Nonvanishing k-flats of Boolean and vectorial functions

Christian Kaspers

Otto von Guericke University Magdeburg

WCC 2026

Paris, June 11, 2026

Vanishing and nonvanishing k-flats

- Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, in short, an (n, m)-function.
- Let A be a k-dimensional affine subspace of $\mathbb{F}_2^n$, in short a k-flat.

Definition

The k-flat A is nonvanishing with respect to F if

$$\sum_{x \in A} F(x) \neq 0.$$

- If $\sum_{x \in A} F(x) = 0$, then A is vanishing with respect to F.
- The concept was introduced by *Li et al. (2020)* motivated by APN functions.

APN functions

Definition (*Nyberg 1994*)

An (n, n)-function F is called almost perfect nonlinear (APN) if the equation

$$F(x + a) + F(x) = b$$

has 0 or 2 solutions for all $a, b \in \mathbb{F}_2^n$ where $a \neq 0$.

APN functions

Definition (*Nyberg 1994*)

An (n,n)-function F is called almost perfect nonlinear (APN) if the equation

$$F(x+a)+F(x)=b$$

has 0 or 2 solutions for all $a,b \in \mathbb{F}_2^n$ where $a \neq 0$.

- Cryptographers like nonlinear functions.
- If F is linear, then $F(x+a)+F(x)=F(a)$, so we have 2^n solutions for $b=F(a)$.
- Least linear would be one solution to $F(x+a)+F(x)=b$ – not possible over $\mathbb{F}_2$.

APN functions are optimal!

APN functions and (non)vanishing 2-flats

Rodier condition

F is APN $\iff \sum_{x \in A} F(x) \neq 0$ for all 2-flats $A \subseteq \mathbb{F}_2^n$.

APN functions and (non)vanishing 2-flats

Rodier condition

F is APN $\iff \sum_{x \in A} F(x) \neq 0$ for all 2-flats $A \subseteq \mathbb{F}_2^n$.

Denote by $N_{\mathcal{A},k}(F)$ the set of nonvanishing k-flats of F.

APN functions and (non)vanishing 2-flats

Rodier condition

F is APN $\iff \sum_{x \in A} F(x) \neq 0$ for all 2-flats $A \subseteq \mathbb{F}_2^n$.

Denote by $N_{\mathcal{A},k}(F)$ the set of nonvanishing k-flats of F.

- For an (n,n)-function F, we have $|N_{\mathcal{A},2}(F)| = 2^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}_2 - \frac{1}{3} \sum_{a,b \in \mathbb{F}_2^n, a \neq 0} \binom{\delta_F(a,b)/2}{2}$, where $\delta_F(a,b)$ is the number of solutions to $F(x+a) + F(x) = b$. *(Li et al. 2020)*
- For an (n,m)-function F, we have $|N_{\mathcal{A},2}(F)| = \frac{2^{4n}(2^m-1)-\omega}{3 \cdot 2^{n+m+3}}$, where $\omega = \sum_{W \in \mathcal{W}_F} W^4$ is the sum of the fourth powers of the Walsh coefficients of F. *(Arshad 2018)*
- For an n-variable Boolean function f, we have $|N_{\mathcal{A},2}(f)| \leq \frac{2^{2n-4}(2^n-1)}{3}$ and equality holds if and only if f is bent. *(Arshad 2018)*

kth-order sum-free functions

Definition (*Carlet 2025b,c*)

An (n, m)-function F is kth-order sum-free if for all k-flats $A \subseteq \mathbb{F}_2^n$ we have

$$\sum_{x \in A} F(x) \neq 0.$$

- F is APN $\iff$ F is 2nd-order sum-free.

kth-order sum-free functions

Definition (*Carlet 2025b,c*)

An (n, m)-function F is kth-order sum-free if for all k-flats $A \subseteq \mathbb{F}_2^n$ we have

$$\sum_{x \in A} F(x) \neq 0.$$

- F is APN $\iff$ F is 2nd-order sum-free.
- $x^{\frac{2^{jk}-1}{2^j-1}}$ is kth-order sum-free if $\gcd(j, n) = 1$, in particular x^{2^k-1}. *(Carlet 2025a,c)*
- For n odd, x^{2^n-2} is kth-order sum-free for $k \in \{1, 2, n-2, n-1\}$ *(Carlet 2025b; Carlet and Hou 2024; Ebeling et al. 2026; Hou and Zhao 2026a,b)*.

kth-order sum-free functions

Definition (*Carlet 2025b,c*)

An (n,m)-function F is kth-order sum-free if for all k-flats $A \subseteq \mathbb{F}_2^n$ we have

$$\sum_{x \in A} F(x) \neq 0.$$

- F is APN $\iff$ F is 2nd-order sum-free.
- $x^{\frac{2^{jk}-1}{2^j-1}}$ is kth-order sum-free if $\gcd(j,n)=1$, in particular x^{2^k-1}. *(Carlet 2025a,c)*
- For n odd, x^{2^n-2} is kth-order sum-free for $k \in \{1,2,n-2,n-1\}$ *(Carlet 2025b; Carlet and Hou 2024; Ebeling et al. 2026; Hou and Zhao 2026a,b)*.
- $m \geq \max\{k+2, n-k+2\}$, and any kth-order sum-free (n,m)-function gives rise to a codimension m linear subcode of $\mathrm{RM}(n-k,n)$ with minimum distance $3 \cdot 2^{k-1}$. *(Heering, Kaspers, and Taranchuk 2026)*

Our contribution

1. We present a new matrix approach to determine the number $|N_{\mathcal{A},k}(f)|$ of nonvanishing k-flats of a Boolean function f of algebraic degree k.

