Geometry of the fundamental polytope

Pascal O. Vontobel
Information Theory Research Group
Hewlett-Packard Laboratories

USC, Los Angeles, CA, November 10, 2006

Overview

- ML Decoding vs. LP Decoding
- Linear programs and relaxed linear programs
- Fundamental polytope and cone definition
- Fundamental polytope and cone for simple codes
- Canonical completion

ML Decoding vs. LP Decoding

- Maximum-likelihood (ML) decoding:

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{x} \in \mathrm{conv}\left(\cap_{j=1}^{m} \mathcal{C}_j\right)} \sum_{i=1}^{n} \gamma_i x_i .$$

- Linear programming (LP) decoding:

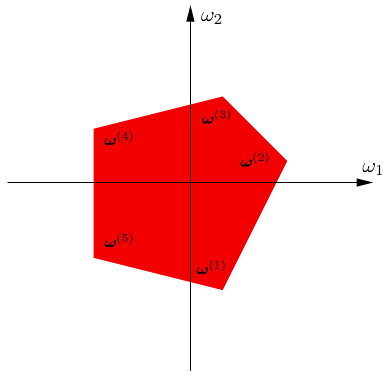
$$\hat{\boldsymbol{\omega}} = \arg \min_{\boldsymbol{\omega} \in \cap_{j=1}^{m} \mathrm{conv}(\mathcal{C}_j)} \sum_{i=1}^{n} \gamma_i \omega_i .$$

$\mathcal{P}(\mathbf{H}) \triangleq \bigcap_{j=1}^{m} \mathrm{conv}(\mathcal{C}_j)$ is called the fundamental polytope.

$\mathcal{K}(\mathbf{H}) \triangleq \bigcap_{j=1}^{m} \mathrm{conic}(\mathcal{C}_j) = \mathrm{conic}(\mathcal{P}(\mathbf{H}))$ is called the fund. cone.

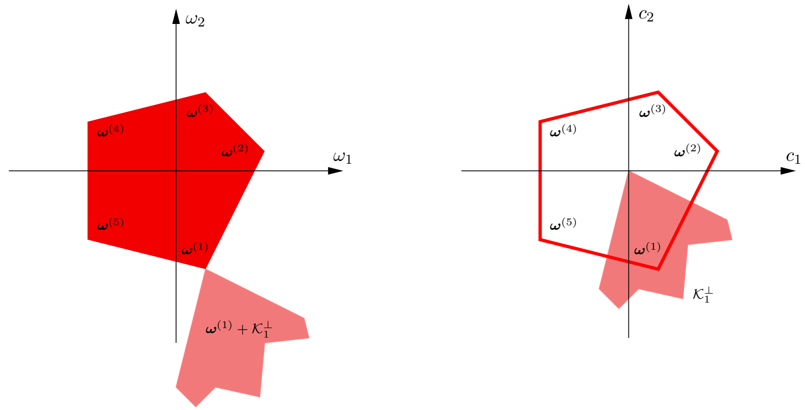
Linear Programs (Part 1)

$$\arg \max_{\boldsymbol{\omega} \in \mathcal{A}} \sum_{i=1}^{n} c_i \omega_i$$



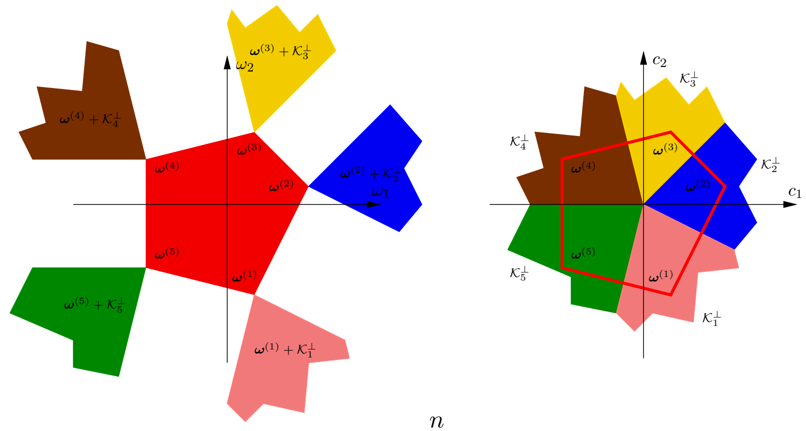
Because the cost function is linear and because $\mathcal{A}$ is a polytope, one of the vertices of $\mathcal{A}$ is always in the solution set.

