Sidon sets in $\mathbb{F}_2^n$ and the vectorial nonlinearity

Gábor P. Nagy

University of Szeged (Hungary) and
Budapest University of Technology and Economics (Hungary)

The 9th International Workshop on
Boolean Functions and their Applications

September 9-13, 2024
Dubrovnik (Croatia)

Outline

1. Nonlinearity vs vectorial nonlinearity
2. Differential uniformity vs vectorial nonlinearity
3. Sidon sets in $\mathbb{F}_2^n$
4. Large Sidon sets in $\mathbb{F}_2^n$
5. Computing the vectorial nonlinearity

Outline

1. Nonlinearity vs vectorial nonlinearity
2. Differential uniformity vs vectorial nonlinearity
3. Sidon sets in $\mathbb{F}_2^n$
4. Large Sidon sets in $\mathbb{F}_2^n$
5. Computing the vectorial nonlinearity

NSUCRYPTO 2021

International Olympiad in Cryptography NSUCRYPTO'2021

Second round   October 18-25   General, Teams

Problem 11. «Distance to affine functions»

Given two functions F and G from $\mathbb{F}_2^n$ (or $\mathbb{F}_{2^n}$) to itself, their Hamming distance equals by definition the number of inputs x at which $F(x) \neq G(x)$.

The minimum Hamming distance between any such function F and all affine functions A is known to be strictly smaller than $2^n - n - 1$.

Find constructions of infinite classes of functions F having a distance to affine functions as large as possible.

International Olympiad in Cryptography NSUCRYPTO'2021

Second round October 18-25 General, Teams

Problem 11. «Distance to affine functions»

Given two functions F and G from $\mathbb{F}_2^n$ (or $\mathbb{F}_{2^n}$) to itself, their Hamming distance equals by definition the number of inputs x at which $F(x) \neq G(x)$.

The minimum Hamming distance between any such function F and all affine functions A is known to be strictly smaller than $2^n - n - 1$.

Find constructions of infinite classes of functions F having a distance to affine functions as large as possible.

NSUCRYPTO 2021

International Olympiad in Cryptography NSUCRYPTO'2021

Second round — October 18-25 — General, Teams

Problem 11. «Distance to affine functions»

Given two functions F and G from $\mathbb{F}_2^n$ (or $\mathbb{F}_{2^n}$) to itself, their Hamming distance equals by definition the number of inputs x at which $F(x) \neq G(x)$.

The minimum Hamming distance between any such function F and all affine functions A is known to be strictly smaller than $2^n - n - 1$.

Find constructions of infinite classes of functions F having a distance to affine functions as large as possible.

Nonlinearity and (n, m)-bent functions

1. The *Hamming distance* of $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$d_H(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|.$$
2. Let $\omega : \mathbb{F}_2^m \to \mathbb{F}_2$ be a nonzero linear functional. The Boolean function $\omega f : \mathbb{F}_2^n \to \mathbb{F}_2$, $(\omega f)(x) = \omega(f(x))$ is called a *component Boolean function* of f.
3. The *nonlinearity* of f is the distance between its component Boolean functions and affine Boolean functions
$$\mathrm{NL}_1(f) = \min_{\substack{\omega \in (\mathbb{F}_2^m)^* \setminus \{0\} \\ \alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2)}} d_H(\omega f, \alpha).$$
4. For all f, the *covering radius (CR)* bound gives
$$\mathrm{NL}_1(f) \leq 2^n - 2^{n/2-1}.$$
5. The functions achieving this bound are called *(n, m)-bent functions.*
6. The *Walsh-Hadamard transform* provides an effective tool for computation with nonlinearity $\mathrm{NL}_1(f)$.

Nonlinearity and (n, m)-bent functions

1. The *Hamming distance* of $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$d_H(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|.$$
2. Let $\omega : \mathbb{F}_2^m \to \mathbb{F}_2$ be a nonzero linear functional. The Boolean function $\omega f : \mathbb{F}_2^n \to \mathbb{F}_2$, $(\omega f)(x) = \omega(f(x))$ is called a *component Boolean function* of f.
3. The *nonlinearity* of f is the distance between its component Boolean functions and affine Boolean functions
$$\mathrm{NL}_1(f) = \min_{\substack{\omega \in (\mathbb{F}_2^m)^* \setminus \{0\} \\ \alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2)}} d_H(\omega f, \alpha).$$
4. For all f, the *covering radius (CR)* bound gives
$$\mathrm{NL}_1(f) \leq 2^n - 2^{n/2-1}.$$
5. The functions achieving this bound are called *(n, m)-bent functions.*
6. The *Walsh-Hadamard transform* provides an effective tool for computation with nonlinearity $\mathrm{NL}_1(f)$.

Nonlinearity and (n, m)-bent functions

1. The *Hamming distance* of $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$d_H(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|.$$
2. Let $\omega : \mathbb{F}_2^m \to \mathbb{F}_2$ be a nonzero linear functional. The Boolean function $\omega f : \mathbb{F}_2^n \to \mathbb{F}_2$, $(\omega f)(x) = \omega(f(x))$ is called a *component Boolean function* of f.
3. The *nonlinearity* of f is the distance between its component Boolean functions and affine Boolean functions
$$\mathrm{NL}_1(f) = \min_{\substack{\omega \in (\mathbb{F}_2^m)^* \setminus \{0\} \\ \alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2)}} d_H(\omega f, \alpha).$$
4. For all f, the *covering radius (CR)* bound gives
$$\mathrm{NL}_1(f) \leq 2^n - 2^{n/2-1}.$$
5. The functions achieving this bound are called *(n, m)-bent functions.*
6. The *Walsh-Hadamard transform* provides an effective tool for computation with nonlinearity $\mathrm{NL}_1(f)$.

Nonlinearity and (n, m)-bent functions

1. The *Hamming distance* of $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$d_H(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|.$$
2. Let $\omega : \mathbb{F}_2^m \to \mathbb{F}_2$ be a nonzero linear functional. The Boolean function $\omega f : \mathbb{F}_2^n \to \mathbb{F}_2$, $(\omega f)(x) = \omega(f(x))$ is called a *component Boolean function* of f.
3. The *nonlinearity* of f is the distance between its component Boolean functions and affine Boolean functions
$$\mathrm{NL}_1(f) = \min_{\substack{\omega \in (\mathbb{F}_2^m)^* \setminus \{0\} \\ \alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2)}} d_H(\omega f, \alpha).$$
4. For all f, the *covering radius (CR)* bound gives
$$\mathrm{NL}_1(f) \leq 2^n - 2^{n/2-1}.$$
5. The functions achieving this bound are called *(n, m)-bent functions.*
6. The *Walsh-Hadamard transform* provides an effective tool for computation with nonlinearity $\mathrm{NL}_1(f)$.

Nonlinearity and (n, m)-bent functions

1. The *Hamming distance* of $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$d_H(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|.$$
2. Let $\omega : \mathbb{F}_2^m \to \mathbb{F}_2$ be a nonzero linear functional. The Boolean function $\omega f : \mathbb{F}_2^n \to \mathbb{F}_2$, $(\omega f)(x) = \omega(f(x))$ is called a *component Boolean function* of f.
3. The *nonlinearity* of f is the distance between its component Boolean functions and affine Boolean functions
$$\mathrm{NL}_1(f) = \min_{\substack{\omega \in (\mathbb{F}_2^m)^* \setminus \{0\} \\ \alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2)}} d_H(\omega f, \alpha).$$
4. For all f, the *covering radius (CR)* bound gives
$$\mathrm{NL}_1(f) \leq 2^n - 2^{n/2-1}.$$
5. The functions achieving this bound are called *(n, m)-bent functions.*
6. The *Walsh-Hadamard transform* provides an effective tool for computation with nonlinearity $\mathrm{NL}_1(f)$.

Nonlinearity and (n, m)-bent functions

1. The *Hamming distance* of $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$d_H(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|.$$
2. Let $\omega : \mathbb{F}_2^m \to \mathbb{F}_2$ be a nonzero linear functional. The Boolean function $\omega f : \mathbb{F}_2^n \to \mathbb{F}_2$, $(\omega f)(x) = \omega(f(x))$ is called a *component Boolean function* of f.
3. The *nonlinearity* of f is the distance between its component Boolean functions and affine Boolean functions
$$\mathrm{NL}_1(f) = \min_{\substack{\omega \in (\mathbb{F}_2^m)^* \setminus \{0\} \\ \alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2)}} d_H(\omega f, \alpha).$$
4. For all f, the *covering radius (CR)* bound gives
$$\mathrm{NL}_1(f) \leq 2^n - 2^{n/2-1}.$$
5. The functions achieving this bound are called *(n, m)-bent functions.*
6. The *Walsh-Hadamard transform* provides an effective tool for computation with nonlinearity $\mathrm{NL}_1(f)$.

