos nós da figura?



Mensagens que o nó de variável v_3 envia aos nós de paridade:

$$q_{31} = K_{31} p_3 r_{33} r_{43} \qquad (\text{sendo } K_{31} = \frac{1}{p_3 r_{33} r_{43} + (1-p_3)(1-r_{33})(1-r_{43})}).$$

$$q_{33} = \frac{p_3 r_{13} r_{43}}{p_3 r_{13} r_{43} + (1-p_3)(1-r_{13})(1-r_{43})}$$

$$q_{34} = \frac{p_3 r_{13} r_{33}}{p_3 r_{13} r_{33} + (1-p_3)(1-r_{13})(1-r_{33})}$$

Mensagens que o nó de paridade f_2 envia aos nós de variáveis:

$$1-2r_{22} = (1-2q_{12})(1-2q_{32})(1-2q_{42}),$$

$$1-2r_{21} = (1-2q_{22})(1-2q_{32})(1-2q_{42})$$

$$1-2r_{23} = (1-2q_{12})(1-2q_{22})(1-2q_{42})$$

$$1-2r_{24} = (1-2q_{12})(1-2q_{22})(1-2q_{32})$$

Expressão alternativa (exemplo para r_{22}):

$$r_{22} = q_{12}(1-q_{32})(1-q_{42}) + q_{32}(1-q_{12})(1-q_{42}) + q_{42}(1-q_{12})(1-q_{32}) + q_{12}q_{32}q_{42}$$

Por que é que é necessário um factor de normalização?

- Sem normalização as estimativas de probabilidades que as variáveis enviariam aos nós de paridade seriam sempre inferiores às estimativas que deles tinham recebido dado estas serem sempre inferiores a um.

  Por exemplo, se uma variável de grau 4 recebesse os valores 0,6, 0,9 e 0,8 de três nós de paridade a estimativa que iria enviar para o quarto nó seria, sem normalização, igual ao produto $0,6 \times 0,9 \times 0,8 = 0,432$.

- Suponhamos um caso simples de uma variável x_1 de grau 3 que recebe as mensagens r_{11} e r_{21} e vai disso informar o nó de paridade 3 enviando-lhe a mensagem

$$q_{13} = K_{13} r_{11} r_{21}$$

Ora deverá também ser

$$1 - q_{13} = K_{13}(1 - r_{11})(1 - r_{21}).$$

Combinando as duas expressões concluímos que o factor de normalização a usar é

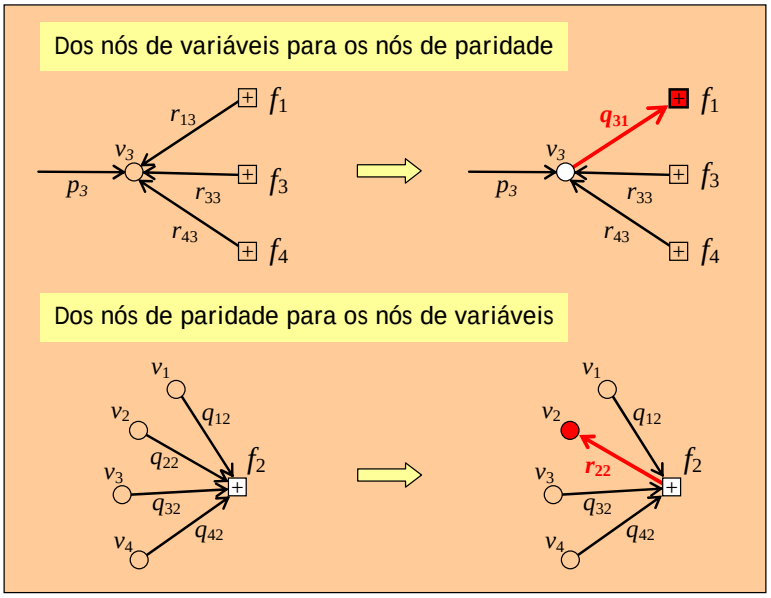
$$K_{13} = \frac{1}{r_{11} r_{21} + (1 - r_{11})(1 - r_{21})}$$

Ou seja, no exemplo inicial a mensagem normalizada vale:

$$\frac{0,6 \times 0,9 \times 0,8}{0,6 \times 0,9 \times 0,8 + 0,4 \times 0,1 \times 0,2} = 0,98$$

o que é bem mais razoável que o valor não normalizado 0,432.

