Relaxations of almost perfect nonlinearity

Alexander Pott[1] [2]

Otto von Guericke University Magdeburg

July 7, 2021

[1] Li, Shuxing; Meidl, Wilfried; Polujan, Alexandr; Pott, Alexander; Riera, Constanza; Stănică, Pantelimon. *Vanishing flats: a combinatorial viewpoint on the planarity of functions and their application.* IEEE Trans. Inform. Theory **66** no. 11 (2020), 7101–7112.

[2] Meidl, Wilfried; Polujan, Alexandr; Pott, Alexander. *Linear codes and incidence structures of bent functions and their generalizations.* arXiv: 2012.06866v1 (29 pages).

Outline

- Perfect nonlinearity, almost perfect nonlinearity ....
- Nonlinearity measure using *vanishing flats*:
  - Motivation.
  - Power mappings.
  - Quadratic mappings.
- Partially almost perfect nonlinear permutations.

I will not cover ...

- The new constructions of Beierle and Leander.[3]
- The new inequivalence results by Kaspers and Zhou.[4]

[3] Beierle, Christian; Leander, Gregor. *New Instances of Quadratic APN Functions.* arXiv: 2009.07204v3 (18 pages).

[4] Kaspers, Christian; Zhou, Yue. *The Number of Almost Perfect Nonlinear Functions Grows Exponentially*. Journal of Cryptology **34** no. 4 (2021).

Perfect nonlinearity

- Linear functions $F : V \to W$ satisfiy $F(x+a) - F(x) = F(a)$, hence $x \mapsto F(x+a) - F(x)$ is **constant** for all $a \in V$.
- If $|V|, |W| < \infty$, being on the other side of the spectrum means

$$x \mapsto F(x+a) - F(x)$$

is **balanced**, hence

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

has $|V|/|W|$ solutions.

Such functions are called perfect nonlinear.

Example

$F(x) = x^2$ with $V = W = \mathbb{F}_{p^n}$, p odd: $(x+a)^2 - x^2 = 2xa + a^2$

Perfect nonlinearity: Four questions

If V and W are abelian groups, we call a mapping $F : V \to W$ perfect nonlinear if $F(x+a) - F(x) = b$ has $|V|/|W|$ solutions. The graph $\{(x, F(x)) : x \in V\} \subset V \times W$ is a relative difference set[5] [6]

1. For which parameters $|V|, |W|$ do we have perfect nonlinear functions?
2. For which groups do we have such perfect nonlinear functions?
3. If we know that for certain groups V and W no perfect nonlinear function exists, what is the (second) best.
4. Classification? How many examples?

---

[5] Carlet, Claude; Ding, Cunsheng. *Highly nonlinear mappings.* J. Complexity **20** (2004), no. 2-3, 205–244.

[6] Pott, Alexander. *Nonlinear functions in abelian groups and relative difference sets.* Discrete Appl. Math. **138** (2004), no. 1-2, 177–193.

From now on: $V = \mathbb{F}_2^n$, $W = \mathbb{F}_2^m$

If $F : V \to W$, then

$$\delta_F(a, b) = |\{x \ : \ F(x + a) + F(x) = b\}|.$$

Definition

Almost perfect nonlinear function $F : V \to V$:

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

has 0 or 2 solutions for all $a \neq 0$ and all b, hence $\delta_F(a, b) \in \{0, 2\}$ for $a \neq 0$.

Example

x^{2^i+1} on $\mathbb{F}_{2^n}$ if $\gcd(i, n) = 1$.

Rodier condition

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN, if and only if

$$F(x) + F(y) + F(z) + F(u) \neq 0$$

whenever $x + y + z + u = 0$ and x, y, z, u are distinct. The sets $\{x, y, z, u\}$ are 2-dimensional affine subspaces of $\mathbb{F}_2^n$.

Definition

Let $F : V \to W$. Then

$$\begin{aligned} \mathcal{V}(F) := \; & \{x, y, z, u \text{ distinct } : F(x) + F(y) + F(z) + F(u) = 0, \\ & \quad x + y + z + u = 0\} \end{aligned}$$

is the set of vanishing 2-dimensional flats.