Our contribution

1. We present a new matrix approach to determine the number $|N_{\mathcal{A},k}(f)|$ of nonvanishing k-flats of a Boolean function f of algebraic degree k.
2. We precisely determine $|N_{\mathcal{A},k}(f)|$ for an infinite family of Boolean functions of algebraic degree k.

Our contribution

1. We present a new matrix approach to determine the number $|N_{\mathcal{A},k}(f)|$ of nonvanishing k-flats of a Boolean function f of algebraic degree k.
2. We precisely determine $|N_{\mathcal{A},k}(f)|$ for an infinite family of Boolean functions of algebraic degree k.
3. We discover a duality between nonvanishing k-flats and nonvanishing $(n-k)$-flats. This gives rise to new $(n-k)$th-order sum-free functions.

Our contribution

1. We precisely determine $|N_{\mathcal{A},k}(f)|$ for an infinite family of Boolean functions of algebraic degree k.
2. We discover a duality between nonvanishing k-flats and nonvanishing $(n-k)$-flats. This gives rise to new $(n-k)$th-order sum-free functions.
3. We present a new matrix approach to determine the number $|N_{\mathcal{A},k}(f)|$ of nonvanishing k-flats of a Boolean function f of algebraic degree k.

Our contribution

1. We precisely determine $|N_{\mathcal{A},k}(f)|$ for an infinite family of Boolean functions of algebraic degree k.
2. We discover a duality between nonvanishing k-flats and nonvanishing $(n-k)$-flats. This gives rise to new $(n-k)$th-order sum-free functions.
3. We present a new matrix approach to determine the number $|N_{\mathcal{A},k}(f)|$ of nonvanishing k-flats of a Boolean function f of algebraic degree k.

Before we start, we need to talk about the algebraic degree!

Nonvanishing k-flats and the algebraic degree

$N_{\mathcal{A},k}(F)$ – nonvanishing k-flats of F,

Nonvanishing k-flats and the algebraic degree

$N_{\mathcal{A},k}(F)$ – nonvanishing k-flats of F,

Observation I

If $\deg_{\text{alg}}(F) < k$, then $|N_{\mathcal{A},k}(F)| = 0$.

Nonvanishing k-flats and the algebraic degree

$N_{\mathcal{A},k}(F)$ – nonvanishing k-flats of F,

Observation I

If $\deg_{\mathrm{alg}}(F) < k$, then $|N_{\mathcal{A},k}(F)| = 0$.

- If F is kth-order sum-free, then $\deg_{\mathrm{alg}}(F) \geq k$.
- Any terms of F of algebraic degree $< k$ are irrelevant for $|N_{\mathcal{A},k}(F)|$.

Nonvanishing k-flats and the algebraic degree

$N_{\mathcal{A},k}(F)$ – nonvanishing k-flats of F,

Observation I

If $\deg_{\text{alg}}(F) < k$, then $|N_{\mathcal{A},k}(F)| = 0$.

- If F is kth-order sum-free, then $\deg_{\text{alg}}(F) \geq k$.
- Any terms of F of algebraic degree $< k$ are irrelevant for $|N_{\mathcal{A},k}(F)|$.

Observation II

If $\deg_{\text{alg}}(F) = k$ and U is a k-subspace, then $\sum_{x \in U} F(x) = \sum_{x \in U+a} F(x)$ for all a.

Nonvanishing k-flats and the algebraic degree

$N_{\mathcal{A},k}(F)$ – nonvanishing k-flats of F, $N_k(F)$ – nonvanishing k-subspaces of F

Observation I

If $\deg_{\mathrm{alg}}(F) < k$, then $|N_{\mathcal{A},k}(F)| = 0$.

- If F is kth-order sum-free, then $\deg_{\mathrm{alg}}(F) \geq k$.
- Any terms of F of algebraic degree $< k$ are irrelevant for $|N_{\mathcal{A},k}(F)|$.

Observation II

If $\deg_{\mathrm{alg}}(F) = k$ and U is a k-subspace, then $\sum_{x \in U} F(x) = \sum_{x \in U+a} F(x)$ for all a.

- If $\deg_{\mathrm{alg}}(F) = k$, then $|N_{\mathcal{A},k}(F)| = 2^{n-k}|N_k(F)|$.