Simplificação: o algoritmo “max product”



Vimos atrás que r_{22}, por exemplo, era calculado assim:

$$1-2r_{22}=(1-2q_{12})(1-2q_{32})(1-2q_{42})$$

ou

$$r_{22}=q_{12}(1-q_{32})(1-q_{42})+q_{32}(1-q_{12})(1-q_{42})+q_{42}(1-q_{12})(1-q_{32})+q_{12}q_{32}q_{42}$$

No algoritmo “max-product”, em vez desta soma toma-se apenas a **maior parcela**:

$$r_{22}\approx\max(q_{12}(1-q_{32})(1-q_{42}),q_{32}(1-q_{12})(1-q_{42}),q_{42}(1-q_{12})(1-q_{32}),q_{12}q_{32}q_{42})$$

Ou seja:

- A regra de actualização das mensagens de variáveis é a mesma que antes (um produto).
- As mensagens dos nós de paridade são calculadas através de uma aproximação (um valor máximo).

Regras de actualização de mensagens logarítmicas

Em vez de probabilidades vamos fazer circular logaritmos de razões de probabilidades ("log-likelihood ratios", LLR):

$$\ln \frac{p(y_i \mid x_i = 1)}{p(y_i \mid x_i = 0)} = \ln \frac{p_i}{1 - p_i} = L(p_i)$$ (em canais binários simétricos)

$$L(r_{ij}) = \ln \frac{r_{ij}(1)}{r_{ij}(0)} = \ln \frac{r_{ij}}{1 - r_{ij}}$$

$$L(q_{ij}) = \ln \frac{q_{ij}(1)}{q_{ij}(0)} = \ln \frac{q_{ij}}{1 - q_{ij}}$$

Actualização de mensagens LLR

- **Do nó de variável x_i para o nó de paridade f_j:**

$$L(q_{ij}) = L(p_i) + \sum_{j' \neq j} L(r_{j'i})$$

- **Do nó de paridade f_j para o nó de variável x_i:**

$$L(r_{ji}) = 2 \tanh^{-1}\left[-\prod_{i' \neq i} \tanh\left(-L(q_{i'j})/2\right) \right] =$$

$$= \Phi^{-1}\left[\prod_{i' \neq i} \Phi\left(L(q_{i'j})\right) \right]$$

No fim das iterações: $L(x_i \mid \mathbf{y}) = L(q_i) = L(p_i) + \sum_j L(r_{ji})$ (limiar de decisão: 0)

Notas:

1. $\tanh(x) = \dfrac{e^x - e^{-x}}{e^x + e^{-x}}$ $\quad \tanh(x/2) = \dfrac{e^x - 1}{e^x + 1}$ $\quad \tanh^{-1}(x) = \dfrac{1}{2} \ln \dfrac{1 + x}{1 - x}$

2. $\Phi(x) = \tanh\left(-x/2\right)$

3. Expressão alternativa equivalente: $\Phi\left(L(r_{ji})\right) = \prod_{i' \neq i} \Phi\left(L(q_{i'j})\right)$

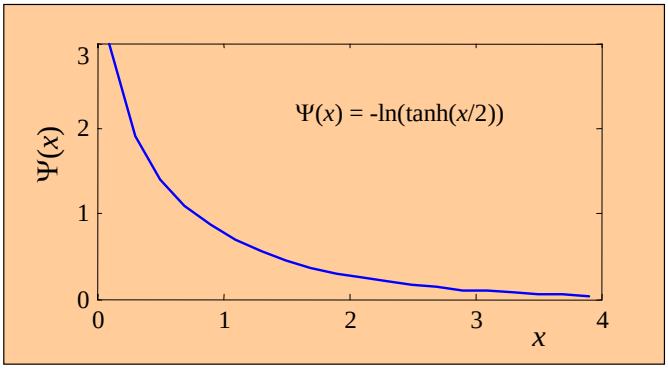
Simplificação: o algoritmo “min-sum”

- As razões LLR são usadas para simplificar cálculos, nomeadamente para substituir multiplicações por somas. Ora, se bem que tenhamos substituído multiplicações por adições no cálculo das mensagens de variáveis, as multiplicações subsistem no cálculo das mensagens dos nós de paridade.

