On the algebraic degree stability of Boolean functions when restricted to affine spaces

13th International Workshop on Coding and Cryptography

Claude Carlet, Serge Feukoua, Ana Sălăgean

Loughborough University

June 2024

Contents

Motivation

- Boolean functions are used in symmetric ciphers, e.g. filter or combining functions in stream ciphers, S-Box in block ciphers.
- Several cryptanalysis methods exploit low algebraic degree e.g. fast algebraic attacks, higher order differential attacks. In those situations we need to ensure the degree is sufficiently high to prevent these attacks.
- In guess and determine attacks the attacker can make assumptions resulting in the fact that the input to the function is restricted to a particular affine space. The algebraic degree should remain high to avoid these attacks.

Motivation

- Boolean functions are used in symmetric ciphers, e.g. filter or combining functions in stream ciphers, S-Box in block ciphers.
- Several cryptanalysis methods exploit low algebraic degree e.g. fast algebraic attacks, higher order differential attacks. In those situations we need to ensure the degree is sufficiently high to prevent these attacks.
- In guess and determine attacks the attacker can make assumptions resulting in the fact that the input to the function is restricted to a particular affine space. The algebraic degree should remain high to avoid these attacks.

Motivation

- Boolean functions are used in symmetric ciphers, e.g. filter or combining functions in stream ciphers, S-Box in block ciphers.
- Several cryptanalysis methods exploit low algebraic degree e.g. fast algebraic attacks, higher order differential attacks. In those situations we need to ensure the degree is sufficiently high to prevent these attacks.
- In guess and determine attacks the attacker can make assumptions resulting in the fact that the input to the function is restricted to a particular affine space. The algebraic degree should remain high to avoid these attacks.

Previous work

- It is therefore important that the algebraic degree of the function remains high when the function is restricted to an affine space of low co-dimension.
- [Carlet, Feukoua, 2017] studied infinite classes of functions whose algebraic degree remains unchanged when they are restricted to any affine hyperplane.
- However, no general characterization was given.

Previous work

- It is therefore important that the algebraic degree of the function remains high when the function is restricted to an affine space of low co-dimension.
- [Carlet, Feukoua, 2017] studied infinite classes of functions whose algebraic degree remains unchanged when they are restricted to any affine hyperplane.
- However, no general characterization was given.

Previous work

- It is therefore important that the algebraic degree of the function remains high when the function is restricted to an affine space of low co-dimension.
- [Carlet, Feukoua, 2017] studied infinite classes of functions whose algebraic degree remains unchanged when they are restricted to any affine hyperplane.
- However, no general characterization was given.

Present work

We start a systematic study of the functions which keep their degree unchanged when restricted to affine spaces of low co-dimension k.
We give results on

- characterizations of these functions.
- the behaviour of symmetric functions restricted to hyperplanes
- the behaviour of direct sums of monomials restricted to any affine space
- experimental results for all the functions in at most 8 variables restricted to any affine space.

Present work

We start a systematic study of the functions which keep their degree unchanged when restricted to affine spaces of low co-dimension k. We give results on

- characterizations of these functions.
- the behaviour of symmetric functions restricted to hyperplanes
- the behaviour of direct sums of monomials restricted to any affine space
- experimental results for all the functions in at most 8 variables restricted to any affine space.

Present work

We start a systematic study of the functions which keep their degree unchanged when restricted to affine spaces of low co-dimension k.
We give results on

- characterizations of these functions.
- the behaviour of symmetric functions restricted to hyperplanes
- the behaviour of direct sums of monomials restricted to any affine space
- experimental results for all the functions in at most 8 variables restricted to any affine space.

Present work

We start a systematic study of the functions which keep their degree unchanged when restricted to affine spaces of low co-dimension k. We give results on

- characterizations of these functions.
- the behaviour of symmetric functions restricted to hyperplanes
- the behaviour of direct sums of monomials restricted to any affine space
- experimental results for all the functions in at most 8 variables restricted to any affine space.

