### On the Typicality of the Linear Code Among the LDPC Coset Code Ensemble

Chih-Chun Wang, Prof. S.R. Kulkarni, and Prof. H.V. Poor

{chihw, kulkarni, poor}@princeton.edu.

Princeton University









• Memoryless channels:  $P(d\underline{y}|\underline{x}) = \prod_{i=1}^{n} P(dy_i|x_i)$ 





- Memoryless channels:  $P(d\underline{y}|\underline{x}) = \prod_{i=1}^{n} P(dy_i|x_i)$
- Symmetric channels:  $\exists T : \mathbf{Y} \mapsto \mathbf{Y}$  s.t.  $T^2(y) = y, \forall y \in \mathbf{Y}$ , and  $\mathsf{P}(dy|x=0) = \mathsf{P}(T(dy)|x=1).$



Memoryless channels:  $P(d\underline{y}|\underline{x}) = \prod_{i=1}^{n} P(dy_i|x_i)$ 

- Symmetric channels:  $\exists T : \mathbf{Y} \mapsto \mathbf{Y}$  s.t.  $T^2(y) = y, \forall y \in \mathbf{Y}$ , and  $\mathsf{P}(dy|x=0) = \mathsf{P}(\mathcal{T}(dy)|x=1).$
- Shannon's channel coding theorem: Let  $C = \max_{P_X} \mathsf{E}_{XY} \log \left( \frac{P_{XY}(X,Y)}{P_X(X)P_Y(Y)} \right)$ . Reliable communication requires R < C.





Memoryless channels:  $P(d\underline{y}|\underline{x}) = \prod_{i=1}^{n} P(dy_i|x_i)$ 

- Symmetric channels:  $\exists T : \mathbf{Y} \mapsto \mathbf{Y}$  s.t.  $T^2(y) = y, \forall y \in \mathbf{Y}$ , and  $\mathsf{P}(dy|x=0) = \mathsf{P}(\mathcal{T}(dy)|x=1).$
- Shannon's channel coding theorem: Let  $C = \max_{P_X} \mathsf{E}_{XY} \log \left( \frac{P_{XY}(X,Y)}{P_X(X)P_Y(Y)} \right)$ . Reliable communication requires R < C.
- Memoryless symmetric channels: Capacity-approaching error correcting codes have been constructed, including turbo codes, low-density parity-check (LDPC) codes, irregular RA codes, LT codes, concatenated tree codes, etc.
- Performance: 0.1~1.5dB away from capacity.

#### Ultra high performance on almost all symmetric channels.









Examples: Z-Channels 1 0 1 1 1 0







Examples:

**Z**-Channels



On/Off Keying w. Rayleigh Fading



Examples:

Z-Channels







Exar Z-Ch  $\begin{bmatrix} Majani \& Rumsey 91 \end{bmatrix}$  showed that the ratio between the symmetric mutual information rate and the capacity is lower bounded by  $\frac{e \ln 2}{2} \approx 0.942$ .  $\begin{bmatrix} Shulman \& Feder 04 \end{bmatrix}$  further proved that the absolute difference is upper bounded by 0.011 bit/sym.

- Low-density parity-check codes and the challenges of non-symmetric memoryless channels
  - Codeword-dependent error resiliency

- Low-density parity-check codes and the challenges of non-symmetric memoryless channels
  - Codeword-dependent error resiliency
- Two approaches:
  - The LDPC coset code ensemble
  - Linear LDPC codes with generalized density evolution

- Low-density parity-check codes and the challenges of non-symmetric memoryless channels
  - Codeword-dependent error resiliency
- Two approaches:
  - The LDPC coset code ensemble
  - Linear LDPC codes with generalized density evolution
- The typicality of linear LDPC codes among the coset code ensemble

- Low-density parity-check codes and the challenges of non-symmetric memoryless channels
  - Codeword-dependent error resiliency
- Two approaches:
  - The LDPC coset code ensemble
  - Linear LDPC codes with generalized density evolution
- The typicality of linear LDPC codes among the coset code ensemble
- The convergence rate consideration

- Low-density parity-check codes and the challenges of non-symmetric memoryless channels
  - Codeword-dependent error resiliency
- Two approaches:
  - The LDPC coset code ensemble
  - Linear LDPC codes with generalized density evolution
- The typicality of linear LDPC codes among the coset code ensemble
- The convergence rate consideration
- Applications

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



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





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



**Belief Propagation:** 



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



 $\mathcal{C}^6(d_v, d_c), d_v = 2, d_c = 3$ 

#### **Belief Propagation:**

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



 $\mathcal{C}^6(d_v, d_c), d_v = 2, d_c = 3$ 

**Belief Propagation:** 

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



 $\mathcal{C}^6(d_v, d_c), d_v = 2, d_c = 3$ 

#### **Belief Propagation:**

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



 $\mathcal{C}^6(d_v, d_c), d_v = 2, d_c = 3$ 

**Belief Propagation:** 



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



#### **Belief Propagation:**

(i)  $m_0$ , (ii)  $\Psi_v(m_0, m_1, \cdots, m_{d_v-1})$ , (iii)  $\Psi_c(m_1, \cdots, m_{d_c-1})$ 

For cycle-free networks, the belief propagation works for non-symmetric channels as well.