If F is APN, then ...

$$\delta_F(a,b) = |\{x \;:\; F(x+a) + F(x) = b\}|.$$

- The maximum of $\delta_F(a,b)$, $a \neq 0$ is 2.
- $\sum \delta_F(a,b)^2$ is as small as possible.
- $\mathcal{V}(F) = \emptyset$.

If $F : V \to W$ is perfect nonlinear, then ...

$$\delta_F(a,b) = |\{x \ : \ F(x+a) + F(x) = b\}|.$$

- The maximum of $\delta_F(a,b)$, $a \neq 0$ is $|V|/|W|$.
- $\sum \delta_F(a,b)^2$ is as small as possible.
- $|\mathcal{V}(F)|$ is as small as possible.

Relaxations

- Maximum $\delta_F(a, b)$, $a \neq 0$ is small (differential uniformity).
- $\sum \delta_F(a, b)^2$ (equivalently: minimizing the fourth powers of the Walsh coefficients) is small.
- $|\mathcal{V}(F)|$ is small.

Knowing the differential spectrum

$$\{* \ \delta_F(a, b) \ : \ a, b \in V \ *\}$$

we know the three quantities above.

Knowing the δ_F, we know $|\mathcal{V}(F)|$.

Lemma

$$|\mathcal{V}(F)| = \sum_{a \neq 0, b} \binom{\delta_F(a,b)/2}{2}.$$

The converse is not true:

Example

$n = 6$

- x^5: differential spectrum $\{64^1, 4^{336}, 0^{3759}\}$
- x^{11}: differential spectrum $\{64^1, 10^{63}, 6^{126}, 2^{1323}, 0^{2584}\}$

In both cases $|\mathcal{V}| = 336$.

$\mathcal{V}(F)$ also carries combinatorial information

If there are functions f_i such that

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix},$$

then

$$\mathcal{V}(F) = \bigcap_{i=1}^{m} \mathcal{V}(f_i)$$

- Which functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2^m$ have small $|\mathcal{V}(f_i)|$.
- Known for n even and $m \leq n/2$: perfect nonlinear functions, bent functions.
- Known for $n = m$: APN (and the minimum is 0).
- Not known for other values.

Strategy to build APN?

Find a large set of boolean functions f_i on $\mathbb{F}_2^n$, $i \in I$, where we can compute $\mathcal{V}(f_i)$, and then find a subset $J \subset I$, $|J| = n$, such that

$$\bigcap_{i \in J} \mathcal{V}(f_i) = \emptyset.$$

Similarly: functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2^{m_i}$. Then choose J such that $\sum_{i \in J} m_i = n$.

- Classical case: $n = 2m$, $m_1 = m_2 = m$ (perfect nonlinear).
- Classical case: $m_i = 1$ and use quadratic boolean functions.
- Why not extend the class of functions f_i from whom we build APN's by functions where $\mathcal{V}(f_i)$ is small.
- It is easy to construct boolean functions which are almost as good as perfect nonlinear functions.[7]

[7] Arshad, Razi. *Contributions to the theory of almost perfect nonlinear functions.* Ph.D. thesis Magdeburg (2018).

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Although the goal is to find $\mathcal{V}(F)$ for functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $m < n$ to build APN functions, we consider here, as a first step, the case $m = n$.

If F is a non-APN power mapping, then

$$|\mathcal{V}(F)| \geq \begin{cases} \frac{2^n+1}{3} & \text{if } n \text{ is odd} \\ \frac{2^n-1}{3} & \text{if } n \text{ is even} \end{cases}$$

The inverse function shows that the bound for n even is sharp. Open for n odd.

Proof

- Let $a_1, a_2 \neq 0$ be in $\mathbb{F}_{2^n}$.

$$(x+a_1)^d+x^d = b \Leftrightarrow \frac{a_2}{a_1}x \text{ is solution of } (x+a_2)^d+x^d = \left(\frac{a_2}{a_1}\right)^d b.$$

- $\{* \ \delta(a,b) \ : \ b \in \mathbb{F}_2^n \ *\}$ is the same for all $a \neq 0$.
- For each $a \neq 0$ there is a b such that $\delta(a,b) \geq 4$ (non-APN).
- Each vanishing flat $\{x,y,z,u\}$ with $F(x)+F(y)+F(z)+F(u)=0$ gives rise to three different (a_i,b_i) with $\delta(a_i,b_i) \geq 4$: $a_1 = x+y$ or $a_2 = x+z$ or $a_3 = x+u$.
- $|\mathcal{V}| \geq (2^n-1)/3$.