Present work

We start a systematic study of the functions which keep their degree unchanged when restricted to affine spaces of low co-dimension k.
We give results on

- characterizations of these functions.
- the behaviour of symmetric functions restricted to hyperplanes
- the behaviour of direct sums of monomials restricted to any affine space
- experimental results for all the functions in at most 8 variables restricted to any affine space.

Contents

Basic concepts

- $\mathbb{F}_2$ the finite field with two elements
- $\mathbb{F}_2^n$ the vector space over $\mathbb{F}_2$ of all binary vectors of length n.
- A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented in *Algebraic Normal Form* (ANF) i.e. as a polynomial function in n variables, of degree at most one in each variable ($x_i^2 = x_i$).
- $\deg(f)$, the *algebraic degree* of f, is the degree of its ANF.
- The Reed-Muller code RM(r,n) is the vector space of all n-variable Boolean functions of algebraic degree at most r.
- $\mathrm{Var}(f)$: the set of all $i \in \{1, \ldots, n\}$ such that x_i appears in the ANF of f.

Basic concepts

- $\mathbb{F}_2$ the finite field with two elements
- $\mathbb{F}_2^n$ the vector space over $\mathbb{F}_2$ of all binary vectors of length n.
- A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented in *Algebraic Normal Form* (ANF) i.e. as a polynomial function in n variables, of degree at most one in each variable $(x_i^2 = x_i)$.
- $\deg(f)$, the *algebraic degree* of f, is the degree of its ANF.
- The Reed-Muller code RM(r,n) is the vector space of all n-variable Boolean functions of algebraic degree at most r.
- $\mathrm{Var}(f)$: the set of all $i \in \{1, \ldots, n\}$ such that x_i appears in the ANF of f.

Basic concepts

- $\mathbb{F}_2$ the finite field with two elements
- $\mathbb{F}_2^n$ the vector space over $\mathbb{F}_2$ of all binary vectors of length n.
- A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented in *Algebraic Normal Form* (ANF) i.e. as a polynomial function in n variables, of degree at most one in each variable $(x_i^2 = x_i)$.
- $\deg(f)$, the *algebraic degree* of f, is the degree of its ANF.
- The Reed-Muller code RM(r,n) is the vector space of all n-variable Boolean functions of algebraic degree at most r.
- $\mathrm{Var}(f)$: the set of all $i \in \{1, \ldots, n\}$ such that x_i appears in the ANF of f.

Basic concepts

- $\mathbb{F}_2$ the finite field with two elements
- $\mathbb{F}_2^n$ the vector space over $\mathbb{F}_2$ of all binary vectors of length n.
- A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented in *Algebraic Normal Form* (ANF) i.e. as a polynomial function in n variables, of degree at most one in each variable $(x_i^2 = x_i)$.
- $\deg(f)$, the *algebraic degree* of f, is the degree of its ANF.
- The Reed-Muller code RM(r,n) is the vector space of all n-variable Boolean functions of algebraic degree at most r.
- $\mathrm{Var}(f)$: the set of all $i \in \{1, \ldots, n\}$ such that x_i appears in the ANF of f.

Basic concepts

- $\mathbb{F}_2$ the finite field with two elements
- $\mathbb{F}_2^n$ the vector space over $\mathbb{F}_2$ of all binary vectors of length n.
- A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely represented in *Algebraic Normal Form* (ANF) i.e. as a polynomial function in n variables, of degree at most one in each variable $(x_i^2 = x_i)$.
- $\deg(f)$, the *algebraic degree* of f, is the degree of its ANF.
- The Reed-Muller code RM(r,n) is the vector space of all n-variable Boolean functions of algebraic degree at most r.
- $\mathrm{Var}(f)$: the set of all $i \in \{1, \ldots, n\}$ such that x_i appears in the ANF of f.

Affine equivalence

Definition

$f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ are said to be affinely equivalent, $f \sim g$, if there exists an invertible affine transformation φ of $\mathbb{F}_2^n$ such that $f = g \circ \varphi$.

- the algebraic degree is invariant to affine equivalence.
- $\sim$ can be extended naturally to an equivalence $\sim_{r-1}$ on the quotient space $RM(r, n)/RM(r-1, n)$.
- $f \sim_{r-1} g$ if and only if there is a function h such that $f \sim h$ and $\deg(g - h) \leq r - 1$.