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



#### **Belief Propagation:**

- For cycle-free networks, the belief propagation works for non-symmetric channels as well.
- By simulation, belief propagation + LDPC codes also have outstanding performance for non-symmetric channels.

























Sym. Chs: Assuming  $\mathbf{x} = \mathbf{0}$ .





$$P^{(l)} = P^{(0)} \otimes \left(Q^{(l-1)}\right)^{\otimes (d_v-1)}$$
$$Q^{(l-1)} = \Gamma^{-1} \left(\left(\Gamma\left(P^{(l-1)}\right)\right)^{\otimes (d_c-1)}\right),$$
### **The Density Evolution**



Coset codes: Any valid codeword x satisfies Ax = s, where A is from the same equiprobable bipartite graph ensemble, and the coset-defining syndrome s is uniformly drawn from {0,1}<sup>n(1-R)</sup>.

• Coset codes: Any valid codeword x satisfies Ax = s, where A is from the same equiprobable bipartite graph ensemble, and the coset-defining syndrome s is uniformly drawn from  $\{0,1\}^{n(1-R)}$ .



- Coset codes: Any valid codeword x satisfies Ax = s, where A is from the same equiprobable bipartite graph ensemble, and the coset-defining syndrome s is uniformly drawn from  $\{0,1\}^{n(1-R)}$ .
- Symmetrizing the non-symmetric channel:



- Coset codes: Any valid codeword x satisfies Ax = s, where A is from the same equiprobable bipartite graph ensemble, and the coset-defining syndrome s is uniformly drawn from  $\{0,1\}^{n(1-R)}$ .
- Symmetrizing the non-symmetric channel:



- Coset codes: Any valid codeword x satisfies Ax = s, where A is from the same equiprobable bipartite graph ensemble, and the coset-defining syndrome s is uniformly drawn from  $\{0,1\}^{n(1-R)}$ .
- Symmetrizing the non-symmetric channel:



- Coset codes: Any valid codeword x satisfies Ax = s, where A is from the same equiprobable bipartite graph ensemble, and the coset-defining syndrome s is uniformly drawn from  $\{0,1\}^{n(1-R)}$ .
- Symmetrizing the non-symmetric channel:





- Coset codes: Any valid codeword x satisfies Ax = s, where A is from the same equiprobable bipartite graph ensemble, and the coset-defining syndrome s is uniformly drawn from  $\{0,1\}^{n(1-R)}$ .
- Symmetrizing the non-symmetric channel:



 $\mathbf{A}\mathbf{\tilde{x}} = \mathbf{A}(\mathbf{x} + \mathbf{b}) = \mathbf{A}\mathbf{x} + \mathbf{A}\mathbf{b} = \mathbf{A}\mathbf{b} = \mathbf{s}$ 

Averaged performance of the LDPC coset code ensemble







strings.





- The difficulty: Maintaining the synchronization of two random strings.
- [Kavčić 03]: Asymptotically, almost all s ∈ {0,1}<sup>n(1-R)</sup> are typical. Namely,

$$\lim_{n\to\infty} \mathsf{P}\left(\mathbf{s}: |p_e(\mathbf{s}) - \mathsf{E}_{\mathbf{s}}\{p_e(\mathbf{s})\}| < \epsilon\right) = 1, \ \forall \epsilon > 0.$$



- The difficulty: Maintaining the synchronization of two random strings.
- [Kavčić 03]: Asymptotically, almost all s ∈ {0,1}<sup>n(1-R)</sup> are typical. Namely,

$$\lim_{n\to\infty} \mathsf{P}\left(\mathbf{s}: |p_e(\mathbf{s}) - \mathsf{E}_{\mathbf{s}}\{p_e(\mathbf{s})\}| < \epsilon\right) = 1, \ \forall \epsilon > 0.$$



- The difficulty: Maintaining the synchronization of two random strings.
- [Kavčić 03]: Asymptotically, almost all  $\mathbf{s} \in \{0, 1\}^{n(1-R)}$  are typical. Namely,

 $\lim_{n\to\infty} \mathsf{P}\left(\mathbf{s}: |p_e(\mathbf{s}) - \mathsf{E}_{\mathbf{s}}\{p_e(\mathbf{s})\}| < \epsilon\right) = 1, \ \forall \epsilon > 0.$ 

Due to their hardware uniformity, linear codes are always the superior choice.





Codeword-dependent performance





Codeword-dependent performance

Codeword Averaging





Codeword-dependent performance

Codeword Averaging

A generalized density evolution.



Codeword-dependent performance

A generalized density evolution.

Codeword Averaging







Codeword-dependent performance

A generalized density evolution.

Codeword Averaging

4

 $\chi_6$ 

 ${x_1x_5x_6:$ 



Codeword-dependent performance

A generalized density evolution.

Averaging the trimmed tree code is not equivalent to averaging the original code.

Codeword Averaging

#### **Perfect Projection Condition**

**Definition 1** (Perfect Projection) The supporting tree  $\mathcal{N}^{2l}$  is perfectly projected, if for any codeword  $\mathbf{x}_t$  of the tree code  $\mathbf{X}_t$ ,

$$\frac{\left|\{\mathbf{x}\in\mathbf{X}:\mathbf{x}|\mathbf{tree}=\mathbf{x}_t\}\right|}{|\mathbf{X}|} = \frac{1}{|\mathbf{X}_t|}.$$

#### **Perfect Projection Condition**

**Definition 1** (Perfect Projection) The supporting tree  $\mathcal{N}^{2l}$  is perfectly projected, if for any codeword  $\mathbf{x}_t$  of the tree code  $\mathbf{X}_t$ ,

$$\frac{\left|\{\mathbf{x}\in\mathbf{X}:\mathbf{x}|\mathbf{tree}=\mathbf{x}_t\}\right|}{|\mathbf{X}|}=\frac{1}{|\mathbf{X}_t|}.$$

In other words, averaging the trimmed tree code is equivalent to averaging over the original code.

