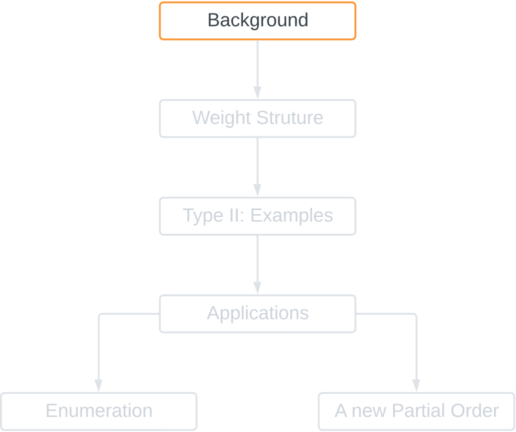
Weight Structure of Low/High-Rate Polar Codes and Its Applications

Mohammad Rowshan†, Vlad-Florin Drăgoi‡, Jinhong Yuan†

†The University of New South Wales, Sydney Australia
‡Aurel Vlaicu University, Arad, Romania

IEEE Int'l Symposium on Information Theory
July 7-12, 2024, Athens, Greece

Outline


Background
Weight Struture
Type II: Examples
Applications
Enumeration
A new Partial Order

Basic Concepts and Notations

- A **monomial** f is a product of some distinct variables $f = \prod_{j \in J} x_j$, where J is the *support* of f; $\text{ind}(f)$.
- The set of all monomials of m variables is denoted by $\mathcal{M}_m$.
- Any monomial set $\mathcal{I} \subseteq \mathcal{M}_m$ can be divided into subsets based on the degree of monomials as $\mathcal{I} = \bigcup_{j=0}^{m} \mathcal{I}_j$, where $\mathcal{I}_j = \{f \in \mathcal{I} \mid \deg(f) = j\}$.
- For every row $\mathbf{g}_i$ of generator matrix $\mathbf{G}$ where $i \in [0, k-1]$ there exists a monomial $f \in \mathcal{I}$ satisfying $\text{ev}(f) = \mathbf{g}_i$.

Bijection b/w row indices and monomials for $m = 2$

i	bin(i)	supp(bin(i))^c	f		$\mathbf{z} = (z_0\ z_1)$:	11	01	10	00
0	$(0,0)$	$\{0,1\}$	x_0x_1	$\mathbf{g}_0$	$\mathrm{ev}\left(x_0x_1\right)$	1	0	0	0
1	$(1,0)$	$\{1\}$	x_1	$\mathbf{g}_1$	$\mathrm{ev}\left(x_1\right)$	1	1	0	0
2	$(0,1)$	$\{0\}$	x_0	$\mathbf{g}_2$	$\mathrm{ev}\left(x_0\right)$	1	0	1	0
3	$(1,1)$	$\emptyset$	$\mathbf{1}$	$\mathbf{g}_3$	$\mathrm{ev}(\mathbf{1})$	1	1	1	1

Reliability-based Partial Order $\preceq$

Definition

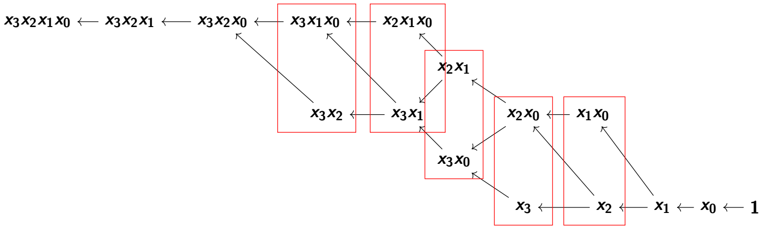
Let m be a positive integer and $f, g \in \mathcal{M}_m$. Then:

- $f \preceq_w g$ if and only if $f|g$, i.e., $\mathrm{ind}(f) \subseteq \mathrm{ind}(g)$.
- When $\deg(f) = \deg(g) = s$ we say that $f \preceq_{sh} g$ if $\forall\, 1 \leq \ell \leq s$ we have $i_\ell \leq j_\ell$, where $f = x_{i_1} \dots x_{i_s}$, $g = x_{j_1} \dots x_{j_s}$.

Definition

A set $\mathcal{I} \subseteq \mathcal{M}_m$ is *decreasing* if and only if ($f \in \mathcal{I}$ and $g \preceq f$) implies $g \in \mathcal{I}$.

Partial Order: A Chain Relation



Permutation Group

- A bijective affine transformation over $\mathbb{F}_2^m$ is represented by a pair $(\mathbf{B}, \varepsilon)$ where $\mathbf{B} = (b_{i,j})$ is an invertible matrix lying in the general linear group $\mathrm{GL}(m, 2)$ and ε in $\mathbb{F}_2^m$.
- For decreasing monomial codes, a lower triangular affine transformation denoted by $\mathrm{LTA}(m, 2)$ is employed where $\mathbf{B} \in \mathrm{GL}(m, 2)$ is a lower triangular binary matrix with $b_{i,i} = 1$ and $b_{i,j} = 0$ whenever $j > i$.

$$\mathbf{z} \to \mathbf{B}\mathbf{z} + \varepsilon,$$

Example

Let $m = 3$, $g = x_0 x_2$ and $\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $\varepsilon = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ We have $(\mathbf{B}, \varepsilon) \cdot g = (x_0 + 1)(x_2 + x_1)$

Orbits

- Orbit:

$$\mathrm{LTA}(m,2)\cdot f = \{(\mathbf{B},\varepsilon)\cdot f \mid (\mathbf{B},\varepsilon)\in \mathrm{LTA}(m,2)\}.$$