- Depois de várias manipulações matemáticas (tendo em conta que $y = \mathrm{sgn}(y)\,|\,y\,|$) a expressão de $L(r_{ji})$ pode escrever-se assim:

$$L(r_{ji}) = (-1)^{d_j} \left(\prod_{i' \neq i} \mathrm{sgn}\left[L(q_{i'j}) \right] \right) \Psi\left(\sum_{i' \neq i} \Psi\left(\left| L(q_{i'j}) \right| \right) \right) \qquad (d_j - \text{grau do nó})$$

em que $\Psi(x) = -\ln\left[\tanh\left(x/2 \right) \right]$, $x > 0$, é uma função auxiliar:



- Como a função Ψ é positiva e fortemente decrescente o somatório das funções Ψ é aproximadamente igual ao termo dominante, correspondente ao menor dos $|L(q_{ji})|$ envolvidos. Além disso, a função Ψ é igual à sua inversa, $\Psi^{-1}(x) = \Psi(x)$, isto é, $\Psi(\Psi(x)) = x$. Logo, a expressão anterior simplifica-se em

$$L(r_{ji}) \approx (-1)^{d_j} \left(\prod_{i' \neq i} \mathrm{sgn}\left[L(q_{i'j}) \right] \right) \Psi\left(\max_{i' \neq i} \left(\Psi\left(\left| L(q_{i'j}) \right| \right) \right) \right) =$$

$$= (-1)^{d_j} \left(\prod_{i' \neq i} \mathrm{sgn}\left[L(q_{i'j}) \right] \right) \min_{i' \neq i} \left(\left| L(q_{i'j}) \right| \right)$$

Simplificação: o algoritmo “min-sum”

Algoritmo “min-sum”

- **Do nó de variável x_i para o nó de paridade f_j:**

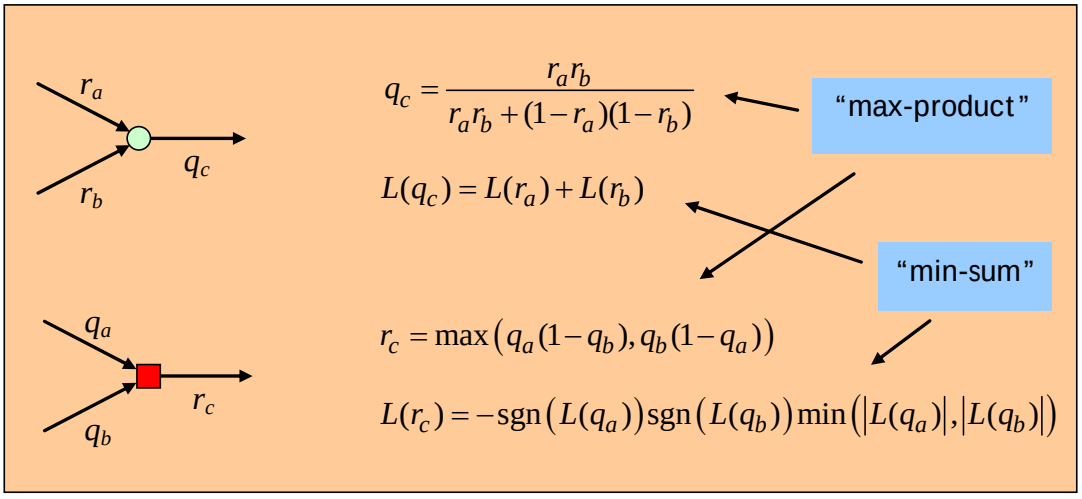
$$L(q_{ij}) = L(p_i) + \sum_{j' \neq j} L(r_{j'i})$$

