A Note on Vectorial Boolean Functions as Embeddings

Augustine Musukwa[1] and Massimiliano Sala[2]

[1,2]University of Trento, Italy

[1]Mzuzu University, Malawi

September 13, 2024

Outline

- Motivation

Outline

- Motivation
- Preliminaries and Notations

Outline

- Motivation
- Preliminaries and Notations
- Preliminary results

Outline

- Motivation
- Preliminaries and Notations
- Preliminary results
- Main results

Motivation

- Recently functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$, have gained attention.

Motivation

- Recently functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$, have gained attention.
- Abbondati et al in 2024 and Taniguchi in 2023 studied APN functions F that satisfy Dillon's property

Motivation

- Recently functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$, have gained attention.
- Abbondati et al in 2024 and Taniguchi in 2023 studied APN functions F that satisfy Dillon's property :

$$\{F(x) + F(y) + F(z) + F(x + y + z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^m.$$

Motivation

- Recently functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$, have gained attention.
- Abbondati et al in 2024 and Taniguchi in 2023 studied APN functions F that satisfy Dillon's property :

$$\{F(x) + F(y) + F(z) + F(x + y + z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^m.$$

- Aragona et al in 2019, injective APN functions were used in a cipher.

Motivation

- Recently functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$, have gained attention.
- Abbondati et al in 2024 and Taniguchi in 2023 studied APN functions F that satisfy Dillon's property :

$$\{F(x) + F(y) + F(z) + F(x + y + z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^m.$$

- Aragona et al in 2019, injective APN functions were used in a cipher.
- In this work, we are interested in injective functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$.

Motivation

- Recently functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$, have gained attention.
- Abbondati et al in 2024 and Taniguchi in 2023 studied APN functions F that satisfy Dillon's property :

$$\{F(x) + F(y) + F(z) + F(x + y + z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^m.$$

- Aragona et al in 2019, injective APN functions were used in a cipher.
- In this work, we are interested in injective functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, with $m > n$.
- We want to understand whether these functions have balanced components.

Preliminaries and Notations

- We denote the field of two elements, 0 and 1, by $\mathbb{F}$.

Preliminaries and Notations

- We denote the field of two elements, 0 and 1, by $\mathbb{F}$.
- $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.

Preliminaries and Notations

- We denote the field of two elements, 0 and 1, by $\mathbb{F}$.
- $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.
- A zero in $\mathbb{F}^n$ is denoted by 0_n.

Preliminaries and Notations

- We denote the field of two elements, 0 and 1, by $\mathbb{F}$.
- $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.
- A zero in $\mathbb{F}^n$ is denoted by 0_n.
- A *Vectorial Boolean function (vBf)* is any function F from $\mathbb{F}^n$ to $\mathbb{F}^m$.

Preliminaries and Notations

- We denote the field of two elements, 0 and 1, by $\mathbb{F}$.
- $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.
- A zero in $\mathbb{F}^n$ is denoted by 0_n.
- A *Vectorial Boolean function (vBf)* is any function F from $\mathbb{F}^n$ to $\mathbb{F}^m$.
- If $m = 1$, we simply say a *Boolean function (Bf)* and denote it by f.

Preliminaries and Notations

- We denote the field of two elements, 0 and 1, by $\mathbb{F}$.
- $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.
- A zero in $\mathbb{F}^n$ is denoted by 0_n.
- A *Vectorial Boolean function (vBf)* is any function F from $\mathbb{F}^n$ to $\mathbb{F}^m$.
- If $m = 1$, we simply say a *Boolean function (Bf)* and denote it by f.
- Algebraic Normal Form:

$$f(x_1, \cdots, x_n) = \sum_{I \subseteq P} a_I \prod_{i \in I} x_i$$

where $P = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}$.

Preliminaries and Notations

- Degree of f: $\deg(f) = \max_{I \subseteq P}\{|I| \mid a_I \neq 0\}$.

Preliminaries and Notations

- Degree of f: $\deg(f) = \max_{I \subseteq P}\{|I| \mid a_I \neq 0\}$.
- If $\deg(f) \leq 1$, f is called *affine*.

Preliminaries and Notations

- Degree of f: $\deg(f) = \max_{I \subseteq P}\{|I| \mid a_I \neq 0\}$.
- If $\deg(f) \leq 1$, f is called *affine*.
- If $\deg(f) \leq 1$ and $f(0_n) = 0$, f is called *linear*.