- $W_{\mathrm{w}_{\min}} = \bigcup_{\deg(f)=r} \mathrm{LTA}(m,2)\cdot f \quad (r \text{ degree max})$

Minimum Weight Codewords

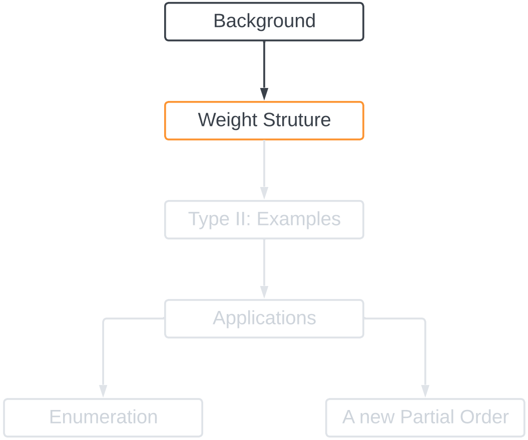
- The degree of freedom on x_i:

$$\lambda_f(x_i) = |\{j \in [0, i) \mid j \notin \mathrm{ind}(f)\}|.$$

- $|\lambda_f(f)| = \sum_{i \in \mathrm{ind}(f)} \lambda_f(x_i)$, (or simply $|\lambda_f|$).

- $|\mathrm{LTA}(m, 2) \cdot g| = 2^{|\lambda_g| + \deg(g)}$.

f $\mathrm{ind}(f)$	$x_0x_1x_2x_3$ $\{0, 1, 2, 3\}$	$x_0x_1x_2x_4$ $\{0, 1, 2, 4\}$	$x_0x_1x_2x_5$ $\{0, 1, 2, 5\}$	$x_0x_1x_3x_4$ $\{0, 1, 3, 4\}$
λ_f	$(0, 0, 0, 0)$	$(1, 0, 0, 0)$	$(2, 0, 0, 0)$	$(1, 1, 0, 0)$
$\lvert\mathrm{LTA}(m, 2)_f \cdot f\rvert$	2^4	2^5	2^6	2^6
$\lvert W_{\mathrm{w_{min}}}\rvert$ or $A_{\mathrm{w_{min}}}$	176			


Background
Weight Struture
Type II: Examples
Applications
Enumeration
A new Partial Order

Structure of Weights less than $2w_{\min}$

Theorem

Let $r < m$ and $P \in \mathbf{R}_m$ be such that $\deg(P) \leq r$ with $0 < \mathrm{w}(\mathrm{ev}(P)) < 2^{m+1-r}$. Then P is affine equivalent to one of the forms [1]

1. **Type I**: $P = y_1 \dots y_{r-\mu}(y_{r-\mu+1} \dots y_r + y_{r+1} \dots y_{r+\mu})$ *where* $m \geq r + \mu, r \geq \mu \geq 3$
2. **Type II**: $P = y_1 \dots y_{r-2}(y_{r-1}y_r + \dots + y_{r+2\mu-3}y_{r+2\mu-2})$ *where* $m - r + 2 \geq 2\mu, 2\mu \geq 2$.

In both cases y_i are linear independent forms and $\mathrm{w}(\mathrm{ev}(P)) = 2^{m+1-r} - 2^{m+1-r-\mu}$.

[1] T. Kasami and N. Tokura, "On the weight structure of Reed-Muller codes," *Trans. Inf. Theory*, vol. 16, no. 6, pp. 752-759, Nov. 1970.

The Weight Structure in terms of $\mathrm{LTA}(m,2)$

Theorem

Let $r < m$ and $P \in \mathbf{R}_m$ be such that $\deg(P) \leq r$ with $0 < \mathrm{w}(\mathrm{ev}(P)) < 2^{m+1-r}$. Then

1. **Type I:** *for $m \geq r+\mu, r \geq \mu \geq 3$*
   $P = y_1 \dots y_{r-\mu}(y_{r-\mu+1} \dots y_r + y_{r+1} \dots y_{r+\mu})$
   $P \in \mathrm{LTA}(m,2) \cdot f + \mathrm{LTA}(m,2) \cdot g$ *with* $f, g \in \mathcal{M}_m$ *having* $\deg(f) = \deg(g) = r$.
2. **Type II:** *for $m - r + 2 \geq 2\mu \geq 2$*
   $P = y_1 \dots y_{r-2}(y_{r-1}y_r + \dots + y_{r+2\mu-3}y_{r+2\mu-2})$
   $P \in \sum_{i=1}^{\mu} \mathrm{LTA}(m,2) \cdot f_i$ *with* $f_i \in \mathcal{M}_m$ *satisfying* $\deg(f_i) = r$.

In both cases, y_i are linear independent forms and $\mathrm{w}(\mathrm{ev}(P)) = 2^{m+1-r} - 2^{m+1-r-\mu}$.

Codeword Weight

Given $\mathrm{w}_{\min} = 2^{m-r}$, the weight of the codewords based on μ is:
$\mathrm{w}(\mathrm{ev}(P)) = 2^{m+1-r} - 2^{m+1-r-\mu} = \left(2 - \frac{1}{2^{\mu-1}}\right)\mathrm{w}_{\min}$.