- **Do nó de paridade f_j para o nó de variável x_i:**

$$L(r_{ji}) = (-1)^{d_j} \left(\prod_{i' \neq i} \operatorname{sgn}\left[L(q_{i'j}) \right] \right) \min_{i' \neq i} \left(\left| L(q_{i'j}) \right| \right)$$

- Quer este algoritmo quer o algoritmo “max-product” só diferem do algoritmo da soma-e-produto “normal” no modo de cálculo, aproximado, das mensagens dos nós de paridade. As mensagens dos nós de variáveis, essas, são calculadas da maneira “normal”.

- Expressões de actualização de nós com os algoritmos simplificados “max-product” (com probabilidades) e “min-sum” (com LLRs) no caso de nós de grau 3:



Actualização de mensagens com canais AWGN

Todas as regras de actualização apresentadas atrás, válidas para canais binários simétricos, podem ser aplicadas a canais com ruído branco aditivo gaussiano (AWGN): basta usar a adequada informação proveniente do canal.

Se se enviar uma sequência binária $x_i = \pm 1$ através de um canal AWGN com ruído de média nula e variância σ^2 e se se receber a sequência de valores reais y_i, a LLR a priori, isto é, aquilo de que necessitamos para iniciar os cálculos, vale

$$L(p_i) = \ln \frac{p(y_i \mid x_i = +1)}{p(y_i \mid x_i = -1)} =$$

$$= \ln \frac{\left(1/\sqrt{2\pi\sigma^2}\right) \exp\left[-(y_i - 1)^2 / 2\sigma^2\right]}{\left(1/\sqrt{2\pi\sigma^2}\right) \exp\left[-(y_i + 1)^2 / 2\sigma^2\right]} =$$

$$= \frac{2y_i}{\sigma^2}$$

O ruído à saída de um filtro adaptado no receptor tem variância $\sigma^2 = \frac{N_0}{2E_c}$, em que $N_0/2$ é a densidade espectral de potência do ruído e $E_c = R_c E_b$ é a energia de cada bit codificado (sendo E_b a energia de cada bit antes da codificação e $R_c = k/n$ a taxa do código). Portanto,

$$L(p_i) = 4\frac{E_c}{N_0} y_i = 4\frac{R_c E_b}{N_0} y_i$$

Agora é só usar este valor nas equações de actualização.

Exemplo numérico de aplicação

- **Código: Hamming (7,4) apresentado antes**
- **Canal: BSC, com probabilidade de erro p = 0,1**
- **Palavra de código transmitida: x = 1 1 0 0 0 1 0**
- **Sequência recebida: y = 1 1 0 1 0 1 0 (4º bit está errado)**

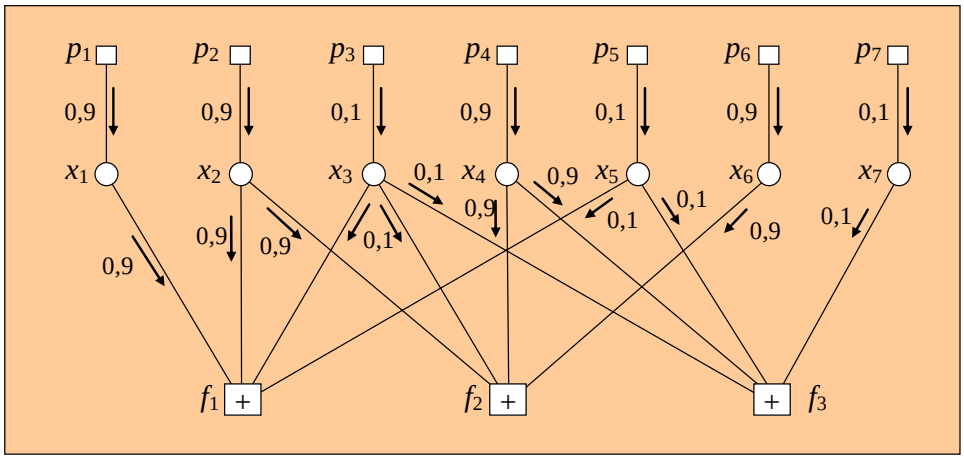
- Só precisamos das probabilidades a priori p_i: $p(y_i \mid x_i = 1) = p_i$

