Efficient Evaluation of the Weight Spectral Shape of Nonbinary Protograph LDPC Codes

Enrico Paolini
University of Bologna, Italy

work with: Mark F. Flanagan

DLR & LNT Coding Workshop
Münich, Germany, July 26th, 2016

Outline

- Some background
- Weight spectral shape of protograph LDPC codes
- Examples
- Conclusion

Weight Spectral Shape

- Used by Gallager to show that his regular LDPC codes have minimum distance growing linearly with the codeword length.
- Weight spectral shape of a sequence of code ensembles

$$G(\omega) := \lim_{n \to \infty} \frac{\log_q \mathcal{A}_{\omega n}}{n}$$

- $\mathcal{A}_{\omega n}$: the expected number of weight ωn for an LDPC code drawn randomly from an ensemble.
- Critical codeword weight ratio

$$\omega^* := \inf\{\omega : G(\omega) > 0\}$$

Weight Spectral Shape

- The minimum distance has a linear growth when

$$\omega^* > 0$$

and

$$\lim_{n\to\infty} \Pr\left(D_{\min} < \omega^* n\right) = 0$$

- In ensemble optimization we are often interested only in ω^* and not in the entire $G(\omega)$.
- **This talk**: develop a tool for the efficient and exact evaluation of $G(\omega)$ and ω^* for protograph LDPC codes over GF(q).

Some Literature

[Gal63] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA, USA: M.I.T. Press, 1963.

[Orl05] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," T-IT, Mar. 2005.

[Di06] C. Di, T. Richardson, and R. Urbanke, "Weight distribution of low-density parity-check codes," T-IT, Nov. 2006.

[Kas11] K. Kasai, C. Poulliat, D. Declercq, and K. Sakaniwa, "Weight distributions of non-binary LDPC codes," IEICE T-Fundamentals, Apr. 2011.

[Abu11] S. Abu-Surra, D. Divsalar, and W. Ryan, "Enumerators for protograph-based ensembles of LDPC and generalized LDPC codes," T-IT, Feb. 2011.

[Fla11] M. Flanagan, E. Paolini, M. Chiani, and M. Fossorier, "On the growth rate of the weight distribution of doubly-generalized LDPC codes," T-IT, Jun. 2011.

[Fla13] M. Flanagan, E. Paolini, M. Chiani, M. Fossorier, "Spectral shape of doubly-generalized LDPC codes: Efficient and exact evaluation, T-IT, Nov. 2013.

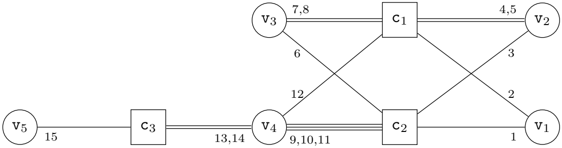
Available Approaches

[Dol14]L. Dolecek, D. Divsalar, Y. Sun, and B. Amiri, "Non-binary protograph-based LDPC codes: Enumerators, analysis, and designs," T-IT, Jul. 2014.

[Gar15]G. Garrammone, D. Declercq, and M. Fossorier, "Weight distributions of non-binary multi-edge type LDPC code ensembles," ISIT 2015.

Protograph LDPC Codes

- A Tanner graph with a relatively small number of nodes.



- The protograph defines an ensemble of LDPC codes over GF(q).
- To draw one code:
  - A *copy-and-permute* operation with copy factor Q.
  - E uniform i.i.d. random variables are drawn from GF(q) $\setminus \{0\}$; the E edges in the Tanner graph are labeled with the obtained E nonzero symbols.