Affine equivalence

Definition

$f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ are said to be affinely equivalent, $f \sim g$, if there exists an invertible affine transformation φ of $\mathbb{F}_2^n$ such that $f = g \circ \varphi$.

- the algebraic degree is invariant to affine equivalence.
- $\sim$ can be extended naturally to an equivalence $\sim_{r-1}$ on the quotient space $RM(r, n)/RM(r-1, n)$.
- $f \sim_{r-1} g$ if and only if there is a function h such that $f \sim h$ and $\deg(g - h) \leq r - 1$.

Affine equivalence

Definition

$f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ are said to be affinely equivalent, $f \sim g$, if there exists an invertible affine transformation φ of $\mathbb{F}_2^n$ such that $f = g \circ \varphi$.

- the algebraic degree is invariant to affine equivalence.
- $\sim$ can be extended naturally to an equivalence $\sim_{r-1}$ on the quotient space $RM(r, n)/RM(r-1, n)$.
- $f \sim_{r-1} g$ if and only if there is a function h such that $f \sim h$ and $\deg(g - h) \leq r - 1$.

Affine equivalence

Definition

$f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ are said to be affinely equivalent, $f \sim g$, if there exists an invertible affine transformation φ of $\mathbb{F}_2^n$ such that $f = g \circ \varphi$.

- the algebraic degree is invariant to affine equivalence.
- $\sim$ can be extended naturally to an equivalence $\sim_{r-1}$ on the quotient space $RM(r, n)/RM(r-1, n)$.
- $f \sim_{r-1} g$ if and only if there is a function h such that $f \sim h$ and $\deg(g-h) \leq r-1$.

Contents

New definitions and notation

f Boolean function in n variables
$A \subseteq \mathbb{F}_2^n$ affine space of co-dimension k

- $f_{|A}$ the restriction of f on A
- A is called a *degree-drop subspace* for f if $\deg(f_{|A}) < \deg(f)$.

Example

$f = x_1x_2x_3 + x_1x_4x_5 + x_2x_3x_5$, $\deg(f) = 3$.
Hyperplane H defined by the equation $x_1 = 0$:
$f_{|H} = x_2x_3x_5$ (H is not a degree-drop hyperplane)
Hyperplane H' defined by $x_1 = x_5$:
$f_{|H'} = x_2x_3x_5 + x_4x_5^2 + x_2x_3x_5 = x_4x_5$ (H' is a degree-drop hyperplane)

New definitions and notation

f Boolean function in n variables
$A \subseteq \mathbb{F}_2^n$ affine space of co-dimension k

- $f_{|A}$ the restriction of f on A
- A is called a *degree-drop subspace* for f if $\deg(f_{|A}) < \deg(f)$.

Example

$f = x_1x_2x_3 + x_1x_4x_5 + x_2x_3x_5$, $\deg(f) = 3$.
Hyperplane H defined by the equation $x_1 = 0$:
$f_{|H} = x_2x_3x_5$ (H is not a degree-drop hyperplane)
Hyperplane H' defined by $x_1 = x_5$:
$f_{|H'} = x_2x_3x_5 + x_4x_5^2 + x_2x_3x_5 = x_4x_5$ (H' is a degree-drop hyperplane)

New definitions and notation

f Boolean function in n variables
$A \subseteq \mathbb{F}_2^n$ affine space of co-dimension k

- $f_{|A}$ the restriction of f on A
- A is called a *degree-drop subspace* for f if $\deg(f_{|A}) < \deg(f)$.

Example

$f = x_1x_2x_3 + x_1x_4x_5 + x_2x_3x_5$, $\deg(f) = 3$.
Hyperplane H defined by the equation $x_1 = 0$:
$f_{|H} = x_2x_3x_5$ (H is not a degree-drop hyperplane)
Hyperplane H' defined by $x_1 = x_5$:
$f_{|H'} = x_2x_3x_5 + x_4x_5^2 + x_2x_3x_5 = x_4x_5$ (H' is a degree-drop hyperplane)

New definitions and notation

f Boolean function in n variables
$A \subseteq \mathbb{F}_2^n$ affine space of co-dimension k

- $f_{|A}$ the restriction of f on A
- A is called a *degree-drop subspace* for f if $\deg(f_{|A}) < \deg(f)$.