  (exemplos: $p(y_1 = 1 \mid x_1 = 1) = 0{,}9$ e $p(y_3 = 0 \mid x_3 = 1) = 0{,}1$)

- Cada variável x_i difunde a mensagem que recebeu do canal pelos nós de paridade aos quais está ligada. Assim, por exemplo,

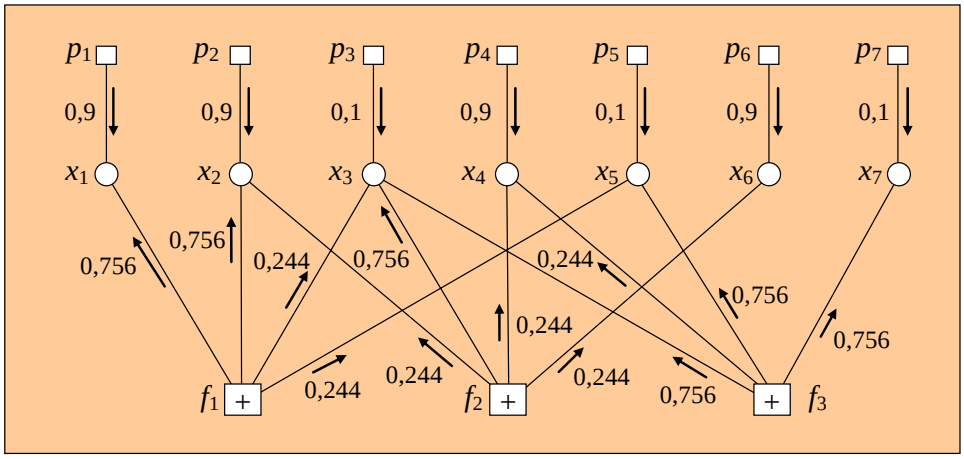
$$q_{21} = q_{22} = p_2 = 0{,}9 \qquad q_{51} = q_{53} = p_5 = 0{,}1$$

Mensagens iniciais enviadas pelas variáveis aos nós de paridade f_j:



Exemplo numérico de aplicação (cont.)

Primeiras mensagens enviadas pelos nós de paridade aos nós de variáveis:

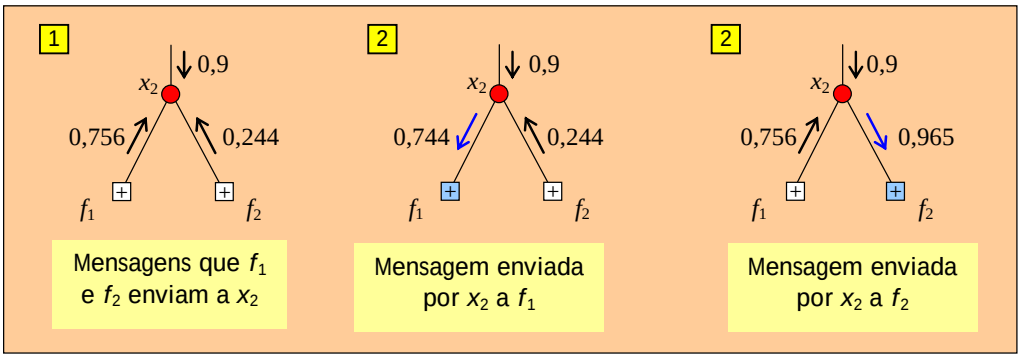


Exemplo de cálculo:

$$r_{11} = \frac{1}{2}\left[1 - \prod_{i\in\{2,3,5\}} (1-2q_{i1})\right] = \frac{1}{2}\left[1-(1-2q_{21})(1-2q_{31})(1-2q_{51})\right] =$$

$$= 0,756$$

Início da 2ª iteração: novas mensagens enviadas por x_2 aos nós de paridade f_1 e f_2