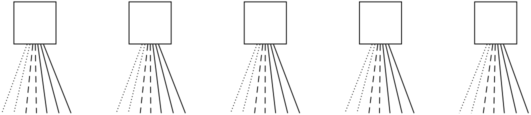
Protograph LDPC Codes

- $\mathcal{J}$: set of n_v protograph VNs; $\mathcal{I}$: set of n_c protograph CNs.
- n_u protograph VNs are transmitted and n_p are punctured.
- Corresponding sets: $\mathcal{J}_u$ and $\mathcal{J}_p$.
- q_j: the degree of VN $j \in \mathcal{J}$; s_i: the degree of CN $i \in \mathcal{I}$.
- e: the number of edges in the protograph; Φ: the set of edge indexes; $|\Phi| = \mathrm{e}$.
- For all $i \in \mathcal{I}$, $\Gamma_i \subseteq \Phi$ is the set which contains the indices of the edges connected to CN i in the protograph.
- For all $j \in \mathcal{J}$, $\Lambda_j \subseteq \Phi$ is the set which contains the indices of the edges connected to VN j in the protograph.

The Approach of [Gar15]

- Developed for multi-edge type LDPC codes.
- May be specialized to the protograph setting.
- To calculate one point of the weight spectral shape function requires solution of a $(3e + 1) \times (3e + 1)$ system of equations.
- It extends to the MET setting the approach of [Fla13].

Composite Codes



- $\mathcal{C}(n,k)$: a linear block code over GF(q) with length n and dimension k.
- Composite code with base code $\mathcal{C}(n,k)$ and replica factor Q, $\mathcal{C}_{\text{com}}(nQ,kQ)$: the linear block code whose codewords are concatenations of Q codewords of $\mathcal{C}(n,k)$.

Vector WEF of Composite Codes

- Consider a composite code with replica factor Q and (s, h) linear block component code $\mathcal{C}$ over $\mathrm{GF}(q)$.
- Vector weight enumerating function:

$$A(\boldsymbol{z}) = \sum_{\boldsymbol{d}} A_{\boldsymbol{d}} \boldsymbol{z}^{\boldsymbol{d}}$$

where $A_{\boldsymbol{d}}$ is the number of composite codewords of vector weight $\boldsymbol{d} = (d_1, d_2, \ldots, d_s)$.

- Notation: $\boldsymbol{z}^{\boldsymbol{d}} = \prod_{t=1}^{s} z_t^{d_t}$; d_t: Hamming weight of the Q replicas of the t-th codeword symbol of the component code.

Vector WEF of Composite CNs [Dol14]

- Consider the $K_i \times s_i$ matrix $\boldsymbol{M}$ containing all distinct supports of the codewords of $\mathcal{C}_i$ (i-th CN).
- x_k: the Hamming weight of the k-th row of $\boldsymbol{M}$.
- We have $K_i = 2^{s_i} - s_i$ if $q > 2$ and $K_i = 2^{s_i - 1}$ if $q = 2$.
- $\boldsymbol{n} = (n_1, n_2, \ldots, n_{K_i})$: a vector whose elements are K_i nonnegative integer numbers whose sum is equal to Q.
- We have

$$A_{i,\boldsymbol{d}_i} = \sum_{\boldsymbol{n} \in \mathcal{N}(\boldsymbol{d}_i)} \binom{Q}{\boldsymbol{n}} \exp\left(\langle \boldsymbol{n}, \boldsymbol{f}_q \rangle\right)$$

where $\mathcal{N}(\boldsymbol{d}_i)$ is the set of all $\boldsymbol{n}$ that are integer-vector solutions of $\boldsymbol{n}\boldsymbol{M} = \boldsymbol{d}_i$ and where $\boldsymbol{f}_q = (f_{q,1}, f_{q,2}, \ldots, f_{q,K_i})$ is such that

$$f_{q,k} = \ln\left(\frac{q-1}{q}\left[(q-1)^{x_k - 1} + (-1)^{x_k}\right]\right).$$

Vector Weight Spectral Shape of Composite CNs [Dol14]

- Let $\boldsymbol{d}_i = Q\boldsymbol{\delta}_i$. Define a *vector* weight spectral shape for a composite code ensemble as

$$\alpha_i(\boldsymbol{\delta}_i) = \lim_{Q\to\infty} \frac{1}{Q} \ln A_{i,Q\boldsymbol{\delta}_i} .$$