#### **Perfect Projection Condition**

**Definition 1** (Perfect Projection) The supporting tree  $\mathcal{N}^{2l}$  is perfectly projected, if for any codeword  $\mathbf{x}_t$  of the tree code  $\mathbf{X}_t$ ,

$$\frac{\left|\{\mathbf{x}\in\mathbf{X}:\mathbf{x}|\mathbf{tree}=\mathbf{x}_t\}\right|}{|\mathbf{X}|} = \frac{1}{|\mathbf{X}_t|}.$$

In other words, averaging the trimmed tree code is equivalent to averaging over the original code. We then have

$$P^{(l)}(x) := \left\langle P^{(l)}(\mathbf{x}) \right\rangle_{\{\mathbf{x} \in \mathbf{X} : \mathbf{x}|_{0} = x\}} = \left\langle P^{(l)}(\mathbf{x}_{t}) \right\rangle_{\{\mathbf{x}_{t} \in \mathbf{X}_{t} : \mathbf{x}_{t}|_{0} = x\}},$$
$$p_{e}^{(l)} = \frac{1}{2} \left( \int_{m = -\infty}^{0} P^{(l)}(\mathbf{0})(dm) + \int_{m = -\infty}^{0} P^{(l)}(\mathbf{1})(dm) \right)$$

#### **New Iterative Formula for DE**



 $x = 0, x_1 x_2 = 00, 11$  $x = 1, x_1 x_2 = 01, 10$ 

$$\forall x \in \{0,1\}, \ P^{(l)}(x) = P^{(0)}(x) \otimes \left(Q^{(l-1)}(x)\right)^{\otimes (d_v-1)}$$
$$Q^{(l-1)}(x) = \Gamma^{-1}\left(\frac{1}{2^{d_c-2}}\sum_{\mathbf{x}^1 \in \mathbf{X}^1(x)} \bigotimes_{v=1}^{d_c-1} \Gamma\left(P^{(l-1)}(x_v)\right)\right)$$



#### **New Iterative Formula for DE**



 $x = 0, x_1 x_2 = 00, 11$  $x = 1, x_1 x_2 = 01, 10$ 

$$\begin{aligned} \forall x \in \{0,1\}, \ P^{(l)}(x) &= P^{(0)}(x) \otimes \left(Q^{(l-1)}(x)\right)^{\otimes (d_v - 1)} \\ Q^{(l-1)}(x) &= \Gamma^{-1}\left(\frac{1}{2^{d_c - 2}} \sum_{\mathbf{x}^1 \in \mathbf{X}^1(x)} \bigotimes_{v=1}^{d_c - 1} \Gamma\left(P^{(l-1)}(x_v)\right)\right) \\ &= \Gamma^{-1}\left(\left(\Gamma\left(\frac{P^{(l-1)}(0) + P^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)} \\ &+ (-1)^x \left(\Gamma\left(\frac{P^{(l-1)}(0) - P^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)}\right) \end{aligned}$$

C-C. Wang, S.R. Kulkarni, and H.V. Poor with Princeton University – p.11/27

Linear code ensemble:

$$\begin{split} P_{linear}^{(l)}(x) &= P_{linear}^{(0)}(x) \otimes \left(Q_{linear}^{(l-1)}(x)\right)^{\otimes (d_v - 1)} \\ Q_{linear}^{(l-1)}(x) &= \Gamma^{-1} \left( \left(\Gamma \left(\frac{P_{linear}^{(l-1)}(0) + P_{linear}^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)} \\ &+ (-1)^x \left(\Gamma \left(\frac{P_{linear}^{(l-1)}(0) - P_{linear}^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)} \right) \\ \left\langle P_{linear}^{(l)} \right\rangle &= \frac{P_{linear}^{(l)}(0) + P_{linear}^{(l)}(1)}{2}. \end{split}$$

Linear code ensemble:

$$\begin{split} P_{linear}^{(l)}(x) &= P_{linear}^{(0)}(x) \otimes \left(Q_{linear}^{(l-1)}(x)\right)^{\otimes (d_v - 1)} \\ Q_{linear}^{(l-1)}(x) &= \Gamma^{-1} \left( \left(\Gamma \left(\frac{P_{linear}^{(l-1)}(0) + P_{linear}^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)} \\ &+ (-1)^x \left(\Gamma \left(\frac{P_{linear}^{(l-1)}(0) - P_{linear}^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)} \right) \\ \left\langle P_{linear}^{(l)} \right\rangle &= \frac{P_{linear}^{(l)}(0) + P_{linear}^{(l)}(1)}{2}. \end{split}$$