Vectorial nonlinearity and Problem 11

1. The *vectorial nonlinearity* of f is its distance from the set of affine functions

$$\mathrm{NL}_{\boldsymbol{v}}(f) = d_H(f, \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)) = \min_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} d_H(f, \alpha).$$

Problem 11 reformulated

Find infinite classes of functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with high vectorial nonlinearity.

The computation of the vectorial nonlinearity $\mathrm{NL}_{\boldsymbol{v}}(f)$ is generally difficult.

Partial solution (Maróti, G Nagy, G Nagy 2021)

Define $n = 2m$, $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$f(x, y) = (xy, 0).$$

Then $\mathrm{NL}_{\boldsymbol{v}}(f) = (2^m - 1)^2 = 2^n - 2 \cdot 2^{n/2} + 1$.

Vectorial nonlinearity and Problem 11

1. The *vectorial nonlinearity* of f is its distance from the set of affine functions

$$\mathrm{NL}_{\mathbf{v}}(f) = d_H(f, \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)) = \min_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} d_H(f, \alpha).$$

Problem 11 reformulated

Find infinite classes of functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with high vectorial nonlinearity.

The computation of the vectorial nonlinearity $\mathrm{NL}_{\mathbf{v}}(f)$ is generally difficult.

Partial solution (Maróti, G Nagy, G Nagy 2021)

Define $n = 2m$, $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$f(x, y) = (xy, 0).$$

Then $\mathrm{NL}_{\mathbf{v}}(f) = (2^m - 1)^2 = 2^n - 2 \cdot 2^{n/2} + 1$.

Vectorial nonlinearity and Problem 11

1. The *vectorial nonlinearity* of f is its distance from the set of affine functions

$$\mathrm{NL}_{\boldsymbol{v}}(f) = d_H(f, \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)) = \min_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} d_H(f, \alpha).$$

Problem 11 reformulated

Find infinite classes of functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with high vectorial nonlinearity.

The computation of the vectorial nonlinearity $\mathrm{NL}_{\boldsymbol{v}}(f)$ is generally difficult.

Partial solution (Maróti, G Nagy, G Nagy 2021)

Define $n = 2m$, $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$f(x, y) = (xy, 0).$$

Then $\mathrm{NL}_{\boldsymbol{v}}(f) = (2^m - 1)^2 = 2^n - 2 \cdot 2^{n/2} + 1$.

Nonlinearity vs vectorial nonlinearity

Trivial bounds:

$$\mathrm{NL}_1(f) \leq \mathrm{NL}_{\boldsymbol{v}}(f) < 2^n - n - 1.$$

Theorem (Carlet, Ding, Yuan 2005)

Let n, m be integers, when n is even. If f is an (n, m)-bent function, then we have

$$\left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right) \leq \mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n + 2^{n/2}\right).$$

Theorem (Liu, Mesnager, Chen 2017)

If an (n, m)-function f satisfies **[...]**, then

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right).$$

Nonlinearity vs vectorial nonlinearity

Trivial bounds:

$$\mathrm{NL}_1(f) \le \mathrm{NL}_{\boldsymbol{v}}(f) < 2^n - n - 1.$$

Theorem (Carlet, Ding, Yuan 2005)

Let n, m be integers, when n is even. If f is an (n, m)-bent function, then we have

$$\left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right) \le \mathrm{NL}_{\boldsymbol{v}}(f) \le \left(1 - \frac{1}{2^m}\right)\left(2^n + 2^{n/2}\right).$$

Theorem (Liu, Mesnager, Chen 2017)

If an (n, m)-function f satisfies **[...]**, then

$$\mathrm{NL}_{\boldsymbol{v}}(f) \le \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right).$$

The Liu-Mesnager-Chen Conjecture (LMCC)

Conjecture (Liu, Mesnager, Chen 2017)

For (n, m)-functions f, the upper bound

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$

is tight.

- LMCC holds for $m = 1$ by the covering radius bound.
- LMCC implies

$$\mathrm{NL}_{\boldsymbol{v}}(f) = \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$

  for (n, m)-bent functions f.
- For $(2m, m)$-bent functions f, LMCC implies $\mathrm{NL}_{\boldsymbol{v}}(f) = (2^m - 1)^2$.

The Liu-Mesnager-Chen Conjecture (LMCC)

Conjecture (Liu, Mesnager, Chen 2017)

For (n, m)-functions f, the upper bound

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$

is tight.

- LMCC holds for $m = 1$ by the covering radius bound.
- LMCC implies

$$\mathrm{NL}_{\boldsymbol{v}}(f) = \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$

  for (n, m)-bent functions f.
- For $(2m, m)$-bent functions f, LMCC implies $\mathrm{NL}_{\boldsymbol{v}}(f) = (2^m - 1)^2$.

The Liu-Mesnager-Chen Conjecture (LMCC)

Conjecture (Liu, Mesnager, Chen 2017)

For (n, m)-functions f, the upper bound

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$

is tight.

- LMCC holds for $m = 1$ by the covering radius bound.
- LMCC implies
$$\mathrm{NL}_{\boldsymbol{v}}(f) = \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$
for (n, m)-bent functions f.
- For $(2m, m)$-bent functions f, LMCC implies $\mathrm{NL}_{\boldsymbol{v}}(f) = (2^m - 1)^2$.

The Liu-Mesnager-Chen Conjecture (LMCC)

Conjecture (Liu, Mesnager, Chen 2017)

For (n, m)-functions f, the upper bound

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$

is tight.

- LMCC holds for $m = 1$ by the covering radius bound.
- LMCC implies

$$\mathrm{NL}_{\boldsymbol{v}}(f) = \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right)$$

  for (n, m)-bent functions f.
- For $(2m, m)$-bent functions f, LMCC implies $\mathrm{NL}_{\boldsymbol{v}}(f) = (2^m - 1)^2$.

Outline

1. Nonlinearity vs vectorial nonlinearity
2. Differential uniformity vs vectorial nonlinearity
3. Sidon sets in $\mathbb{F}_2^n$
4. Large Sidon sets in $\mathbb{F}_2^n$
5. Computing the vectorial nonlinearity

Differential uniformity

1. The *differential uniformity* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\delta_f = \max_{\substack{a \in \mathbb{F}_2^n \setminus \{0\} \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n \mid f(x) + f(x+a) = b\}|.$$
2. $\delta_f \geq 2$.
3. If $n = m$ and $\delta_f = 2$, then the function f is called *almost perfect nonlinear (APN).*

Notation

The *graph* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^{n+m}.$$

Lemma 1

$$\delta_f = \max_{(a,b) \in \mathbb{F}_2^{2n} \setminus \{(0,0)\}} |\Gamma_f \cap (\Gamma_f + (a,b))|.$$

Differential uniformity

1. The *differential uniformity* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\delta_f = \max_{\substack{a \in \mathbb{F}_2^n \setminus \{0\} \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n \mid f(x) + f(x+a) = b\}|.$$
2. $\delta_f \geq 2$.
3. If $n = m$ and $\delta_f = 2$, then the function f is called *almost perfect nonlinear (APN).*

Notation

The *graph* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^{n+m}.$$

Lemma 1

$$\delta_f = \max_{(a,b) \in \mathbb{F}_2^{2n} \setminus \{(0,0)\}} |\Gamma_f \cap (\Gamma_f + (a,b))|.$$

Differential uniformity

1. The *differential uniformity* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\delta_f = \max_{\substack{a \in \mathbb{F}_2^n \setminus \{0\} \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n \mid f(x) + f(x+a) = b\}|.$$
2. $\delta_f \geq 2$.
3. If $n = m$ and $\delta_f = 2$, then the function f is called *almost perfect nonlinear (APN).*

Notation

The *graph* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^{n+m}.$$

Lemma 1

$$\delta_f = \max_{(a,b) \in \mathbb{F}_2^{2n} \setminus \{(0,0)\}} |\Gamma_f \cap (\Gamma_f + (a, b))|.$$

Differential uniformity

1. The *differential uniformity* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\delta_f = \max_{\substack{a \in \mathbb{F}_2^n \setminus \{0\} \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n \mid f(x) + f(x+a) = b\}|.$$
2. $\delta_f \geq 2$.
3. If $n = m$ and $\delta_f = 2$, then the function f is called *almost perfect nonlinear (APN).*

Notation

The *graph* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^{n+m}.$$

Lemma 1

$$\delta_f = \max_{(a,b) \in \mathbb{F}_2^{2n} \setminus \{(0,0)\}} |\Gamma_f \cap (\Gamma_f + (a, b))|.$$

Differential uniformity

1. The *differential uniformity* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\delta_f = \max_{\substack{a \in \mathbb{F}_2^n \setminus \{0\} \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n \mid f(x) + f(x+a) = b\}|.$$
2. $\delta_f \geq 2$.
3. If $n = m$ and $\delta_f = 2$, then the function f is called *almost perfect nonlinear (APN).*

Notation

The *graph* of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is
$$\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^{n+m}.$$

Lemma 1

$$\delta_f = \max_{(a,b) \in \mathbb{F}_2^{2n} \setminus \{(0,0)\}} |\Gamma_f \cap (\Gamma_f + (a, b))|.$$

Differential uniformity vs vectorial nonlinearity

- Carlet (2021) proved a lower bound for $\mathrm{NL}_{\boldsymbol{v}}(f)$ in terms of the differential uniformity.
- Carlet's bound has been slightly improved:

Theorem (GN 2022, Ryabov 2023)

For all $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we have

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{\delta_f} \cdot 2^{n/2} - \frac{1}{2}.$$

In particular, for an APN function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$,

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}.$$

- **"APN functions are good candidates for approaching the Liu-Mesnager-Chen Conjecture."**
- **The trick:** Study the structure of the level sets $f^{-1}(b)$.