- Let $\boldsymbol{n} = Q\boldsymbol{\nu}$. Note that $\langle \boldsymbol{n}, \boldsymbol{f}_q \rangle = Q\langle \boldsymbol{\nu}, \boldsymbol{f}_q \rangle$ and that $\boldsymbol{\nu}$ is a probability mass function.
- We have

$$\alpha_i(\boldsymbol{\delta}_i) = \max_{\boldsymbol{\nu}} \left\{ \mathrm{H}(\boldsymbol{\nu}) + \langle \boldsymbol{\nu}, \boldsymbol{f}_q \rangle \right\}$$

where $\mathrm{H}(\boldsymbol{\nu}) = -\sum_{k=1}^{K_i} \nu_k \ln \nu_k$ is the entropy of $\boldsymbol{\nu}$ in nats and where the maximization is subject to $\sum_{k=1}^{K_i} \nu_k = 1$ and to $\boldsymbol{\nu}\boldsymbol{M} = \boldsymbol{\delta}_i$ (as well as $0 \le \nu_k \le 1$ for all $k \in \{1, 2, \ldots, K_i\}$).

Average Number of Protograph-LDPC Codewords

- Easy to show that

$$\mathcal{A}_w = \sum_{\boldsymbol{w}} \frac{\prod_{i \in \mathcal{I}} A_{i,\boldsymbol{d}_i(\boldsymbol{w})}}{\prod_{j \in \mathcal{J}} \binom{Q}{w_j}^{q_j - 1} (\mathrm{q}-1)^{(q_j-1)w_j}}$$

where the vector weight $\boldsymbol{w} = (w_1, w_2, \ldots, w_{n_v})$ is subject to the constraint $\sum_{j \in \mathcal{J}_u} w_j = w$.

- The function $G(\omega)$ fulfills the identity

$$G(\omega) = \frac{r(\omega n_v)}{n_v \ln \mathrm{q}}$$

where the function $r(\delta)$ is defined as

$$r(\delta) = \lim_{Q \to \infty} \frac{1}{Q} \ln \mathcal{A}_{\delta Q} .$$

$r(\delta)$ Solution Method [Dol14]

- We have

$$r(\delta) = \max_{\boldsymbol{\delta}} \left\{ \sum_{i \in \mathcal{I}} \alpha_i(\boldsymbol{\delta}_i) - \sum_{j \in \mathcal{J}} (t_j - 1)\left(\delta_j \ln(\mathrm{q} - 1) + \mathrm{h}(\delta_j)\right) \right\}$$

subject to the constraint $\sum_{j \in \mathcal{J}_u} \delta_j = \delta$, as well as $0 \leq \delta_j \leq \delta$ for all $j \in \mathcal{J}$.

- Vector $\boldsymbol{\delta}$ has n_v elements. Each vector $\boldsymbol{\delta}_i$, $i \in \mathcal{I}$, has s_i elements.

- To calculate one point of $r(\delta)$:
    - Solve *numerically* the constrained maximization problem;
    - In the objective function, each of the n_c terms $\alpha_i(\boldsymbol{\delta}_i)$ must be calculated by solving *numerically* a constrained maximization problem "nested" in the main one.

Using Generating Functions

- Approach: Use generating functions properties.

Lemma

The number $A_{i,\boldsymbol{d}_i}$ of codewords with vector weight $\boldsymbol{d}_i$ in the composite code is given by ($a_i(\boldsymbol{z}_i)$ vector WEF of CN)

$$A_{i,\boldsymbol{d}_i} = \mathrm{coeff}\left(\left(a_i(\boldsymbol{z}_i)\right)^Q, \boldsymbol{z}_i^{\boldsymbol{d}_i} \right) .$$

- We then have

$$\mathcal{A}_w = \sum_{\boldsymbol{w} \in \mathcal{W}_w} \frac{\prod_{i \in \mathcal{I}} \mathrm{coeff}\left(\left(a_i(\boldsymbol{z}_i)\right)^Q, \boldsymbol{z}_i^{\boldsymbol{d}_i(\boldsymbol{w})} \right)}{\prod_{j \in \mathcal{J}} \binom{Q}{w_j}^{q_j - 1} (\mathrm{q}-1)^{(q_j-1)w_j}} . \qquad (1)$$