Nonvanishing k-flats and the algebraic degree

$N_{\mathcal{A},k}(F)$ – nonvanishing k-flats of F, $N_k(F)$ – nonvanishing k-subspaces of F

Observation I

If $\deg_{\mathrm{alg}}(F) < k$, then $|N_{\mathcal{A},k}(F)| = 0$.

- If F is kth-order sum-free, then $\deg_{\mathrm{alg}}(F) \geq k$.
- Any terms of F of algebraic degree $< k$ are irrelevant for $|N_{\mathcal{A},k}(F)|$.

Observation II

If $\deg_{\mathrm{alg}}(F) = k$ and U is a k-subspace, then $\sum_{x \in U} F(x) = \sum_{x \in U+a} F(x)$ for all a.

- If $\deg_{\mathrm{alg}}(F) = k$, then $|N_{\mathcal{A},k}(F)| = 2^{n-k}|N_k(F)|$.

If $\deg_{\mathrm{alg}}(F) = k$, then study only the degree-k terms of F and $|N_k(F)|$!

Nonvanishing k-flats of d-intersecting Boolean functions

If $m = x_{i_1} \dots x_{i_r}$, write $\mathrm{Var}(m) = \{i_1, \dots, i_r\}$.

Definition

Let $m_1, \dots, m_t$ be monomials and $f = m_1 + \dots + m_t$. We say f is d-intersecting if there is a set D with $|D| = d$ such that $\mathrm{Var}(m_i) \cap \mathrm{Var}(m_j) = D$ for all $i \neq j$.

- $f = x_1x_2 + x_3x_4 + x_5x_6$ is 0-intersecting
- $f = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5$ is 2-intersecting (with $D = \{1, 2\}$)

Nonvanishing k-flats of d-intersecting Boolean functions

If $m = x_{i_1} \dots x_{i_r}$, write $\mathrm{Var}(m) = \{i_1, \dots, i_r\}$.

Definition

Let $m_1, \dots, m_t$ be monomials and $f = m_1 + \dots + m_t$. We say f is d-intersecting if there is a set D with $|D| = d$ such that $\mathrm{Var}(m_i) \cap \mathrm{Var}(m_j) = D$ for all $i \neq j$.

- $f = x_1x_2 + x_3x_4 + x_5x_6$ is 0-intersecting
- $f = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5$ is 2-intersecting (with $D = \{1, 2\}$)

Nonvanishing k-flats of d-intersecting Boolean functions

If $m = x_{i_1} \dots x_{i_r}$, write $\mathrm{Var}(m) = \{i_1, \dots, i_r\}$.

Definition

Let $m_1, \dots, m_t$ be monomials and $f = m_1 + \dots + m_t$. We say f is d-intersecting if there is a set D with $|D| = d$ such that $\mathrm{Var}(m_i) \cap \mathrm{Var}(m_j) = D$ for all $i \neq j$.

- $f = x_1x_2 + x_3x_4 + x_5x_6$ is 0-intersecting
- $f = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5$ is 2-intersecting (with $D = \{1, 2\}$)

Theorem (K 2026)

Let f be a d-intersecting, k-homogeneous n-variable Boolean function with t terms. We have

$$|N_k(f)| = \sum_{\ell=1}^{t} (-2)^{\ell-1} \binom{t}{\ell} 2^{k(n-\ell k+(\ell-1)d)} \prod_{i=0}^{k-d-1} (2^k - 2^{i+d})^{\ell-1}.$$

Duality between nonvanishing k- and $(n-k)$-flats

Definition

Let m be an n-variable monomial. We call the monomial $\overline{m}$ with $\mathrm{Var}(\overline{m}) = \{1, \ldots, n\} \setminus \mathrm{Var}(m)$ the complement of m. Analogous, for $f = m_1 + \cdots + m_t$ define $\overline{f} = \overline{m_1} + \cdots + \overline{m_t}$

- example for $n = 5$: for $f = x_1x_2 + x_2x_3$, we have $\overline{f} = x_3x_4x_5 + x_1x_4x_5$.

Duality between nonvanishing k- and $(n-k)$-flats

Definition

Let m be an n-variable monomial. We call the monomial $\overline{m}$ with $\mathrm{Var}(\overline{m}) = \{1, \ldots, n\} \setminus \mathrm{Var}(m)$ the complement of m. Analogous, for $f = m_1 + \cdots + m_t$ define $\overline{f} = \overline{m_1} + \cdots + \overline{m_t}$

- example for $n = 5$: for $f = x_1x_2 + x_2x_3$, we have $\overline{f} = x_3x_4x_5 + x_1x_4x_5$.
- $\deg(m) = k \implies \deg(\overline{m}) = n - k$

Duality between nonvanishing k- and $(n-k)$-flats

Definition

Let m be an n-variable monomial. We call the monomial $\overline{m}$ with $\mathrm{Var}(\overline{m}) = \{1, \dots, n\} \setminus \mathrm{Var}(m)$ the complement of m. Analogous, for $f = m_1 + \cdots + m_t$ define $\overline{f} = \overline{m_1} + \cdots + \overline{m_t}$