Coset code ensemble:

$$P_{coset}^{(0)} = \frac{P_{linear}^{(0)}(0) + P_{linear}^{(0)}(1)}{2}$$

$$P_{coset}^{(l)} = P_{coset}^{(0)} \otimes \left(Q_{coset}^{(l-1)}\right)^{\otimes (d_v - 1)}$$

$$Q_{coset}^{(l-1)} = \Gamma^{-1} \left(\left(\Gamma\left(P_{coset}^{(l-1)}\right)\right)^{\otimes (d_c - 1)}$$

- **Symmetry**:
- **•** Monotonicity:





- **•** Symmetry:
  - For all  $l \in \mathbb{N}$ , both  $\left\langle P_{linear}^{(l)} \right\rangle$  and  $P_{coset}^{(l)}$  are symmetric.
- **•** Monotonicity:





- **Symmetry**:
  - For all  $l \in \mathbb{N}$ , both  $\langle P_{linear}^{(l)} \rangle$  and  $P_{coset}^{(l)}$  are symmetric.
- Monotonicity: Let  $p_{e,linear}^{(l)} = \int_{m=\infty}^{0^{-}} \left\langle P_{linear}^{(l)} \right\rangle (dm)$   $p_{e,coset}^{(l)} = \int_{m=\infty}^{0^{-}} P_{coset}^{(l)} (dm).$

Stability Conditions:

- **Symmetry**:
  - For all  $l \in \mathbb{N}$ , both  $\langle P_{linear}^{(l)} \rangle$  and  $P_{coset}^{(l)}$  are symmetric.
- Monotonicity: Let  $p_{e,linear}^{(l)} = \int_{m=\infty}^{0^{-}} \left\langle P_{linear}^{(l)} \right\rangle (dm)$   $p_{e,coset}^{(l)} = \int_{m=\infty}^{0^{-}} P_{coset}^{(l)} (dm).$ 
  - Both  $p_{e,linear}^{(l)}$  and  $p_{e,coset}^{(l)}$  are monotonically decreasing w.r.t. *l*.
- Stability Conditions:

- **Symmetry**:
  - For all  $l \in \mathbb{N}$ , both  $\langle P_{linear}^{(l)} \rangle$  and  $P_{coset}^{(l)}$  are symmetric.
- Monotonicity: Let  $p_{e,linear}^{(l)} = \int_{m=\infty}^{0^{-}} \left\langle P_{linear}^{(l)} \right\rangle (dm)$   $p_{e,coset}^{(l)} = \int_{m=\infty}^{0^{-}} P_{coset}^{(l)} (dm).$ 
  - Both  $p_{e,linear}^{(l)}$  and  $p_{e,coset}^{(l)}$  are monotonically decreasing w.r.t. *l*.
- **Stability Conditions**: Let  $\lambda(x) := \sum \lambda_k x^{k-1}$  and  $\rho(x) := \sum \rho_k x^{k-1}$  denote the edge degree distribution poly., and  $\langle CB^{(0)} \rangle = \int e^{-\frac{m}{2}} \langle P_{linear}^{(0)} \rangle (dm) = \int e^{\frac{m}{2}} P_{coset}^{(0)}(dm).$

- **Symmetry**:
  - For all  $l \in \mathbb{N}$ , both  $\langle P_{linear}^{(l)} \rangle$  and  $P_{coset}^{(l)}$  are symmetric.
- Monotonicity: Let  $p_{e,linear}^{(l)} = \int_{m=\infty}^{0^{-}} \left\langle P_{linear}^{(l)} \right\rangle (dm)$   $p_{e,coset}^{(l)} = \int_{m=\infty}^{0^{-}} P_{coset}^{(l)} (dm).$ 
  - Both  $p_{e,linear}^{(l)}$  and  $p_{e,coset}^{(l)}$  are monotonically decreasing w.r.t. *l*.
- Stability Conditions: Let \(\lambda(x)) := \sum \lambda\_k x^{k-1}\) and \(\rho(x)) := \sum \rho\_k x^{k-1}\) denote the edge degree distribution poly., and \(\lambda(CB^{(0)}\) = \int e^{-\frac{m}{2}} \langle P^{(0)}\_{linear} \rangle (dm) = \int e^{\frac{m}{2}} P^{(0)}\_{coset}(dm).\)
  Having the same stability conditions: \(\lambda(CB^{(0)}\) \rightarrow \frac{1}{\lambda\_2\rho'(1)}\).

Linear codes:



Linear codes:



Their stability conditions and many other properties coincide.

Linear codes:



Their stability conditions and many other properties coincide.

Nearly identical performance under Monte-Carlo simulations.

Linear codes:



Their stability conditions and many other properties coincide.

Nearly identical performance under Monte-Carlo simulations.
# **A Short Answer**

Not equivalent:

$$P_{linear}^{(l)}(x) = P_{linear}^{(0)}(x) \otimes \left(Q_{linear}^{(l-1)}(x)\right)^{\otimes (d_v - 1)}$$

$$Q_{linear}^{(l-1)}(x) = \Gamma^{-1} \left( \left(\Gamma \left(\frac{P_{linear}^{(l-1)}(0) + P_{linear}^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)} + (-1)^x \left(\Gamma \left(\frac{P_{linear}^{(l-1)}(0) - P_{linear}^{(l-1)}(1)}{2}\right)\right)^{\otimes (d_c - 1)} \right)$$



# **A Short Answer**

Not equivalent:



Number of Iterations

# **Typicality of Linear LDPC Codes**

$(\lambda, \rho)$	$(x^2, x^3)$	$(x^2, x^5)$	$(x^2, 0.5x^2 + 0.5x^3)$	$(x^2, 0.5x^4 + 0.5x^5)$
Linear	0.4540	0.2305	0.5888	0.2689
Coset	0.4527	0.2304	0.5908	0.2690

# **Typicality of Linear LDPC Codes**

$(\lambda, \rho)$	$(x^2, x^3)$	$(x^2, x^5)$	$(x^2, 0.5x^2 + 0.5x^3)$	$(x^2, 0.5x^4 + 0.5x^5)$
Linear	0.4540	0.2305	0.5888	0.2689
Coset	0.4527	0.2304	0.5908	0.2690



# **Typicality of Linear LDPC Codes**

$(\lambda, \rho)$	$(x^2, x^3)$	$(x^2, x^5)$	$(x^2, 0.5x^2 + 0.5x^3)$	$(x^2, 0.5x^4 + 0.5x^5)$
Linear	0.4540	0.2305	0.5888 % ↑ 0.17%	0.2689
Coset	0.4527	0.2304	0.5908	0.2690

**Theorem 1** (Main Theorem) Consider non-symmetric channels and a fixed pair of degree polynomials  $\lambda$  and  $\rho$ . The shifted check node polynomial is denoted by  $\rho_{\Delta} = x^{\Delta} \cdot \rho$ . Let  $P_{linear}^{(l)}$  and  $P_{coset}^{(l)}$  denote the evolved densities of the linear and coset code ensemble with degrees  $(\lambda, \rho_{\Delta})$ . Then,  $\forall l_0 \in \mathbb{N}, \lim_{\Delta \to \infty} \langle P_{linear}^{(l_0)} \rangle \stackrel{\mathcal{D}}{=} P_{coset}^{(l_0)}$  in distribution, with the convergence rate being  $\mathcal{O}(\text{const}^{\Delta})$  for some const < 1.

# Intuition

• Consider the 1st check node iteration. Suppose for all possible  $\{P_{linear}^{(0)}(x)\}, Q_{linear}^{(0)}(0) = Q_{linear}^{(0)}(1) = Q_{coset}^{(0)}$ . Then

$$P_{linear}^{(1)}(x) = P_{linear}^{(0)}(x) \otimes \left(Q_{coset}^{(0)}\right)^{\otimes (d_v - 1)}$$

$$\left\langle P_{linear}^{(1)} \right\rangle = \frac{P_{linear}^{(0)}(0) + P_{linear}^{(0)}(1)}{2} \otimes \left(Q_{coset}^{(0)}\right)^{\otimes (d_v - 1)} = P_{coset}^{(1)}.$$

# Intuition

• Consider the 1st check node iteration. Suppose for all possible  $\{P_{linear}^{(0)}(x)\}, Q_{linear}^{(0)}(0) = Q_{linear}^{(0)}(1) = Q_{coset}^{(0)}$ . Then

$$P_{linear}^{(1)}(x) = P_{linear}^{(0)}(x) \otimes \left(Q_{coset}^{(0)}\right)^{\otimes (d_v - 1)}$$

$$\left\langle P_{linear}^{(1)} \right\rangle = \frac{P_{linear}^{(0)}(0) + P_{linear}^{(0)}(1)}{2} \otimes \left(Q_{coset}^{(0)}\right)^{\otimes (d_v - 1)} = P_{coset}^{(1)}.$$

• Furthermore,  $Q_{linear}^{(1)}(0) = Q_{linear}^{(1)}(1) = Q_{coset}^{(1)}$ .

# Intuition

• Consider the 1st check node iteration. Suppose for all possible  $\{P_{linear}^{(0)}(x)\}, Q_{linear}^{(0)}(0) = Q_{linear}^{(0)}(1) = Q_{coset}^{(0)}$ . Then

$$P_{linear}^{(1)}(x) = P_{linear}^{(0)}(x) \otimes \left(Q_{coset}^{(0)}\right)^{\otimes (d_v - 1)}$$

$$\left\langle P_{linear}^{(1)} \right\rangle = \frac{P_{linear}^{(0)}(0) + P_{linear}^{(0)}(1)}{2} \otimes \left(Q_{coset}^{(0)}\right)^{\otimes (d_v - 1)} = P_{coset}^{(1)}.$$

- Furthermore,  $Q_{linear}^{(1)}(0) = Q_{linear}^{(1)}(1) = Q_{coset}^{(1)}$ .
- Since the iterative equations of DE are continuous, we need only to prove that for all possible  $\left\{P_{linear}^{(0)}(x)\right\}$ ,

$$\lim_{\Delta \to \infty} Q_{linear}^{(0)}(0) \stackrel{\mathcal{D}}{=} \lim_{\Delta \to \infty} Q_{linear}^{(0)}(1) \stackrel{\mathcal{D}}{=} Q_{coset}^{(0)}$$

• 
$$m = \log \frac{\mathsf{P}(X=0|Y)}{\mathsf{P}(X=1|Y)}$$
.



• 
$$m = \log \frac{\mathsf{P}(X=0|Y)}{\mathsf{P}(X=1|Y)}$$
.

• 
$$\gamma(m) = (1_{\{m < 0\}}, \log \operatorname{cot} \left| \frac{m}{2} \right|)$$

• 
$$m = \log \frac{\mathsf{P}(X=0|Y)}{\mathsf{P}(X=1|Y)}$$
.