Differential uniformity vs vectorial nonlinearity

- Carlet (2021) proved a lower bound for $\mathrm{NL}_{\boldsymbol{v}}(f)$ in terms of the differential uniformity.
- Carlet's bound has been slightly improved:

Theorem (GN 2022, Ryabov 2023)

For all $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we have

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{\delta_f} \cdot 2^{n/2} - \frac{1}{2}.$$

In particular, for an APN function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$,

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}.$$

- **"APN functions are good candidates for approaching the Liu-Mesnager-Chen Conjecture."**
- **The trick:** Study the structure of the level sets $f^{-1}(b)$.

Differential uniformity vs vectorial nonlinearity

- Carlet (2021) proved a lower bound for $\mathrm{NL}_{\boldsymbol{v}}(f)$ in terms of the differential uniformity.
- Carlet's bound has been slightly improved:

Theorem (GN 2022, Ryabov 2023)

For all $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we have

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{\delta_f} \cdot 2^{n/2} - \frac{1}{2}.$$

In particular, for an APN function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$,

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}.$$

- **"APN functions are good candidates for approaching the Liu-Mesnager-Chen Conjecture."**
- **The trick:** Study the structure of the level sets $f^{-1}(b)$.

Differential uniformity vs vectorial nonlinearity

- Carlet (2021) proved a lower bound for $\mathrm{NL}_{\mathbf{v}}(f)$ in terms of the differential uniformity.
- Carlet's bound has been slightly improved:

Theorem (GN 2022, Ryabov 2023)

For all $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we have

$$\mathrm{NL}_{\mathbf{v}}(f) \geq 2^n - \sqrt{\delta_f} \cdot 2^{n/2} - \frac{1}{2}.$$

In particular, for an APN function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$,

$$\mathrm{NL}_{\mathbf{v}}(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}.$$

- **"APN functions are good candidates for approaching the Liu-Mesnager-Chen Conjecture."**
- **The trick:** Study the structure of the level sets $f^{-1}(b)$.

Differential uniformity vs vectorial nonlinearity

- Carlet (2021) proved a lower bound for $\mathrm{NL}_{\boldsymbol{v}}(f)$ in terms of the differential uniformity.
- Carlet's bound has been slightly improved:

Theorem (GN 2022, Ryabov 2023)

For all $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we have

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{\delta_f} \cdot 2^{n/2} - \frac{1}{2}.$$

In particular, for an APN function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$,

$$\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}.$$

- **"APN functions are good candidates for approaching the Liu-Mesnager-Chen Conjecture."**
- **The trick:** Study the structure of the level sets $f^{-1}(b)$.

Outline

1 Nonlinearity vs vectorial nonlinearity

2 Differential uniformity vs vectorial nonlinearity

3 Sidon sets in $\mathbb{F}_2^n$

4 Large Sidon sets in $\mathbb{F}_2^n$

5 Computing the vectorial nonlinearity

Sidon sets in abelian groups

Simon Sidon (or Szidon, 1892–1941) Hungarian hobby mathematician

Definition (S. Sidon 1932)

Let A be a finite abelian group. We say that $S \subseteq A$ is a *Sidon set* in A, if for any $x, y, z, w \in S$ of which **at least three are different,**

$$x + y \neq z + w.$$

Equivalently,

$$x - z \neq w - y.$$

- Sidon sets and sequences are studied since the 1930's.
- Sidon sequences are Sidon sets in $\mathbb{Z}$.
- Sidon sequences are closely related to Sidon sets in cyclic groups.
- **Problems:** How *large* Sidon sets can be? How *dense* Sidon sequences can be?

Sidon sets in abelian groups

Simon Sidon (or Szidon, 1892–1941) Hungarian hobby mathematician

Definition (S. Sidon 1932)

Let A be a finite abelian group. We say that $S \subseteq A$ is a *Sidon set* in A, if for any $x, y, z, w \in S$ of which **at least three are different,**

$$x + y \neq z + w.$$

Equivalently,

$$x - z \neq w - y.$$

- Sidon sets and sequences are studied since the 1930's.
- Sidon sequences are Sidon sets in $\mathbb{Z}$.
- Sidon sequences are closely related to Sidon sets in cyclic groups.
- **Problems:** How *large* Sidon sets can be? How *dense* Sidon sequences can be?

Sidon sets in abelian groups

Simon Sidon (or Szidon, 1892–1941) Hungarian hobby mathematician

Definition (S. Sidon 1932)

Let A be a finite abelian group. We say that $S \subseteq A$ is a *Sidon set* in A, if for any $x, y, z, w \in S$ of which **at least three are different,**

$$x + y \neq z + w.$$

Equivalently,

$$x - z \neq w - y.$$

- Sidon sets and sequences are studied since the 1930's.
- Sidon sequences are Sidon sets in $\mathbb{Z}$.
- Sidon sequences are closely related to Sidon sets in cyclic groups.
- **Problems:** How *large* Sidon sets can be? How *dense* Sidon sequences can be?

Sidon sets in abelian groups

Simon Sidon (or Szidon, 1892–1941) Hungarian hobby mathematician

Definition (S. Sidon 1932)

Let A be a finite abelian group. We say that $S \subseteq A$ is a *Sidon set* in A, if for any $x, y, z, w \in S$ of which **at least three are different,**

$$x + y \neq z + w.$$

Equivalently,

$$x - z \neq w - y.$$

- Sidon sets and sequences are studied since the 1930's.
- Sidon sequences are Sidon sets in $\mathbb{Z}$.
- Sidon sequences are closely related to Sidon sets in cyclic groups.
- **Problems:** How *large* Sidon sets can be? How *dense* Sidon sequences can be?

Sidon sets in abelian groups

Simon Sidon (or Szidon, 1892–1941) Hungarian hobby mathematician

Definition (S. Sidon 1932)

Let A be a finite abelian group. We say that $S \subseteq A$ is a *Sidon set* in A, if for any $x, y, z, w \in S$ of which **at least three are different,**

$$x + y \neq z + w.$$

Equivalently,

$$x - z \neq w - y.$$

- Sidon sets and sequences are studied since the 1930's.
- Sidon sequences are Sidon sets in $\mathbb{Z}$.
- Sidon sequences are closely related to Sidon sets in cyclic groups.
- **Problems:** How *large* Sidon sets can be? How *dense* Sidon sequences can be?

Sidon sets and the parameter t

Proposition 1

Let A be a finite abelian group, and $T \subseteq A$. Define

$$t = \max_{a \in A \setminus \{0\}} |T \cap (T + a)|.$$

1. *In general,* $t = 1 \Rightarrow$ Sidon $\Rightarrow t \leq 2$.
2. If A has *odd order,* then Sidon $\Leftrightarrow t = 1$.
3. If A has *exponent* 2, then Sidon $\Leftrightarrow t = 2$.
4. We have

$$|T| \leq \sqrt{t|A|} + \frac{1}{2}.$$

Reformulation of Lemma 1

Let Γ_f be the graph of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then $t(\Gamma_f) = \delta_f$.

Sidon sets and the parameter t

Proposition 1

Let A be a finite abelian group, and $T \subseteq A$. Define

$$t = \max_{a \in A \setminus \{0\}} |T \cap (T + a)|.$$

1. *In general,* $t = 1 \Rightarrow$ Sidon $\Rightarrow t \leq 2$.
2. If A has *odd order,* then Sidon $\Leftrightarrow t = 1$.
3. If A has *exponent* 2, then Sidon $\Leftrightarrow t = 2$.
4. We have

$$|T| \leq \sqrt{t|A|} + \frac{1}{2}.$$

Reformulation of Lemma 1

Let Γ_f be the graph of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then $t(\Gamma_f) = \delta_f$.

