"Self-Orthogonal Minimal Codes From (Vectorial) Plateaued p-Ary Functions"

René Rodríguez[1] Enes Pasalic[1,2] Fengrong Zhang[3] Yongzhuang Wei[2]

The 9th International Workshop on Boolean Functions and their Applications (BFA), Dubrovnik, Croatia

[1]University of Primorska & Institute Andrej Marušič, Slovenia
[2]Guilin University of Electronic Technology, China
[3]Xidian University, China

Sep 12, 2024

Happy (belated) birthday!

Happy (belated) birthday!

Plateaued Functions

Plateaued Functions

For a prime power p^n, $\mathbb{F}_{p^n}$ is the finite field with p^n elements.

Plateaued Functions

For a prime power p^n, $\mathbb{F}_{p^n}$ is the finite field with p^n elements.

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$.

Plateaued Functions

For a prime power p^n, $\mathbb{F}_{p^n}$ is the finite field with p^n elements.

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p,\ F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$.

Recall $W_f(\omega) = \sum_{x\in\mathbb{F}_{p^n}} \xi_p^{f(x)+Tr(\omega x)}$ and
$W_F(a,\omega) = W_{Tr(aF)}(\omega) = \sum_{x\in\mathbb{F}_{p^n}} \xi_p^{Tr(aF(x))+Tr(\omega x)}$.

Plateaued Functions

For a prime power p^n, $\mathbb{F}_{p^n}$ is the finite field with p^n elements.

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$.

Recall $W_f(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{f(x)+Tr(\omega x)}$ and
$W_F(a, \omega) = W_{Tr(aF)}(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{Tr(aF(x))+Tr(\omega x)}$.

A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is s-**plateaued** if $|W_f(\omega)|^2 \in \{0, p^{n+s}\}$ for each $\omega \in \mathbb{F}_{p^n}$.

Plateaued Functions

For a prime power p^n, $\mathbb{F}_{p^n}$ is the finite field with p^n elements.

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p,\ F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$.

Recall $W_f(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{f(x)+Tr(\omega x)}$ and
$W_F(a, \omega) = W_{Tr(aF)}(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{Tr(aF(x))+Tr(\omega x)}$.

A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is ***s*-plateaued** if $|W_f(\omega)|^2 \in \{0, p^{n+s}\}$ for each $\omega \in \mathbb{F}_{p^n}$. Similarly, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is **vectorial plateaued** if its components are plateaued with possibly different amplitudes. F is **vectorial *s*-plateaued** if all components are s-plateaued.

Linear Codes

Linear Codes

A p-ary $[n, k, d]_p$ **linear code** C is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d.

Linear Codes

A p-ary $[n, k, d]_p$ **linear code** C is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d.

A code is **minimal** if there are no linearly independent codewords that cover each other (i.e. $supp(c) \not\subseteq supp(c')$ for any lin. indep. $c, c' \in \mathbb{F}_p^n$).

Linear Codes

A p-ary $[n, k, d]_p$ **linear code** C is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d.

A code is **minimal** if there are no linearly independent codewords that cover each other (i.e. $supp(c) \not\subseteq supp(c')$ for any lin. indep. $c, c' \in \mathbb{F}_p^n$).

A code is **self-dual** if $C = C^\perp$ and it is **self-orthogonal** if $C \subset C^\perp$, where $C^\perp$ is the (Euclidean) dual $C^\perp := \{x \in \mathbb{F}_p^n : \forall y \in C \ \langle x, y \rangle = 0\}$.

Codes from (vectorial) p-ary functions

Codes from (vectorial) p-ary functions

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

Codes from (vectorial) p-ary functions

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

Fixing an order (usually lexicoraphic), the truth table of f uniquely determines a vector in $(\mathbb{F}_p)^{p^n}$.

Codes from (vectorial) p-ary functions

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

Fixing an order (usually lexicoraphic), the truth table of f uniquely determines a vector in $(\mathbb{F}_p)^{p^n}$. For every $v \in \mathbb{F}_{p^n}$, consider the linear functions $l_v : \mathbb{F}_{p^n} \to \mathbb{F}_p$ given by $l_v(x) = \mathrm{Tr}(vx)$.