μ	$\mathrm{w}(\mathrm{ev}(P))$
1	$\mathrm{w}_{\min}$ [1]
2	$1.5\,\mathrm{w}_{\min}$
3	$1.75\,\mathrm{w}_{\min}$
$\vdots$	$\vdots$

Example

$\mathcal{R}(2,7)$:

- $\mathrm{w}_{\min} = 2^5 = 32$: $x_i x_j$
- $1.5\,\mathrm{w}_{\min} = 2^6 - 2^4 = 48 \Rightarrow \mu = 2$: $x_0x_1 + x_2x_3$
- $1.75\,\mathrm{w}_{\min} = 2^6 - 2^8 = 56 \Rightarrow \mu = 3$: $x_0x_1 + x_2x_3 + x_4x_5$
- $2\,\mathrm{w}_{\min} = 2^6 = 64$

Our Previous Work: $1.5w_{\min}$-weight Codewords [1,2]

Theorem

Let $\mathcal{C}(\mathcal{I})$ be a DMC, with $r = \max_{f \in \mathcal{I}} \deg(f)$. Any codeword of weight $1.5\,\mathrm{w}_{\min}$ in $\mathcal{C}(\mathcal{I})$ is the evaluation of a polynomial $P \in \mathrm{LTA}(m,2)_h \cdot h \cdot \left(\mathrm{LTA}(m,2)_f \cdot \frac{f}{h} + \mathrm{LTA}(m,2)_g \cdot \frac{g}{h}\right)$, with $f, g \in \mathcal{I}_r, h = \gcd(f,g)$, and $\deg(h) = r - 2$.

[1] M. Rowshan, V-F Drăgoi, J. Yuan, "On the Closed-form Weight Enumeration of Polar Codes: 1.5d-weight Codewords", May, 2023, arXiv:2305.02921.

[2] V.-F. Drăgoi, M. Rowshan, and J. Yuan, "On the closed-form weight enumeration of polar codes: 1.5 d-weight codewords," *IEEE Trans. on Communications*, 2024. DoI: 10.1109/ TCOMM.2024.3394749.

[3] Z. Ye, Y. Li, H. Zhang, J. Wang, G. Yan, Z. Ma, "On the Distribution of Weights Less than $2w_{\min}$ in Polar Codes", August, 2023, arXiv:2308.10024.

Main challenges

A complete characterization of codewords in terms of orbits $(\mathrm{LTA}(m, 2))$

- Minkowski sums of orbits are much harder to characterize than simple orbits
- We give a closed formula for the size of a Minkowski orbit (count collisions, much harder than $\mathsf{w}_{\mathsf{min}}$)
- The Minkowski sums of two distinct pairs (f, g) and (f^*, g^*) are disjoints
- Reunite all properties under a complete counting and charcterisation theorem

Generalise these properties to a finite sum of orbits!

Type II Structure

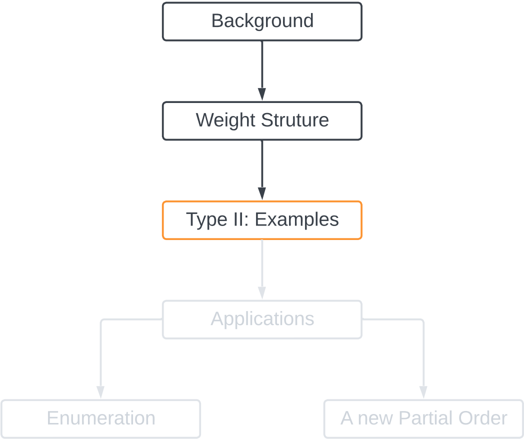
Generalisation: Any Type II codeword of a DMC resides within the sum of μ orbits of monomials from $\mathcal{I}_r$.

Theorem (Characterisation)

Let $\mathcal{C}(\mathcal{I})$ be a DMC with $r = \max_{f \in \mathcal{I}} \deg(f)$. Any Type II codeword of weight $2^{m+1-r} - 2^{m+1-r-\mu}$ with $m - r + 2 \geq 2\mu \geq 2$ belongs to

$$\mathrm{LTA}(m,2)_h \cdot h \cdot \sum_{i=1}^{\mu} \mathrm{LTA}(m,2)_{f_i} \cdot \frac{f_i}{h}$$

where $\forall i, f_i \in \mathcal{I}_r$, $h = \gcd(f_i, f_j)$, for all $i, j \in [1, \mu]$ $(i \neq j)$ and $\deg(h) = r - 2$.

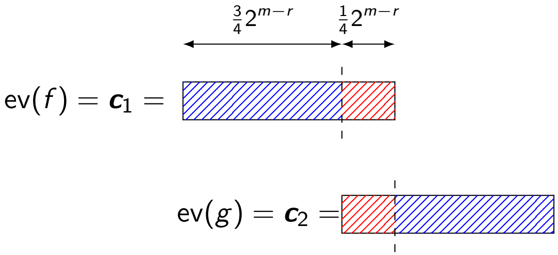

Background
Weight Struture
Type II: Examples
Applications
Enumeration
A new Partial Order