Main Result

Theorem

The weight spectral shape of a protograph ensemble over GF(q) *is*

$$G(\omega) = \frac{1}{n_u \ln \mathrm{q}} \Bigg[\sum_{i \in \mathcal{I}} \Bigg(\ln a_i(\boldsymbol{x}_i) - n_u \sum_{g \in \Gamma_i} \omega_g \ln x_g \Bigg) - \sum_{j \in \mathcal{J}} \big((q_j - 1)\mathrm{h}(n_u \omega_j) + n_u \omega_j (q_j - 1) \ln(\mathrm{q} - 1) \big) \Bigg]$$

where the values $\{x_g\}$ *for* $g \in \Phi$ *are the positive solutions to*

$$x_g \frac{\partial a_i}{\partial x_g}(\boldsymbol{x}_i) = n_u \omega_g \, a_i(\boldsymbol{x}_i) \qquad \forall i \in \mathcal{I}, g \in \Gamma_i \,, \tag{2}$$

which also satisfy, for every $j \in \mathcal{J}$*,*

$$(q_j - 1) \ln \left(\frac{n_u \omega_j / (\mathrm{q} - 1)}{1 - n_u \omega_j} \right) - \sum_{g \in \Lambda_j} \ln x_g = \begin{cases} \mu & \text{if } j \in \mathcal{J}_u \\ 0 & \text{if } j \in \mathcal{J}_p \,. \end{cases} \tag{3}$$

System Dimension, Augmented System

- The evaluation of the weight spectral shape via the proposed method requires solution of a system of equations.
- There are $n_v + \mathrm{e} + 1$ variables: $\{w_j\}$ (n_v variables); $\{x_g\}$ (e variables); and μ (1 variable).
- There are also $n_v + \mathrm{e} + 1$ equations: (2) for each $i \in \mathcal{I}$, $g \in \Gamma_i$ (together giving e equations); (3) for each $j \in \mathcal{J}$ (together giving n_v equations); and $\sum_{j \in \mathcal{J}_u} \omega_j = \omega$.
- The critical codeword weight ratio can be **directly** efficiently computed using the proposed method, simply by adding the equation $G(\omega^*) = 0$ to the system of equations to be solved, yielding an $(n_v + \mathrm{e} + 2) \times (n_v + \mathrm{e} + 2)$ system.

Proof Sketch

- Let $\omega = w/n$ and $\boldsymbol{\omega} = (\omega_j)_{j \in \mathcal{J}} = (1/n)\boldsymbol{w}$. Moreover, let $\boldsymbol{\lambda}_i(\boldsymbol{\omega}) = (1/n)\, \boldsymbol{l}_i(n\boldsymbol{\omega})$.

- From previous Lemma

$$\operatorname{coeff}\left((a_i(\boldsymbol{z}_i))^Q, \boldsymbol{z}_i^{\boldsymbol{l}_i(\boldsymbol{w})} \right) = \operatorname{coeff}\left((a_i(\boldsymbol{z}_i))^Q, \boldsymbol{z}_i^{n_u \boldsymbol{\lambda}_i(\boldsymbol{\omega}) Q} \right)$$
$$\doteq \exp\left\{ n \left[\frac{1}{n_u} \ln a_i(\boldsymbol{x}_i) - \sum_{g \in \Gamma_i} \omega_g \ln x_g \right] \right\}$$

- The vector $\boldsymbol{x}_i = (x_g)_{g \in \Gamma_i}$ contains the positive solutions to the equations

$$x_g \frac{\partial a_i}{\partial x_g}(\boldsymbol{x}_i) = n_u \omega_g \, a_i(\boldsymbol{x}_i) \qquad g \in \Gamma_i \, .$$

Proof Sketch

- Regarding the expression at the denominator of denominator applied to the denominator of (1) simply note that

$$\prod_{j\in\mathcal{J}} \binom{Q}{w_j}^{q_j-1} (\mathsf{q}-1)^{(q_j-1)w_j}$$

$$\doteq \exp\left\{ n \left[\frac{1}{n_u} \sum_{j\in\mathcal{J}} (q_j-1)\mathsf{h}(n_u\omega_j) + \omega_j(q_j-1)\ln(\mathsf{q}-1) \right] \right\}$$

- In the previous expression, $\mathsf{h}(x)$ is the binary entropy function in nats.