• 
$$\gamma(m) = (1_{\{m < 0\}}, \log \operatorname{cot} \left| \frac{m}{2} \right|)$$

•  $P_{linear}^{(0)}(x)(dm) \mapsto P'_x(d\gamma) \text{ and } Q_{linear}^{(0)}(x)(dm) \mapsto Q'_x(d\gamma).$ 

• 
$$m = \log \frac{\mathsf{P}(X=0|Y)}{\mathsf{P}(X=1|Y)}$$
.

• 
$$\gamma(m) = (1_{\{m < 0\}}, \log \operatorname{cot} \left|\frac{m}{2}\right|)$$

- $P_{linear}^{(0)}(x)(dm) \mapsto P'_x(d\gamma) \text{ and } Q_{linear}^{(0)}(x)(dm) \mapsto Q'_x(d\gamma).$
- The characteristic function:  $\Phi_P(\lambda_1, \lambda_2) = \mathsf{E}(-1)^{\lambda_1 \gamma_1} e^{i\lambda_2 \gamma_2}$ .

• 
$$m = \log \frac{\mathsf{P}(X=0|Y)}{\mathsf{P}(X=1|Y)}$$
.

• 
$$\gamma(m) = (1_{\{m < 0\}}, \log \operatorname{cot} \left| \frac{m}{2} \right|)$$

- $P_{linear}^{(0)}(x)(dm) \mapsto P'_x(d\gamma) \text{ and } Q_{linear}^{(0)}(x)(dm) \mapsto Q'_x(d\gamma).$
- The characteristic function:  $\Phi_P(\lambda_1, \lambda_2) = \mathsf{E}(-1)^{\lambda_1 \gamma_1} e^{i\lambda_2 \gamma_2}$ .
- By induction,

$$\Phi_{Q'_{0}}(\lambda_{1},\lambda_{2}) - \Phi_{Q'_{1}}(\lambda_{1},\lambda_{2}) = 2\left(\frac{\Phi_{P'_{0}}(\lambda_{1},\lambda_{2}) - \Phi_{P'_{1}}(\lambda_{1},\lambda_{2})}{2}\right)^{\Delta}$$

• 
$$m = \log \frac{\mathsf{P}(X=0|Y)}{\mathsf{P}(X=1|Y)}$$
.

• 
$$\gamma(m) = (1_{\{m < 0\}}, \log \operatorname{cot} \left|\frac{m}{2}\right|)$$

- $P_{linear}^{(0)}(x)(dm) \mapsto P'_x(d\gamma) \text{ and } Q_{linear}^{(0)}(x)(dm) \mapsto Q'_x(d\gamma).$
- The characteristic function:  $\Phi_P(\lambda_1, \lambda_2) = \mathsf{E}(-1)^{\lambda_1 \gamma_1} e^{i\lambda_2 \gamma_2}$ .
- By induction,

$$\Phi_{Q_0'}(\lambda_1, \frac{\lambda_2}{\Delta}) - \Phi_{Q_1'}(\lambda_1, \frac{\lambda_2}{\Delta}) = 2\left(\frac{\Phi_{P_0'}(\lambda_1, \frac{\lambda_2}{\Delta}) - \Phi_{P_1'}(\lambda_1, \frac{\lambda_2}{\Delta})}{2}\right)^{\Delta}$$

٨

• 
$$m = \log \frac{\mathsf{P}(X=0|Y)}{\mathsf{P}(X=1|Y)}$$
.

• 
$$\gamma(m) = (1_{\{m < 0\}}, \log \operatorname{cot} \left|\frac{m}{2}\right|)$$

- $P_{linear}^{(0)}(x)(dm) \mapsto P'_x(d\gamma) \text{ and } Q_{linear}^{(0)}(x)(dm) \mapsto Q'_x(d\gamma).$
- The characteristic function:  $\Phi_P(\lambda_1, \lambda_2) = \mathsf{E}(-1)^{\lambda_1 \gamma_1} e^{i\lambda_2 \gamma_2}$ .
- By induction,

$$\Phi_{Q'_0}(\lambda_1, \frac{\lambda_2}{\Delta}) - \Phi_{Q'_1}(\lambda_1, \frac{\lambda_2}{\Delta}) = 2\left(\frac{\Phi_{P'_0}(\lambda_1, \frac{\lambda_2}{\Delta}) - \Phi_{P'_1}(\lambda_1, \frac{\lambda_2}{\Delta})}{2}\right)^{\Delta}$$

Solution By Taylor's expansion, the RHS converges to zero for all  $\lambda_1, \lambda_2$ and the convergence rate is exponential.