Preliminaries and Notations

- Degree of f: $\deg(f) = \max_{I \subseteq P}\{|I| \mid a_I \neq 0\}$.
- If $\deg(f) \leq 1$, f is called *affine*.
- If $\deg(f) \leq 1$ and $f(0_n) = 0$, f is called *linear*.
- If $\deg(f) = 2$, f is called *quadratic*.

Preliminaries and Notations

- Degree of f: $\deg(f) = \max_{I \subseteq P}\{|I| \mid a_I \neq 0\}$.
- If $\deg(f) \leq 1$, f is called *affine*.
- If $\deg(f) \leq 1$ and $f(0_n) = 0$, f is called *linear*.
- If $\deg(f) = 2$, f is called *quadratic*.
- The *weight* of a Boolean function f: $\mathrm{wt}(f) = |\{x \in \mathbb{F}^n \mid f(x) = 1\}|$.

Preliminaries and Notations

- Degree of f: $\deg(f) = \max_{I \subseteq P}\{|I| \mid a_I \neq 0\}$.
- If $\deg(f) \leq 1$, f is called *affine*.
- If $\deg(f) \leq 1$ and $f(0_n) = 0$, f is called *linear*.
- If $\deg(f) = 2$, f is called *quadratic*.
- The *weight* of a Boolean function f: $\mathrm{wt}(f) = |\{x \in \mathbb{F}^n \mid f(x) = 1\}|$.
- f is balanced if $\mathrm{wt}(f) = 2^{n-1}$.

Preliminaries and Notations

- We can write $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m$ are Boolean functions called *coordinate functions* of F.

Preliminaries and Notations

- We can write $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m$ are Boolean functions called *coordinate functions* of F.
- For any nonzero $\lambda \in \mathbb{F}^m$, we call $F_\lambda = \lambda \cdot F$ a component of F.

Preliminaries and Notations

- We can write $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m$ are Boolean functions called *coordinate functions* of F.
- For any nonzero $\lambda \in \mathbb{F}^m$, we call $F_\lambda = \lambda \cdot F$ a component of F.
- F is balanced if and only if all its components are balanced.

Preliminaries and Notations

- We can write $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m$ are Boolean functions called *coordinate functions* of F.
- For any nonzero $\lambda \in \mathbb{F}^m$, we call $F_\lambda = \lambda \cdot F$ a component of F.
- F is balanced if and only if all its components are balanced.
- An *image* of F is defined by $\mathrm{Im}(F) = \{F(x) : x \in \mathbb{F}^n\}$.

Preliminaries and Notations

- We can write $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m$ are Boolean functions called *coordinate functions* of F.
- For any nonzero $\lambda \in \mathbb{F}^m$, we call $F_\lambda = \lambda \cdot F$ a component of F.
- F is balanced if and only if all its components are balanced.
- An *image* of F is defined by $\mathrm{Im}(F) = \{F(x) : x \in \mathbb{F}^n\}$.
- We say that F is *injective* if $|\mathrm{Im}(F)| = 2^n$.

Preliminaries and Notations

- We can write $F = (f_1, \ldots, f_m)$, where $f_1, \ldots, f_m$ are Boolean functions called *coordinate functions* of F.
- For any nonzero $\lambda \in \mathbb{F}^m$, we call $F_\lambda = \lambda \cdot F$ a component of F.
- F is balanced if and only if all its components are balanced.
- An *image* of F is defined by $\mathrm{Im}(F) = \{F(x) : x \in \mathbb{F}^n\}$.
- We say that F is *injective* if $|\mathrm{Im}(F)| = 2^n$.
- We call injective functions from $\mathbb{F}^n$ into $\mathbb{F}^m$ *embeddings*.

Preliminaries and Notations

- The *Walsh transform* of a Bf f:

$$\mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a \cdot x},$$

for all $a \in \mathbb{F}^n$.

Preliminaries and Notations

- The *Walsh transform* of a Bf f:

$$\mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a \cdot x},$$

for all $a \in \mathbb{F}^n$.

- We define $\mathcal{F}(f)$ as

$$\mathcal{F}(f) = \mathcal{W}_f(0_n) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)} = 2^n - 2\mathrm{wt}(f).$$

Preliminaries and Notations

- The *Walsh transform* of a Bf f:

$$\mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a\cdot x},$$

for all $a \in \mathbb{F}^n$.

- We define $\mathcal{F}(f)$ as

$$\mathcal{F}(f) = \mathcal{W}_f(0_n) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)} = 2^n - 2\mathrm{wt}(f).$$

- Observe that f is balanced if and only if $\mathcal{F}(f) = 0$.