Example

$f = x_1x_2x_3 + x_1x_4x_5 + x_2x_3x_5$, $\deg(f) = 3$.
Hyperplane H defined by the equation $x_1 = 0$:
$f_{|H} = x_2x_3x_5$ (H is not a degree-drop hyperplane)
Hyperplane H' defined by $x_1 = x_5$:
$f_{|H'} = x_2x_3x_5 + x_4x_5^2 + x_2x_3x_5 = x_4x_5$ (H' is a degree-drop hyperplane)

New definitions and notation

f Boolean function in n variables
$A \subseteq \mathbb{F}_2^n$ affine space of co-dimension k

- $f_{|A}$ the restriction of f on A
- A is called a *degree-drop subspace* for f if $\deg(f_{|A}) < \deg(f)$.

Example

$f = x_1x_2x_3 + x_1x_4x_5 + x_2x_3x_5$, $\deg(f) = 3$.
Hyperplane H defined by the equation $x_1 = 0$:
$f_{|H} = x_2x_3x_5$ (H is not a degree-drop hyperplane)
Hyperplane H' defined by $x_1 = x_5$:
$f_{|H'} = x_2x_3x_5 + x_4x_5^2 + x_2x_3x_5 = x_4x_5$ (H' is a degree-drop hyperplane)

New definitions and notation

f Boolean function in n variables
$A \subseteq \mathbb{F}_2^n$ affine space of co-dimension k

- $f_{|A}$ the restriction of f on A
- A is called a *degree-drop subspace* for f if $\deg(f_{|A}) < \deg(f)$.

Example

$f = x_1x_2x_3 + x_1x_4x_5 + x_2x_3x_5$, $\deg(f) = 3$.
Hyperplane H defined by the equation $x_1 = 0$:
$f_{|H} = x_2x_3x_5$ (H is not a degree-drop hyperplane)
Hyperplane H' defined by $x_1 = x_5$:
$f_{|H'} = x_2x_3x_5 + x_4x_5^2 + x_2x_3x_5 = x_4x_5$ (H' is a degree-drop hyperplane)

New definitions and notation

- The degree stability of f, $\mathrm{deg\_stab}(f)$ is defined as the largest k such that f has no degree-drop space of co-dimension k
- From a cryptographic point of view, we are interested in functions with a large degree stability.
- $\mathrm{deg\_stab}(r, n)$ is defined as the largest value of $\mathrm{deg\_stab}(f)$ among all f of degree r in n variables (such functions f would be optimal from this point of view).

New definitions and notation

- The degree stability of f, $\mathrm{deg\_stab}(f)$ is defined as the largest k such that f has no degree-drop space of co-dimension k
- From a cryptographic point of view, we are interested in functions with a large degree stability.
- $\mathrm{deg\_stab}(r, n)$ is defined as the largest value of $\mathrm{deg\_stab}(f)$ among all f of degree r in n variables (such functions f would be optimal from this point of view).

New definitions and notation

- The degree stability of f, $\mathrm{deg\_stab}(f)$ is defined as the largest k such that f has no degree-drop space of co-dimension k
- From a cryptographic point of view, we are interested in functions with a large degree stability.
- $\mathrm{deg\_stab}(r, n)$ is defined as the largest value of $\mathrm{deg\_stab}(f)$ among all f of degree r in n variables (such functions f would be optimal from this point of view).

Properties

Lemma

Let f, g of degree r such that $f \sim_{r-1} g$ with $f = g \circ \varphi + h$ where h is of degree at most r-1.
Then A is a degree-drop space for f if and only if $\varphi(A)$ is a degree-drop space for g.