Sidon sets and the parameter t

Proposition 1

Let A be a finite abelian group, and $T \subseteq A$. Define

$$t = \max_{a \in A \setminus \{0\}} |T \cap (T + a)|.$$

1. *In general,* $t = 1 \Rightarrow$ Sidon $\Rightarrow t \leq 2$.
2. If A has *odd order,* then Sidon $\Leftrightarrow t = 1$.
3. If A has *exponent* 2, then Sidon $\Leftrightarrow t = 2$.
4. We have

$$|T| \leq \sqrt{t|A|} + \frac{1}{2}.$$

Reformulation of Lemma 1

Let Γ_f be the graph of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then $t(\Gamma_f) = \delta_f$.

Sidon sets and the parameter t

Proposition 1

Let A be a finite abelian group, and $T \subseteq A$. Define

$$t = \max_{a \in A \setminus \{0\}} |T \cap (T + a)|.$$

1. *In general*, $t = 1 \Rightarrow$ Sidon $\Rightarrow t \leq 2$.
2. If A has *odd order*, then Sidon $\Leftrightarrow t = 1$.
3. If A has *exponent 2*, then Sidon $\Leftrightarrow t = 2$.
4. We have

$$|T| \leq \sqrt{t|A|} + \frac{1}{2}.$$

Reformulation of Lemma 1

Let Γ_f be the graph of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then $t(\Gamma_f) = \delta_f$.

Sidon sets and the parameter t

Proposition 1

Let A be a finite abelian group, and $T \subseteq A$. Define

$$t = \max_{a \in A \setminus \{0\}} |T \cap (T + a)|.$$

1. *In general,* $t = 1 \Rightarrow$ Sidon $\Rightarrow t \leq 2$.
2. If A has *odd order,* then Sidon $\Leftrightarrow t = 1$.
3. If A has *exponent 2,* then Sidon $\Leftrightarrow t = 2$.
4. We have

$$|T| \leq \sqrt{t|A|} + \frac{1}{2}.$$

Reformulation of Lemma 1

Let Γ_f be the graph of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then $t(\Gamma_f) = \delta_f$.

Sidon sets and the parameter t

Proposition 1

Let A be a finite abelian group, and $T \subseteq A$. Define

$$t = \max_{a \in A \setminus \{0\}} |T \cap (T + a)|.$$

1. *In general,* $t = 1 \Rightarrow$ Sidon $\Rightarrow t \leq 2$.
2. If A has *odd order,* then Sidon $\Leftrightarrow t = 1$.
3. If A has *exponent* 2*,* then Sidon $\Leftrightarrow t = 2$.
4. We have

$$|T| \leq \sqrt{t|A|} + \frac{1}{2}.$$

Reformulation of Lemma 1

Let Γ_f be the graph of the function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then $t(\Gamma_f) = \delta_f$.

The obvious upper bound

Proposition 2 (Obvious upper bound)

Let S be a *Sidon set* in the abelian group A. Then

$$|S| \leq \sqrt{2|A|} + \frac{1}{2}.$$

In particular, for $A = \mathbb{F}_2^n$,

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

The known constructions are far from the upper bound

$A = \mathbb{F}_2^n$ has Sidon sets of size

$$|S| \geq \begin{cases} 2^{n/2} & \text{if } n \text{ is even,} \\ 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} \cong \frac{1}{\sqrt{2}} 2^{n/2} & \text{if } n \text{ is odd.} \end{cases}$$

Remark. In cyclic groups, the obvious upper bound is asymptotically sharp. (Erdős, Turán 1941)

The obvious upper bound

Proposition 2 (Obvious upper bound)

Let S be a *Sidon set* in the abelian group A. Then

$$|S| \leq \sqrt{2|A|} + \frac{1}{2}.$$

In particular, for $A = \mathbb{F}_2^n$,

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

The known constructions are far from the upper bound

$A = \mathbb{F}_2^n$ has Sidon sets of size

$$|S| \geq \begin{cases} 2^{n/2} & \text{if } n \text{ is even,} \\ 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} \cong \frac{1}{\sqrt{2}} 2^{n/2} & \text{if } n \text{ is odd.} \end{cases}$$

Remark. In cyclic groups, the obvious upper bound is asymptotically sharp. (Erdős, Turán 1941)

The obvious upper bound

Proposition 2 (Obvious upper bound)

Let S be a *Sidon set* in the abelian group A. Then

$$|S| \leq \sqrt{2|A|} + \frac{1}{2}.$$

In particular, for $A = \mathbb{F}_2^n$,

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

The known constructions are far from the upper bound

$A = \mathbb{F}_2^n$ has Sidon sets of size

$$|S| \geq \begin{cases} 2^{n/2} & \text{if } n \text{ is even,} \\ 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} \cong \frac{1}{\sqrt{2}} 2^{n/2} & \text{if } n \text{ is odd.} \end{cases}$$

Remark. In cyclic groups, the obvious upper bound is asymptotically sharp. (Erdős, Turán 1941)

The obvious upper bound

Proposition 2 (Obvious upper bound)

Let S be a *Sidon set* in the abelian group A. Then

$$|S| \leq \sqrt{2|A|} + \frac{1}{2}.$$

In particular, for $A = \mathbb{F}_2^n$,

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

The known constructions are far from the upper bound

$A = \mathbb{F}_2^n$ has Sidon sets of size

$$|S| \geq \begin{cases} 2^{n/2} & \text{if } n \text{ is even,} \\ 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} \cong \frac{1}{\sqrt{2}} 2^{n/2} & \text{if } n \text{ is odd.} \end{cases}$$

Remark. In cyclic groups, the obvious upper bound is asymptotically sharp. (Erdős, Turán 1941)

Sidon sets and APN functions

Theorem (Lindström 1969)

Let $n = 2m$ even, and identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

$$\{(x, x^3) \mid x \in \mathbb{F}_{2^m}\}$$

is a Sidon set in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

Theorem (folklore)

The function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if its graph is Sidon in $\mathbb{F}_2^{2n}$.

Sidon sets and APN functions

Theorem (Lindström 1969)

Let $n = 2m$ even, and identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

$$\{(x, x^3) \mid x \in \mathbb{F}_{2^m}\}$$

is a Sidon set in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

Theorem (folklore)

The function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if its graph is Sidon in $\mathbb{F}_2^{2n}$.

Proof of the lower bound

Lemma 3

Let f, α be (n, m)-functions, f APN, α affine.

1. The graph Γ_α is an affine subspace of dimension n in $\mathbb{F}_2^{n+m}$.
2. $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set in Γ_α.

Lemma 4

$$\mathrm{NL}_v(f) = 2^n - \max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha|.$$

The proof of $\mathrm{NL}_v(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}$.

It follows from the obvious upper bound

$$|T| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}$$

on the size of a Sidon set T in $\mathbb{F}_2^n$. □

Proof of the lower bound

Lemma 3

Let f, α be (n, m)-functions, f APN, α affine.

1. The graph Γ_α is an affine subspace of dimension n in $\mathbb{F}_2^{n+m}$.
2. $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set in Γ_α.

Lemma 4

$$\mathrm{NL}_v(f) = 2^n - \max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha|.$$

The proof of $\mathrm{NL}_v(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}$.

It follows from the obvious upper bound

$$|T| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}$$

on the size of a Sidon set T in $\mathbb{F}_2^n$. □

Proof of the lower bound

Lemma 3

Let f, α be (n,m)-functions, f APN, α affine.

1. The graph Γ_α is an affine subspace of dimension n in $\mathbb{F}_2^{n+m}$.
2. $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set in Γ_α.

Lemma 4

$$\mathrm{NL}_v(f) = 2^n - \max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha|.$$

The proof of $\mathrm{NL}_v(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}$.

It follows from the obvious upper bound

$$|T| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}$$

on the size of a Sidon set T in $\mathbb{F}_2^n$. □

Proof of the lower bound

Lemma 3

Let f, α be (n, m)-functions, f APN, α affine.

1. The graph Γ_α is an affine subspace of dimension n in $\mathbb{F}_2^{n+m}$.
2. $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set in Γ_α.

Lemma 4

$$\mathrm{NL}_{\boldsymbol{v}}(f) = 2^n - \max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha|.$$

The proof of $\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}$.

It follows from the obvious upper bound

$$|T| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}$$

on the size of a Sidon set T in $\mathbb{F}_2^n$. □

Proof of the lower bound

Lemma 3

Let f, α be (n, m)-functions, f APN, α affine.

1. The graph Γ_α is an affine subspace of dimension n in $\mathbb{F}_2^{n+m}$.
2. $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set in Γ_α.

Lemma 4

$$\mathrm{NL}_{\boldsymbol{v}}(f) = 2^n - \max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha|.$$

The proof of $\mathrm{NL}_{\boldsymbol{v}}(f) \geq 2^n - \sqrt{2} \cdot 2^{n/2} - \frac{1}{2}$.

It follows from the obvious upper bound

$$|T| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}$$

on the size of a Sidon set T in $\mathbb{F}_2^n$. □

The challenges

Challenge 1

Prove or disprove the Liu-Mesnager-Chen Conjecture

$$\mathrm{NL}_{\mathbf{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right).$$

Challenge 2

Use the Liu-Mesnager-Chen Conjecture to produce **large Sidon sets** in odd dimension.