- Nonlinearity of a Bf f:

$$N(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}^n} |\mathcal{W}_f(a)| \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Preliminaries and Notations

- Nonlinearity of a Bf f:

$$N(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}^n} |\mathcal{W}_f(a)| \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

- f is called *bent* if $N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and this happens only when n is even.

Preliminaries and Notations

- Nonlinearity of a Bf f:

$$N(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}^n}|\mathcal{W}_f(a)| \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

- f is called *bent* if $N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and this happens only when n is even.
- f is called *semi-bent* if $N(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$ and this happens only when n is odd.

First-order derivatives of Bf and vBf

- The *first-order derivative* of f at $a \in \mathbb{F}^n$: $D_a f(x) = f(x+a) + f(x)$.

First-order derivatives of Bf and vBf

- The *first-order derivative* of f at $a \in \mathbb{F}^n$: $D_a f(x) = f(x+a) + f(x)$.
- The *first-order derivative* of F at $a \in \mathbb{F}^n$: $D_a F(x) = F(x+a) + F(x)$.

Preliminaries and Notations

First-order derivatives of Bf and vBf

- The *first-order derivative* of f at $a \in \mathbb{F}^n$: $D_a f(x) = f(x+a) + f(x)$.
- The *first-order derivative* of F at $a \in \mathbb{F}^n$: $D_a F(x) = F(x+a) + F(x)$.
- An element $a \in \mathbb{F}^n$ is called a *linear structure* of f if $D_a f$ is constant.

Preliminaries and Notations

First-order derivatives of Bf and vBf

- The *first-order derivative* of f at $a \in \mathbb{F}^n$: $D_a f(x) = f(x+a) + f(x)$.
- The *first-order derivative* of F at $a \in \mathbb{F}^n$: $D_a F(x) = F(x+a) + F(x)$.
- An element $a \in \mathbb{F}^n$ is called a *linear structure* of f if $D_a f$ is constant.
- The set of all linear structures of f is denoted by $V(f)$.

Preliminaries and Notations

First-order derivatives of Bf and vBf

- The *first-order derivative* of f at $a \in \mathbb{F}^n$: $D_a f(x) = f(x+a) + f(x)$.
- The *first-order derivative* of F at $a \in \mathbb{F}^n$: $D_a F(x) = F(x+a) + F(x)$.
- An element $a \in \mathbb{F}^n$ is called a *linear structure* of f if $D_a f$ is constant.
- The set of all linear structures of f is denoted by $V(f)$.
- It is well-known that $V(f)$ is a subspace of $\mathbb{F}^n$.

Preliminaries and Notations

- It is well-known that f is called *bent* if and only if $D_a f$ is balanced, for all nonzero $a \in \mathbb{F}^n$.

Preliminaries and Notations

- It is well-known that f is called *bent* if and only if $D_a f$ is balanced, for all nonzero $a \in \mathbb{F}^n$.
- It follows that if f is bent, then $\dim V(f) = 0$.

Preliminaries and Notations

- It is well-known that f is called *bent* if and only if $D_a f$ is balanced, for all nonzero $a \in \mathbb{F}^n$.
- It follows that if f is bent, then $\dim V(f) = 0$.
- It is well-known that for a quadratic semi-bent f we have $\dim V(f) = 1$.

Preliminaries and Notations

- It is well-known that f is called *bent* if and only if $D_a f$ is balanced, for all nonzero $a \in \mathbb{F}^n$.
- It follows that if f is bent, then $\dim V(f) = 0$.
- It is well-known that for a quadratic semi-bent f we have $\dim V(f) = 1$.
- For any unbalanced quadratic Boolean function f, it is known that $\mathcal{F}(f) = \pm 2^{\frac{n+k}{2}}$, where $k = \dim V(f)$.

Remark 2

For any given Bf f, it can be easily shown that

$$\mathcal{F}^2(f) = \sum_{a \in \mathbb{F}^n} \mathcal{F}(D_a f).$$

Preliminary Results

Remark 2

For any given Bf f, it can be easily shown that

$$\mathcal{F}^2(f) = \sum_{a\in\mathbb{F}^n} \mathcal{F}(D_a f).$$

Remark 3

Let f be a Bf on n variables. Then

$$\sum_{a\in\mathbb{F}^n} \mathrm{wt}(D_a f) = 2^{2n-1} - \frac{1}{2}\mathcal{F}^2(f).$$

Preliminary Results

Lemma 4

Let f be a Bf on n variables. Then

$$\sum_{a \in \mathbb{F}^n} \mathrm{wt}(D_a f) \leq 2^{2n-1}.$$

Furthermore, equality holds if and only if f is balanced.