Codes from (vectorial) p-ary functions

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

Fixing an order (usually lexicoraphic), the truth table of f uniquely determines a vector in $(\mathbb{F}_p)^{p^n}$. For every $v \in \mathbb{F}_{p^n}$, consider the linear functions $l_v : \mathbb{F}_{p^n} \to \mathbb{F}_p$ given by $l_v(x) = \mathrm{Tr}(vx)$.

Theorem

For a non-affine function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that $f(0) = 0$, the set

$$C_f = \{(f(x) + l_v(x))_{x \in \mathbb{F}^{\star}_{p^n}} : v \in \mathbb{F}_{p^n}\}$$

is a linear code with parameters $[p^n - 1, n + 1]$.

Codes from (vectorial) p-ary functions

$f : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

Fixing an order (usually lexicoraphic), the truth table of f uniquely determines a vector in $(\mathbb{F}_p)^{p^n}$. For every $v \in \mathbb{F}_{p^n}$, consider the linear functions $l_v : \mathbb{F}_{p^n} \to \mathbb{F}_p$ given by $l_v(x) = \mathrm{Tr}(vx)$.

Theorem

For a non-affine function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that $f(0) = 0$, the set

$$C_f = \{(f(x) + l_v(x))_{x \in \mathbb{F}^\star_{p^n}} : v \in \mathbb{F}_{p^n}\}$$

is a linear code with parameters $[p^n - 1, n + 1]$.

For vectorial $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ with $F(0) = 0$, $C_F = \cup_{a \in \mathbb{F}_{p^m}} C_{\mathrm{Tr}(aF)}$.

Regularity of plateaued functions

Regularity of plateaued functions

It can be proved that for a plateaued function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$,
$W_f(\omega) = \pm \nu \xi_p^{f^*(\omega)} p^{\frac{n+s}{2}}$, where $\nu \in \{1, \sqrt{-1}\}$.

Regularity of plateaued functions

It can be proved that for a plateaued function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $W_f(\omega) = \pm\nu\xi_p^{f^*(\omega)} p^{\frac{n+s}{2}}$, where $\nu \in \{1, \sqrt{-1}\}$.

We call f weakly regular if the sign of $W_f(\omega)$ doesn't depend on ω, otherwise f is non-weakly regular.

What has been done?

What has been done?

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;
- Mesnager (2017): Weakly regular bent functions;

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;
- Mesnager (2017): Weakly regular bent functions;
- Mesnager, Özbudak, Sınak (2018): Weakly regular plateaued functions;

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;
- Mesnager (2017): Weakly regular bent functions;
- Mesnager, Özbudak, Sınak (2018): Weakly regular plateaued functions;
- Pelen (2020): Non-weakly regular bent;

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;
- Mesnager (2017): Weakly regular bent functions;
- Mesnager, Özbudak, Sınak (2018): Weakly regular plateaued functions;
- Pelen (2020): Non-weakly regular bent;
- Rodriguez, Pasalic, Zhang, Wei (2023): Non-weakly regular plateaued functions;

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;
- Mesnager (2017): Weakly regular bent functions;
- Mesnager, Özbudak, Sınak (2018): Weakly regular plateaued functions;
- Pelen (2020): Non-weakly regular bent;
- Rodriguez, Pasalic, Zhang, Wei (2023): Non-weakly regular plateaued functions;
- Wu, Yang, Feng (2023): Planar case in general (arxiv);

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;
- Mesnager (2017): Weakly regular bent functions;
- Mesnager, Özbudak, Sınak (2018): Weakly regular plateaued functions;
- Pelen (2020): Non-weakly regular bent;
- Rodriguez, Pasalic, Zhang, Wei (2023): Non-weakly regular plateaued functions;
- Wu, Yang, Feng (2023): Planar case in general (arxiv);
- Wei, Wang, Wei-Fu (2023): Non-weakly regular plateaued functions II (arxiv);

What has been done?

- Carlet, Ding, Yuan (2004): Introduced the method for planar functions;
- Li, Qu, Ling (2008): Extended to all known planar functions;
- Mesnager (2017): Weakly regular bent functions;
- Mesnager, Özbudak, Sınak (2018): Weakly regular plateaued functions;
- Pelen (2020): Non-weakly regular bent;
- Rodriguez, Pasalic, Zhang, Wei (2023): Non-weakly regular plateaued functions;
- Wu, Yang, Feng (2023): Planar case in general (arxiv);
- Wei, Wang, Wei-Fu (2023): Non-weakly regular plateaued functions II (arxiv);
- Li, Kan, Liu, Peng, Zheng, Zhuo (2024): Minimal ternary linear codes from regular vectorial functions (arxiv).

