Optimality Considerations of Short-Length LDPC Codes Construction

Dejan Vukobratovic

Department of Telecommunications and Signal Processing
University of Novi Sad
Serbia and Montenegro

November, 3rd 2005
COST 289 - 9th meeting, Madrid

Outline

Finite-Length Analysis

- Asymptotic Analysis
  - Density Evolution and approximations
  - Outputs capacity-approaching degree distributions
- Finite-Length Analysis
  - Well developed in the BEC case
    - Stopping Sets
  - Pseudocodewords Theory
    - Promising direction in finite-length analysis

Pseudocodewords of Tanner Graphs

- Concept introduced by Wiberg
  - Pseudocodewords on Computation Trees
  - N. Wiberg:"Codes and Decoding on General Graphs", PhD Thesis, Linkoping University, 1996.
- Further Refined by Koetter and Vontobel
  - Pseudocodewords on Graph Covers
  - R. Koetter and P. O. Vontobel:"Graph covers and iterative decoding of finite-length codes", Proc. of the 3rd intl. Conf on Turbo Codes and Related Topics, 2003.

ML Decoding as a Linear Program

- Easy to convert ML decoding into:

$$\hat{\boldsymbol{x}}_{ML}(\boldsymbol{y}) = \hat{\boldsymbol{x}}_{ML}(\boldsymbol{\lambda}) = \arg \min_{\boldsymbol{x} \in CH(C)} \sum_{i=1}^{n} \lambda_i \cdot x_i \qquad (1)$$

- CH(C): Convex Hull of set C
- Log Likelihood Ratio: $LLR(y_i) = \lambda_i = \ln\left(\frac{Pr[\, y_i \,|\, x_i = 0\,]}{Pr[\, y_i \,|\, x_i = 1\,]}\right)$
- CH(C) is of exponential description complexity
- Fails to give a practical ML decoder

Fundamental Polytope

- Use standard Relaxation Technique from LP theory:
  - Replace CH(C) with less complex polytope
- Fundamental Polytope:
  - Each row [$\mathbf{h_i}$] of [$\mathbf{H}$] defines local SPC code C_i

$$\mathcal{P}(H) = \bigcap_{i}^{m} CH(C_i) \tag{2}$$

- If $w_H(\mathbf{h_i})$ is bounded by a constant as n grows:
  - Valid for LDPC codes
  - Linear number of constraints with n
  - Practical but suboptimal decoder

LP Decoding

- LP Decoding:

$$\hat{\boldsymbol{x}}_{LP}(\boldsymbol{y}) = \hat{\boldsymbol{x}}_{LP}(\boldsymbol{\lambda}) = \arg\min_{\boldsymbol{x}\in\mathcal{P}} \sum_{i=1}^{n} \lambda_i \cdot x_i \tag{3}$$

- LP solution is always a vertex of optimization domain
- LP Pseudocodewords: set of vertices of $\mathcal{P}$, $V(\mathcal{P})$
  - $C \subset V(\mathcal{P})$
  - $F(\mathcal{P}) = V(\mathcal{P}) \backslash C$ - Set of Fractional Solutions
- J. Feldman and M.J. Wainwright and D.R. Karger:"Using linear programming to decode binary linear codes", Trans. on Inform. Theory, pp. 954-972, March 2005.

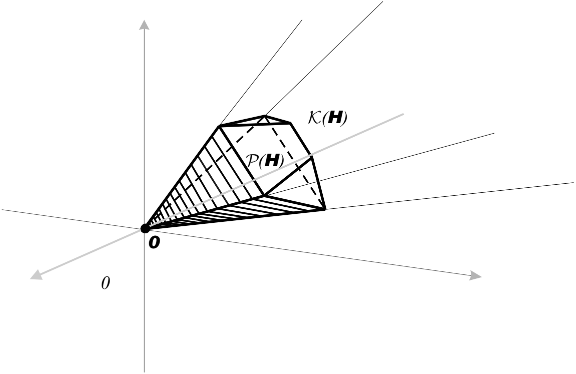
BP vs LP decoding

- LP decoder: Suboptimal decoder with a strong connections with BP decoder
  - Equivalent with BP decoder on BEC
    - D. Vukobratovic:"On the equivalence of BP and LP decoding on the BEC Channel", Proc. of the 4th Intl'. Workshop on Optimal Codes and Related Topics, 2005.
  - On AWGN Channel:
    - Same characterization of the set of Pseudocodewords
    - Fundamental Polytope
  - Further references on BP and LP connections:
    - P. O. Vontobel and R. Koetter:"On the relationship between linear-programming decoding and min-sum algorithm decoding", Proc. of the ISITA, 2004.