The inverse function

Theorem
Let n be even and α be a primitive element of $\mathbb{F}_{2^n}$ and $\zeta = \alpha^{\frac{2^n-1}{3}}$.

$$\mathcal{V}(x^{-1}) = \left\{ \{0, \alpha^i, \alpha^i\zeta, \alpha^i\zeta^2\} \mid 0 \leq i \leq \frac{2^n-4}{3} \right\}.$$

We not only know $|\mathcal{V}(x^{-1})| = \frac{2^n-1}{3}$ but also the set!

The GOLD power functions

Theorem

Let $F(x) = x^{2^t+1}$ *be a function over* $\mathbb{F}_{2^n}$ *with* $\gcd(n,t) = s > 1$. *For* $a \in \mathbb{F}_{2^s} \setminus \{0,1\}$ *and* $x \in \mathbb{F}_{2^n}^*$, *we define a* 2*-dimensional vector space* $V_{a,x} = \{0, x, ax, (1+a)x\}$ *and*

$$U_{a,x} = \{\{c, x+c, ax+c, (1+a)x+c\} : c \text{ coset representatives of } V_{a,x}\}.$$

Then $\mathcal{V}(F) = \bigcup_{\substack{a \in \mathbb{F}_{2^s} \setminus \{0,1\} \\ x \in \mathbb{F}_{2^n}^*}} U_{a,x}$ *and*

$$|\mathcal{V}(F)| = \frac{2^{n-2}(2^s-2)(2^n-1)}{6}$$

The number of vanishing flats of x^d over $\mathbb{F}_{2^n}$, for $2 \le n \le 8$, $\star$: unexplained.

n	$(d, \ |\mathcal{V}(x^d)|)$
2	$(1,1)$
3	$(1,14)$, $(3,0)$
4	$(1,140)$, $(3,0)$, $(5,20)$, $(7,5)$
5	$(1,1240)$, $(3,0)$, $(5,0)$, $(15,0)$
6	$(1,10416)$, $(3,0)$, $(5,336)$, $(7,84)$, $(9,1008)$, $(11,336)^\star$, $(15,126)$, $(21,2520)^\star$, $(27,1260)^\star$, $(31,21)$
7	$(1,85344)$, $(3,0)$, $(5,0)$, $(7,889)$, $(9,0)$, $(11,0)$, $(19,889)^\star$, $(21,889)$, $(23,0)$, $(63,0)$
8	$(1,690880)$, $(3,0)$, $(5,5440)$, $(7,3655)$, $(9,0)$, $(11,5185)^\star$, $(13,5185)^\star$, $(15,1785)$, $(17,38080)$, $(19,4420)^\star$, $(21,2040)$, $(23,4930)^\star$, $(25,4420)^\star$, $(27,15810)^\star$, $(31,2380)$, $(39,0)$, $(43,27625)^\star$, $(45,1785)^\star$, $(51,66300)^\star$, $(53,7480)^\star$, $(55,5440)^\star$, $(63,3570)$, $(85,174760)^\star$, $(87,24480)^\star$, $(95,2380)^\star$, $(111,1020)^\star$, $(119,41905)^\star$, $(127,85)$

The quadratic case, Dembowski-Ostrom polynomials

Theorem

Let $F(x) = \sum_{0 \le i < j < n} c_{i,j} x^{2^i + 2^j}$ *be a quadratic polynomial.*