- example for $n = 5$: for $f = x_1x_2 + x_2x_3$, we have $\overline{f} = x_3x_4x_5 + x_1x_4x_5$.
- $\deg(m) = k \implies \deg(\overline{m}) = n - k$

Recall the orthogonal complement of U: $U^\perp := \{v \in \mathbb{F}_2^n : \langle v, u\rangle = 0 \ \forall u \in U\}$

- $\dim U = k \implies \dim U^\perp = n - k$

Duality between nonvanishing k- and $(n-k)$-flats

Definition

Let m be an n-variable monomial. We call the monomial $\overline{m}$ with $\mathrm{Var}(\overline{m}) = \{1, \ldots, n\} \setminus \mathrm{Var}(m)$ the complement of m. Analogous, for $f = m_1 + \cdots + m_t$ define $\overline{f} = \overline{m_1} + \cdots + \overline{m_t}$

- example for $n = 5$: for $f = x_1x_2 + x_2x_3$, we have $\overline{f} = x_3x_4x_5 + x_1x_4x_5$.
- $\deg(m) = k \implies \deg(\overline{m}) = n - k$

Recall the orthogonal complement of U: $U^\perp := \{v \in \mathbb{F}_2^n : \langle v, u \rangle = 0 \ \forall u \in U\}$

- $\dim U = k \implies \dim U^\perp = n - k$

Theorem (K 2026)

Let f be a k-homogeneous n-variable Boolean function. Then $U \in N_k(f)$ iff $U^\perp \in N_{n-k}(\overline{f})$.

Consequences of the duality between nonvanishing k- and $(n-k)$-flats

For Boolean functions:

For vectorial functions:

Consequences of the duality between nonvanishing k- and $(n-k)$-flats

For Boolean functions:

Corollary (K 2026)

Complements of quadratic bent functions have the most nonvanishing $(n-2)$-flats.

For vectorial functions:

Consequences of the duality between nonvanishing k- and $(n-k)$-flats

For Boolean functions:

Corollary (K 2026)

Complements of quadratic bent functions have the most nonvanishing $(n-2)$-flats.

For vectorial functions: for $F(x) = (f_1(x), \ldots, f_m(x))$ define $\overline{F}(x) = (\overline{f_1}(x), \ldots, \overline{f_m}(x))$.

Consequences of the duality between nonvanishing k- and $(n-k)$-flats

For Boolean functions:

Corollary (K 2026)

Complements of quadratic bent functions have the most nonvanishing $(n-2)$-flats.

For vectorial functions: for $F(x) = (f_1(x), \ldots, f_m(x))$ define $\overline{F}(x) = (\overline{f_1}(x), \ldots, \overline{f_m}(x))$.

Corollary (K 2026)

Let F be a k-homogeneous (n, m)-function. Then $U \in N_k(F)$ iff $U^\perp \in N_{n-k}(\overline{F})$.

Consequences of the duality between nonvanishing k- and $(n-k)$-flats

For Boolean functions:

Corollary (K 2026)

Complements of quadratic bent functions have the most nonvanishing $(n-2)$-flats.

For vectorial functions: for $F(x) = (f_1(x), \ldots, f_m(x))$ define $\overline{F}(x) = (\overline{f_1}(x), \ldots, \overline{f_m}(x))$.

Corollary (K 2026)

Let F be a k-homogeneous (n, m)-function. Then $U \in N_k(F)$ iff $U^\perp \in N_{n-k}(\overline{F})$.

Corollary (K 2026)

Let F be a k-homogeneous (n, m)-function. Then F is k-th order sum-free iff $\overline{F}$ is $(n-k)$th-order sum-free.

Example: $(n-k)$th-order sum-free from kth-order sum-free

- $f(x) = x^3$ is quadratic and 2nd-order sum-free (APN) on $\mathbb{F}_2^5$
- ANF

$$x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_1,$$
$$x_1x_2 + x_1x_4 + x_4x_5 + x_3 + x_4 + x_5,$$
$$x_1x_2 + x_1x_3 + x_1x_5 + x_2x_3 + x_3x_5 + x_4x_5 + x_5,$$
$$x_1x_5 + x_3x_4 + x_3x_5 + x_2 + x_3 + x_4 + x_5,$$
$$x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_4$$

Example: $(n-k)$th-order sum-free from kth-order sum-free

- $f(x) = x^3$ is quadratic and 2nd-order sum-free (APN) on $\mathbb{F}_2^5$
- ANF – remove the terms of degree < 2

$$x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_1,$$
$$x_1x_2 + x_1x_4 + x_4x_5 + x_3 + x_4 + x_5,$$
$$x_1x_2 + x_1x_3 + x_1x_5 + x_2x_3 + x_3x_5 + x_4x_5 + x_5,$$
$$x_1x_5 + x_3x_4 + x_3x_5 + x_2 + x_3 + x_4 + x_5,$$
$$x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_4$$

