On the Equivalence between Pre-transformed and Parity-check Monomial Codes

Yuanxin Guo*[1], Zihan Tang[2], Bin Li[2]

1: Wireless Technology Laboratory, Huawei Technologies & The Chinese University of Hong Kong, Shenzhen
2: Wireless Technology Laboratory, Huawei Technologies

Highlights

- **All pre-transformed monomial codes can be regarded as parity-check monomial codes, vice versa.**
- Algorithm: reduce any *pre-transformation* to a *parity-check transformation*
- Pre-transformation preserves the code distance for *decreasing monomial codes*.
- Pre-transformation reduce #. min. distance codewords for certain monomial codes.

Pre-transformed monomial codes

- **Monomial codes**: For some subset $\mathcal{F}$ of monomials over n variables,
$$\mathcal{C}(\mathcal{F}) = \text{span}\{(f(\boldsymbol{u}))_{\boldsymbol{u}\in\mathbb{F}_2^n} : f \in \mathcal{F}\} \qquad (1)$$
is the *monomial code* generated by $\mathcal{F}$.
- **Matrix form**: The evaluation vectors of monomials $f(\boldsymbol{u})_{\boldsymbol{u}\in\mathbb{F}_2^n}$ and the rows in $\boldsymbol{H}_N = \left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right]^{\otimes n}$ has a 1-1 correspondence [2]. Generally, a monomial code has the form:
$$\mathcal{C} := \{\boldsymbol{c} = \boldsymbol{u}\boldsymbol{H}_N : u_j = 0 \text{ if } j \notin \mathcal{I}\}, \qquad (2)$$
where $\mathcal{I} \subset [N]$ is the *information set* of $\mathcal{C}$.
Lemma. *RM codes and polar codes are monomial codes.*
- **Pre-transformed monomial code [3]**: Given monomial code (2), the code
$$\mathcal{C}_T := \{\boldsymbol{c} = \boldsymbol{u}\boldsymbol{T}\boldsymbol{H}_N : u_j = 0 \text{ if } j \notin \mathcal{I}\} \qquad (3)$$
is the *pre-transformed code* of $\mathcal{C}$ by $\boldsymbol{T}$, where
$$\boldsymbol{T} \in \mathcal{T}_N = \{\boldsymbol{A} \in \mathbb{F}_2^{n\times n} : A_{i,i} = 1,\ A_{i,j} = 0,\ \forall i < j\}$$

Contact Information

- Yuanxin Guo: yuanxinguo@link.cuhk.edu.cn
- Zihan Tang: tangzihan1@huawei.com
- Bin Li: binli.binli@huawei.com

Equivalence between parity-check and pre-transformation

- **Parity-check monomial codes**: for code (2), a *parity-check equation* of bit $j \in \mathcal{I}^C = [N] \setminus \mathcal{I}$ for a bit sequence $\boldsymbol{u} \in \mathbb{F}_2^N$ takes the form
$$u_j \oplus \bigoplus_{i\in\mathcal{I}_j} u_i = 0,\ \mathcal{I}_j \subset ([j-1] \cap \mathcal{I}).$$
This changes a *frozen bit* into a *parity bit*. A *parity-check monomial code* of $\mathcal{C}$ takes the form
$$\tilde{\mathcal{C}} := \{\boldsymbol{c} = \boldsymbol{u}\boldsymbol{H}_N : u_j \oplus \bigoplus_{i\in\mathcal{I}_j} u_i = 0 \text{ if } j \notin \mathcal{I}\}$$
- **Parity-check as pre-transformation**: construct $\boldsymbol{S}$ such that $S_{i,j} = 1$ iff $i = j$ or $(i,j) \in \mathcal{I}_j \times \mathcal{I}^C$. Then $\boldsymbol{S} \in \mathcal{T}_N$ and $\tilde{\mathcal{C}} = \mathcal{C}_S$.

A parity-check of $\mathcal{C}$ can be regarded as a pre-transformation of $\mathcal{C}$.