1. For APN functions, the LMCC is

$$\max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha| \geq 2^{n/2} + 1 - \frac{1}{2^{n/2}}.$$

2. In other words, for any APN function f, there must be an affine function α such that $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set of size at least

$$2^{n/2} + 1$$

in $\Gamma_\alpha \cong \mathbb{F}_2^n$.

The challenges

Challenge 1

Prove or disprove the Liu-Mesnager-Chen Conjecture

$$\mathrm{NL}_{\mathbf{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right).$$

Challenge 2

Use the Liu-Mesnager-Chen Conjecture to produce **large Sidon sets** in odd dimension.

1. For APN functions, the LMCC is

$$\max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha| \geq 2^{n/2} + 1 - \frac{1}{2^{n/2}}.$$

2. In other words, for any APN function f, there must be an affine function α such that $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set of size at least

$$2^{n/2} + 1$$

in $\Gamma_\alpha \cong \mathbb{F}_2^n$.

The challenges

Challenge 1

Prove or disprove the Liu-Mesnager-Chen Conjecture

$$\mathrm{NL}_{\mathbf{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right).$$

Challenge 2

Use the Liu-Mesnager-Chen Conjecture to produce **large Sidon sets** in odd dimension.

1. For APN functions, the LMCC is

$$\max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha| \geq 2^{n/2} + 1 - \frac{1}{2^{n/2}}.$$

2. In other words, for any APN function f, there must be an affine function α such that $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set of size at least

$$2^{n/2} + 1$$

in $\Gamma_\alpha \cong \mathbb{F}_2^n$.

The challenges

Challenge 1

Prove or disprove the Liu-Mesnager-Chen Conjecture

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq \left(1 - \frac{1}{2^m}\right)\left(2^n - 2^{n/2}\right).$$

Challenge 2

Use the Liu-Mesnager-Chen Conjecture to produce **large Sidon sets** in odd dimension.

1. For APN functions, the LMCC is
$$\max_{\alpha \in \mathrm{Aff}(\mathbb{F}_2^n, \mathbb{F}_2^m)} |\Gamma_f \cap \Gamma_\alpha| \geq 2^{n/2} + 1 - \frac{1}{2^{n/2}}.$$
2. In other words, for any APN function f, there must be an affine function α such that $\Gamma_f \cap \Gamma_\alpha$ is a Sidon set of size at least
$$2^{n/2} + 1$$
in $\Gamma_\alpha \cong \mathbb{F}_2^n$.

The challenges

1. The obvious upper bound for Sidon sets is

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

2. **No Sidon sets** of this size are known.

Challenge 3

Improve the obvious upper bound for the size of Sidon sets.

1. Brouwer, Tolhuizen (1993) sharpened the obvious upper bound by 2 for Sidon sets in odd dimension.
2. Partial results by Czerwinski, Pott (2023) for even dimension.

The challenges

1. The obvious upper bound for Sidon sets is
$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$
2. **No Sidon sets** of this size are known.

Challenge 3

Improve the obvious upper bound for the size of Sidon sets.

1. Brouwer, Tolhuizen (1993) sharpened the obvious upper bound by 2 for Sidon sets in odd dimension.
2. Partial results by Czerwinski, Pott (2023) for even dimension.

The challenges

1. The obvious upper bound for Sidon sets is

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

2. **No Sidon sets** of this size are known.

Challenge 3

Improve the obvious upper bound for the size of Sidon sets.

1. Brouwer, Tolhuizen (1993) sharpened the obvious upper bound by 2 for Sidon sets in odd dimension.
2. Partial results by Czerwinski, Pott (2023) for even dimension.

The challenges

1. The obvious upper bound for Sidon sets is

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

2. **No Sidon sets** of this size are known.

Challenge 3

Improve the obvious upper bound for the size of Sidon sets.

1. Brouwer, Tolhuizen (1993) sharpened the obvious upper bound by 2 for Sidon sets in odd dimension.
2. Partial results by Czerwinski, Pott (2023) for even dimension.

The challenges

1. The obvious upper bound for Sidon sets is

$$|S| \leq \sqrt{2} \cdot 2^{n/2} + \frac{1}{2}.$$

2. **No Sidon sets** of this size are known.

Challenge 3

Improve the obvious upper bound for the size of Sidon sets.

1. Brouwer, Tolhuizen (1993) sharpened the obvious upper bound by 2 for Sidon sets in odd dimension.
2. Partial results by Czerwinski, Pott (2023) for even dimension.

Outline

1. Nonlinearity vs vectorial nonlinearity
2. Differential uniformity vs vectorial nonlinearity
3. Sidon sets in $\mathbb{F}_2^n$
4. Large Sidon sets in $\mathbb{F}_2^n$
5. Computing the vectorial nonlinearity

What is large?

Definition: Large

We say that the Sidon set S in $\mathbb{F}_2^n$ is *large,* if $|S| > 2^{n/2}$.

- If n is even, then graphs of APN functions $\mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$ are Sidon sets of size $2^{n/2}$.

Definition

The Sidon set S is *complete (or maximal),* if for any $a \in A \setminus S$, $S \cup \{a\}$ is not a Sidon set.

What is large?

Definition: Large

We say that the Sidon set S in $\mathbb{F}_2^n$ is *large,* if $|S| > 2^{n/2}$.

- If n is even, then graphs of APN functions $\mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$ are Sidon sets of size $2^{n/2}$.

Definition

The Sidon set S is *complete (or maximal),* if for any $a \in A \setminus S$, $S \cup \{a\}$ is not a Sidon set.

What is large?

Definition: Large

We say that the Sidon set S in $\mathbb{F}_2^n$ is *large,* if $|S| > 2^{n/2}$.

- If n is even, then graphs of APN functions $\mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$ are Sidon sets of size $2^{n/2}$.

Definition

The Sidon set S is *complete (or maximal),* if for any $a \in A \setminus S$, $S \cup \{a\}$ is not a Sidon set.

Completeness of graphs of APN functions

- Redman (2021) and Carlet (2022) investigated the completeness of those Sidon sets, that can be obtained as graphs of APN functions.
- Carlet (2022) observed that the incompleteness of the graph of the APN function f is equivalent with the existence of another APN function g such that their Hamming distance is $d_H(f,g) = 1$.
- Budaghyan, Carlet, Helleseth, Li and Sun (2018) conjectured that $d_H(f,g) = 1$ is impossible for two APN functions f, g.

Theorem (Carlet 2022?)

The graphs of plateaued APN functions are complete Sidon sets.

Completeness of graphs of APN functions

- Redman (2021) and Carlet (2022) investigated the completeness of those Sidon sets, that can be obtained as graphs of APN functions.
- Carlet (2022) observed that the incompleteness of the graph of the APN function f is equivalent with the existence of another APN function g such that their Hamming distance is $d_H(f, g) = 1$.
- Budaghyan, Carlet, Helleseth, Li and Sun (2018) conjectured that $d_H(f, g) = 1$ is impossible for two APN functions f, g.

Theorem (Carlet 2022?)

The graphs of plateaued APN functions are complete Sidon sets.

Completeness of graphs of APN functions

- Redman (2021) and Carlet (2022) investigated the completeness of those Sidon sets, that can be obtained as graphs of APN functions.
- Carlet (2022) observed that the incompleteness of the graph of the APN function f is equivalent with the existence of another APN function g such that their Hamming distance is $d_H(f, g) = 1$.
- Budaghyan, Carlet, Helleseth, Li and Sun (2018) conjectured that $d_H(f, g) = 1$ is impossible for two APN functions f, g.

Theorem (Carlet 2022?)

The graphs of plateaued APN functions are complete Sidon sets.

Completeness of graphs of APN functions

- Redman (2021) and Carlet (2022) investigated the completeness of those Sidon sets, that can be obtained as graphs of APN functions.
- Carlet (2022) observed that the incompleteness of the graph of the APN function f is equivalent with the existence of another APN function g such that their Hamming distance is $d_H(f, g) = 1$.
- Budaghyan, Carlet, Helleseth, Li and Sun (2018) conjectured that $d_H(f, g) = 1$ is impossible for two APN functions f, g.

Theorem (Carlet 2022?)

The graphs of plateaued APN functions are complete Sidon sets.

Multiplicative subgroups as large Sidon sets

Theorem (Carlet, Mesnager 2020)

Let $q = 2^m$, $n = 2m$, and G_{q+1} be the cyclic subgroup of $\mathbb{F}_{q^2}$ of order $q+1$.

1. G_{q+1} is a Sidon sets in the additive group of $\mathbb{F}_{q^2}$.
2. G_{q+1} is sum-free if and only if $4 \mid n$.
3. In other words, $G_{q+1} \cup \{0\}$ is Sidon if and only if $4 \mid n$.