$\mu = 2$ codewords: $w = 1.5\,\mathrm{w}_{\min}$

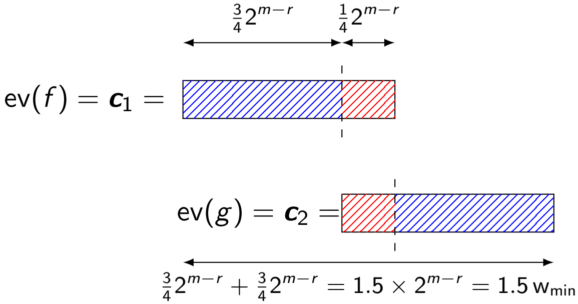
$$\mathrm{ev}(f) = \boldsymbol{c}_1 = \boxed{}$$

$$\mathrm{ev}(g) = \boldsymbol{c}_2 = \boxed{}$$

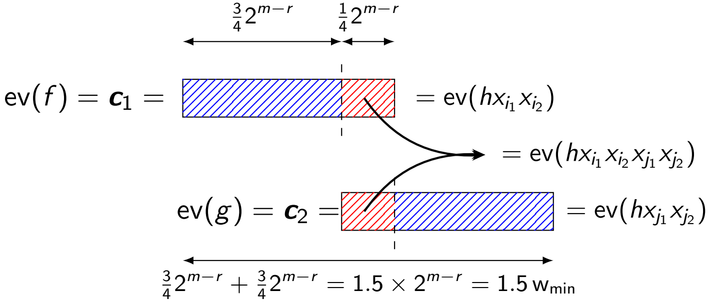
$\mu = 2$ codewords: $w = 1.5\,\mathrm{w}_{\min}$



$\mu = 2$ codewords: $w = 1.5\,\mathrm{w}_{\min}$



$\mu = 2$ codewords: $w = 1.5\,\mathrm{w}_{\min}$



$\mu = 3$ codedwords: $w = 1.75\,\mathrm{w}_{\min}$

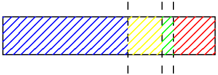
$$\mathrm{ev}(x_0x_1) = \boldsymbol{c}_1 = \boxed{}$$

$$\mathrm{ev}(x_2x_3) = \boldsymbol{c}_2 = \boxed{}$$

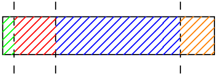
$$\mathrm{ev}(x_4x_5) = \boldsymbol{c}_3 = \qquad \boxed{} \qquad \boxed{}$$

$\mu = 3$ codedwords: $w = 1.75\,\mathrm{w}_{\min}$

$\mathrm{ev}(x_0x_1) = \boldsymbol{c}_1 =$



$\mathrm{ev}(x_2x_3) = \boldsymbol{c}_2 =$



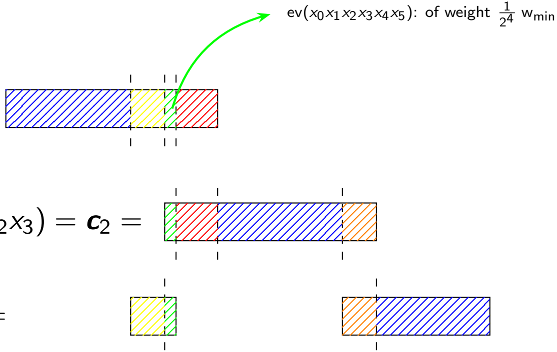
$\mathrm{ev}(x_4x_5) = \boldsymbol{c}_3 =$

