Universität Rostock Traditio et Innovatio

Image sets and the univariate representation of APN maps

Gohar M. Kyureghyan

University of Rostock, Germany

Coding Theory and Cryptography:
A Conference in Honor of Joachim Rosenthal's 60th Birthday

July 11, 2022

APN maps

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $a \neq 0, b \in \mathbb{F}_{2^n}$ be fixed. Then the equation

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

has always an even number of solutions, since x solves it if and only if $x + a$ does so.

A map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called almost perfect nonlinear (APN), if

$$\max_{a \neq 0, b \in \mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} : f(x + a) + f(x) = b\}| = 2.$$

APN maps

Equivalent definitions are:

(1) A map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if the map $x \mapsto f(x+a) + f(x)$ is 2-to-1 for any non-zero $a \in \mathbb{F}_{2^n}$.

(2) A map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if for any $x, y, u, v \in \mathbb{F}_{2^n}$ such that

$$x + y + u + v = 0$$

it holds

$$f(x) + f(y) + f(u) + f(v) \neq 0.$$

APN maps: existence of special families

All currently known APN families are (or can be constructed from) monomials $x \mapsto x^d$ or quadratic $x \mapsto \sum_{i,j} a_{ij} x^{2^i+2^j}$.

Probably, more general APN maps do exist. Currently, we have not the key ideas allowing to find them, both numerically and theoretically.

A lower bound for the image sets of APN maps

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN. Then

$$|Im(f)| \geq \begin{cases} \frac{2^n+1}{3} & n \text{ is odd,} \\ \frac{2^n+2}{3} & n \text{ is even.} \end{cases}$$

The first results on the image sets of APN maps were obtained in

I. Czerwinski, On the minimal value set size of APN functions, Cryptology ePrint Archive, Report 2020/705, June 2020.

The lower bound was published (in an equivalent form) already in

C. Carlet, A. Heuser and S. Picek, Trade-Offs for S-Boxes: Cryptographic Properties and Side-Channel Resilience, Proceedings of ACNS 2017, LNCS 10355, 393-414, 2017.

For $a \in \mathbb{F}$ let $\omega(a)$ denote the size of $f^{-1}(\{a\})$.

Theorem 6 *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN. Then*

$$|Im(f)| \geq \begin{cases} \frac{2^n+1}{3} & n \text{ is odd,} \\ \frac{2^n+2}{3} & n \text{ is even.} \end{cases}$$

If n is odd and

$$|Im(f)| = \frac{2^n+1}{3},$$

then $\omega(y_0) = 2$ for one element $y_0 \in Im(f)$ and $\omega(y) = 3$ for $y \in Im(f) \setminus \{y_0\}$.

If n is even and

$$|Im(f)| = \frac{2^n+2}{3},$$

then one of the following cases must occur:

1. *$\omega(y_0) = 1$ for one element $y_0 \in Im(f)$ and $\omega(y) = 3$ for all $y \in Im(f) \setminus \{y_0\}$, that is f is almost-3-to-1.*
2. *$\omega(y_i) = 2$ for two elements $y_0, y_1 \in Im(f)$ and $\omega(y) = 3$ for all $y \in Im(f) \setminus \{y_0, y_1\}$.*
3. *$\omega(y_i) = 2$ for three elements $y_0, y_1, y_2 \in Im(f)$, $\omega(y_3) = 4$ for a unique $y_3 \in Im(f) \setminus \{y_0, y_1, y_2\}$ and $\omega(y) = 3$ for all $y \in Im(f) \setminus \{y_0, \ldots, y_3\}$.*

L.Kölsch, B.Kriepke and G.Kyureghyan, Image sets of perfectly nonlinear maps, arXiv, December 2020.

APN maps with the minimal image sizes

For n even, an astonishing amount of the known APN families are almost-3-to-1.