Linear Programs (Part 2)



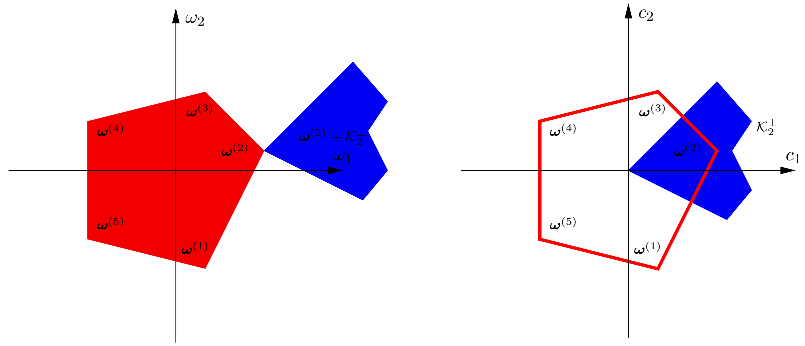
$$\arg\max_{\omega \in \mathcal{A}} \sum_{i=1}^{n} c_i \omega_i$$

Linear Programs (Part 2)



$$\arg\max_{\omega \in \mathcal{A}} \sum_{i=1}^{n} c_i \omega_i$$

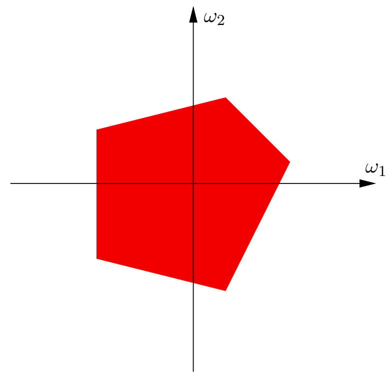
Linear Programs (Part 2)



$$\arg\max_{\omega \in \mathcal{A}} \sum_{i=1}^{n} c_i \omega_i$$

Relaxed Linear Programs (Part 1)

$$\arg\max_{\omega \in \mathcal{A}} \sum_{i=1}^{n} c_i \omega_i$$

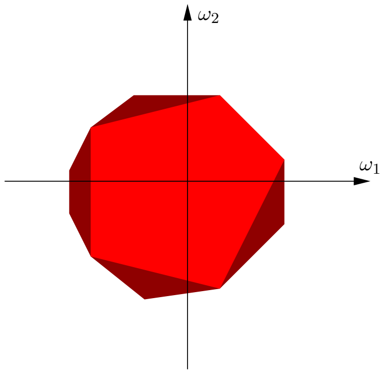


Relaxed Linear Programs (Part 1)

$$\arg\max_{\omega\in\mathcal{A}} \sum_{i=1}^{n} c_i\omega_i$$

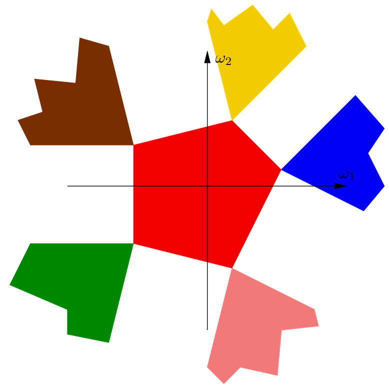
is replaced by

$$\arg\max_{\omega\in\mathcal{A}'} \sum_{i=1}^{n} c_i\omega_i$$



Relaxed Linear Programs (Part 2)

$$\arg\max_{\omega\in\mathcal{A}} \sum_{i=1}^{n} c_i\omega_i$$

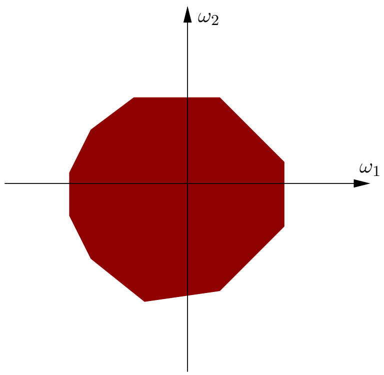


Relaxed Linear Programs (Part 1)