## **The Weak Convergence**



### **Typicality in Terms of the Decod**able Threshold

Z-Channels:



### **Typicality in Terms of the Decodable Threshold**

Z-Channels:

**Corollary 1** (Typicality Results for Z-Channels) For any  $\epsilon > 0$ , there exists a  $\Delta \in \mathbb{N}$  such that

$$\left|p_{1\to 0,linear}^* - p_{1\to 0,coset}^*\right| < \epsilon.$$

$$p_{1 \rightarrow 0, linear}^* > p_{1 \rightarrow 0, coset}^* - \epsilon := p_{temp}$$



$$p_{1 \rightarrow 0, linear}^* > p_{1 \rightarrow 0, coset}^* - \epsilon := p_{temp}$$



Def: 
$$\exists l_0, P_{coset}^{(l_0)}$$
 is in its stability region  $\Leftrightarrow \lim_{l \to \infty} p_{e,coset}^{(l)} = 0.$ 



$$p_{1 \rightarrow 0, linear}^* > p_{1 \rightarrow 0, coset}^* - \epsilon := p_{temp}$$

Def:  $\exists l_0, P_{coset}^{(l_0)}$  is in its stability region  $\Leftrightarrow \lim_{l \to \infty} p_{e,coset}^{(l)} = 0.$ 

■ By definition, when  $p_{1\to 0} = p_{temp}$ ,  $\exists l_0$  such that after  $l_0$  iterations,  $P_{coset}^{(l_0)}$  is in its stability region, which is an open set.



$$p_{1 \rightarrow 0, linear}^* > p_{1 \rightarrow 0, coset}^* - \epsilon := p_{temp}$$

Def:  $\exists l_0, P_{coset}^{(l_0)}$  is in its stability region  $\Leftrightarrow \lim_{l \to \infty} p_{e,coset}^{(l)} = 0.$ 

- By definition, when  $p_{1\to 0} = p_{temp}$ ,  $\exists l_0$  such that after  $l_0$  iterations,  $P_{coset}^{(l_0)}$  is in its stability region, which is an open set.
- Note: The stability region is continuous w.r.t. weak convergence. By Theorem 1, there exists a  $\Delta \in \mathbb{N}$  such that  $\left\langle P_{linear}^{(l_0)} \right\rangle$  is also in the stability region of the coset code ensemble.



$$p_{1 \rightarrow 0, linear}^* > p_{1 \rightarrow 0, coset}^* - \epsilon := p_{temp}$$

Def:  $\exists l_0, P_{coset}^{(l_0)}$  is in its stability region  $\Leftrightarrow \lim_{l \to \infty} p_{e,coset}^{(l)} = 0.$ 

- By definition, when  $p_{1\to 0} = p_{temp}$ ,  $\exists l_0$  such that after  $l_0$  iterations,  $P_{coset}^{(l_0)}$  is in its stability region, which is an open set.
- Note: The stability region is continuous w.r.t. weak convergence. By Theorem 1, there exists a  $\Delta \in \mathbb{N}$  such that  $\left\langle P_{linear}^{(l_0)} \right\rangle$  is also in the stability region of the coset code ensemble.
- Note: The stability regions of the coset code ensembles and the linear codes are identical.

$$p_{1 \rightarrow 0, linear}^* > p_{1 \rightarrow 0, coset}^* - \epsilon := p_{temp}$$

Def:  $\exists l_0, P_{coset}^{(l_0)}$  is in its stability region  $\Leftrightarrow \lim_{l \to \infty} p_{e,coset}^{(l)} = 0.$ 

- By definition, when  $p_{1\to 0} = p_{temp}$ ,  $\exists l_0$  such that after  $l_0$  iterations,  $P_{coset}^{(l_0)}$  is in its stability region, which is an open set.
- Note: The stability region is continuous w.r.t. weak convergence. By Theorem 1, there exists a  $\Delta \in \mathbb{N}$  such that  $\left\langle P_{linear}^{(l_0)} \right\rangle$  is also in the stability region of the coset code ensemble.
- Note: The stability regions of the coset code ensembles and the linear codes are identical.
- By the definition of the stability condition,  $\lim_{l\to\infty} p_{e,linear}^{(l)} = 0$ .

### **Typicality in Terms of the Decodable Threshold**

Z-Channels:

**Corollary 1** (Typicality Results for Z-Channels) For any  $\epsilon > 0$ , there exists a  $\Delta \in \mathbb{N}$  such that

$$\left|p_{1\to 0,linear}^* - p_{1\to 0,coset}^*\right| < \epsilon.$$

## **Typicality in Terms of the Decodable Threshold**

Z-Channels:

$$0 \longrightarrow 0 \qquad p_{1\to 0}^* \lim_{l\to 0, linear} := \sup \left\{ p_{1\to 0} > 0 : \lim_{l\to\infty} p_{e,linear}^{(l)} = 0 \right\}$$
  
$$1 \longrightarrow 1 \qquad \text{and} \ p_{1\to 0,coset}^* := \sup \left\{ p_{1\to 0} > 0 : \lim_{l\to\infty} p_{e,coset}^{(l)} = 0 \right\}.$$

**Corollary 1** (Typicality Results for Z-Channels) For any  $\epsilon > 0$ , there exists a  $\Delta \in \mathbb{N}$  such that

$$\left| p_{1 \to 0, linear}^* - p_{1 \to 0, coset}^* \right| < \epsilon.$$

Similar corollaries can be easily derived for other types of channel models.

• Exponential convergence rate  $\mathcal{O}(\text{const}^{\Delta})$ : The thresholds are nearly identical (the discrepancy is < 0.05%) when  $d_c \ge 6$ .

- Exponential convergence rate  $\mathcal{O}(\text{const}^{\Delta})$ : The thresholds are nearly identical (the discrepancy is < 0.05%) when  $d_c \ge 6$ .
- Revisit the check node iteration:

- Exponential convergence rate  $\mathcal{O}(\text{const}^{\Delta})$ : The thresholds are nearly identical (the discrepancy is < 0.05%) when  $d_c \ge 6$ .
- Revisit the check node iteration:
  - Consider a check node of degree 10000.