Exemplo de cálculo:

$$q_{21} = K_{21} p_2 r_{22} = \frac{p_2 r_{22}}{p_2 r_{22} + (1-p_2)(1-r_{22})} = \frac{0,9 \times 0,244}{0,2952} = 0,744$$

$$q_{22} = K_{22} p_2 r_{12} = \frac{p_2 r_{12}}{p_2 r_{12} + (1-p_2)(1-r_{12})} = \frac{0,680}{0,705} = 0,965$$

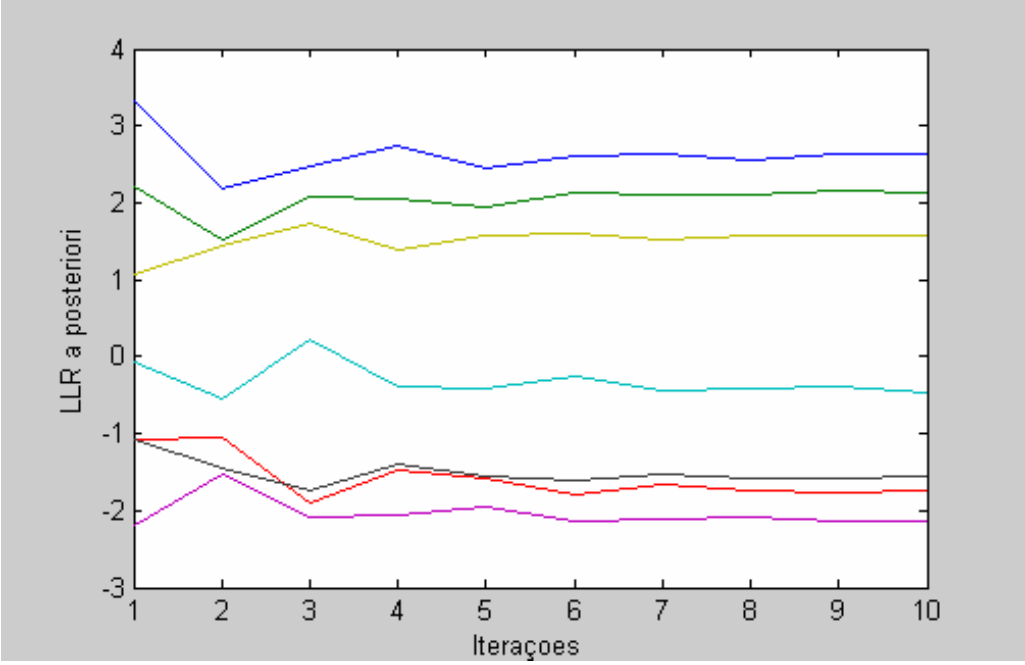
Exemplo numérico de aplicação (cont.)

- No fim do vai-e-vem de transferências a estimativa da probabilidade que cada nó de variável produz é igual ao produto normalizado de todas as estimativas que a ele confluem, incluindo a proveniente do canal.

LLR a posteriori durante cinco iterações:

Iteração nº	$L(x_1\|\mathbf{y})$	$L(x_2\|\mathbf{y})$	$L(x_3\|\mathbf{y})$	$L(x_4\|\mathbf{y})$	$L(x_5\|\mathbf{y})$	$L(x_6\|\mathbf{y})$	$L(x_7\|\mathbf{y})$
1	3,33	2,20	-1,07	-0,06	-2,20	1,07	-1,07
2	2,18	1,53	-1,06	-0,55	-1,53	1,44	-1,44
3	2,47	2,08	-1,89	0,21	-2,08	1,74	-1,74
4	2,73	2,06	-1,48	-0,39	-2,06	1,39	-1,39
5	2,44	1,95	-1,59	-0,42	-1,95	1,57	-1,57

LLR a posteriori ao longo de 10 iterações:



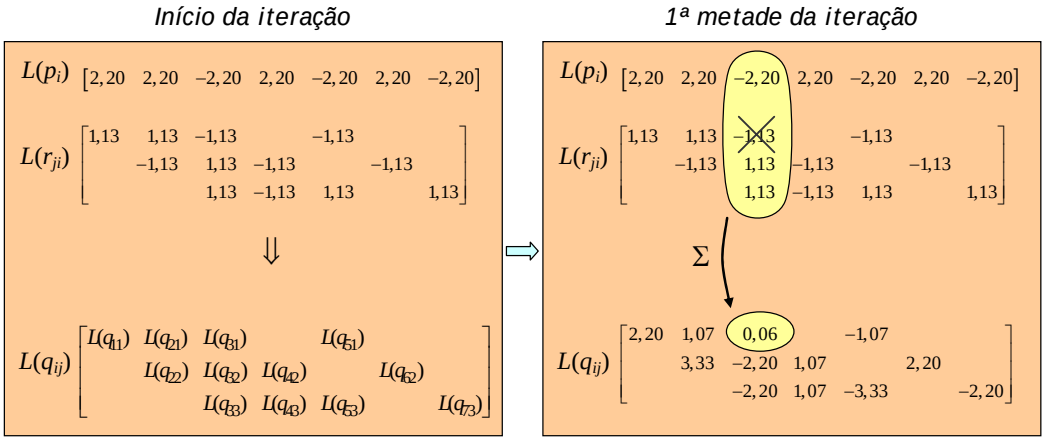
Estimativa da sequência binária transmitida:

$$\hat{\mathbf{x}} = \hat{x}_1, \hat{x}_2, \ldots, \hat{x}_7 = 1100010$$

O erro foi corrigido!

Exemplo numérico com mensagens logarítmicas

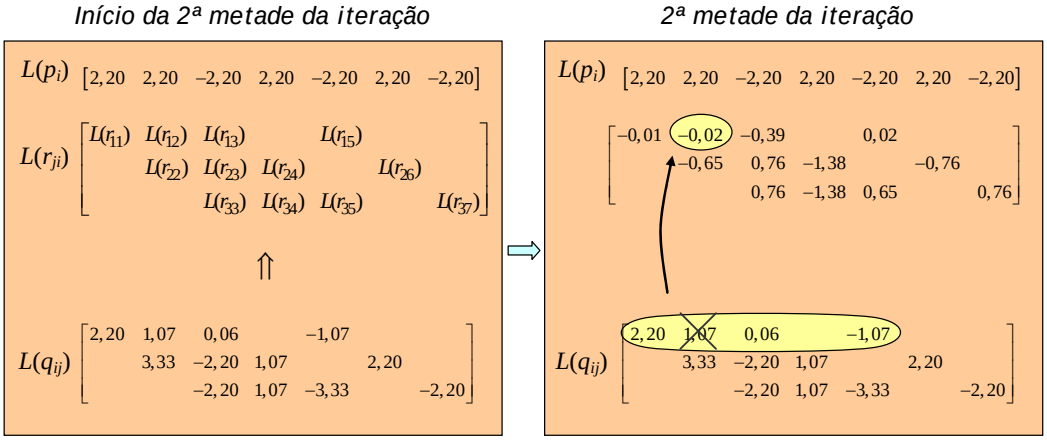
Valores de LLRs no início da segunda iteração:



Exemplo de cálculo:

$$L(q_{31}) = L(p_3) + L(r_{23}) + L(r_{33}) = -2,20 + 1,13 + 1,13 = 0,06$$

Valores de LLRs no fim da segunda iteração:



Exemplo de cálculo:

$$\Phi\left(L(r_{12})\right) = \Phi\left(L(q_{11})\right)\Phi\left(L(q_{31})\right)\Phi\left(L(q_{51})\right) = \Phi(2,20)\Phi(0,06)\Phi(-1,07) =$$

$$= -0,08 \times (-0,03) \times 0,49 = 0,01 \quad \Rightarrow \quad L(r_{12}) = \Phi^{-1}(0,01) = -0,02$$

Quanto valem as LLR a posteriori, por exemplo $L(x_5|\mathrm{y})$?

$$L(x_5|\mathbf{y}) = L(p_5) + L(r_{15}) + L(r_{35}) = -2,20 + 0,02 + 0,65 = -1,53$$