$$\arg\max_{\omega\in\mathcal{A}} \sum_{i=1}^{n} c_i\omega_i$$

is replaced by

$$\arg\max_{\omega\in\mathcal{A}'} \sum_{i=1}^{n} c_i\omega_i$$

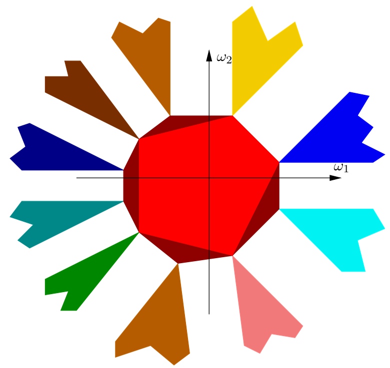


Relaxed Linear Programs (Part 2)

$$\arg\max_{\omega\in\mathcal{A}} \sum_{i=1}^{n} c_i\omega_i$$

is replaced by

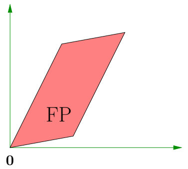
$$\arg\max_{\omega\in\mathcal{A}'} \sum_{i=1}^{n} c_i\omega_i$$



Fundamental Polytope

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{matrix} \Rightarrow \mathcal{C}_1 & \Rightarrow \mathrm{conv}(\mathcal{C}_1) \\ \Rightarrow \mathcal{C}_2 & \Rightarrow \mathrm{conv}(\mathcal{C}_2) \\ \Rightarrow \mathcal{C}_3 & \Rightarrow \mathrm{conv}(\mathcal{C}_3) \end{matrix}$$

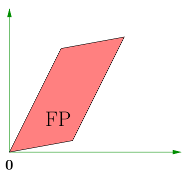
$$\Rightarrow \mathcal{C} = \bigcap_{j=1}^{m} \mathcal{C}_j \quad \Rightarrow \underbrace{\mathcal{P}(\mathbf{H}) = \bigcap_{j=1}^{m} \mathrm{conv}(\mathcal{C}_j)}_{\text{Fundamental polytope}}$$

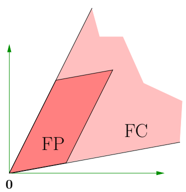


Fundamental Polytope / Cone (Part 1)

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{matrix} \Rightarrow \mathrm{conv}(\mathcal{C}_1) & \Rightarrow \mathrm{conic}(\mathcal{C}_1) \\ \Rightarrow \mathrm{conv}(\mathcal{C}_2) & \Rightarrow \mathrm{conic}(\mathcal{C}_2) \\ \Rightarrow \mathrm{conv}(\mathcal{C}_3) & \Rightarrow \mathrm{conic}(\mathcal{C}_3) \end{matrix}$$

$$\Rightarrow \underbrace{\mathcal{P}(\mathbf{H}) = \bigcap_{j=1}^{m} \mathrm{conv}(\mathcal{C}_j)}_{\text{Fundamental polytope}} \quad \Rightarrow \underbrace{\mathcal{K}(\mathbf{H}) = \bigcap_{j=1}^{m} \mathrm{conic}(\mathcal{C}_j)}_{\text{Fundamental Cone}}$$





Convex Hull of Simple Codes (Part 1)

Let $\mathcal{C}$ be defined by the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

Then

$$\mathcal{C} = \{(0,0),\ (1,1)\}$$

and

$$\mathrm{conv}(\mathcal{C}) = \left\{ \boldsymbol{\omega} \in [0,1]^2 \ \middle|\ \begin{matrix} -\omega_1 + \omega_2 \geq 0 \\ +\omega_1 - \omega_2 \geq 0 \end{matrix} \right\},$$

where $[0,1] = \{r \in \mathbb{R} \mid 0 \leq r \leq 1\}$.