Example: $(n-k)$th-order sum-free from kth-order sum-free

- $f(x) = x^3$ is quadratic and 2nd-order sum-free (APN) on $\mathbb{F}_2^5$
- ANF of homogeneous $f' \sim f$

$$
\begin{aligned}
&x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4,\\
&x_1x_2 + x_1x_4 + x_4x_5,\\
&x_1x_2 + x_1x_3 + x_1x_5 + x_2x_3 + x_3x_5 + x_4x_5,\\
&x_1x_5 + x_3x_4 + x_3x_5,\\
&x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5
\end{aligned}
$$

Example: $(n-k)$th-order sum-free from kth-order sum-free

- $f(x) = x^3$ is quadratic and 2nd-order sum-free (APN) on $\mathbb{F}_2^5$
- ANF of homogeneous $f' \sim f$
  $x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4,$
  $x_1x_2 + x_1x_4 + x_4x_5,$
  $x_1x_2 + x_1x_3 + x_1x_5 + x_2x_3 + x_3x_5 + x_4x_5,$
  $x_1x_5 + x_3x_4 + x_3x_5,$
  $x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5$
- determine the complement $\overline{f'}$:
  $x_2x_3x_4 + x_1x_4x_5 + x_1x_3x_5 + x_1x_2x_5,$
  $x_3x_4x_5 + x_2x_3x_5 + x_1x_2x_3,$
  $x_3x_4x_5 + x_2x_4x_5 + x_2x_3x_4 + x_1x_4x_5 + x_1x_2x_4 + x_1x_2x_3,$
  $x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_4,$
  $x_2x_4x_5 + x_2x_3x_4 + x_1x_4x_5 + x_1x_3x_5 + x_1x_3x_4 + x_1x_2x_5 + x_1x_2x_4 + x_1x_2x_3$
- $\overline{f'}$ is $5 - 2 = 3$rd-order sum-free on $\mathbb{F}_2^5$

Example: $(n-k)$th-order sum-free from kth-order sum-free

- $f(x) = x^3$ is quadratic and 2nd-order sum-free (APN) on $\mathbb{F}_2^5$
- ANF of homogeneous $f' \sim f$
  $x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4,$
  $x_1x_2 + x_1x_4 + x_4x_5,$
  $x_1x_2 + x_1x_3 + x_1x_5 + x_2x_3 + x_3x_5 + x_4x_5,$
  $x_1x_5 + x_3x_4 + x_3x_5,$
  $x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5$
- determine the complement $\overline{f'}$:
  $x_2x_3x_4 + x_1x_4x_5 + x_1x_3x_5 + x_1x_2x_5,$
  $x_3x_4x_5 + x_2x_3x_5 + x_1x_2x_3,$
  $x_3x_4x_5 + x_2x_4x_5 + x_2x_3x_4 + x_1x_4x_5 + x_1x_2x_4 + x_1x_2x_3,$
  $x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_4,$
  $x_2x_4x_5 + x_2x_3x_4 + x_1x_4x_5 + x_1x_3x_5 + x_1x_3x_4 + x_1x_2x_5 + x_1x_2x_4 + x_1x_2x_3$
- $\overline{f'}$ is $5-2=3$rd-order sum-free on $\mathbb{F}_2^5$

  univariate representation:

  $\overline{f'} = a^{12}x^{28} + a^{10}x^{26} + a^{3}x^{25} + a^{27}x^{24} + a^{5}x^{22} + a^{17}x^{21} + a^{22}x^{20} + a^{7}x^{19} + a^{3}x^{18} + a^{26}x^{17} + a^{19}x^{16} + a^{17}x^{14} + a^{27}x^{13} + a^{30}x^{12} + a^{7}x^{11} + a^{16}x^{10} + a^{10}x^{9} + a^{26}x^{8} + a^{25}x^{7} + a^{25}x^{6} + a^{19}x^{5} + a^{25}x^{4} + a^{6}x^{3} + ax^{2} + a^{19}x$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (I)

- Which 2-subspaces are nonvanishing with respect to $x_1 x_2$?

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (I)

- Which 2-subspaces are nonvanishing with respect to x_1x_2?

We represent a 2-subspace U by its corresponding matrix G_U in RREF:

$$G_U = \begin{pmatrix} 10000 \\ 01000 \end{pmatrix} \sim U = \begin{smallmatrix} 00000 \\ 10000 \\ 01000 \\ 11000 \end{smallmatrix}, \qquad G_V = \begin{pmatrix} 10010 \\ 00110 \end{pmatrix} \sim V = \begin{smallmatrix} 00000 \\ 10010 \\ 00110 \\ 10100 \end{smallmatrix}$$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (I)

- Which 2-subspaces are nonvanishing with respect to x_1x_2?

We represent a 2-subspace U by its corresponding matrix G_U in RREF:

$$G_U = \begin{pmatrix} 10000 \\ 01000 \end{pmatrix} \sim U = \begin{matrix} 00000 \\ 10000 \\ 01000 \\ 11000 \end{matrix}, \qquad G_V = \begin{pmatrix} 10010 \\ 00110 \end{pmatrix} \sim V = \begin{matrix} 00000 \\ 10010 \\ 00110 \\ 10100 \end{matrix}$$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (I)

- Which 2-subspaces are nonvanishing with respect to $x_1 x_2$?