- These are **large Sidon sets** of size $2^{n/2}+1$ and $2^{n/2}+2$.
- We can interpret them as **conics** in the affine plane.

Multiplicative subgroups as large Sidon sets

Theorem (Carlet, Mesnager 2020)

Let $q = 2^m$, $n = 2m$, and G_{q+1} be the cyclic subgroup of $\mathbb{F}_{q^2}$ of order $q + 1$.

1. G_{q+1} is a Sidon sets in the additive group of $\mathbb{F}_{q^2}$.
2. G_{q+1} is sum-free if and only if $4 \mid n$.
3. In other words, $G_{q+1} \cup \{0\}$ is Sidon if and only if $4 \mid n$.

- These are **large Sidon sets** of size $2^{n/2} + 1$ and $2^{n/2} + 2$.
- We can interpret them as **conics** in the affine plane.

Multiplicative subgroups as large Sidon sets

Theorem (Carlet, Mesnager 2020)

Let $q = 2^m$, $n = 2m$, and G_{q+1} be the cyclic subgroup of $\mathbb{F}_{q^2}$ of order $q + 1$.

1. G_{q+1} is a Sidon sets in the additive group of $\mathbb{F}_{q^2}$.
2. G_{q+1} is sum-free if and only if $4 \mid n$.
3. In other words, $G_{q+1} \cup \{0\}$ is Sidon if and only if $4 \mid n$.

- These are **large Sidon sets** of size $2^{n/2} + 1$ and $2^{n/2} + 2$.
- We can interpret them as **conics** in the affine plane.

Multiplicative subgroups as large Sidon sets

Theorem (Carlet, Mesnager 2020)

Let $q = 2^m$, $n = 2m$, and G_{q+1} be the cyclic subgroup of $\mathbb{F}_{q^2}$ of order $q + 1$.

1. G_{q+1} is a Sidon sets in the additive group of $\mathbb{F}_{q^2}$.
2. G_{q+1} is sum-free if and only if $4 \mid n$.
3. In other words, $G_{q+1} \cup \{0\}$ is Sidon if and only if $4 \mid n$.

- These are **large Sidon sets** of size $2^{n/2} + 1$ and $2^{n/2} + 2$.
- We can interpret them as **conics** in the affine plane.

Multiplicative subgroups as large Sidon sets

Theorem (Carlet, Mesnager 2020)

Let $q = 2^m$, $n = 2m$, and G_{q+1} be the cyclic subgroup of $\mathbb{F}_{q^2}$ of order $q + 1$.

1. G_{q+1} is a Sidon sets in the additive group of $\mathbb{F}_{q^2}$.
2. G_{q+1} is sum-free if and only if $4 \mid n$.
3. In other words, $G_{q+1} \cup \{0\}$ is Sidon if and only if $4 \mid n$.

- These are **large Sidon sets** of size $2^{n/2} + 1$ and $2^{n/2} + 2$.
- We can interpret them as **conics** in the affine plane.

Multiplicative subgroups as large Sidon sets

Theorem (Carlet, Mesnager 2020)

Let $q = 2^m$, $n = 2m$, and G_{q+1} be the cyclic subgroup of $\mathbb{F}_{q^2}$ of order $q + 1$.

1. G_{q+1} is a Sidon sets in the additive group of $\mathbb{F}_{q^2}$.
2. G_{q+1} is sum-free if and only if $4 \mid n$.
3. In other words, $G_{q+1} \cup \{0\}$ is Sidon if and only if $4 \mid n$.

- These are **large Sidon sets** of size $2^{n/2} + 1$ and $2^{n/2} + 2$.
- We can interpret them as **conics** in the affine plane.

Conics in the affine plane

- $q = 2^m$.
- $\gamma \in \mathbb{F}_q$ such that $X^2 + \gamma X + 1$ is irreducible in $\mathbb{F}_{q^2}$.
- Affine conics are:

$$\begin{aligned} \text{hyperbola:} \quad & H : XY = 1, \\ \text{parabola:} \quad & P : Y = X^2, \\ \text{ellipse:} \quad & E : X^2 + \gamma XY + Y^2 = 1. \end{aligned}$$

- $|H| = q - 1$, $|P| = q$, $|E| = q + 1$.
- Nucleus of H and E is $(0, 0)$.

Conics in the affine plane

- $q = 2^m$.
- $\gamma \in \mathbb{F}_q$ such that $X^2 + \gamma X + 1$ is irreducible in $\mathbb{F}_{q^2}$.
- Affine conics are:

$$\begin{aligned} \text{hyperbola:} \quad & H : XY = 1, \\ \text{parabola:} \quad & P : Y = X^2, \\ \text{ellipse:} \quad & E : X^2 + \gamma XY + Y^2 = 1. \end{aligned}$$

- $|H| = q - 1$, $|P| = q$, $|E| = q + 1$.
- Nucleus of H and E is $(0, 0)$.

Conics in the affine plane

- $q = 2^m$.
- $\gamma \in \mathbb{F}_q$ such that $X^2 + \gamma X + 1$ is irreducible in $\mathbb{F}_{q^2}$.
- Affine conics are:

$$\begin{aligned} \text{hyperbola:} \quad & H : XY = 1, \\ \text{parabola:} \quad & P : Y = X^2, \\ \text{ellipse:} \quad & E : X^2 + \gamma XY + Y^2 = 1. \end{aligned}$$

- $|H| = q - 1$, $|P| = q$, $|E| = q + 1$.
- Nucleus of H and E is $(0, 0)$.

Conics in the affine plane

- $q = 2^m$.
- $\gamma \in \mathbb{F}_q$ such that $X^2 + \gamma X + 1$ is irreducible in $\mathbb{F}_{q^2}$.
- Affine conics are:

$$\begin{aligned} \text{hyperbola:} \qquad & H : XY = 1, \\ \text{parabola:} \qquad & P : Y = X^2, \\ \text{ellipse:} \qquad & E : X^2 + \gamma XY + Y^2 = 1. \end{aligned}$$

- $|H| = q - 1$, $|P| = q$, $|E| = q + 1$.
- Nucleus of H and E is $(0, 0)$.

Conics in the affine plane

- $q = 2^m$.
- $\gamma \in \mathbb{F}_q$ such that $X^2 + \gamma X + 1$ is irreducible in $\mathbb{F}_{q^2}$.
- Affine conics are:

$$\begin{aligned} \text{hyperbola:} &\quad H : XY = 1, \\ \text{parabola:} &\quad P : Y = X^2, \\ \text{ellipse:} &\quad E : X^2 + \gamma XY + Y^2 = 1. \end{aligned}$$

- $|H| = q - 1$, $|P| = q$, $|E| = q + 1$.
- Nucleus of H and E is $(0, 0)$.

Completeness results

Theorem (GN 2022)

Let $m \geq 4$ be an integer, $q = 2^m$. Let C be an ellipse or a hyperbola in the affine plane $AG(2, q)$. Let N be the nucleus of C.

1. When m is even and C is a hyperbola, or when m is odd and C is an ellipse, then C is a complete Sidon set in $\mathbb{F}_q^2$.
2. When m is odd and C is a hyperbola, or when m is even and C is an ellipse, then $C \cup \{N\}$ is a complete Sidon set in $\mathbb{F}_q^2$.

- If m is odd, then $S = H \cup N$ is Sidon of size q. This is the graph of the AES substitution box function $x \mapsto x^{q-2}$.
- The ellipse E is isomorphic to the Carlet-Mesnager Sidon set G_{q+1}.
- If m is even, then $E \cup \{N\}$ is isomorphic to $G_{q+1} \cup \{0\}$.
- E is also equivalent to the Goppa code Sidon set of size $q + 1$.

Completeness results

Theorem (GN 2022)

Let $m \geq 4$ be an integer, $q = 2^m$. Let C be an ellipse or a hyperbola in the affine plane $AG(2, q)$. Let N be the nucleus of C.

1. When m is even and C is a hyperbola, or when m is odd and C is an ellipse, then C is a complete Sidon set in $\mathbb{F}_q^2$.
2. When m is odd and C is a hyperbola, or when m is even and C is an ellipse, then $C \cup \{N\}$ is a complete Sidon set in $\mathbb{F}_q^2$.

- If m is odd, then $S = H \cup N$ is Sidon of size q. This is the graph of the AES substitution box function $x \mapsto x^{q-2}$.
- The ellipse E is isomorphic to the Carlet-Mesnager Sidon set G_{q+1}.
- If m is even, then $E \cup \{N\}$ is isomorphic to $G_{q+1} \cup \{0\}$.
- E is also equivalent to the Goppa code Sidon set of size $q + 1$.

Completeness results

Theorem (GN 2022)

Let $m \geq 4$ be an integer, $q = 2^m$. Let C be an ellipse or a hyperbola in the affine plane $AG(2, q)$. Let N be the nucleus of C.