Convex Hull of Simple Codes (Part 2)

Let $\mathcal{C}$ be defined by the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

Then

$$\mathcal{C} = \{(0,0,0),\ (1,1,0),\ (1,0,1),\ (0,1,1)\}$$

and

$$\mathrm{conv}(\mathcal{C}) = \left\{ \boldsymbol{\omega} \in [0,1]^3 \ \middle|\ \begin{matrix} -\omega_1 + \omega_2 + \omega_3 \geq 0 \\ +\omega_1 - \omega_2 + \omega_3 \geq 0 \\ +\omega_1 + \omega_2 - \omega_3 \geq 0 \\ -\omega_1 - \omega_2 - \omega_3 \geq -2 \end{matrix} \right\}.$$

Conic Hull of Simple Codes (Part 1)

Let $\mathcal{C}$ be defined by the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

Then

$$\mathcal{C} = \{(0,0),\ (1,1)\}$$

and

$$\mathrm{conic}(\mathcal{C}) = \left\{ \boldsymbol{\omega} \in \mathbb{R}_+^2 \;\middle|\; \begin{array}{l} -\omega_1 + \omega_2 \geq 0 \\ +\omega_1 - \omega_2 \geq 0 \end{array} \right\},$$

where $\mathbb{R}_+ = \{r \in \mathbb{R} \mid r \geq 0\}$.

Conic Hull of Simple Codes (Part 2)

Let $\mathcal{C}$ be defined by the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

Then

$$\mathcal{C} = \{(0,0,0),\ (1,1,0),\ (1,0,1),\ (0,1,1)\}$$

and

$$\mathrm{conic}(\mathcal{C}) = \left\{ \boldsymbol{\omega} \in \mathbb{R}_+^3 \;\middle|\; \begin{array}{l} -\omega_1 + \omega_2 + \omega_3 \geq 0 \\ +\omega_1 - \omega_2 + \omega_3 \geq 0 \\ +\omega_1 + \omega_2 - \omega_3 \geq 0 \end{array} \right\}.$$

Simple Code (Part 1)

As before, let us consider the length-3 code $\mathcal{C}$ defined by the parity-check matrix

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

The code $\mathcal{C}$ can be written as $\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$ with

$$\mathcal{C}_1 = \{(0,0,0),\ (1,1,0),\ (0,0,1),\ (1,1,1)\}$$
$$\mathcal{C}_2 = \{(0,0,0),\ (1,1,0),\ (1,0,1),\ (0,1,1)\}$$
$$\mathcal{C}_3 = \{(0,0,0),\ (0,1,1),\ (1,0,0),\ (1,1,1)\}$$

Simple Code (Part 2)

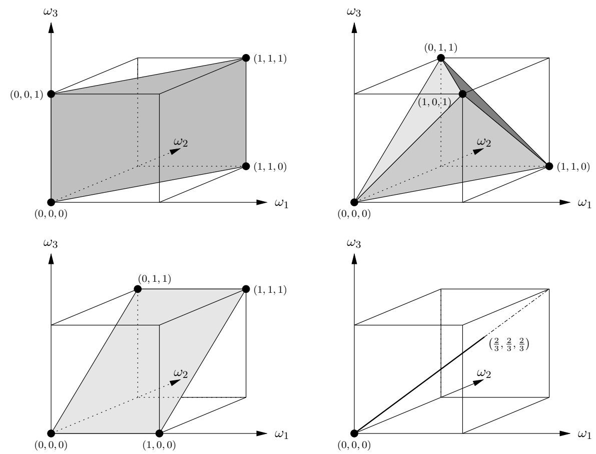
The fundamental polytope is $\mathcal{P}(\mathbf{H}) = \mathrm{conv}(\mathcal{C}_1) \cap \mathrm{conv}(\mathcal{C}_2) \cap \mathrm{conv}(\mathcal{C}_3)$ with

$$\mathrm{conv}(\mathcal{C}_1) = \mathrm{conv}\left(\{(0,0,0),\ (1,1,0),\ (0,0,1),\ (1,1,1)\}\right) = \left\{ \boldsymbol{\omega} \in [0,1]^3 \;\middle|\; \begin{array}{l} -\omega_1 + \omega_2 \geq 0 \\ +\omega_1 - \omega_2 \geq 0 \end{array} \right\}$$

$$\mathrm{conv}(\mathcal{C}_2) = \mathrm{conv}\left(\{(0,0,0),\ (1,1,0),\ (1,0,1),\ (0,1,1)\}\right) = \left\{ \boldsymbol{\omega} \in [0,1]^3 \;\middle|\; \begin{array}{l} -\omega_1 + \omega_2 + \omega_3 \geq 0 \\ +\omega_1 - \omega_2 + \omega_3 \geq 0 \\ +\omega_1 + \omega_2 - \omega_3 \geq 0 \\ -\omega_1 - \omega_2 - \omega_3 \geq -2 \end{array} \right\}$$