$\mu = 3$ codedwords: $w = 1.75\,\mathrm{w}_{\min}$

$\mathrm{ev}(x_0x_1) = \boldsymbol{c}_1 =$

$\mathrm{ev}(x_2x_3) = \boldsymbol{c}_2 =$

$\mathrm{ev}(x_4x_5) = \boldsymbol{c}_3 =$

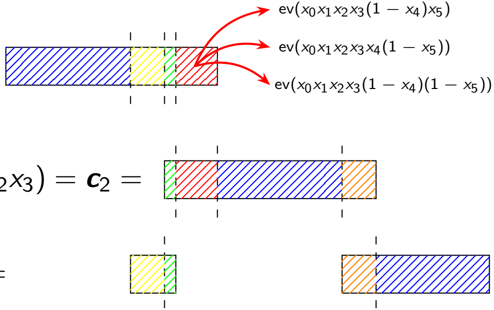


$\mu = 3$ codedwords: $w = 1.75\,\mathrm{w}_{\min}$

$\mathrm{ev}(x_0 x_1) = \boldsymbol{c}_1 =$

$\mathrm{ev}(x_2 x_3) = \boldsymbol{c}_2 =$

$\mathrm{ev}(x_4 x_5) = \boldsymbol{c}_3 =$

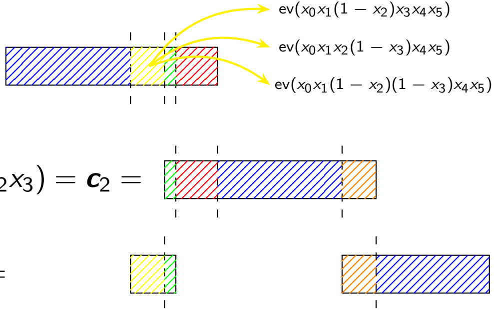


$\mu = 3$ codedwords: $w = 1.75\,\mathrm{w}_{\min}$

$\mathrm{ev}(x_0x_1) = \boldsymbol{c}_1 =$

$\mathrm{ev}(x_2x_3) = \boldsymbol{c}_2 =$

$\mathrm{ev}(x_4x_5) = \boldsymbol{c}_3 =$

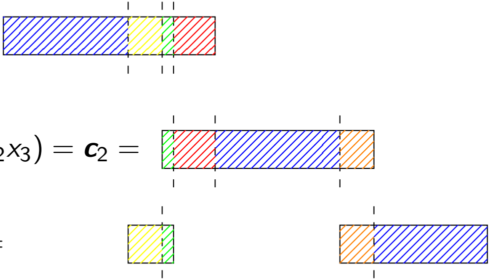


$\mu = 3$ codedwords: $w = 1.75\,\mathrm{w_{min}}$

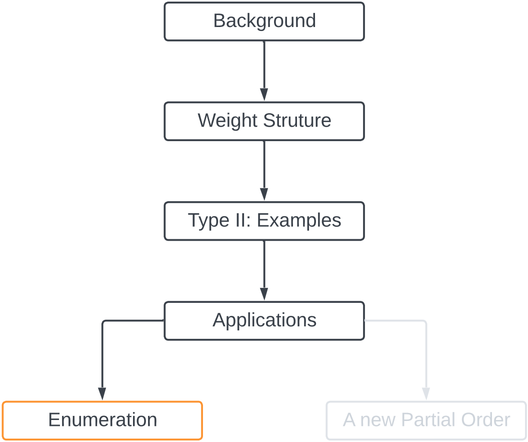
$\mathrm{ev}(x_0x_1) = \boldsymbol{c}_1 =$

$\mathrm{ev}(x_2x_3) = \boldsymbol{c}_2 =$

$\mathrm{ev}(x_4x_5) = \boldsymbol{c}_3 =$

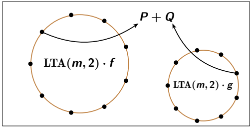


$\frac{9}{16}\,\mathrm{w_{min}} + \frac{1}{16}\,\mathrm{w_{min}} + \frac{9}{16}\,\mathrm{w_{min}} + \frac{9}{16}\,\mathrm{w_{min}} = \frac{7}{4}\,\mathrm{w_{min}}$


Background
Weight Struture
Type II: Examples
Applications
Enumeration
A new Partial Order

Enumeration for $\mu = 2$

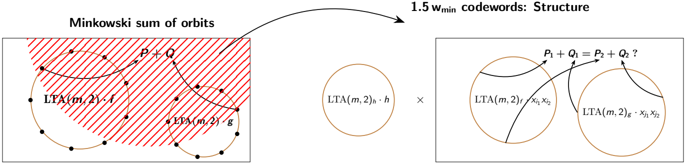
Minkowski sum of orbits



$\mathrm{LTA}(m,2) \cdot f + \mathrm{LTA}(m,2) \cdot g$

$h = \mathrm{gcd}(f,g), \mathrm{deg}(h) = r - 2$

Enumeration for $\mu = 2$

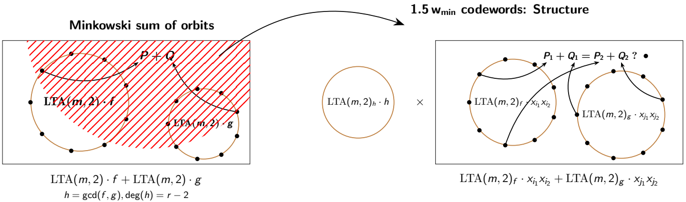


$\mathrm{LTA}(m,2) \cdot f + \mathrm{LTA}(m,2) \cdot g$

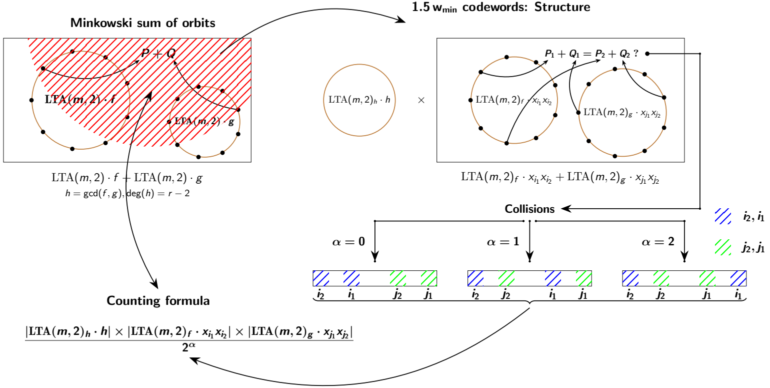
$h = \mathrm{gcd}(f,g), \mathrm{deg}(h) = r - 2$

$\mathrm{LTA}(m,2)_f \cdot x_{i_1} x_{i_2} + \mathrm{LTA}(m,2)_g \cdot x_{j_1} x_{j_2}$

Enumeration for $\mu = 2$



Enumeration for $\mu = 2$



Collision

Challenge

While we know how to find the cardinality of orbits (# of polynomials representing codewords), the Minkowski sum of orbits may produce redundant polynomials due to collision.

Definition

Let $f = x_{i_2}x_{i_1}$ and $g = x_{j_2}x_{j_1}$ with $\gcd(f, g) = 1$ and $i_2 > j_2$. The *degree of collision* of f and g is

$$\alpha_{f,g} = \begin{cases} 0 & i_2 > i_1 > j_2 > j_1 \\ 1 & i_2 > j_2 > i_1 > j_1 \\ 2 & i_2 > j_2 > j_1 > i_1 \end{cases}.$$

Collision

Example

Suppose $f = x_2x_6$ and $g = x_3x_5$ hence $\alpha_{f,g} = 2$.
Map every x_i into a "new variable" (y_i), where
$y_i = x_i + \sum_{j=0, j\notin \text{ind}(f)}^{i-1} b_{i,j}x_j$.
- $P_1 = y_1y_2 = (x_2)(x_6 + x_3)$ and $Q_1 = y_3y_4 = (x_3 + x_2)(x_5)$.
- $P_2 = y_1y_2 = (x_2)(x_6 + x_5)$ and $Q_2 = y_3y_4 = (x_3)(x_5 + x_2)$.