Proof Sketch

- Applying the above asymptotic results yields

$$G(\omega) = \frac{1}{\ln \mathrm{q}} \left(\max_{\boldsymbol{\omega}} S(\boldsymbol{\omega}) \right)$$

where

$$S(\boldsymbol{\omega}) = \sum_{i \in \mathcal{I}} \left(\frac{1}{n_u} \ln a_i(\boldsymbol{x}_i) - \sum_{g \in \Gamma_i} \omega_g \ln x_g \right) - \sum_{j \in \mathcal{J}} \left[\left(\frac{q_j - 1}{n_u} \right) \mathrm{h}(n_u \omega_j) + \omega_j (q_j - 1) \ln(\mathrm{q} - 1) \right]$$

- Maximization is subject to $R(\boldsymbol{\omega}) = \sum_{j \in \mathcal{J}_u} \omega_j = \omega$ and $0 \leq \omega_j \leq \frac{1}{n_u}$ $\forall j \in \mathcal{J}$.
- Solution yields the statement.

Reducing the System Size

Lemma

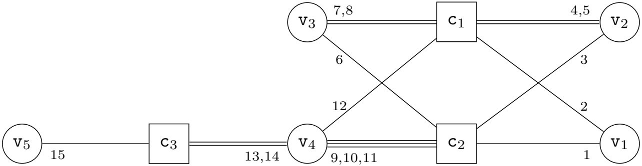
If two edges $a, b \in \Phi$ are connected to the same VN–CN pair in the protograph, then $x_a = x_b$.

Proof.

- Consider two parallel edges $a, b \in \Phi$ which connect VN $j \in \mathcal{J}$ to CN $i \in \mathcal{I}$.
- As the local weight enumerator $a_i(\boldsymbol{x}_i)$ is symmetric in the variables $\{x_g\}$, $g \in \Gamma_i$, it follows that if a solution exists with $(x_a, x_b) = (\alpha, \beta)$, then another solution must exist with $(x_a, x_b) = (\beta, \alpha)$ (all other variables being unchanged).
- Then, the hypothesis that $\beta \neq \alpha$ contradicts the uniqueness of the positive solution x_i to (2) for CN type i.

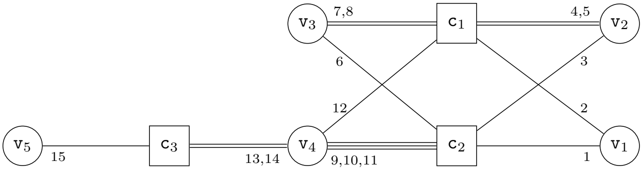
□

Example: An $R = 1/2$ AR4JA Protograph



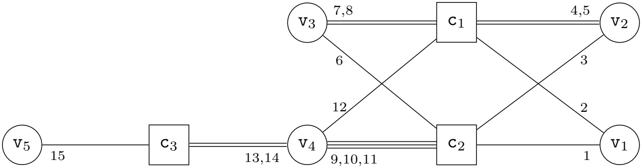
- $n_c = 3$ CNs, $n_v = 5$ VNs, e $= 15$ edges.
- $\mathcal{J}_u = \{1, 2, 3, 5\}$, $\mathcal{J}_p = \{4\}$, $R = 1/2$.
- Since there are punctured VNs the method of [Garr15] cannot be applied to this protograph.

Example: An $R = 1/2$ AR4JA Protograph



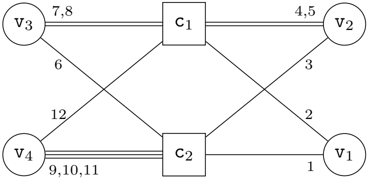
- The method of [Dol14] requires maximization of a multidimensional objective function over a space of dimension 5 to calculate one point of the weight spectral shape function.
- Evaluation of this objective function requires solution of further maximization problems over spaces of dimension equal to 58 for any $q > 2$.