Preliminary Results

Lemma 4

Let f be a Bf on n variables. Then

$$\sum_{a \in \mathbb{F}^n} \mathrm{wt}(D_a f) \leq 2^{2n-1}.$$

Furthermore, equality holds if and only if f is balanced.

Proposition 5

Let f be any quadratic Bf on n variables. Then

$$\sum_{a \in \mathbb{F}^n} \mathrm{wt}(D_a f) = \begin{cases} 2^{2n-1} & \text{if } f \text{ is balanced} \\ 2^{2n-1} - 2^{n+k-1} & \text{otherwise,} \end{cases}$$

where $k = \dim V(f)$.

Main Results

Remark 6

Let $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ be any vBf. For any $a, x \in \mathbb{F}^n$, we have

$$\sum_{\lambda \in \mathbb{F}^m} (-1)^{\lambda \cdot [F(x)+F(x+a)]} = \begin{cases} 2^m & \text{if } F(x) = F(x+a) \\ 0 & \text{otherwise.} \end{cases}$$

Main Results

Remark 6

Let $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ be any vBf. For any $a, x \in \mathbb{F}^n$, we have

$$\sum_{\lambda \in \mathbb{F}^m} (-1)^{\lambda \cdot [F(x)+F(x+a)]} = \begin{cases} 2^m & \text{if } F(x) = F(x+a) \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 7

Let F be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m \geq n$. Then

$$\sum_{\lambda \in \mathbb{F}^m} \mathcal{F}^2(F_\lambda) \geq 2^{n+m}.$$

Moreover, equality holds if and only if F is an embedding.

Main Results

Corollary 8

Let $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$, with $m \geq n$, be any vBf. Then

$$\sum_{\lambda, a \in \mathbb{F}^m} \mathcal{F}(D_a F_\lambda) \geq 2^{n+m}.$$

Moreover, equality holds if and only if F is an embedding.

Main Results

Corollary 8

Let $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$, with $m \geq n$, be any vBf. Then

$$\sum_{\lambda, a \in \mathbb{F}^m} \mathcal{F}(D_a F_\lambda) \geq 2^{n+m}.$$

Moreover, equality holds if and only if F is an embedding.

Theorem 9

Let F be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m \geq n$. Then

$$\sum_{\lambda \in \mathbb{F}^m \setminus \{0_m\}} \sum_{a \in \mathbb{F}^n} \mathrm{wt}(D_a F_\lambda) \leq 2^{2n-1}(2^m - 2^{m-n}).$$

Moreover, equality holds if and only if F is an embedding.

Main Results

Definition

Let F be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m \geq n$. Define the set of balanced components of F by $B(F) = \{\lambda \in \mathbb{F}^m \mid \mathrm{wt}(F_\lambda) = 2^{n-1}\}$.

Main Results

Definition

Let F be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m \geq n$. Define the set of balanced components of F by $B(F) = \{\lambda \in \mathbb{F}^m \mid \mathrm{wt}(F_\lambda) = 2^{n-1}\}$.

Corollary 10

Let F be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m \geq n$. Then $|B(F)| \leq 2^m - 2^{m-n}$. Furthermore, equality holds if and only if 2^{m-n} are constant components and F is an embedding.

Main Results

Definition

Let F be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m \geq n$. Define the set of balanced components of F by $B(F) = \{\lambda \in \mathbb{F}^m \mid \mathrm{wt}(F_\lambda) = 2^{n-1}\}$.

Corollary 10

Let F be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m \geq n$. Then $|B(F)| \leq 2^m - 2^{m-n}$. Furthermore, equality holds if and only if 2^{m-n} are constant components and F is an embedding.

Remark 11

Observe from Corollary 10 that no vBf from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m > n$, can have all its components balanced.

Main Results

Next we give a lower bound on the number of balanced components of quadratic embeddings from $\mathbb{F}^n$ into $\mathbb{F}^m$.

Main Results

Next we give a lower bound on the number of balanced components of quadratic embeddings from $\mathbb{F}^n$ into $\mathbb{F}^m$.

Theorem 12

Let F be a quadratic embedding from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m > n$.

Main Results

Next we give a lower bound on the number of balanced components of quadratic embeddings from $\mathbb{F}^n$ into $\mathbb{F}^m$.