Let f be a homogeneous function of degree r in n variables

- If f has only one monomial in its ANF, or if $\deg(f) \in \{1, n-1, n\}$ then f has degree-drop hyperplanes.
- If $\deg(g) = n-2$, $\mathrm{deg\_stab}(n-2, n) = 0$ if n is odd, and $\mathrm{deg\_stab}(n-2, n) = 1$ if n even.
- $\mathrm{deg\_stab}(r, n) \leq \mathrm{deg\_stab}(r, n+1) \leq \mathrm{deg\_stab}(r, n) + 1$.

Properties

Lemma

Let f, g of degree r such that $f \sim_{r-1} g$ with $f = g \circ \varphi + h$ where h is of degree at most r-1.
Then A is a degree-drop space for f if and only if $\varphi(A)$ is a degree-drop space for g.

Let f be a homogeneous function of degree r in n variables

- If f has only one monomial in its ANF, or if $\deg(f) \in \{1, n-1, n\}$ then f has degree-drop hyperplanes.
- If $\deg(g) = n-2$, $\mathrm{deg\_stab}(n-2, n) = 0$ if n is odd, and $\mathrm{deg\_stab}(n-2, n) = 1$ if n even.
- $\mathrm{deg\_stab}(r, n) \leq \mathrm{deg\_stab}(r, n+1) \leq \mathrm{deg\_stab}(r, n) + 1$.

Properties

Lemma

Let f, g of degree r such that $f \sim_{r-1} g$ with $f = g \circ \varphi + h$ where h is of degree at most r-1.
Then A is a degree-drop space for f if and only if $\varphi(A)$ is a degree-drop space for g.

Let f be a homogeneous function of degree r in n variables

- If f has only one monomial in its ANF, or if $\deg(f) \in \{1, n-1, n\}$ then f has degree-drop hyperplanes.
- If $\deg(g) = n-2$, $\mathrm{deg\_stab}(n-2, n) = 0$ if n is odd, and $\mathrm{deg\_stab}(n-2, n) = 1$ if n even.
- $\mathrm{deg\_stab}(r, n) \leq \mathrm{deg\_stab}(r, n+1) \leq \mathrm{deg\_stab}(r, n) + 1$.

Properties

Lemma

Let f, g of degree r such that $f \sim_{r-1} g$ with $f = g \circ \varphi + h$ where h is of degree at most r-1.
Then A is a degree-drop space for f if and only if $\varphi(A)$ is a degree-drop space for g.

Let f be a homogeneous function of degree r in n variables

- If f has only one monomial in its ANF, or if $\deg(f) \in \{1, n-1, n\}$ then f has degree-drop hyperplanes.
- If $\deg(g) = n-2$, $\mathrm{deg\_stab}(n-2, n) = 0$ if n is odd, and $\mathrm{deg\_stab}(n-2, n) = 1$ if n even.
- $\mathrm{deg\_stab}(r, n) \leq \mathrm{deg\_stab}(r, n+1) \leq \mathrm{deg\_stab}(r, n) + 1$.

Properties

Lemma

Let f, g of degree r such that $f \sim_{r-1} g$ with $f = g \circ \varphi + h$ where h is of degree at most r-1.
Then A is a degree-drop space for f if and only if $\varphi(A)$ is a degree-drop space for g.

Let f be a homogeneous function of degree r in n variables

- If f has only one monomial in its ANF, or if $\deg(f) \in \{1, n-1, n\}$ then f has degree-drop hyperplanes.
- If $\deg(g) = n-2$, $\mathrm{deg\_stab}(n-2, n) = 0$ if n is odd, and $\mathrm{deg\_stab}(n-2, n) = 1$ if n even.
- $\mathrm{deg\_stab}(r, n) \leq \mathrm{deg\_stab}(r, n+1) \leq \mathrm{deg\_stab}(r, n) + 1$.

Theorem

The following statements are equivalent:
(i) f has a degree-drop hyperplane.
(ii) $f(x_1, \ldots, x_n) \sim_{r-1} x_1 f_1(x_2, \ldots, x_n)$ for some homogeneous function f_1 of degree $r-1$.