Let's have a look

Let's have a look

The "standard" approach focuses on computing the preimages of the dual.

Let's have a look

The "standard" approach focuses on computing the preimages of the dual.

Define $A_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = \nu\xi_p^j p^{\frac{n+s}{2}}\}|$ and
$B_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = -\nu\xi_p^j p^{\frac{n+s}{2}}|\}$.

Let's have a look

The "standard" approach focuses on computing the preimages of the dual.

Define $A_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = \nu \xi_p^j p^{\frac{n+s}{2}}\}|$ and
$B_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = -\nu \xi_p^j p^{\frac{n+s}{2}}|\}$.

- Parseval's identity:
  $p^n = \sum_{\omega \in \mathbb{F}_{p^n}} W_f(\omega) = \nu p^{\frac{n+s}{2}} \sum_{j \in \mathbb{F}_p^\star} (A_j - B_j - (A_0 - B_0))\xi_p^j$.

Let's have a look

The "standard" approach focuses on computing the preimages of the dual.

Define $A_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = \nu \xi_p^j p^{\frac{n+s}{2}}\}|$ and
$B_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = -\nu \xi_p^j p^{\frac{n+s}{2}}|\}$.

- Parseval's identity:
  $p^n = \sum_{\omega \in \mathbb{F}_{p^n}} W_f(\omega) = \nu p^{\frac{n+s}{2}} \sum_{j \in \mathbb{F}_p^\star} (A_j - B_j - (A_0 - B_0))\xi_p^j$.
- Use known solutions for equations in $\mathbb{Q}(\xi_p)$ to express $A_j - B_j$ in terms of $A_0 - B_0$.

Let's have a look

The "standard" approach focuses on computing the preimages of the dual.

Define $A_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = \nu \xi_p^j p^{\frac{n+s}{2}}\}|$ and
$B_j = |\{\omega \in \mathbb{F}_{p^n} \colon W_f(\omega) = -\nu \xi_p^j p^{\frac{n+s}{2}}|\}$.

- Parseval's identity:
  $p^n = \sum_{\omega \in \mathbb{F}_{p^n}} W_f(\omega) = \nu p^{\frac{n+s}{2}} \sum_{j \in \mathbb{F}_p^\star} (A_j - B_j - (A_0 - B_0))\xi_p^j$.
- Use known solutions for equations in $\mathbb{Q}(\xi_p)$ to express $A_j - B_j$ in terms of $A_0 - B_0$.
- This is possible since $\{\xi_p, \ldots, \xi_p^{p-1}\}$ is an integral basis for $\mathbb{Q}(\xi_p)$.

Aha!

Aha!

There's a minor detail...

Aha!

There's a minor detail...

The values of $A_j - B_j$ of the integral polynomial in ξ_p could be zero.

Aha!

There's a minor detail...

The values of $A_j - B_j$ of the integral polynomial in ξ_p could be zero. These cases must be considered separately.

Adapting the previous approach to these possibilities, we get the following.

Adapting the previous approach to these possibilities, we get the following.

Lemma

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be any s-plateaued function. Let $f(0) = 0$. Then $A_0 \neq B_0$.

Adapting the previous approach to these possibilities, we get the following.

Lemma

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be any s-plateaued function. Let $f(0) = 0$. Then $A_0 \neq B_0$. The distribution values A_j, B_j associated to f satisfy exactly one of the following.

Adapting the previous approach to these possibilities, we get the following.

Lemma

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be any s-plateaued function. Let $f(0) = 0$. Then $A_0 \neq B_0$. The distribution values A_j, B_j associated to f satisfy exactly one of the following.

i) $A_j \neq B_j$ for every j;

Adapting the previous approach to these possibilities, we get the following.

Lemma

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be any s-plateaued function. Let $f(0) = 0$. Then $A_0 \neq B_0$. The distribution values A_j, B_j associated to f satisfy exactly one of the following.