- Monomials, the first non-monomial examples $x^3 + ux^{36}$ on $\mathbb{F}_{2^{10}}$, the first switching $x^3 + tr(x^9)$. More generally all 3-divisible APN maps $h(x^3)$.
- but also Zhou-Pott, Göloglu, Göloglu-Kölsch bivariate APN families, which are huge.

Ch. Kaspers and Yue Zhou, A lower bound on the number of inequivalent APN functions, arXiv 2020.

F.Göloglu and L. Kölsch, Equivalences of biprojective almost perfect nonlinear functions, arXiv 2021.

APN maps with the minimal image sizes

Theorem (Kölsch-Kriepke-K.)

Let n be even and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a component-wise plateaud APN map satisfying

- $f(0) = 0$,
- every $y \in Im(f) \setminus \{0\}$ has at least 3 preimages.

Then f is almost-3-to-1 and f has the classical Walsh spectrum.

This result describes an easy method for proving that the most of known APN maps have the classical Walsh spectrum.

The fact that almost-3-to-1 component-wise plateaud APN maps have the classical Walsh spectrum is mentioned in

`C.Carlet, Boolean and vectorial plateaued functions and APN functions, IEEE Transactions on Information Theory, 61(11), 2015.`

APN maps which are not almost 3-to-1

Among the extended Walsh spectra of the APN functions found for $n = 8$, there are three that do not correspond to any of the previously-known quadratic 8-bit APN functions. In particular, there are four pairwise CCZ-inequivalent APN functions in dimension 8 having linearity 2^7. One such example is the APN function

$$\begin{aligned} x \mapsto\ & x^3 + g^{60}x^5 + g^{191}x^6 + g^{198}x^9 + g^{232}x^{10} + g^{120}x^{12} + g^{54}x^{17} + g^{64}x^{18} + g^{159}x^{20} + \\ & g^{144}x^{24} + g^{248}x^{33} + g^{203}x^{34} + g^{32}x^{36} + g^{18}x^{40} + g^{216}x^{48} + g^{78}x^{65} + g^{46}x^{66} + g^{91}x^{68} + \\ & g^{27}x^{72} + g^{70}x^{80} + g^{52}x^{96} + g^{224}x^{129} + g^{18}x^{130} + g^{197}x^{136} + g^{253}x^{144} + x^{160} \end{aligned}$$

over $\mathbb{F}_{2^8}$, where $g \in \mathbb{F}_{2^8}^*$ is an element with minimal polynomial $X^8 + X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.

Ch. Beierle and G. Leander, New Instances of Quadratic APN Functions, arXiv 2020.

A generalization of Dobbertin's Result on Monomials

Dobbertin's Result: If n is even, then any APN monomial x^d of $\mathbb{F}_{2^n}$ is 3-divisible, that is d is divisible by 3.

Theorem (K.21) Let n be even and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN with $f(0) = 0$. Then the univariate representation of f satisfies

$$f(x) = x^2 h_2(x^3) + x h_1(x^3) + h(x^3),$$

with $h, h_1, h_2 \in \mathbb{F}_{2^n}[x]$ such that $h(x^3)$ has no zero in $\mathbb{F}_{2^n} \setminus \{0\}$. In particular, any APN map has non-zero 3-divisible terms in its univariate representation.

Proof: Let

$$f(x) = x^2 h_2(x^3) + x h_1(x^3) + h(x^3),$$

and $y \in \mathbb{F}_{2^n} \setminus \{0\}$ satisfy $h(y^3) = 0$. Let $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and hence $1 + \omega + \omega^2 = 0$. Then

$$0 + y + y\omega + y\omega^2 = 0,$$

and consequently

$$f(0) + f(y) + f(\omega y) + f(\omega^2 y) =$$
$$y^2(1 + \omega^2 + \omega)h_2(y^3) + y(1 + \omega + \omega^2)h_1(y^3) = 0$$

implying that f is not APN.

Coding theory and cryptography

A conference in honor of Joachim Rosenthal's 60th birthday

July 11 - 15, 2022 | University of Zurich

Herzliche Glückwünsche und

eine schöne Woche mit Kollegen