- Exponential convergence rate  $\mathcal{O}(\text{const}^{\Delta})$ : The thresholds are nearly identical (the discrepancy is < 0.05%) when  $d_c \ge 6$ .
- Revisit the check node iteration:
  - Consider a check node of degree 10000.
  - All information will be erased after the check node, and it is equivalent to an erasure channel.

$$\lim_{\Delta \to \infty} Q_{linear}^{(1)}(0) \stackrel{\mathcal{D}}{=} \lim_{\Delta \to \infty} Q_{linear}^{(1)}(1) \stackrel{\mathcal{D}}{=} \lim_{\Delta \to \infty} Q_{coset}^{(1)} = \delta_0$$

- Exponential convergence rate  $\mathcal{O}(\text{const}^{\Delta})$ : The thresholds are nearly identical (the discrepancy is < 0.05%) when  $d_c \ge 6$ .
- Revisit the check node iteration:
  - Consider a check node of degree 10000.
  - All information will be erased after the check node, and it is equivalent to an erasure channel.

$$\lim_{\Delta \to \infty} Q_{linear}^{(1)}(0) \stackrel{\mathcal{D}}{=} \lim_{\Delta \to \infty} Q_{linear}^{(1)}(1) \stackrel{\mathcal{D}}{=} \lim_{\Delta \to \infty} Q_{coset}^{(1)} = \delta_0$$

• No error correcting capability.  $p_{1\to 0,linear}^* = p_{1\to,coset}^* = 0.$ 

- Exponential convergence rate  $\mathcal{O}(\text{const}^{\Delta})$ : The thresholds are nearly identical (the discrepancy is < 0.05%) when  $d_c \ge 6$ .
- Revisit the check node iteration:
  - Consider a check node of degree 10000.
  - All information will be erased after the check node, and it is equivalent to an erasure channel.

$$\lim_{\Delta \to \infty} Q_{linear}^{(1)}(0) \stackrel{\mathcal{D}}{=} \lim_{\Delta \to \infty} Q_{linear}^{(1)}(1) \stackrel{\mathcal{D}}{=} \lim_{\Delta \to \infty} Q_{coset}^{(1)} = \delta_0$$

- No error correcting capability.  $p_{1\to 0,linear}^* = p_{1\to,coset}^* = 0.$
- We have proved that the convergence rate is  $\mathcal{O}\left(\frac{1}{\Delta}\right)$ .

## **The Weak Convergence**



## Comparisons

Linear codes:



[Kavčić 03]: Asymptotically, almost all  $\mathbf{s} \in \{0, 1\}^{n(1-R)}$  are typical.

C-C. Wang, S.R. Kulkarni, and H.V. Poor with Princeton University – p.25/27

# Comparisons

Linear codes:



- [Kavčić 03]: Asymptotically, almost all  $\mathbf{s} \in \{0, 1\}^{n(1-R)}$  are typical.
- Our results can be viewed as a complementing theorem explicitly describing the typicality of individual s (including linear codes, s = 0, as a special case).

# Comparisons

Linear codes:



- [Kavčić 03]: Asymptotically, almost all  $\mathbf{s} \in \{0, 1\}^{n(1-R)}$  are typical.
- Our results can be viewed as a complementing theorem explicitly describing the typicality of individual s (including linear codes, s = 0, as a special case).
- Not much improvement left for choosing the optimal s.


On a solid basis to interchangeably use the linear codes and the coset code ensemble when  $d_c$  is of moderate size.

# **Applications**

On a solid basis to interchangeably use the linear codes and the coset code ensemble when  $d_c$  is of moderate size.

Analysis: Use the fast density evolution (for coset codes) or the EXIT chart to optimize the degree distribution of linear codes for non-symmetric channels.

# **Applications**

On a solid basis to interchangeably use the linear codes and the coset code ensemble when  $d_c$  is of moderate size.

- Analysis: Use the fast density evolution (for coset codes) or the EXIT chart to optimize the degree distribution of linear codes for non-symmetric channels.
- Finite code simulation: The codeword-averaged performance of linear codes vs. the all-zero codeword performance of coset codes.

# **Applications**

On a solid basis to interchangeably use the linear codes and the coset code ensemble when  $d_c$  is of moderate size.

- Analysis: Use the fast density evolution (for coset codes) or the EXIT chart to optimize the degree distribution of linear codes for non-symmetric channels.
- Finite code simulation: The codeword-averaged performance of linear codes vs. the all-zero codeword performance of coset codes.
- Implementation: Use solely linear codes.



#### Non-symmetric channels

- Non-symmetric channels
- Linear codes vs. the coset code ensemble



- Non-symmetric channels
- Linear codes vs. the coset code ensemble
- Convergence in distribution with respect to the check node degree  $d_c$

- Non-symmetric channels
- Linear codes vs. the coset code ensemble
- Convergence in distribution with respect to the check node degree  $d_c$
- Typicality results on Z channels: < 0.05% when  $d_c \ge 6$



- Non-symmetric channels
- Linear codes vs. the coset code ensemble
- Convergence in distribution with respect to the check node degree  $d_c$
- Typicality results on Z channels: < 0.05% when  $d_c \ge 6$
- Analysis, simulations, and implementations