Theorem

The following statements are equivalent:
(i) f has a degree-drop space of co-dimension k.
(ii) $f \sim_{r-1} g$ for some homogeneous function g of degree r such that each monomial of g contains at least one of the variables $x_1, x_2, \ldots, x_k$.

Theorem

The following statements are equivalent:
(i) f has a degree-drop hyperplane.
(ii) $f(x_1, \ldots, x_n) \sim_{r-1} x_1 f_1(x_2, \ldots, x_n)$ for some homogeneous function f_1 of degree $r-1$.

Theorem

The following statements are equivalent:
(i) f has a degree-drop space of co-dimension k.
(ii) $f \sim_{r-1} g$ for some homogeneous function g of degree r such that each monomial of g contains at least one of the variables $x_1, x_2, \ldots, x_k$.

Lemma

Let f be an n-variable Boolean function. Let A be an affine subspace of $\mathbb{F}_2^n$ and 1_A its indicator function. If $f1_A$ is not the identically zero function, we have

$$\deg(f1_A) = \deg(f_{|A}) + \deg(1_A).$$

Proposition

A space A of co-dimension k is not a degree-drop space for the n-variable function f if and only if $\deg(f1_A) = \deg(f) + k$.

Lemma

Let f be an n-variable Boolean function. Let A be an affine subspace of $\mathbb{F}_2^n$ and 1_A its indicator function. If $f1_A$ is not the identically zero function, we have

$$\deg(f1_A) = \deg(f_{|A}) + \deg(1_A).$$

Proposition

A space A of co-dimension k is not a degree-drop space for the n-variable function f if and only if $\deg(f1_A) = \deg(f) + k$.

Theorem

f sum of p monomials of degree r, $f = \sum_{j=1}^{p} m_j$

- *If f satisfies the conditions*

$$\begin{aligned} \cap_{i=1}^{p} \mathrm{Var}(m_i) &= \emptyset \\ |\mathrm{Var}(m_i) \cap \mathrm{Var}(m_j)| &\leq r-2, \text{ for all } i \neq j, \end{aligned}$$

  then f has no degree-drop hyperplane.

- *More generally, for any $k < r$, if*

$$|\mathrm{Var}(m_i) \cap \mathrm{Var}(m_j)| \leq r-k-1, \text{ for all } i \neq j,$$

  and for any set of k distinct variables $x_{j_1}, \ldots, x_{j_k}$, there is at least one monomial in f which does not contain any of the variables $x_{j_1}, \ldots, x_{j_k}$, then f has no degree-drop space of co-dimension k.

Theorem

f sum of p monomials of degree r, $f = \sum_{j=1}^{p} m_j$

- *If f satisfies the conditions*

$$\begin{aligned} \cap_{i=1}^{p} \mathrm{Var}(m_i) &= \emptyset \\ |\mathrm{Var}(m_i) \cap \mathrm{Var}(m_j)| &\leq r-2, \text{ for all } i \neq j, \end{aligned}$$

  then f has no degree-drop hyperplane.

- *More generally, for any $k < r$, if*

$$|\mathrm{Var}(m_i) \cap \mathrm{Var}(m_j)| \leq r-k-1, \text{ for all } i \neq j,$$

  and for any set of k distinct variables $x_{j_1}, \ldots, x_{j_k}$, there is at least one monomial in f which does not contain any of the variables $x_{j_1}, \ldots, x_{j_k}$, then f has no degree-drop space of co-dimension k.

Theorem

f sum of p monomials of degree r, $\quad f = \sum_{j=1}^{p} m_j$
If for all $i \in \mathrm{Var}(f)$, there exists a monomial m_{j_i} in f such that:

- $i \notin \mathrm{Var}(m_{j_i})$
- *for all $t \in \mathrm{Var}(m_{j_i})$, the monomial $\frac{x_i m_{j_i}}{x_t}$ is not in f,*

then, f has no degree-drop hyperplane.

Symmetric functions

Theorem

Let f be a symmetric Boolean function in n variables of degree r. $2 \leq r \leq n-2$.
(i) If r is even, then f has no degree-drop hyperplane.
(ii) If r is odd, then f has exactly one degree-drop linear hyperplane, of equation $x_1 + x_2 + \ldots + x_n = 0$.