Example: An $R = 1/2$ AR4JA Protograph



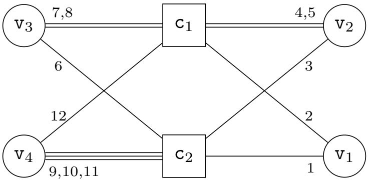
- The proposed method requires solution of a 21×21 system to calculate one point of the weight spectral shape function.
- Use of Lemma 3 reduces this to a 16×16 system.
- Use of the augmented 17×17 system allows solving **directly** for ω^*.

Example: An $R = 1/2$ RJA Protograph



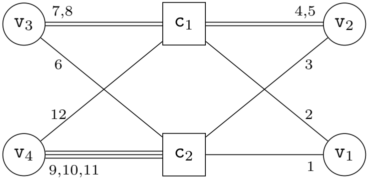
- $n_c = 3$ CNs, $n_v = 4$ VNs, $e = 12$ edges.
- $\mathcal{J}_u = \{1, 2, 3, 4\}$, $\mathcal{J}_p = \{\,\}$, $R = 1/2$.
- The method of [Garr15] requires solution of a 37×37 system of equations to calculate one point of the spectral shape function.

Example: An $R = 1/2$ RJA Protograph



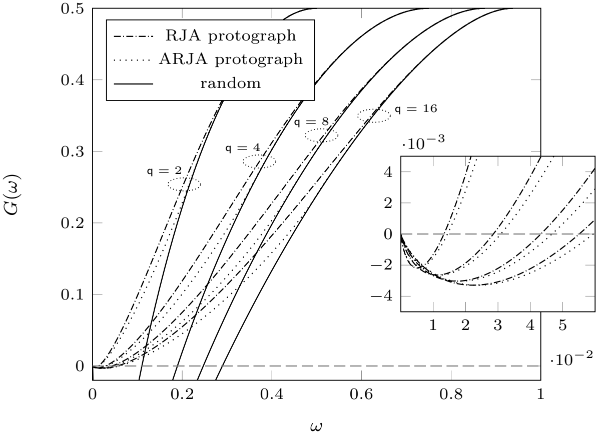
- The method of [DoI14] requires maximization of a multidimensional objective function over a space of dimension 4 to calculate one point of the weight spectral shape function.
- Evaluation of this objective function requires solution of further maximization problems over spaces of dimension equal to 58 for any $q > 2$.

Example: An $R = 1/2$ RJA Protograph



- The proposed method requires solution of a 17×17 system to calculate one point of the weight spectral shape function.
- Use of Lemma 3 reduces this to a 13×13 system.
- Use of the augmented 14×14 system allows solving **directly** for ω^*.

$G(\omega)$ Plots for ARJA and RJA Protographs



- "random": $G_{\mathrm{rand}}(\omega) = \frac{1}{\ln q}\left(h(\omega) + \omega \ln(q-1) - (1-R)\ln q\right)$ (rate-1/2 parity-check ensemble).

ω^* Values for ARJA and RJA Protographs

- Critical fractional codeword weight values for rate-1/2 ARJA and RJA protograph ensembles over GF(q), for $q \in \{2, 4, 8, 16\}$:

q	ω^* (ARJA)	ω^* (RJA)
2	0.014401	0.013316
4	0.030871	0.028576
8	0.046681	0.043253
16	0.059427	0.055104

- In all cases the run-time for a direct calculation of ω^* was approximately equal to 50 ms.

Conclusion

- The method is efficient and exact; it allows solving directly for ω^* (good for ensemble optimization).
- Can be extended to stopping sets, ..., and to GLDPC codes.

- E. Paolini and Mark F. Flanagan, "Efficient and exact evaluation of the weight spectral shape and typical minimum distance of protograph LDPC codes," *IEEE Commun. Lett.*, to appear.
- M. Chiani, G. Liva, B. Matuz, E. Paolini, *Coding for Erasure Channels*. Cambridge University Press, upcoming.