Observe that

$$P_1 + Q_1 = x_6x_2 + x_3x_2 \ + \ x_5x_3 + x_5x_2,$$

$$P_2 + Q_2 = x_6x_2 + x_5x_2 \ + \ x_5x_3 + x_3x_2.$$

where we have $P_1 + Q_1 = P_2 + Q_2$.

Enumeration of Type II codewords - Single Combination

Proposition (Size of μ-Minkowski sum)

Let $\mathcal{I}$ be a DMSet with $r = \max_{f \in \mathcal{I}} \deg(f)$ and $\mu \geq 2$. Also, let $f_i \in \mathcal{I}_r$ for $i \in [1, \mu]$ with $\gcd(f_i, f_j) = h$ for any pair $(i, j) \in [1, \mu] \times [1, \mu]$ with $i \neq j$, and $\deg(h) = r - 2$. Then

$$\left| \mathrm{LTA}(m,2)_h \cdot h \cdot \sum_{i=1}^{\mu} \mathrm{LTA}(m,2)_{f_i} \cdot \frac{f_i}{h} \right| =$$

$$|\mathrm{LTA}(m,2)_h \cdot h| \times \frac{\prod_{i=1}^{\mu} |\mathrm{LTA}(m,2)_{f_i} \cdot \frac{f_i}{h}|}{2^{\sum_{i \neq j} \alpha_{\frac{f_i}{h}, \frac{f_j}{h}}}} \quad (1)$$

Constructive Formula for Type II codewords - Total

Theorem

Let $\mathcal{I}$ be a DMSet and $r = \max_{f \in \mathcal{I}} \deg(f)$. Let $\mathrm{w}_\mu = 2^{m+1-r} - 2^{m+1-r-\mu}$ with $2 \leq 2\mu \leq m - r + 2$. The number of weight w_μ codewords of Type II is

$$|W_{\mathrm{w}_\mu}(\mathcal{I})| = \sum_{\substack{1 \leq i \leq \mu,\ f_i \in \mathcal{I}_r \\ h = \gcd(f_i, f_j) \in \mathcal{I}_{r-2}}} \frac{2^{r-2+2\mu+|\lambda_h|+\sum_{i=1}^{\mu} |\lambda_{f_i}(\frac{f_i}{h})|}}{2^{\sum_{(f_i,f_j)} \alpha_{\frac{f_i}{h}, \frac{f_j}{h}}}}.$$

$2w_{\min}$-weight Codewords

Lemma

Let $P \in \mathbf{R}_m$ with $\deg(P) = 2$. Then $\mathrm{w}(\mathrm{ev}(P)) = 2^{m-1}$ if and only if P is affine equivalent to $x_1x_2 + \cdots + x_{2l-1}x_{2l} + x_{2l+1}$ for $0 \leq l \leq (m-1)/2$, where x_i's are mutually independent [1].

Any polynomial $Q \in \mathrm{LTA}(m, 2) \cdot x_i$ satisfying $\mathrm{w}(\mathrm{ev}(Q)) = 2^{m-1}$ represents the x_{2l+1} term.
Observe that $2\,\mathrm{w}_{\min}$ are thus expressed as linear combinations of a 2^{m-1}-weight codeword and $\mathrm{w}_{\min}$-weight codewords.

[1] T. Kasami and N. Tokura, "On the weight structure of Reed-Muller codes," *Trans. Inf. Theory*, vol. 16, no. 6, pp. 752-759, Nov. 1970.

The complete weight distribution of Subcodes of $\mathcal{R}(2, m)$

$\lvert W_{\mathrm{w}}\rvert$	w
1	$\mathrm{w} = 0, \mathrm{w} = 2^m$
$\sum\limits_{f \in \mathcal{I}_2} 2^{2+\lvert\lambda_f\rvert}$	$\mathrm{w} = 2^{m-2}, 2^m - 2^{m-2}$
$\sum\limits_{\substack{1 \le i \le \mu,\ f_i \in \mathcal{I}_2 \\ \gcd(f_i, f_j)=1}} \frac{2^{2\mu + \sum_{i=1}^{\mu} \lvert\lambda_{f_i}\rvert}}{2^{\sum_{(f_i,f_j)} \alpha_{f_i,f_j}}}$	$\mathrm{w} = 2^{m-1} \pm 2^{m-1-\mu}$
$\sum\limits_{l=0}^{\frac{m-1}{2}} \sum\limits_{\substack{1 \le i \le l,\ f_i \in \mathcal{I}_2 \\ \gcd(x_j, f_i)=1 \\ \gcd(f_i, f_j)=1}} \frac{2^{2\mu + \sum_{i=1}^{l} \lvert\lambda_{f_i}\rvert + 1 + \lvert\lambda_{f_1 \dots f_l}(x_j)\rvert}}{2^{\sum_{(f_i,f_j)} \alpha_{f_i,f_j}}}$	$\mathrm{w} = 2^{m-1} = 2\,\mathrm{w}_{\min}$

Table Complete weight distribution for decreasing monomial code $\mathcal{C}(\mathcal{I})$ satisfying $\mathcal{R}(1, m) \subseteq \mathcal{C}(\mathcal{I}) \subseteq \mathcal{R}(2, m)$.

High-rate Weight Distribution

Use the MacWilliams identities on the weight enumerator polynomial of $\mathcal{C}(\mathcal{I})$ and its dual $\mathcal{C}(\mathcal{I})^{\perp}$ [2], to compute the weight distribution of the dual code.