We represent a 2-subspace U by its corresponding matrix G_U in RREF:

$$G_U = \begin{pmatrix} 10000 \\ 01000 \end{pmatrix} \sim U = \begin{matrix} 00000 \\ 10000 \\ 01000 \\ 11000 \end{matrix}, \qquad G_V = \begin{pmatrix} 10010 \\ 00110 \end{pmatrix} \sim V = \begin{matrix} 00000 \\ 10010 \\ 00110 \\ 10100 \end{matrix}$$

- We have $U \in N_2(x_1 x_2)$ and $V \notin N_2(x_1 x_2)$.

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (I)

- Which 2-subspaces are nonvanishing with respect to x_1x_2?

We represent a 2-subspace U by its corresponding matrix G_U in RREF:

$$G_U = \begin{pmatrix} 10000 \\ 01000 \end{pmatrix} \sim U = \begin{smallmatrix} 00000 \\ 10000 \\ 01000 \\ 11000 \end{smallmatrix}, \qquad G_V = \begin{pmatrix} 10010 \\ 00110 \end{pmatrix} \sim V = \begin{smallmatrix} 00000 \\ 10010 \\ 00110 \\ 10100 \end{smallmatrix}$$

- We have $U \in N_2(x_1x_2)$ and $V \notin N_2(x_1x_2)$.
- So $U \in N_2(x_ix_j)$ iff columns i and j of G_U are linearly independent.

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (I)

- Which 2-subspaces are nonvanishing with respect to x_1x_2?

We represent a 2-subspace U by its corresponding matrix G_U in RREF:

$$G_U = \begin{pmatrix} 10000 \\ 01000 \end{pmatrix} \sim U = \begin{matrix} 00000 \\ 10000 \\ 01000 \\ 11000 \end{matrix}, \qquad G_V = \begin{pmatrix} 10010 \\ 00110 \end{pmatrix} \sim V = \begin{matrix} 00000 \\ 10010 \\ 00110 \\ 10100 \end{matrix}$$

- We have $U \in N_2(x_1x_2)$ and $V \notin N_2(x_1x_2)$.
- So $U \in N_2(x_ix_j)$ iff columns i and j of G_U are linearly independent.

For example

$$N_2(x_1x_2) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} 10 * ** \\ 01 * ** \end{pmatrix} \right\}$$

$$N_2(x_3x_4) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} * * * * * \\ * * * * * \end{pmatrix} \text{ and rank} \begin{pmatrix} ** \\ ** \end{pmatrix} = 2 \right\}.$$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (II)

- We now determine $|N_k(m)|$ for a monomial m of degree k.

$$N_2(x_1x_2) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} 10 * ** \\ 01 * ** \end{pmatrix} \right\}$$

$$N_2(x_3x_4) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} * * * * * \\ * * * * * \end{pmatrix} \text{ and rank} \begin{pmatrix} ** \\ ** \end{pmatrix} = 2 \right\}$$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (II)

- We now determine $|N_k(m)|$ for a monomial m of degree k.

$$N_2(x_1x_2) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} 10 * ** \\ 01 * ** \end{pmatrix} \right\}$$

$$N_2(x_3x_4) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} * * * * * \\ * * * * * \end{pmatrix} \text{ and rank } \begin{pmatrix} ** \\ ** \end{pmatrix} = 2 \right\}$$

- For x_1x_2 we can choose each $* \in \mathbb{F}_2$ arbitrarily $\implies |N_2(x_1x_2)| = 2^{k(n-k)} = 2^6 = 64$.

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (II)

- We now determine $|N_k(m)|$ for a monomial m of degree k.

$$N_2(x_1x_2) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} 10 * ** \\ 01 * ** \end{pmatrix} \right\}$$

$$N_2(x_3x_4) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} * * * * * \\ * * * * * \end{pmatrix} \text{ and rank } \begin{pmatrix} ** \\ ** \end{pmatrix} = 2 \right\}$$

- For x_1x_2 we can choose each $* \in \mathbb{F}_2$ arbitrarily $\implies |N_2(x_1x_2)| = 2^{k(n-k)} = 2^6 = 64$.

Theorem

Let m be an n-variable monomial of degree k. Then $|N_2(m)| = 2^{k(n-k)}$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (II)

- We now determine $|N_k(m)|$ for a monomial m of degree k.

$$N_2(x_1x_2) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} 10 * ** \\ 01 * ** \end{pmatrix} \right\}$$

$$N_2(x_3x_4) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} * * * * * \\ * * * * * \end{pmatrix} \text{ and rank} \begin{pmatrix} ** \\ ** \end{pmatrix} = 2 \right\}$$

- For x_1x_2 we can choose each $* \in \mathbb{F}_2$ arbitrarily $\implies |N_2(x_1x_2)| = 2^{k(n-k)} = 2^6 = 64$.