1. When m is even and C is a hyperbola, or when m is odd and C is an ellipse, then C is a complete Sidon set in $\mathbb{F}_q^2$.
2. When m is odd and C is a hyperbola, or when m is even and C is an ellipse, then $C \cup \{N\}$ is a complete Sidon set in $\mathbb{F}_q^2$.

- If m is odd, then $S = H \cup N$ is Sidon of size q. This is the graph of the AES substitution box function $x \mapsto x^{q-2}$.
- The ellipse E is isomorphic to the Carlet-Mesnager Sidon set G_{q+1}.
- If m is even, then $E \cup \{N\}$ is isomorphic to $G_{q+1} \cup \{0\}$.
- E is also equivalent to the Goppa code Sidon set of size $q + 1$.

Completeness results

Theorem (GN 2022)

Let $m \geq 4$ be an integer, $q = 2^m$. Let C be an ellipse or a hyperbola in the affine plane $AG(2, q)$. Let N be the nucleus of C.

1. When m is even and C is a hyperbola, or when m is odd and C is an ellipse, then C is a complete Sidon set in $\mathbb{F}_q^2$.
2. When m is odd and C is a hyperbola, or when m is even and C is an ellipse, then $C \cup \{N\}$ is a complete Sidon set in $\mathbb{F}_q^2$.

- If m is odd, then $S = H \cup N$ is Sidon of size q. This is the graph of the AES substitution box function $x \mapsto x^{q-2}$.
- The ellipse E is isomorphic to the Carlet-Mesnager Sidon set G_{q+1}.
- If m is even, then $E \cup \{N\}$ is isomorphic to $G_{q+1} \cup \{0\}$.
- E is also equivalent to the Goppa code Sidon set of size $q + 1$.

Completeness results

Theorem (GN 2022)

Let $m \geq 4$ be an integer, $q = 2^m$. Let C be an ellipse or a hyperbola in the affine plane $AG(2, q)$. Let N be the nucleus of C.

1. When m is even and C is a hyperbola, or when m is odd and C is an ellipse, then C is a complete Sidon set in $\mathbb{F}_q^2$.
2. When m is odd and C is a hyperbola, or when m is even and C is an ellipse, then $C \cup \{N\}$ is a complete Sidon set in $\mathbb{F}_q^2$.

- If m is odd, then $S = H \cup N$ is Sidon of size q. This is the graph of the AES substitution box function $x \mapsto x^{q-2}$.
- The ellipse E is isomorphic to the Carlet-Mesnager Sidon set G_{q+1}.
- If m is even, then $E \cup \{N\}$ is isomorphic to $G_{q+1} \cup \{0\}$.
- E is also equivalent to the Goppa code Sidon set of size $q + 1$.

Completeness results

Theorem (GN 2022)

Let $m \geq 4$ be an integer, $q = 2^m$. Let C be an ellipse or a hyperbola in the affine plane $AG(2, q)$. Let N be the nucleus of C.

1. When m is even and C is a hyperbola, or when m is odd and C is an ellipse, then C is a complete Sidon set in $\mathbb{F}_q^2$.
2. When m is odd and C is a hyperbola, or when m is even and C is an ellipse, then $C \cup \{N\}$ is a complete Sidon set in $\mathbb{F}_q^2$.

- If m is odd, then $S = H \cup N$ is Sidon of size q. This is the graph of the AES substitution box function $x \mapsto x^{q-2}$.
- The ellipse E is isomorphic to the Carlet-Mesnager Sidon set G_{q+1}.
- If m is even, then $E \cup \{N\}$ is isomorphic to $G_{q+1} \cup \{0\}$.
- E is also equivalent to the Goppa code Sidon set of size $q + 1$.

Completeness results

Theorem (GN 2022)

Let $m \geq 4$ be an integer, $q = 2^m$. Let C be an ellipse or a hyperbola in the affine plane $AG(2, q)$. Let N be the nucleus of C.

1. When m is even and C is a hyperbola, or when m is odd and C is an ellipse, then C is a complete Sidon set in $\mathbb{F}_q^2$.
2. When m is odd and C is a hyperbola, or when m is even and C is an ellipse, then $C \cup \{N\}$ is a complete Sidon set in $\mathbb{F}_q^2$.

- If m is odd, then $S = H \cup N$ is Sidon of size q. This is the graph of the AES substitution box function $x \mapsto x^{q-2}$.
- The ellipse E is isomorphic to the Carlet-Mesnager Sidon set G_{q+1}.
- If m is even, then $E \cup \{N\}$ is isomorphic to $G_{q+1} \cup \{0\}$.
- E is also equivalent to the Goppa code Sidon set of size $q + 1$.

Sidon sets and double-error correcting codes

Proposition (folklore)

Sidon sets of size s in $\mathbb{F}_2^n$ and $[s-1, s-1-n, \geq 5]$ binary linear codes are essentially the same thing.

- Redman, Rose and Walker (2021)
- In the seminal "CCZ paper" Carlet, Charpin, Zinoviev (1998), for an APN function F, the minimum distance 5 linear code

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \cdots & F(\alpha^{N-1}) \end{bmatrix}$$

  has been investigated.
- Codes from the **online database** [Grassl] yield maximal Sidon sets for $n \leq 10$.
- Shortening of BCH codes and full support Goppa codes yield Sidon sets of size $2^{n/2} + 1$, n even.

Sidon sets and double-error correcting codes

Proposition (folklore)

Sidon sets of size s in $\mathbb{F}_2^n$ and $[s-1, s-1-n, \geq 5]$ binary linear codes are essentially the same thing.

- Redman, Rose and Walker (2021)
- In the seminal "CCZ paper" Carlet, Charpin, Zinoviev (1998), for an APN function F, the minimum distance 5 linear code

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \cdots & F(\alpha^{N-1}) \end{bmatrix}$$

  has been investigated.
- Codes from the **online database** [Grassl] yield maximal Sidon sets for $n \leq 10$.
- Shortening of BCH codes and full support Goppa codes yield Sidon sets of size $2^{n/2} + 1$, n even.

Sidon sets and double-error correcting codes

Proposition (folklore)

Sidon sets of size s in $\mathbb{F}_2^n$ and $[s-1, s-1-n, \geq 5]$ binary linear codes are essentially the same thing.

- Redman, Rose and Walker (2021)
- In the seminal "CCZ paper" Carlet, Charpin, Zinoviev (1998), for an APN function F, the minimum distance 5 linear code

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \cdots & F(\alpha^{N-1}) \end{bmatrix}$$

has been investigated.

- Codes from the **online database** [Grassl] yield maximal Sidon sets for $n \leq 10$.
- Shortening of BCH codes and full support Goppa codes yield Sidon sets of size $2^{n/2} + 1$, n even.

Sidon sets and double-error correcting codes

Proposition (folklore)

Sidon sets of size s in $\mathbb{F}_2^n$ and $[s-1, s-1-n, \geq 5]$ binary linear codes are essentially the same thing.

- Redman, Rose and Walker (2021)
- In the seminal “CCZ paper” Carlet, Charpin, Zinoviev (1998), for an APN function F, the minimum distance 5 linear code
$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \cdots & F(\alpha^{N-1}) \end{bmatrix}$$
has been investigated.
- Codes from the **online database** [Grassl] yield maximal Sidon sets for $n \leq 10$.
- Shortening of BCH codes and full support Goppa codes yield Sidon sets of size $2^{n/2}+1$, n even.

Sidon sets and double-error correcting codes

Proposition (folklore)

Sidon sets of size s in $\mathbb{F}_2^n$ and $[s-1, s-1-n, \geq 5]$ binary linear codes are essentially the same thing.

- Redman, Rose and Walker (2021)
- In the seminal "CCZ paper" Carlet, Charpin, Zinoviev (1998), for an APN function F, the minimum distance 5 linear code

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \cdots & F(\alpha^{N-1}) \end{bmatrix}$$

  has been investigated.
- Codes from the **online database** [Grassl] yield maximal Sidon sets for $n \leq 10$.
- Shortening of BCH codes and full support Goppa codes yield Sidon sets of size $2^{n/2} + 1$, n even.

Other known large Sidon sets

n	$2^{n/2}$	known max $\|S\|$	Structure
2	2	3	
3	2.83	4	
4	4	6	
5	5.66	7	
6	8	9	ellipse
7	11.31	12	??
8	16	18	ellipse plus nucleus
9	22.63	24	??
10	32	34	?? (Chen 1991)
11	45.25	48	?? (Chen 1991)

- **No infinite class** of large Sidon sets in odd dimension is known.
- The best known class has size

$$\frac{1}{\sqrt{2}}2^{n/2} + C \cdot 2^{n/4}.$$

Other known large Sidon sets

n	$2^{n/2}$	known max $\|S\|$	Structure
2	2	3	
3	2.83	4	
4	4	6	
5	5.66	7	
6	8	9	ellipse
7	11.31	12	??
8	16	18	ellipse plus nucleus
9	22.63	24	??
10	32	34	?? (Chen 1991)
11	45.25	48	?? (Chen 1991)

- **No infinite class** of large Sidon sets in odd dimension is known.
- The best known class has size

$$\frac{1}{\sqrt{2}}2^{n/2} + C \cdot 2^{n/4}.$$

Algorithms for Sidon sets

- **Constructions.**
- **Automorphisms** and **isomorphisms** using the design of minimum weight codewords.
- The vertex set of the design is S, the set of blocks is

$$\mathcal{B} = \{B \subseteq S \mid |B| = 5, 6, \sum_{x \in B} x = 0\}.$$

- Efficient for $n \leq 12$.
- **Classification** of complete Sidon sets up to dimension 8.