- Define $\mathcal{S}_\mathcal{C} \subset \mathcal{T}_N$ to be the set of *parity-check transform matrices* w.r.t. code $\mathcal{C}$:
$$\mathcal{S}_\mathcal{C} = \{\boldsymbol{A} \in \mathcal{T}_N : A_{i,j} = 0,\ \forall i < j,\ (i \in \mathcal{I}^C \text{ or } j \in \mathcal{I})\}$$
A matrix $\boldsymbol{S} \in \mathcal{S}_\mathcal{C}$ defines a parity-check of code $\mathcal{C}$.
- **Theorem**. *Given length-N monomial code $\mathcal{C}$, For any $\boldsymbol{T} \in \mathcal{T}_N$, $\exists\, \boldsymbol{S} \in \mathcal{S}_\mathcal{C}$ such that $\mathcal{C}_T = \mathcal{C}_S$.*
- **Algorithm**:

Require: $\boldsymbol{T} \in \mathcal{T}_N$.
Ensure: $\boldsymbol{S} \in \mathcal{S}_\mathcal{C}$ s.t. $\mathcal{C}_T = \mathcal{C}_S$.
for $i \in \mathcal{I}^C$ **do**
  $\boldsymbol{t}^{(i)}$ (i-th row of $\boldsymbol{T}$) $\leftarrow \boldsymbol{e}_i$ (i-th unit vector)
Initialize $\boldsymbol{U} \leftarrow \boldsymbol{I}_N$ ($N \times N$ identity matrix)
for $i \in \mathcal{I}$ **do**
  $\boldsymbol{u}^{(i)} \leftarrow \boldsymbol{t}^{(i)} \wedge (j \in \mathcal{I})_{j=1}^n$ ($\wedge$: logical AND)
$\boldsymbol{S} = \boldsymbol{U} \setminus \boldsymbol{T}$ (solve $\boldsymbol{U}\boldsymbol{S} = \boldsymbol{T}$)

A pre-transformation of $\mathcal{C}$ can be regarded as a parity-check of $\mathcal{C}$.

- **Remark**: Usually, $|\mathcal{S}_\mathcal{C}| << |\mathcal{T}_N|$.
e.g. For (32, 16)-RM codes $\mathcal{R}(5, 2)$, $|\mathcal{T}| = 2^{496}$, whereas $|\mathcal{S}_\mathcal{C}| = 2^{35}$.

Minimum distance

- **Pre-transformation increases distance**: for any length-N monomial code $\mathcal{C}$ and $\boldsymbol{T} \in \mathcal{T}_N$, $d(\mathcal{C}) \le d(\mathcal{C}_T)$ [3].
- **Decreasing monomial codes** [2]: impose order '$\preceq$' on monomials over n variables. Code (1) is *decreasing* if $f \in \mathcal{F},\ g \preceq f \Rightarrow g \in \mathcal{F}$.
Lemma. *RM codes and polar codes are* decreasing *monomial codes.*
- **Theorem.** *Given length-N monomial code $\mathcal{C}$ and any $\boldsymbol{S} \in \mathcal{S}_\mathcal{C}$, $d(\mathcal{C}) = d(\mathcal{C}_S)$.*
Idea: construct $\boldsymbol{c} \in \mathcal{C} \cap \mathcal{C}_S$ with $\text{wt}(\boldsymbol{c}) = d(\mathcal{C})$.

Pre-transformation preserves the code distance for decreasing monomial codes.