Theorem

Let m be an n-variable monomial of degree k. Then $|N_2(m)| = 2^{k(n-k)}$

- Now what about $f = x_1x_2 + x_3x_4$?

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (III)

Let $f = x_1x_2 + x_3x_4$ and observe that $\sum_{x\in U} f(x) = \sum_{x\in U} x_1x_2 + \sum_{x\in U} x_3x_4$.

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (III)

Let $f = x_1x_2 + x_3x_4$ and observe that $\sum_{x \in U} f(x) = \sum_{x \in U} x_1x_2 + \sum_{x \in U} x_3x_4$.

- $U \in N_2(f)$ iff either $U \in N_2(x_1x_2)$ or $U \in N_2(x_3x_4)$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (III)

Let $f = x_1x_2 + x_3x_4$ and observe that $\sum_{x \in U} f(x) = \sum_{x \in U} x_1x_2 + \sum_{x \in U} x_3x_4$.

- $U \in N_2(f)$ iff either $U \in N_2(x_1x_2)$ or $U \in N_2(x_3x_4)$
- $N_2(f) = N_2(x_1x_2) \triangle N_2(x_3x_4)$ and

$$|N_2(f)| = |N_2(x_1x_2)| + |N_2(x_3x_4)| - 2|N_2(x_1x_2) \cap N_2(x_3x_4)|$$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (III)

Let $f = x_1x_2 + x_3x_4$ and observe that $\sum_{x\in U} f(x) = \sum_{x\in U} x_1x_2 + \sum_{x\in U} x_3x_4$.

- $U \in N_2(f)$ iff either $U \in N_2(x_1x_2)$ or $U \in N_2(x_3x_4)$
- $N_2(f) = N_2(x_1x_2) \triangle N_2(x_3x_4)$ and

$$|N_2(f)| = |N_2(x_1x_2)| + |N_2(x_3x_4)| - 2|N_2(x_1x_2) \cap N_2(x_3x_4)|$$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (III)

Let $f = x_1x_2 + x_3x_4$ and observe that $\sum_{x\in U} f(x) = \sum_{x\in U} x_1x_2 + \sum_{x\in U} x_3x_4$.

- $U \in N_2(f)$ iff either $U \in N_2(x_1x_2)$ or $U \in N_2(x_3x_4)$
- $N_2(f) = N_2(x_1x_2) \triangle N_2(x_3x_4)$ and

$$|N_2(f)| = |N_2(x_1x_2)| + |N_2(x_3x_4)| - 2|N_2(x_1x_2) \cap N_2(x_3x_4)|$$

$$N_2(x_1x_2) \cap N_2(x_3x_4) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} 10 * ** \\ 01 * ** \end{pmatrix} \text{ and rank } \begin{pmatrix} ** \\ ** \end{pmatrix} = 2 \right\}$$

- So $|N_2(f)| = 64 + 64 - 2 \cdot 6 \cdot 4 = 80$

Matrix approach to determine $|N_k(f)|$ – Example with $n = 5, k = 2$ (III)

Let $f = x_1x_2 + x_3x_4$ and observe that $\sum_{x \in U} f(x) = \sum_{x \in U} x_1x_2 + \sum_{x \in U} x_3x_4$.

- $U \in N_2(f)$ iff either $U \in N_2(x_1x_2)$ or $U \in N_2(x_3x_4)$
- $N_2(f) = N_2(x_1x_2) \triangle N_2(x_3x_4)$ and

$$|N_2(f)| = |N_2(x_1x_2)| + |N_2(x_3x_4)| - 2|N_2(x_1x_2) \cap N_2(x_3x_4)|$$

$$N_2(x_1x_2) \cap N_2(x_3x_4) = \left\{ U \subseteq \mathbb{F}_2^5 : G_U = \begin{pmatrix} 10 * ** \\ 01 * ** \end{pmatrix} \text{ and rank} \begin{pmatrix} ** \\ ** \end{pmatrix} = 2 \right\}$$

- So $|N_2(f)| = 64 + 64 - 2 \cdot 6 \cdot 4 = 80$

We can determine $|N_k(f)|$ by counting matrices in RREF with prescribed sets of linearly independent columns and using the PIE!

A matrix approach to determine $|N_k(f)|$

Theorem (K 2026)

Let f be a k-homogeneous n-variable Boolean function with t terms: $f = m_1 + \cdots + m_t$. Then

$$|N_k(f)| = \sum_{\ell=1}^{t} (-2)^{\ell-1} \sum_{\{i_1,\ldots,i_\ell\} \in \binom{n}{\ell}} \left| \bigcap_{j=1}^{\ell} N_k(m_{i_j}) \right|$$

and

$$\bigcap_{j=1}^{\ell} N_k(m_j) = \{U \subseteq \mathbb{F}_2^n : \mathrm{rank}(G_U[\mathrm{Var}(m_j)]) = k \text{ for } j \in \{1,\ldots,\ell\}\},$$

where $G_U[\mathrm{Var}(m_j)]$ is the $k \times k$ matrix consisting of the columns $i \in \mathrm{Var}(m_j)$ of G_U.