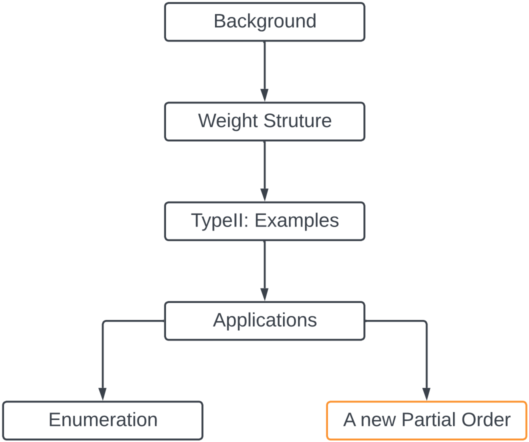
$$\sum_{j=0}^{n-\nu} \binom{n-j}{\nu} |W_j(\mathcal{C})| = 2^{k-\nu} \sum_{j=0}^{\nu} \binom{n-j}{n-\nu} |W_j(\mathcal{C}^{\perp})|, \quad (2)$$

for $\nu = 0, 1, \ldots, n$. Furthermore, the following holds:

$$\mathcal{R}(1, m) \subseteq \mathcal{C}(\mathcal{I}) \subseteq \mathcal{R}(2, m)$$
$$\mathcal{R}(m-2, m) \supseteq \mathcal{C}(\mathcal{I})^{\perp} \supseteq \mathcal{R}(m-3, m).$$

Note that the weight distribution of $\mathcal{C}(\mathcal{I})^{\perp}$ is also symmetric.

[2] J. Macwilliams, "A theorem on the distribution of weights in a systematic code," *The Bell System Technical Journal*, vol. 42, no. 1, pp. 79-94, 1963.


Background
Weight Struture
TypeII: Examples
Applications
Enumeration
A new Partial Order

Introducing a new Partial Order

Given a generating set $\mathcal{I}$, we can have PARTIAL ORDERs:

- based on channel reliability (known)
- based on weight contribution (new)

Definition

Let $\mathcal{C}(\mathcal{I}), \mathcal{C}(\mathcal{J})$ be two decreasing monomial codes. Let $\mathrm{w} \in [0, 2^m]$ and define[a]

$$\mathcal{C}(\mathcal{I}) \preccurlyeq_{\mathrm{w}} \mathcal{C}(\mathcal{J}) \text{ if } |W_{\mathrm{w}}(\mathcal{J})| \leq |W_{\mathrm{w}}(\mathcal{I})|.$$

$$\mathcal{C}(\mathcal{I}) \preccurlyeq_{[\mathrm{w}_1,\mathrm{w}_2]} \mathcal{C}(\mathcal{J}) \text{ if } \forall\, \mathrm{w} \in [\mathrm{w}_1, \mathrm{w}_2]\; \mathcal{C}(\mathcal{I}) \preccurlyeq_{\mathrm{w}} \mathcal{C}(\mathcal{J}).$$

[a] We use the symbol $\preccurlyeq$ instead of $\preceq$ to distinguish it from the partial order of reliability.

Introducing a new Partial Order

We extend the definition $\preccurlyeq_{\mathrm{w}}$ to monomials as follows.

Definition

Let r be the maximum-degree of monomials and $f, g \in \mathcal{I}_r$. Then, we have $f \preccurlyeq_{\mathrm{w_{min}}} g$ if and only if $|\lambda_f| < |\lambda_g|$.

Recall: $|\lambda_f|$ is the total number of free variables on all x_i in f:

$$|\lambda_f| = \sum_{i \in \mathrm{ind}(f)} \lambda_f(x_i),$$

$$|\mathrm{LTA}(m,2) \cdot f| = 2^{|\lambda_f| + \deg(f)}.$$

To each degree r, one can associate the partial order set (poset) of $\mathcal{I}_r$ defined by $\preceq$ and $\preccurlyeq_{\mathrm{w_{min}}}$.

Symmetric property and non-comparable elements

The order $\preccurlyeq_{\mathrm{w_{min}}}$ adds more restrictions and hence reduces the number of non-comparable elements.

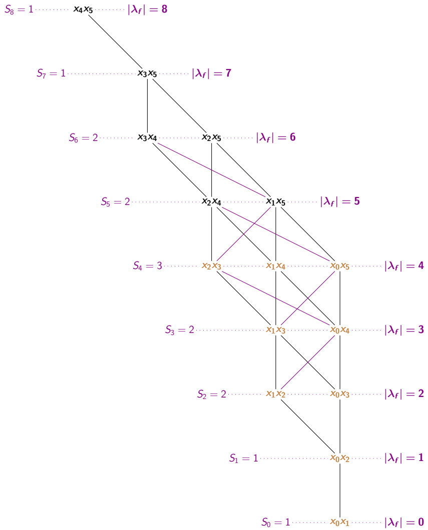
Lemma

Let $S_\ell = \{f \in \mathcal{I}_2 : |\lambda_f| = \ell\}$. Then, for all $\ell \in [0, m-2]$, we have

- *Symmetry:* $|S_\ell| = |S_{m-2+\ell}|$,
- *Cardinality:* $|S_l| = \lfloor \frac{\ell+2}{2} \rfloor$.

Hence, the sequence S_ℓ is not only **symmetric**, but also **uni-modal**, with a maximum at $|S_{m-2}| = m-2$ where we have $|S_{m-2}| = \lfloor \frac{m}{2} \rfloor$.
Example: For $m = 6$, the sequence $1, 1, 2, 2, 3, 2, 2, 1, 1$ gives $|S_\ell| = |\{f \in \mathcal{I}_2 : |\lambda_f| = \ell\}|$.