Theorem 12

Let F be a quadratic embedding from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m > n$. Then

(i) $|B(F)| \geq 2^n - 1$, for n even and equality holds if and only if all the other components are bent,

Main Results

Next we give a lower bound on the number of balanced components of quadratic embeddings from $\mathbb{F}^n$ into $\mathbb{F}^m$.

Theorem 12

Let F be a quadratic embedding from $\mathbb{F}^n$ into $\mathbb{F}^m$, with $m > n$. Then

(i) $|B(F)| \geq 2^n - 1$, for n even and equality holds if and only if all the other components are bent,

(ii) $|B(F)| \geq 2^{m-1} + 2^{n-1} - 1$, for n odd and equality holds if and only if all the other components are unbalanced semi-bent.

Main Results

Example 1

The coordinate functions of a quadratic embedding F from $\mathbb{F}^3$ into $\mathbb{F}^4$:

$$
\begin{aligned}
f_1 &= x_1x_2 + x_1 + x_2 + x_3, \\
f_2 &= x_1x_3 + x_1 + x_2 + x_3, \\
f_3 &= x_2x_3 + x_1 + x_2, \\
f_4 &= x_1 + x_3
\end{aligned}
$$

Main Results

Example 1

The coordinate functions of a quadratic embedding F from $\mathbb{F}^3$ into $\mathbb{F}^4$:

$$\begin{aligned} f_1 &= x_1x_2 + x_1 + x_2 + x_3, \\ f_2 &= x_1x_3 + x_1 + x_2 + x_3, \\ f_3 &= x_2x_3 + x_1 + x_2, \\ f_4 &= x_1 + x_3 \end{aligned}$$

F has 11 balanced components and 4 unbalanced semi-bent components.

Main Results

Example 1

The coordinate functions of a quadratic embedding F from $\mathbb{F}^3$ into $\mathbb{F}^4$:

$$\begin{aligned} f_1 &= x_1x_2 + x_1 + x_2 + x_3, \\ f_2 &= x_1x_3 + x_1 + x_2 + x_3, \\ f_3 &= x_2x_3 + x_1 + x_2, \\ f_4 &= x_1 + x_3 \end{aligned}$$

F has 11 balanced components and 4 unbalanced semi-bent components.

14 components are quadratic, while only one component is linear.

Main Results

Example 2

The coordinate functions of a quadratic embedding F from $\mathbb{F}^4$ into $\mathbb{F}^5$:

$$
\begin{aligned}
f_1 &= x_1x_2 + x_4,\\
f_2 &= x_1x_3 + x_3 + x_4,\\
f_3 &= x_1x_4 + x_3x_4 + x_2,\\
f_4 &= x_2x_3 + x_3x_4 + x_1 + x_4,\\
f_5 &= x_1x_3 + x_2x_4.
\end{aligned}
$$

Main Results

Example 2

The coordinate functions of a quadratic embedding F from $\mathbb{F}^4$ into $\mathbb{F}^5$:

$$\begin{aligned} f_1 &= x_1x_2 + x_4, \\ f_2 &= x_1x_3 + x_3 + x_4, \\ f_3 &= x_1x_4 + x_3x_4 + x_2, \\ f_4 &= x_2x_3 + x_3x_4 + x_1 + x_4, \\ f_5 &= x_1x_3 + x_2x_4. \end{aligned}$$

F has 15 balanced components and 16 bent components.

Main Results

Next we consider a special case where the image of F is subspace of $\mathbb{F}^m$.

Main Results

Next we consider a special case where the image of F is subspace of $\mathbb{F}^m$.

Theorem 13

Let $F : \mathbb{F}^n \longrightarrow \mathbb{F}^m$, with $m \geq n$, be an embedding and $\mathrm{Im}(F)$ be a subspace of $\mathbb{F}^m$. Then, for all $\lambda \in \mathbb{F}^m$, there are only two cases: either F_λ is constant or balanced. Precisely, $|B(F)| = 2^m - 2^{m-n}$ and 2^{m-n} constant components of F.

References

1 Abbondati, M., Calderini, M. and Villa, I.: On Dillon's property of (n, m)-functions. Cryptogr. Commun. (2024). https://doi.org/10.1007/s12095-024-00730-1

2 Aragona, R., Calderini, M., Civino, R., Sala, M., Zappatore, I.: Wave shaped round functions and primitive groups. Adv. Math. Commun. 13(1), (2019), 67-88.

3 Taniguchi, H.: D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$. Cryptography and Communications, 15 (2023), 627–647.

THANK YOU FOR YOUR ATTENTION