1. $A_j \neq B_j$ for every j;
2. The number $n - s$ is even and $A_j = B_j$ for each $j \neq 0$.

Adapting the previous approach to these possibilities, we get the following.

Lemma

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be any s-plateaued function. Let $f(0) = 0$. Then $A_0 \neq B_0$. The distribution values A_j, B_j associated to f satisfy exactly one of the following.

1. $A_j \neq B_j$ for every j;
2. The number $n - s$ is even and $A_j = B_j$ for each $j \neq 0$.
3. The number $n - s$ is odd and $A_j = B_j$ for $j \in \mathcal{I}$ and $A_j - B_j = 2\sigma \left(\frac{j}{p}\right) p^{\frac{n-s-1}{2}}$ for $j \notin \mathcal{I}$, where

$$\sigma = \begin{cases} 1, & p \equiv 1 \pmod 4; \\ -1, & p \equiv 3 \pmod 4; \end{cases}$$

and

$$\mathcal{I} = \begin{cases} QR^*, & \frac{A_0 - B_0}{|A_0 - B_0|} = -\sigma; \\ NQR, & \textit{otherwise}. \end{cases}$$

Thus we can partition the set of plateaued functions into three classes that we call $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$.

Thus we can partition the set of plateaued functions into three classes that we call $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$.

Example (see the whiteboard).

The codes

The codes

Considering this partition, the WD of all codes C_f from plateaued functions for $n+s$ odd is obtained (in terms of $wt(f^*)$).

The codes

Considering this partition, the WD of all codes C_f from plateaued functions for $n+s$ odd is obtained (in terms of $wt(f^*)$).

Theorem

Suppose that $n+s$ is odd. Let f be any s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0)=0$ such that $f \notin \mathcal{P}_2$[a]. The code $\mathcal{C}_f$ is a three-valued code with parameters $[p^n-1, n+1, (p-1)p^{n-1} - p^{\frac{n+s-1}{2}}]$.

[a] This class contains the degenerate cases which yield 2-weight codes

We can also establish the weight distribution of codes C_f for $n+s$ even in terms of the dual weight and $A_0 - B_0$.

We can also establish the weight distribution of codes C_f for $n+s$ even in terms of the dual weight and $A_0 - B_0$.

Theorem

Suppose that $n+s$ is even. Let $f \in \mathcal{C}_1$ be an s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0) = f^*(0) = 0$. The code $\mathcal{C}_f$ is a five-valued code with parameters $[p^n - 1, n+1, p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)]$.

We can also establish the weight distribution of codes C_f for $n+s$ even in terms of the dual weight and $A_0 - B_0$.

Theorem

Suppose that $n+s$ is even. Let $f \in \mathcal{C}_1$ be an s-plateaued function defined over $\mathbb{F}_{p^n}$ with $f(0) = f^*(0) = 0$. The code $\mathcal{C}_f$ is a five-valued code with parameters $[p^n - 1, n+1, p^n - p^{n-1} - p^{(n+s-2)/2}(p-1)]$.

Similar results for $f \in \mathcal{C}_2$.

Some results...

Some results...

Imposing some conditions on the dual (e.g. $W_{f^*}(0) = \pm\nu' p^{\frac{\theta}{2}}$) we can derive more precise values for the weight distributions...

Some results...

Imposing some conditions on the dual (e.g. $W_{f^*}(0) = \pm\nu' p^{\frac{\theta}{2}}$) we can derive more precise values for the weight distributions...

It's also not too hard to show that the codes are minimal and self-orthogonal!

A similar approach

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

Two interesting examples:

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

Two interesting examples:

Example

For an integer k with $n/\gcd(n,k)$ odd,

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

Two interesting examples:

Example

For an integer k with $n/\gcd(n,k)$ odd,

- $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(x) = x^{(p^{2k}+1)/2}$.

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

Two interesting examples:

Example

For an integer k with $n/\gcd(n,k)$ odd,

- $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(x) = x^{(p^{2k}+1)/2}$.
- $F'\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F'(x) = x^{p^{2k}-p^k+1}$.

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

Two interesting examples:

Example

For an integer k with $n/\gcd(n,k)$ odd,

- $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(x) = x^{(p^{2k}+1)/2}$.
- $F'\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F'(x) = x^{p^{2k}-p^k+1}$.