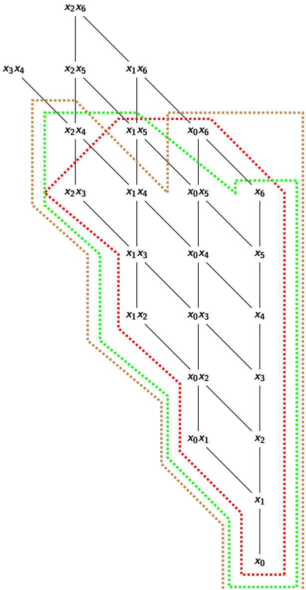
The monomials in $\mathcal{I}$ (bold brown) are defined by $f \preceq x_1x_4$, $f \preceq x_0x_5$ and $f \preceq x_2x_4$. Each level gives $|\lambda_f|$.



Black lines for $\preceq$, black/violet lines for $\preccurlyeq_{w_{min}}$.
Elements at the same level S_ℓ have an identical weight contribution, thus defining different codes with the same weight distribution.

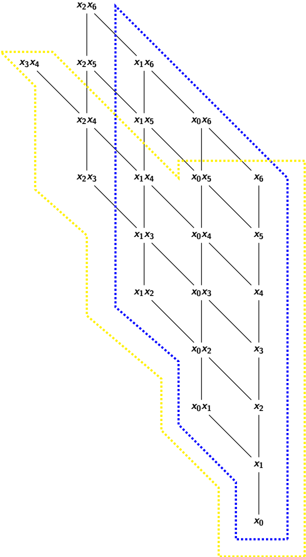
Example: $m = 7$, selecting 19 monomials from $\mathcal{I}'$

$\mathcal{I}' = \{f : f \preceq x_3x_4, f \preceq x_2x_6\}$.
Note that the monomial 1 is not included in the figure.
Red-enclosed monomials:
$\mathcal{I} = \{f \mid f \preceq x_0x_6, f \preceq x_1x_5, f \preceq x_2x_3\}$.
$W(\mathcal{I}, X) = 1 + 556X^{32} + 21312X^{48} + 36864X^{56} + 406822X^{64}$.
Green-enclosed monomials:
$\mathcal{I} = \{f : f \preceq x_2x_4, f \preceq x_1x_5, f \preceq x_6\}$.
$W(\mathcal{I}, X) = 1 + 556X^{32} + 21312X^{48} + 36864X^{56} + 406822X^{64}$
Brown-enclosed monomials:
$\mathcal{I} = \{f : f \preceq x_2x_4, f \preceq x_0x_5, f \preceq x_6\}$.
$W(\mathcal{I}, X) = 1 + 556X^{32} + 21312X^{48} + 36864X^{56} + 406822X^{64}$



Example: $m = 7$, selecting 19 monomials from $\mathcal{I}'$

$\mathcal{I}' = \{f : f \preceq x_3x_4, f \preceq x_2x_6\}$.
Note that the monomial 1 is not included in the figure.
Yellow line:
$\mathcal{I} = \{f : f \preceq x_1x_6, f \preceq x_0x_5, f \preceq x_6\}$.
$W(\mathcal{I}, X) = 1 + 684X^{32} + 22848X^{48} + 28672x^{56} + 419878X^{64}$.
Blue line:
$\mathcal{I} = \{f : f \preceq x_1x_6\}$.
$W(\mathcal{I}, X) = 1 + 748X^{32} + 29760X^{48} + 463270X^{64}$.



Ordering Procedure

For the subcodes of $\mathcal{R}(2, m)$ with $1 + m < K < 1 + m + \binom{m}{2}$:

1. Based on $\preccurlyeq_{\mathrm{w}_{\min}}$, select the monomials on the first $\ell - 1$ levels, where $1 + m + \sum_{j=0}^{\ell-1} \lfloor \frac{j+2}{2} \rfloor \leq K < 1 + m + \sum_{j=0}^{\ell} \lfloor \frac{j+2}{2} \rfloor$.
2. The remaining monomials, all from level l will be selected based on the reliability rule, where the reliability can be calculated using different methods such has beta-expansion.

Permutation Group

While two permutation equivalent codes will have an identical weight distribution, the converse is not always true [3].

Example

Let us consider the codes in the previous example with $m = 6$. The three codes have different permutation groups and thus are not equivalent.
$\mathcal{C}(\mathcal{I} \setminus \{x_0x_5\})$ has a group of order $2^{30} \times 3^2$,
$\mathcal{C}(\mathcal{I} \setminus \{x_1x_4\})$ has a group of order $2^{28} \times 3^3 \times 7$,
$\mathcal{C}(\mathcal{I} \setminus \{x_2x_3\})$ has a group of order $2^{28} \times 3 \times 7$.

[3] E. Cheon, "Equivalence of linear codes with the same weight enumerator," Scientiae Mathematicae Japonicae, vol. 64, no. 1, p. 163, 2006.

Potential future directions and Further Resources

Open Problems:

- Finding formulas for higher wieight codewords,
- Extending the formulas to the variants of polar codes,
- Discovering more propeties of the introduced partial order and further investigation on how to used them in code construction,

MATLAB script and Slides:

- https://github.com/mohammad-rowshan/closed-form-weight-enumeration-of-polar-codes

Feel free to get in touch:

- m.rowshan@unsw.edu.au