Direct sum of monomials

Proposition (Carlet, Feukoua, 2020)

The function $f(x_1, \ldots, x_n) = x_1x_2 + x_3x_4 + \cdots + x_{2p-1}x_{2p}$ (with $2p \leq n$) has no degree-drop space of co-dimension $p-1$ but has degree-drop space of co-dimension p;
hence, $\mathrm{deg\_stab}(f) = p-1$ *and* $\mathrm{deg\_stab}(2,n) = \lfloor \frac{n}{2} \rfloor - 1$.

Theorem

Let $2 \leq r < n$ and $2 \leq p \leq \lfloor \frac{n}{r} \rfloor$. The function in n variables which is the direct sum of p monomials of degree r

$$f(x_1, \ldots, x_n) = x_1x_2 \cdots x_r + \cdots + x_{(p-1)r+1}x_{(p-1)r+2} \cdots x_{pr}$$

has no degree-drop space of co-dimension $p-1$ but has degree-drop space of co-dimension p, i.e. $\mathrm{deg\_stab}(f) = p-1$. *Consequently* $\mathrm{deg\_stab}(r,n) \geq \lfloor \frac{n}{r} \rfloor - 1$.

Direct sum of monomials

Proposition (Carlet, Feukoua, 2020)

The function $f(x_1, \ldots, x_n) = x_1x_2 + x_3x_4 + \cdots + x_{2p-1}x_{2p}$ *(with* $2p \leq n$*) has no degree-drop space of co-dimension* $p-1$ *but has degree-drop space of co-dimension* p*;*
hence, $\mathrm{deg\_stab}(f) = p - 1$ *and* $\mathrm{deg\_stab}(2, n) = \lfloor \frac{n}{2} \rfloor - 1$.

Theorem

Let $2 \leq r < n$ *and* $2 \leq p \leq \lfloor \frac{n}{r} \rfloor$*. The function in* n *variables which is the direct sum of* p *monomials of degree* r

$$f(x_1, \ldots, x_n) = x_1x_2 \cdots x_r + \cdots + x_{(p-1)r+1}x_{(p-1)r+2} \cdots x_{pr}$$

has no degree-drop space of co-dimension $p-1$ *but has degree-drop space of co-dimension* p*, i.e.* $\mathrm{deg\_stab}(f) = p - 1$*. Consequently* $\mathrm{deg\_stab}(r, n) \geq \lfloor \frac{n}{r} \rfloor - 1$.

Bounds

Corollary

We have the following bounds when $2 \leq r \leq n-1$:

$$\left\lfloor \frac{n}{r} \right\rfloor - 1 \leq \mathrm{deg\_stab}(r, n) \leq n - r - 1.$$

When $r = 2$ equality is achieved for the lower bound; when $r = n-1$ or when $r = n-2$ and n is even, equality is achieved for the upper bound.

Experimental results

- We computed the number of degree-drop spaces for all the functions in up to $n = 8$ variables.
- For degree 3 (and 5) we used the 31 non-zero classes under $\sim_2$ given by [Hou, 1996]
- For degree 4, we used the 998 non-zero classes (under $\sim_3$) given by [Langevin, Leander, 2007]

Experimental results

- We computed the number of degree-drop spaces for all the functions in up to $n = 8$ variables.
- For degree 3 (and 5) we used the 31 non-zero classes under $\sim_2$ given by [Hou, 1996]
- For degree 4, we used the 998 non-zero classes (under $\sim_3$) given by [Langevin, Leander, 2007]

Experimental results

- We computed the number of degree-drop spaces for all the functions in up to $n = 8$ variables.
- For degree 3 (and 5) we used the 31 non-zero classes under $\sim_2$ given by [Hou, 1996]
- For degree 4, we used the 998 non-zero classes (under $\sim_3$) given by [Langevin, Leander, 2007]