All components of F and F' have zero duals... The WD of codes C_F are easily derived.

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

Two interesting examples:

Example

For an integer k with $n/\gcd(n,k)$ odd,

- $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(x) = x^{(p^{2k}+1)/2}$.
- $F'\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F'(x) = x^{p^{2k}-p^k+1}$.

All components of F and F' have zero duals... The WD of codes C_F are easily derived. Another infinite family: $G(x,y) = x^2 + y^7$ for $x, y \in \mathbb{F}_{3^3}$.

A similar approach

Unfortunately, not too much is known about vectorial plateaued functions (non-planar nor quadratic?) :(

Two interesting examples:

Example

For an integer k with $n/\gcd(n,k)$ odd,

- $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F(x) = x^{(p^{2k}+1)/2}$.
- $F'\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $F'(x) = x^{p^{2k}-p^k+1}$.

All components of F and F' have zero duals... The WD of codes C_F are easily derived. Another infinite family: $G(x,y) = x^2 + y^7$ for $x, y \in \mathbb{F}_{3^3}$. **Its components have different amplitudes but WD can be easily computed.**

A beautiful place

A beautiful place

Bonus result

Bonus result

All the presented codes are **self-orthogonal and minimal.**

Bonus result

All the presented codes are **self-orthogonal and minimal.** That's somewhat the best we can expect due to the following:

Bonus result

All the presented codes are **self-orthogonal and minimal.** That's somewhat the best we can expect due to the following:

Proposition

There are no self-dual minimal linear codes for $q > 3$. The only self-dual minimal ternary code is the tetracode $[4, 2, 3]_3$, whereas the only self-dual minimal binary code is the repetition code $[2, 1, 2]_2$.

Bonus result

All the presented codes are **self-orthogonal and minimal.** That's somewhat the best we can expect due to the following:

Proposition

There are no self-dual minimal linear codes for $q > 3$. The only self-dual minimal ternary code is the tetracode $[4, 2, 3]_3$, whereas the only self-dual minimal binary code is the repetition code $[2, 1, 2]_2$.

(Very short) sketch of proof:

Bonus result

All the presented codes are **self-orthogonal and minimal.** That's somewhat the best we can expect due to the following:

Proposition

There are no self-dual minimal linear codes for $q > 3$. The only self-dual minimal ternary code is the tetracode $[4, 2, 3]_3$, whereas the only self-dual minimal binary code is the repetition code $[2, 1, 2]_2$.

(Very short) sketch of proof:

- For $q > 3$, $\frac{n}{2} + q - 2 \leq d_{min} \leq d_{max} \leq \frac{n}{2} + 1$.

Bonus result

All the presented codes are **self-orthogonal and minimal.** That's somewhat the best we can expect due to the following:

Proposition

There are no self-dual minimal linear codes for $q > 3$. The only self-dual minimal ternary code is the tetracode $[4, 2, 3]_3$, whereas the only self-dual minimal binary code is the repetition code $[2, 1, 2]_2$.

(Very short) sketch of proof:

- For $q > 3$, $\frac{n}{2} + q - 2 \leq d_{min} \leq d_{max} \leq \frac{n}{2} + 1$.
- The cases $q = 2, 3$ require the known machinery developed for self-dual codes, i.e. Type I, Type II, Type III arguments.

Open questions

Open questions

- Find infinite families in $\mathcal{C}_2$ and $\mathcal{C}_3$ for each p and n;

Open questions

- Find infinite families in $\mathcal{C}_2$ and $\mathcal{C}_3$ for each p and n;
- Explicitly compute the values of A_0 and B_0;

Open questions

- Find infinite families in $\mathcal{C}_2$ and $\mathcal{C}_3$ for each p and n;
- Explicitly compute the values of A_0 and B_0;
- Find more families of vectorial plateaued functions;

Open questions

- Find infinite families in $\mathcal{C}_2$ and $\mathcal{C}_3$ for each p and n;
- Explicitly compute the values of A_0 and B_0;
- Find more families of vectorial plateaued functions;
- And many more...

Open questions

- Find infinite families in $\mathcal{C}_2$ and $\mathcal{C}_3$ for each p and n;
- Explicitly compute the values of A_0 and B_0;
- Find more families of vectorial plateaued functions;
- And many more...

Thank you for your attention.