Minimum weight codewords

- **#. minimum weight codewords**:
$$M(\mathcal{C}) = |\{\boldsymbol{c} \in \mathcal{C} : \text{wt}(\boldsymbol{c}) = d(\mathcal{C}).\}|$$
A 'metric' for the weight spectrum of code $\mathcal{C}$.
Motivation: since $d(\mathcal{C}_S) = d(\mathcal{C})$, use this to study the weight spectrum after pre-transformation.
- **Assumptions**: for monomial code (2), assume
(i) $\mathcal{C}$ is decreasing;
(ii) $i^* = \min\{i \in \mathcal{I} : \text{wt}(\boldsymbol{h}^{(i)}) = d(\mathcal{C})\}$, then $\exists\, \ell > i^*,\ \ell \in \mathcal{I}^C$ s.t. $\text{wt}(\boldsymbol{h}^{(\ell)}) < d(\mathcal{C})$
(iii) $e = \min\{e' \in \mathbb{N} : N - i^* > 2^{n-e'}\}$, $\Delta(\mathcal{C}) = \min_{\boldsymbol{c}\in\mathcal{C},\,\text{wt}(\boldsymbol{c})>d(\mathcal{C})}\{(\text{wt}(\boldsymbol{c}) - d(\mathcal{C}))\}$, then $\Delta(\mathcal{C}) > 2^e$.
- **Proposition**. *For code $\mathcal{C}$ satisfying assumptions, $\exists\, \boldsymbol{S} \in \mathcal{S}_\mathcal{C}$ s.t. $M(\mathcal{C}_S) < M(\mathcal{C})$*
- **Corollary**. For RM codes $\mathcal{C} = \mathcal{R}(n, r)$ with $n - 1 \ge 2r, r \ge 2$, $\exists\, \boldsymbol{S} \in \mathcal{S}_\mathcal{C}$ s.t. $M(\mathcal{C}_S) < M(\mathcal{C})$.

Pre-transformation improves the weight spectrum of certain monomial codes.

Simulation (selected)

- **PAC codes** [1]: A *PAC code* specified by $(N, k, \mathcal{I}, \boldsymbol{g})$ is given by (3) with $\boldsymbol{T}$ being the Toeplitz matrix generated by $(\boldsymbol{g}, \boldsymbol{0})$ and
$$\mathcal{I} = \arg\max\{\sum_{i\in\mathcal{I}} \text{wt}((i-1)_2) : |\mathcal{I}| = k\}$$

Table 1:Weight Spectrum of $\mathcal{C} = (32, 16, \mathcal{I}, (1))$

0	8	12	16	20	24	32
1	620	13888	36518	13888	620	1

Table 2:Simulation Results of $\mathcal{C}' = (32, 16, \mathcal{I}, (1, 1, 0, 1))$

Weight Spectrum of $\mathcal{C}' = (32, 16, \mathcal{I}, (1, 1, 0, 1))$										
0	8	10	12	14	16	18	20	22	24	32
1	364	2048	6720	14336	18598	14336	6720	2048	364	1
Weight Spectrum of Transformed PC Monomial Code										
0	8	10	12	14	16	18	20	22	24	32
1	364	2048	6720	14336	18598	14336	6720	2048	364	1
Parity Check Equations										
$u_9 \oplus u_8 = 0$ $u_{11} \oplus u_8 = 0$ $u_{13} \oplus u_{12} = 0$ $u_{17} \oplus u_{12} \oplus u_{15} \oplus u_{16} = 0$ $u_{18} \oplus u_{12} \oplus u_{14} \oplus u_{15} = 0$ $u_{19} \oplus u_{12} \oplus u_{14} \oplus u_{15} \oplus u_{16} = 0$ $u_{21} \oplus u_{20} = 0$ $u_{25} \oplus u_{20} \oplus u_{23} \oplus u_{24} = 0$										

- Our simulation shows:
(i) the correctness of **Algorithm**;
(ii) PAC codes have improved weight spectrum.

References

[1] Erdal Arıkan.
From sequential decoding to channel polarization and back again.
arXiv preprint arXiv:1908.09594, 2019.

[2] Magali Bardet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich.
Algebraic properties of polar codes from a new polynomial formalism.
In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 230–234. IEEE, 2016.

[3] Bin Li, Huazi Zhang, and Jiaqi Gu.
On pre-transformed polar codes.
arXiv preprint arXiv:1912.06359, 2019.