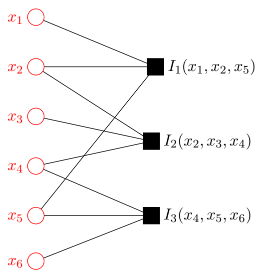
$$\mathrm{conv}(\mathcal{C}_3) = \mathrm{conv}\left(\{(0,0,0),\ (0,1,1),\ (1,0,0),\ (1,1,1)\}\right) = \left\{ \boldsymbol{\omega} \in [0,1]^3 \;\middle|\; \begin{array}{l} -\omega_2 + \omega_3 \geq 0 \\ +\omega_2 - \omega_3 \geq 0 \end{array} \right\}$$

Simple Code (Part 3)



conv($\mathcal{C}_1$)	conv($\mathcal{C}_2$)
conv($\mathcal{C}_3$)	$\mathcal{P}(\mathbf{H})$

Tanner / Factor graphs



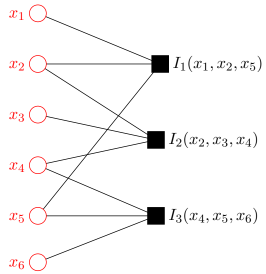
$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

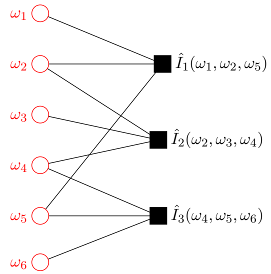
Codeword indicator function:

$$I_1(x_1, x_2, x_5) \cdot I_2(x_2, x_3, x_4) \cdot I_3(x_4, x_5, x_6) = \big[(x_1, x_2, x_5) \in \mathcal{C}_1\big] \cdot \big[(x_2, x_3, x_4) \in \mathcal{C}_2\big] \cdot \big[(x_4, x_5, x_6) \in \mathcal{C}_3\big]$$

Note: $x_i \in \{0, 1\}$

Pseudo-Codewords / Fundamental Polytope





Codeword indicator function:

$$I_1(x_1, x_2, x_5) \cdot I_2(x_2, x_3, x_4) \cdot I_3(x_4, x_5, x_6) = \big[(x_1, x_2, x_5) \in \mathcal{C}_1\big] \cdot \big[(x_2, x_3, x_4) \in \mathcal{C}_2\big] \cdot \big[(x_4, x_5, x_6) \in \mathcal{C}_3\big]$$

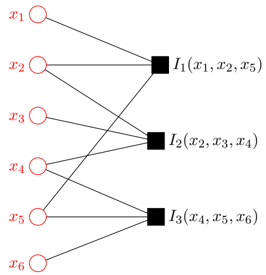
Note: $x_i \in \{0, 1\}$

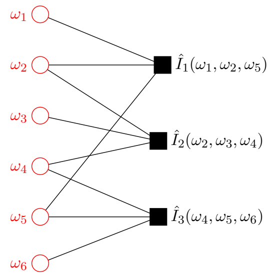
Pseudo-codeword indicator function:

$$\hat{I}_1(\omega_1, \omega_2, \omega_5) \cdot \hat{I}_2(\omega_2, \omega_3, \omega_4) \cdot \hat{I}_3(\omega_4, \omega_5, \omega_6) = \big[(\omega_1, \omega_2, \omega_5) \in \mathrm{conv}(\mathcal{C}_1)\big] \cdot \big[(\omega_2, \omega_3, \omega_4) \in \mathrm{conv}(\mathcal{C}_2)\big] \cdot \big[(\omega_4, \omega_5, \omega_6) \in \mathrm{conv}(\mathcal{C}_3)\big]$$