Fundamental Polytope and Fundamental Cone

- Conic Hull of the Fundamental Polytope $\mathcal{P}$

$$K(\mathbf{H}) = \{\alpha \boldsymbol{x} | \alpha \geq 0, \boldsymbol{x} \in \mathcal{P}\} \tag{4}$$



$$\forall j \in \mathcal{J} \quad : \quad \omega_j \geq 0, \tag{5}$$

$$\forall i \in \mathcal{I}, \forall j \in \mathcal{J}_i \quad : \quad \sum_{j' \in \mathcal{J}_i \setminus \{j\}} \omega_{j'} \geq \omega_j. \tag{6}$$

All-Zero Codeword LP Decoding Region

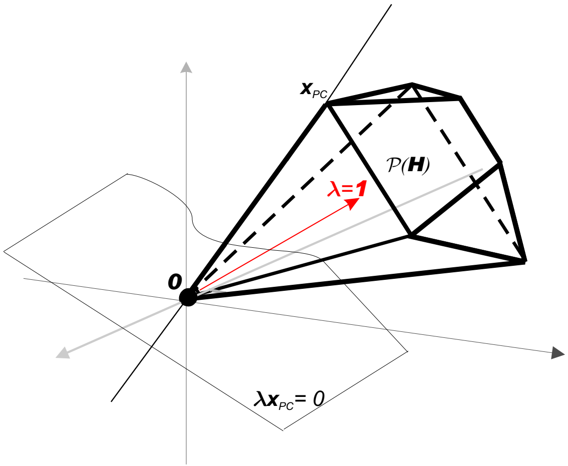
$$D_{\mathbf{0}}^{LP} = \{\boldsymbol{\lambda} | \boldsymbol{\lambda} \cdot \boldsymbol{x} \geq 0, \forall \boldsymbol{x} \neq 0, \boldsymbol{x} \in V(\mathcal{P})\} \tag{7}$$

- Convex Cone with apex in the origin
- Most of the $\boldsymbol{x} \in V(\mathcal{P})$ are redundant
- Minimal Pseudocodewords $M(\mathcal{P}) \subseteq V(\mathcal{P})$ describes $D_{\mathbf{0}}^{LP}$

$$D_{\mathbf{0}}^{LP} = \{\boldsymbol{\lambda} | \boldsymbol{\lambda} \cdot \boldsymbol{x} \geq 0, \forall \boldsymbol{x} \neq 0, \boldsymbol{x} \in M(\mathcal{P})\} \tag{8}$$

- The Fundamental Cone and the All-Zero Codeword Decoding Region are Dual Cones

The Dual Cone Relationship



Pseudo-weight of the pseudocodewords

- Generalization of the Hamming weight
- AWGN Pseudo-weight

$$\omega_P^{AWGNC}(\boldsymbol{x}) = \frac{\| \boldsymbol{x} \|_1^2}{\| \boldsymbol{x} \|_2^2} \tag{9}$$

- Distance between plane $\{\gamma \in \mathbb{R}^n \mid y\gamma^\tau = 0\}$ and point $+\mathbf{1} = (1, 1, \ldots, 1)$
- Inversely proportional to $\angle(\boldsymbol{x}, \mathbf{1})$
- We are interested in the Minimal Pseudocodeword Weight Spectrum

Finite Geometries Codes

- Experimentally observed very good performance with BP decoding
  - Y. Kou and S. Lin and M.P.C. Fossorier:"Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results", Trans. on Inform. Theory, pp. 2711-2736, Nov 2001.
- Families of Type I PG-LDPC and Type I EG-LDPC Codes
- Parity-Check Matrix **H** defined by an incidence structure of points and lines in the projective plane PG(2,q)

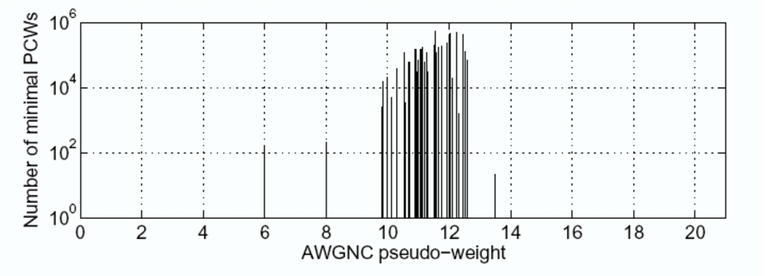
Pseudoweight Spectrum Gap

- Pseudoweight Spectrum Gap $g(\mathbf{H})$
  - The difference between d_{min} and the minimum pseudoweight over the set of fractional (non-codeword) pseudocodewords
- Examine the Pseudoweight Spectrum Gap of Finite Geometries Codes
- P.O. Vontobel and R. Smarandache and N. Kiyavash and J. Teutsch and D. Vukobratovic: "On the Minimal Pseudocodewords of Codes from Finite Geometries", Proc. of the ISIT 2005.