A matrix approach to determine $|N_k(f)|$

Theorem (K 2026)

Let f be a k-homogeneous n-variable Boolean function with t terms: $f = m_1 + \cdots + m_t$. Then

$$|N_k(f)| = \sum_{\ell=1}^{t} (-2)^{\ell-1} \sum_{\{i_1,\ldots,i_\ell\} \in \binom{n}{\ell}} \left| \bigcap_{j=1}^{\ell} N_k(m_{i_j}) \right|$$

and

$$\bigcap_{j=1}^{\ell} N_k(m_j) = \{U \subseteq \mathbb{F}_2^n : \mathrm{rank}(G_U[\mathrm{Var}(m_j)]) = k \text{ for } j \in \{1,\ldots,\ell\}\},$$

where $G_U[\mathrm{Var}(m_j)]$ is the $k \times k$ matrix consisting of the columns $i \in \mathrm{Var}(m_j)$ of G_U.

How to count matrices in RREF with prescribed sets of independent columns?

Summary and further questions

Main results:

- A new approach to study the nonvanishing k-flats of functions of algebraic degree k
- Determining the precise number of nonvanishing k-flats for k-homogeneous d-intersecting Boolean functions
- Establishing a duality between nonvanishing k-flats and nonvanishing $(n-k)$-flats

Summary and further questions

Main results:

- A new approach to study the nonvanishing k-flats of functions of algebraic degree k
- Determining the precise number of nonvanishing k-flats for k-homogeneous d-intersecting Boolean functions
- Establishing a duality between nonvanishing k-flats and nonvanishing $(n-k)$-flats

Open problems:

- Can this matrix approach be used algorithmically to effectively compute $|N_k(f)|$?
- Can we use the matrix approach to tackle other Boolean funtions?

Summary and further questions

Main results:

- A new approach to study the nonvanishing k-flats of functions of algebraic degree k
- Determining the precise number of nonvanishing k-flats for k-homogeneous d-intersecting Boolean functions
- Establishing a duality between nonvanishing k-flats and nonvanishing $(n-k)$-flats

Open problems:

- Can this matrix approach be used algorithmically to effectively compute $|N_k(f)|$?
- Can we use the matrix approach to tackle other Boolean funtions?

Merci beaucoup de votre attention!

References I

[1] R. Arshad. Contributions to the theory of almost perfect nonlinear functions. PhD thesis. Magdeburg: Otto von Guericke University, 2018. DOI: 10.25673/13406.

[2] C. Carlet. A notion on S-boxes for a partial resistance to some integral attacks. Cryptology ePrint Archive, Paper 2024/1693. 2025.

[3] C. Carlet. On the vector subspaces of $\mathbb{F}_{2^n}$ over which the multiplicative inverse function sums to zero. In: Des. Codes Cryptogr. 93.4 (2025), pp. 1237–1254. DOI: 10.1007/s10623-024-01531-6.

[4] C. Carlet. Two generalizations of almost perfect nonlinearity. In: J. Cryptology 38.2 (2025), Paper No. 20, 32. DOI: 10.1007/s00145-025-09538-5.

[5] C. Carlet and X.-d. Hou. More on the sum-freedom of the multiplicative inverse function. arXiv:2407.14660. 2024. arXiv: 2407.14660 [math.NT].

[6] A. Ebeling, X.-d. Hou, A. Rydell, and S. Zhao. On sum-free functions. In: Finite Fields Appl. 110 (2026), Paper No. 102744, 32. DOI: 10.1016/j.ffa.2025.102744.

[7] P. Heering, C. Kaspers, and V. Taranchuk. On Reed-Muller subcodes, Grassmannian partitions and sum-free functions. 2026. arXiv: 2605.22958 [cs.IT].

References II

[8] X.-d. Hou and S. Zhao. On a conjecture about the sum-freedom of the binary multiplicative inverse function. In: Des. Codes Cryptogr. 94.4 (2026), Paper No. 86. DOI: 10.1007/s10623-026-01819-9.

[9] X.-d. Hou and S. Zhao. Two absolutely irreducible polynomials over $\mathbb{F}_2$ and their applications to a conjecture by Carlet. In: Finite Fields Appl. 109 (2026), Paper No. 102713, 17. DOI: 10.1016/j.ffa.2025.102713.

[10] C. Kaspers. Nonvanishing k-flats of Boolean and vectorial functions. 2026. arXiv: 2603.28266 [math.CO].

[11] S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and P. Stănică. Vanishing flats: a combinatorial viewpoint on the planarity of functions and their application. In: IEEE Trans. Inform. Theory 66.11 (2020), pp. 7101–7112. DOI: 10.1109/TIT.2020.3002993.

[12] K. Nyberg. Differentially uniform mappings for cryptography. In: Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993). Vol. 765. Lecture Notes in Comput. Sci. Springer, Berlin, 1994, pp. 55–64. DOI: 10.1007/3-540-48285-7\{_}6.