Note: $0 \leq \omega_i \leq 1$

Pseudo-Codewords / Fundamental Cone





Codeword indicator function:

$$I_1(x_1, x_2, x_5) \cdot I_2(x_2, x_3, x_4) \cdot I_3(x_4, x_5, x_6) = \big[(x_1, x_2, x_5) \in \mathcal{C}_1\big] \cdot \big[(x_2, x_3, x_4) \in \mathcal{C}_2\big] \cdot \big[(x_4, x_5, x_6) \in \mathcal{C}_3\big]$$

Note: $x_i \in \{0, 1\}$

Pseudo-codeword indicator function:

$$\hat{I}_1(\omega_1, \omega_2, \omega_5) \cdot \hat{I}_2(\omega_2, \omega_3, \omega_4) \cdot \hat{I}_3(\omega_4, \omega_5, \omega_6) = \big[(\omega_1, \omega_2, \omega_5) \in \mathrm{conic}(\mathcal{C}_1)\big] \cdot \big[(\omega_2, \omega_3, \omega_4) \in \mathrm{conic}(\mathcal{C}_2)\big] \cdot \big[(\omega_4, \omega_5, \omega_6) \in \mathrm{conic}(\mathcal{C}_3)\big]$$

Note: $0 \leq \omega_i$

Pseudo-Codewords / Fundamental Cone

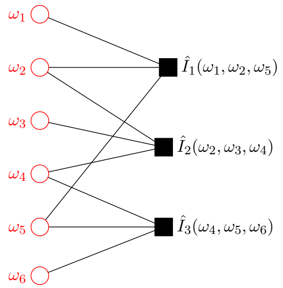
E.g.

$$[(\omega_1, \omega_2, \omega_5) \in \text{conic}(\mathcal{C}_1)] = 1$$

if and only if

$$\omega_1 \leq \omega_2 + \omega_5$$
$$\omega_2 \leq \omega_1 + \omega_5$$
$$\omega_5 \leq \omega_1 + \omega_2$$

$$\omega_1 \geq 0$$
$$\omega_2 \geq 0$$
$$\omega_3 \geq 0$$



Pseudo-codeword indicator function:

$$\hat{I}_1(\omega_1, \omega_2, \omega_5) \cdot \hat{I}_2(\omega_2, \omega_3, \omega_4) \cdot \hat{I}_3(\omega_4, \omega_5, \omega_6)$$
$$= [(\omega_1, \omega_2, \omega_5) \in \text{conic}(\mathcal{C}_1)] \cdot$$
$$[(\omega_2, \omega_3, \omega_4) \in \text{conic}(\mathcal{C}_2)] \cdot$$
$$[(\omega_4, \omega_5, \omega_6) \in \text{conic}(\mathcal{C}_3)]$$

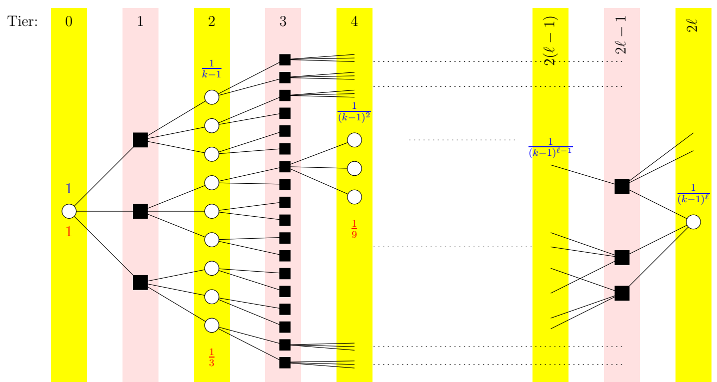
Note: $0 \leq \omega_i$

References

For more info, see e.g.

- P. O. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes", submitted to IEEE Trans. on Inform. Theory, Dec. 2005. [http://www.arxiv.org/abs/cs.IT/0512078]

The Canonical Completion



The canonical completion for a $(j = 3, k = 4)$-regular LDPC code. On check-regular graphs the (scaled) canonical completion always gives a (valid) pseudo-codeword.