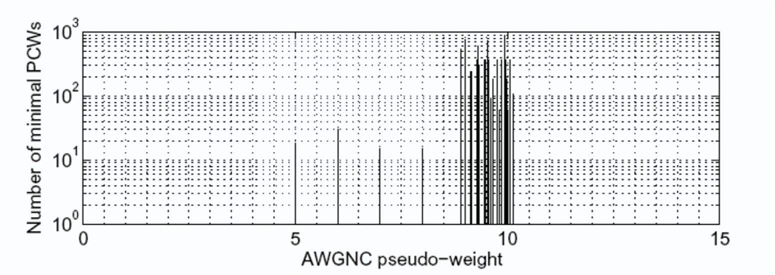
Numerical Results for Type I PG-LDPC Codes

- PG(2,2) code: $\mathcal{C}_{PG(2,2)}$ [7,3,4]-code
    - $g(\mathbf{H}_{PG(2,2)})$=6.25-4=2.25
- PG(2,4) code: $\mathcal{C}_{PG(2,4)}$ [21,11,6]-code
    - $g(\mathbf{H}_{PG(2,4)})$=9.8-6=3.8
- PG(2,8 code): $\mathcal{C}_{PG(2,8)}$ [73,45,10]-code
    - $g(\mathbf{H}_{PG(2,8)}) \approx 6$

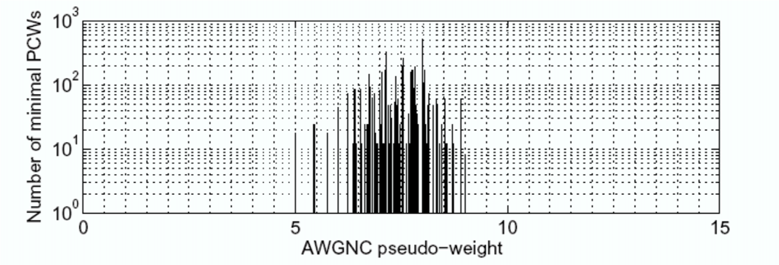
Pseudoweight Spectrum of PG(2,4) code



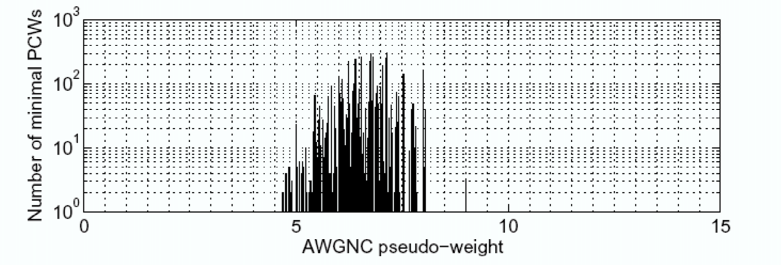
Pseudoweight Spectrum of 15x15 EG(2,4) code



Pseudoweight Spectrum of 9x15 EG(2,4) code



Pseudoweight Spectrum of 8x15 EG(2,4) code



Optimality Considerations

- Choosing a code $\mathcal{C}$ we choose d_{min}
  - Performance guarantees for ML decoding
- Choosing the parity-check matrix **H** we choose minimum pseudoweight
  - Performance guarantees for LP and BP decoding
- Problem: Find families of **H** that have large Pseudoweight Spectrum Gaps
- Fact: Adding redundant rows improves performance

Pseudoweight Spectrum Gap Characteristic of Code

- To define $[n, k]$ binary linear code $\mathcal{C}$:
    - $m \times n$ parity check matrix $\mathbf{H}$
    - spans the space orthogonal to $\mathcal{C}$
    - $m \in M = \{n - k, \ldots, 2^{n-k} - 1\}$
- $g_{\mathcal{C}}(m) = \max_{\mathbf{H} \in \mathcal{H}_m(\mathcal{C})} g(\mathbf{H}), \qquad m \in M$
- $\mathcal{H}_m(\mathcal{C})$: set of all $m \times n$ parity check matrices spanning the space orthogonal to the $\mathcal{C}$.
- $g_{\mathcal{C}}(m)$: characteristic of the code $\mathcal{C}$.

Pseudoweight Spectrum Gap Characteristic of Code

- The Stopping Redundancy

$$\rho(\mathcal{C}) = \min\{m | g_{\mathcal{C}}(m) \geq 0\} \quad (10)$$