The polynomials of degree 3 in 8 variables

$$
\begin{aligned}
f_2 &= 123\\
f_3 &= 123 + 145\\
f_4 &= 123 + 456\\
f_5 &= 123 + 245 + 346\\
f_6 &= 123 + 145 + 246 + 356 + 456\\
f_7 &= 127 + 347 + 567\\
f_8 &= 123 + 456 + 147\\
f_9 &= 123 + 245 + 346 + 147\\
f_{10} &= 123 + 456 + 147 + 257\\
f_{11} &= 123 + 145 + 246 + 356 + 456 + 167\\
f_{12} &= 123 + 145 + 246 + 356 + 456 + 167 + 247\\
f_{13} &= 123 + 456 + 178;\\
f_{14} &= 123 + 456 + 178 + 478;\\
f_{15} &= 123 + 245 + 678 + 147;\\
f_{16} &= 123 + 245 + 346 + 378
\end{aligned}
$$

$$
\begin{aligned}
f_{17} &= 123 + 145 + 246 + 356 + 456 + 178;\\
f_{18} &= 123 + 145 + 246 + 356 + 456 + 167 + 238;\\
f_{19} &= 123 + 145 + 246 + 356 + 456 + 158 + 237 + 678;\\
f_{20} &= 123 + 145 + 246 + 356 + 456 + 278 + 347 + 168;\\
f_{21} &= 145 + 246 + 356 + 456 + 278 + 347 + 168 + 237 + 147;\\
f_{22} &= 123 + 234 + 345 + 456 + 567 + 678 + 128 + 238 + 348 + 458 +\\
f_{23} &= 123 + 145 + 246 + 356 + 456 + 167 + 578;\\
f_{24} &= 123 + 145 + 246 + 356 + 456 + 167 + 568;\\
f_{25} &= 123 + 145 + 246 + 356 + 456 + 167 + 348;\\
f_{26} &= 123 + 456 + 147 + 257 + 268 + 278 + 348;\\
f_{27} &= 123 + 456 + 147 + 257 + 168 + 178 + 248 + 358;\\
f_{28} &= 127 + 347 + 567 + 258 + 368;\\
f_{29} &= 123 + 456 + 147 + 368;\\
f_{30} &= 123 + 456 + 147 + 368 + 578;\\
f_{31} &= 123 + 456 + 147 + 368 + 478 + 568;
\end{aligned}
$$

Experimental results

Table: Number of degree-drop linear spaces for degree 3 in 8 var

Representative	co-dim 1 lin spaces	co-dim 2 lin spaces	co-dim 2 new lin spaces	co-dim 3 lin spaces	co-dim 3 new lin spaces
f_2	7	875	0	17795	0
f_3	1	187	60	6147	0
f_7	1	127	0	3747	1080
f_4	0	49	49	3059	168
f_5	0	35	35	2371	256
f_6	0	21	21	1683	360
f_8	0	13	13	1427	636
f_9	0	7	7	995	568
f_{13}	0	7	7	847	420
f_{16}	0	7	7	739	312
f_{10}	0	3	3	867	678
f_{29}	0	2	2	459	333
f_{11}	0	1	1	563	500
f_{14}	0	1	1	459	396
f_{15}	0	1	1	351	288
f_{24}	0	1	1	307	244
f_{17}	0	1	1	243	180
f_{28}	0	1	1	243	180
f_{26}	0	1	1	135	72
f_{12}	0	0	0	651	651
f_{31}	0	0	0	243	243
f_{18}	0	0	0	167	167
f_{25}	0	0	0	155	155
f_{19}	0	0	0	151	151
f_{30}	0	0	0	151	151
f_{22}	0	0	0	105	105
f_{23}	0	0	0	91	91
f_{32}	0	0	0	91	91
f_{21}	0	0	0	75	75
f_{20}	0	0	0	45	45
f_{27}	0	0	0	15	15

The values of $\mathrm{deg\_stab}(r, n)$ for $n = 6, 7, 8$

Table: $\mathrm{deg\_stab}(r, n)$ for $n = 6, 7, 8$

$n \setminus r$	1	2	3	4	5	6	7	8
6	0	2	1	1	0	0	-	-
7	0	2	2	1	0	0	0	-
8	0	3	2	2	1	1	0	0

THANK YOU FOR YOUR ATTENTION