Problem

Improve the automorphism/isomorphism algorithms using Kaleyski's APN invariants (2022).

Algorithms for Sidon sets

- **Constructions.**
- **Automorphisms** and **isomorphisms** using the design of minimum weight codewords.
- The vertex set of the design is S, the set of blocks is

$$\mathcal{B} = \{B \subseteq S \mid |B| = 5, 6, \sum_{x \in B} x = 0\}.$$

- Efficient for $n \leq 12$.
- **Classification** of complete Sidon sets up to dimension 8.

Problem

Improve the automorphism/isomorphism algorithms using Kaleyski's APN invariants (2022).

Algorithms for Sidon sets

- **Constructions.**
- **Automorphisms** and **isomorphisms** using the design of minimum weight codewords.
- The vertex set of the design is S, the set of blocks is

$$\mathcal{B} = \{B \subseteq S \mid |B| = 5, 6, \sum_{x \in B} x = 0\}.$$

- Efficient for $n \leq 12$.
- **Classification** of complete Sidon sets up to dimension 8.

Problem

Improve the automorphism/isomorphism algorithms using Kaleyski's APN invariants (2022).

Algorithms for Sidon sets

- **Constructions.**
- **Automorphisms** and **isomorphisms** using the design of minimum weight codewords.
- The vertex set of the design is S, the set of blocks is

$$\mathcal{B} = \{B \subseteq S \mid |B| = 5, 6, \sum_{x \in B} x = 0\}.$$

- Efficient for $n \leq 12$.
- **Classification** of complete Sidon sets up to dimension 8.

Problem

Improve the automorphism/isomorphism algorithms using Kaleyski's APN invariants (2022).

Algorithms for Sidon sets

- **Constructions.**
- **Automorphisms** and **isomorphisms** using the design of minimum weight codewords.
- The vertex set of the design is S, the set of blocks is
$$\mathcal{B} = \{B \subseteq S \mid |B| = 5, 6, \sum_{x \in B} x = 0\}.$$
- Efficient for $n \leq 12$.
- **Classification** of complete Sidon sets up to dimension 8.

Problem

Improve the automorphism/isomorphism algorithms using Kaleyski's APN invariants (2022).

Algorithms for Sidon sets

- **Constructions.**
- **Automorphisms** and **isomorphisms** using the design of minimum weight codewords.
- The vertex set of the design is S, the set of blocks is

$$\mathcal{B} = \{B \subseteq S \mid |B| = 5, 6, \sum_{x \in B} x = 0\}.$$

- Efficient for $n \leq 12$.
- **Classification** of complete Sidon sets up to dimension 8.

Problem

Improve the automorphism/isomorphism algorithms using Kaleyski's APN invariants (2022).

Outline

1 Nonlinearity vs vectorial nonlinearity

2 Differential uniformity vs vectorial nonlinearity

3 Sidon sets in $\mathbb{F}_2^n$

4 Large Sidon sets in $\mathbb{F}_2^n$

5 Computing the vectorial nonlinearity

Results for $n = 4, 5$

Theorem (Ryabov 2023)

n	$\max|S|$	APN functions	$\mathrm{NL}_{\mathbf{v}}(f)$	LMCC
4	6	2 EA-equivalence classes	$10 = 2^4 - 6$	11.25
5	7	7 EA-equivalence classes	$25 = 2^5 - 7$	25.52

- LMCC holds.
- The vectorial nonlinearity is EA-invariant.

Results for $n = 4, 5$

Theorem (Ryabov 2023)

n	$\max \lvert S \rvert$	APN functions	$\mathrm{NL}_{\mathbf{v}}(f)$	LMCC
4	6	2 EA-equivalence classes	$10 = 2^4 - 6$	11.25
5	7	7 EA-equivalence classes	$25 = 2^5 - 7$	25.52

- LMCC holds.
- The vectorial nonlinearity is EA-invariant.

Results for $n = 4, 5$

Theorem (Ryabov 2023)

n	$\max \lvert S \rvert$	APN functions	$\mathrm{NL}_{\boldsymbol{v}}(f)$	LMCC
4	6	2 EA-equivalence classes	$10 = 2^4 - 6$	11.25
5	7	7 EA-equivalence classes	$25 = 2^5 - 7$	25.52

- LMCC holds.
- The vectorial nonlinearity is EA-invariant.

Results for $n = 6, 7$

Theorem (GN 2024?)

n	$\max\lvert S\rvert$	APN functions	$\mathrm{NL}_{\boldsymbol{v}}(f)$	LMCC
6	9	14 CCZ-equivalence classes	$55 = 2^6 - 9$	55.125
7	12	x^3, x^9	$117 = 2^7 - 11$	115.77
		other known 488 functions	$116 = 2^7 - 12$	

- LMCC does not hold for $n = 7$.

Problem

Is the vectorial nonlinearity CCZ-invariant?

Results for $n = 6, 7$

Theorem (GN 2024?)

n	$\max\|S\|$	APN functions	$\mathrm{NL}_{\boldsymbol{v}}(f)$	LMCC
6	9	14 CCZ-equivalence classes	$55 = 2^6 - 9$	55.125
7	12	x^3, x^9	$117 = 2^7 - 11$	115.77
		other known 488 functions	$116 = 2^7 - 12$	

- LMCC does not hold for $n = 7$.

Problem

Is the vectorial nonlinearity CCZ-invariant?

Results for $n = 6, 7$

Theorem (GN 2024?)

n	$\max \lvert S \rvert$	APN functions	$\mathrm{NL}_{\boldsymbol{v}}(f)$	LMCC
6	9	14 CCZ-equivalence classes	$55 = 2^6 - 9$	55.125
7	12	x^3, x^9	$117 = 2^7 - 11$	115.77
		other known 488 functions	$116 = 2^7 - 12$	

- LMCC does not hold for $n = 7$.

Problem

Is the vectorial nonlinearity CCZ-invariant?

Results for $n = 8, 9$

Theorem (GN 2024?)

n	$\max \lvert S \rvert$	APN functions	$\mathrm{NL}_{\boldsymbol{v}}(f)$	LMCC
8	18	x^9	$238 = 2^8 - 18$	239.06
		x^3, x^{57}	$\geq 240 = 2^8 - 16$	
9	24	Gold exponents $d = 3, 5, 17, 31, 103, 171$	$\geq 491 = 2^9 - 21$	488.42

- LMCC does not hold for $n = 8, 9$.

Results for $n = 8, 9$

Theorem (GN 2024?)

n	$\max\|S\|$	APN functions	$\mathrm{NL}_{\boldsymbol{v}}(f)$	LMCC
8	18	x^9	$238 = 2^8 - 18$	239.06
		x^3, x^{57}	$\geq 240 = 2^8 - 16$	
9	24	Gold exponents $d = 3, 5, 17, 31, 103, 171$	$\geq 491 = 2^9 - 21$	488.42

- LMCC does not hold for $n = 8, 9$.

LMCC for a class of APN functions

Theorem (GN 2024?)

Let n be divisible by 4, $d = 2^{n/2-1} + 1$ and $f(x) = x^d$ monomial Gold APN function. Then

$$\mathrm{NL}_{\boldsymbol{v}}(f) \leq 2^n - 2^{n/2} - 2.$$

In particular, LMCC holds for f.

Proof.

Use the affine function $\alpha(x) = x^{\frac{1}{2}} = x^{2^{n-1}}$. $\square$

LMCC for a class of APN functions

Theorem (GN 2024?)

Let n be divisible by 4, $d = 2^{n/2-1} + 1$ and $f(x) = x^d$ monomial Gold APN function. Then

$$\mathrm{NL}_{\mathbf{v}}(f) \leq 2^n - 2^{n/2} - 2.$$

In particular, LMCC holds for f.

Proof.

Use the affine function $\alpha(x) = x^{\frac{1}{2}} = x^{2^{n-1}}$. □

THANK YOU FOR YOUR ATTENTION!

ÉS BOLDOG

75. SZÜLETÉSNAPOT,

KEDVES CLAUDE!!

ÉS BOLDOG 75. SZÜLETÉSNAPOT, KEDVES CLAUDE!!