- *If* $\{x_1, x_2, x_3, x_4\} \in \mathcal{V}(F)$, *then* $\{\{x_1 + a, x_2 + a, x_3 + a, x_4 + a\} \mid a \in \mathbb{F}_{2^n}\} \subset \mathcal{V}(F)$ *for each* $a \in \mathbb{F}_{2^n}$. *Consequently,* 2^{n-2} *divides* $|\mathcal{V}(F)|$.
- *For each* $a \in \mathbb{F}_{2^n}$, *the subset* $\{a, x_1 + a, x_2 + a, x_1 + x_2 + a\} \in \mathcal{V}(F)$ *if and only if*

$$\sum_{0 \le i < j < n} c_{i,j} \left(x_1^{2^i} x_2^{2^j} + x_1^{2^j} x_2^{2^i} \right) = 0.$$

Corollary

$|\mathcal{V}(F)| \ge 2^{n-2}$ *if* F *is not APN.* *Is this sharp? Power DO (Gold) are far away from this bound.*

The BIG APN problem

Is there a permutation APN if n is even? For n odd: x^3, x^{-1}.

- No, if $n = 4$.
- Yes, if $n = 6$ [8]

[8] Browning, K. A.; Dillon, J. F.; McQuistan, M. T.; Wolfe, A. J. An APN permutation in dimension six. Finite fields: theory and applications, 33–42, Contemp. Math., **518**, Amer. Math. Soc., Providence, RI, 2010.

Partially APN permutations[9]

Definition

Functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that for all $a \neq 0$

$$F(x+a) + F(x) \neq F(a) + F(0)$$

for all $x \neq 0, a$ are partially APN.

Alternatively: $F(x) + F(x+a) + F(a) + F(0) \neq 0$ or (if $F(0) = 0$)

$F(x)+F(y)+F(z) \neq 0$ for all distinct $x, y, z \neq 0$ with $x + y + z = 0$.

- There are many more partially APN than APN.
- They found many partially APN permutations, but no infinite family.

[9] Budaghyan, Lilya; Kaleyski, Nikolay S.; Kwon, Soonhak; Riera, Constanza; Stănică, Pantelimon. *Partially APN Boolean functions and classes of functions that are not APN infinitely often.* Cryptogr. Commun. **12** (2020), no. 3, 527–545.

Steiner systems

STEINER triple systems:

- v points
- blocks of size 3
- Any two different points are contained in exactly one block.

Classical example on $\mathbb{F}_2^n \setminus \{0\}$: points and 2-dimensional subspaces.

STEINER quadruple systems:

- v points
- blocks of size 4
- Any three different points are contained in exactly one block.

Classical example on $\mathbb{F}_2^n$: points and 2-dimensional affine subspaces.

Partially APN permutations

Theorem (P.)

For any $n \geq 3$ there are partially APN permutations on $\mathbb{F}_2^n$.

Proof:

- The blocks $\{x, y, z \,:\, x, y, z \text{ different}\}$ form the classical STEINER triple system on $\mathbb{F}_2^n \setminus \{0\}$ (any two different points are contained in exactly one triple).
- TEIRLINCK[10] proved that **any** two STEINER triple systems $\mathcal{S}$ and $\mathcal{T}$ defined on a point set V have a disjoint realization.
- That means, there is an isomorphic copy $\mathcal{T}'$ of $\mathcal{T}$ on V such that no triple occurs both in $\mathcal{S}$ and $\mathcal{T}'$.
- If we begin with the classical STEINER triple systems $\mathcal{T} = \mathcal{S}$, then $\mathcal{T}'$ provides us with the desired permutation.

[10] Teirlinck, Luc. On making two Steiner triple systems disjoint. J. Combinatorial Theory Ser. A **23** (1977), no. 3, 349–350.

TEIRLINCK's result

- has a short (1 page) and elementary but non-trivial proof;
- is needed only for the classical STEINER triple system;
- is not constructive;
- is far away from using finite fields!

APN permutations and STEINER quadruple systems

If F is APN on $\mathbb{F}_2^n$, then $F(x) + F(y) + F(z) + F(u) \neq 0$ if $\{x, y, z, u\}$ is an affine subspace of $\mathbb{F}_2^n$.

Observation:

There is an APN permutation F iff there are two disjoint realizations of the classical Steiner quadruple system on $\mathbb{F}_2^n$.

APN permutations and quadruple systems

- We tried to generalize the result to quadruple systems, without success.
- Hope that a non algebraic approach solves the BIG APN problem?
- APN for arbitrary quadruple systems (vanishing quadruples).