Almost perfect nonlinear functions

Alexander Pott

Otto von Guericke University Magdeburg

Agenda

Definition of almost perfect nonlinear (APN) functions, including crypto motivation.

1.) BIG open problem: APN permutations if n is even.
    - Problem solved for partially APN.
    - Designs?
2.) Apparently there are many APN functions. Find nice constructions of some of them and show inequivalence.
3.) Find non-quadratic APNs: not much progress after 2006.

Cryptography

Try to find functions f_K depending on a **key** K

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

such that there is confusion and diffusion SHANNON (1949):

- **Confusion**: Changing the input has inpredictable effect on the output.
- **Diffusion**: Changing few entries in the input changes many entries in the output.

Because of confusion, linear functions are **out**.

The core of many cryptographic systems

Many cryptographic schemes use, as a main ingredient, S-boxes (S: substitution):

$$S : \mathbb{F}_2^n \to \mathbb{F}_2^m.$$

Then

$$f_K : \mathbb{F}_2^n \to \mathbb{F}_2^m, \qquad x \mapsto S(x + K).$$

Function S should be highly nonlinear to provide confusion.

Nice to have: S is a permutation and n is even.

Problem

How can we measure nonlinearity?

Perfect nonlinearity

Since cryptographers are paranoid, they want to create functions which are perfect nonlinear:

Definition

Let p be a prime. A function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is perfect nonlinear, if

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

is a permutation for all $a \neq 0$.

The function $x \mapsto F(x+a) - F(x)$ is called the derivative of F,

The case $\mathbb{F}_2^n$

Cryptographers want $\mathbb{F}_2^n$. BUT: There is no perfect nonlinear function on $\mathbb{F}_2^n$:

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

for $y = x + a$.

Definition

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is almost perfect nonlinear (APN) if

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

is 2 to 1 for all $a \neq 0$.

In other words: $F(x+a)+F(x)=b$ has 0 or 2 solutions for $a \neq 0$.

A simple example

We identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$.

$$F(x) = x^3$$

defined on $\mathbb{F}_q$ with $q = 2^n$ even:

$$F(x+a) + F(x) = x^2a + a^2x + a^3 = b$$

has at most 2 solutions for all $a \neq 0$, hence APN.

This is a permutation if n is odd, but not if n is even.

The inverse function

Consider

$$F(x) = x^{-1}$$

defined on $\mathbb{F}_q$ with $q = 2^n$ even. It is a permutation.

It is APN if n is odd, but not if n is even.

This is the core substitution box for the Advanced Encryption Standard where n is even (and x^{-1} is only almost APN).

Code interpretation of APN functions

Let F be APN.

$$\begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix}_{x \in \mathbb{F}_2^n} \qquad \in \mathbb{F}_2^{(2n+1, 2^n)}$$

row space generates a code. The dual code has minimum weight 6:

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

for all **distinct** $z, x+z, y+z, x+y+z$.

Conversely: Any such code with minimum weight 6 defines APN function.

Equivalence of functions is code equivalence!

Monomial APNs x^d on $\mathbb{F}_{2^n}$

	d	Condition
Gold	$2^k + 1$	$\gcd(k, n) = 1$
Kasami	$2^{2k} - 2^k + 1$	$\gcd(k, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1,\ t$ even $2^t + 2^{\frac{3t+1}{2}} - 1,\ t$ odd	$n = 2t + 1$
inverse function	-1	$n = 2t + 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

If n is even, none of them are permutations.

Problem 1: The BIG APN problem

Find APN permutations on $\mathbb{F}_2^n$ with n even and $n > 6$.

Browning, Dillon, McQuistan, Wolfe (2010) found an APN permutation in $\mathbb{F}_{2^6}$. They started with the APN function on $\mathbb{F}_{2^6}$

$$x \mapsto x^3 + x^{10} + \alpha x^{24},$$

for some α and then applied code equivalence.

The race for more APN permutations is still going on!

Another Interesting APN

```
g(x) =


w^59*x^60 + w^34*x^58 + w^8*x^57 + w^23*x^56 + w^21*x^54 + w^39*x^53 + w^48*x^52
    + w^48*x^51 + w^56*x^50 + w^24*x^49 + w^44*x^48 + w^26*x^46 + w^2*x^45 +
    w^13*x^44 + w^54*x^43 + w^45*x^42 + w^32*x^41 + w^41*x^40 + w^48*x^39 +
    w^45*x^38 + w^32*x^37 + w^14*x^36 + w^57*x^35 + w^50*x^34 + x^33 + w^5*x^32
    + w^31*x^30 + w^45*x^29 + w^51*x^28 + w^32*x^27 + w^30*x^26 + w^8*x^25 +
    w^33*x^24 + w^39*x^23 + w^36*x^22 + w^4*x^21 + w^38*x^20 + w^52*x^19 +
    w^17*x^18 + w^15*x^17 + w^31*x^16 + w^42*x^15 + w^5*x^14 + w^25*x^13 +
    w^9*x^12 + w^3*x^11 + w*x^10 + w^30*x^9 + w^22*x^8 + w^23*x^7 + w^54*x^6 +
    w^46*x^5 + w^60*x^4 + w^29*x^3 + w^20*x^2 + w^61*x
```

A promising approach: Butterflies?

Let $n = 2m$ and $x, y \in \mathbb{F}_2^m$. Consider

$$\begin{pmatrix} 1 \\ x \\ y \\ R(x,y) \\ R(y,x) \end{pmatrix}_{x,y \in \mathbb{F}_2^m} \qquad \in \mathbb{F}_2^{(2n+1, 2^n)}$$

where $R : \mathbb{F}_2^{2m} \to \mathbb{F}_2^m$ such that $x \mapsto R(x, y_0)$ is a permutation for all y_0. Assume this is APN (**bivariate representation**).

Swapping

$$\begin{pmatrix} 1 \\ x \\ R(x,y) \\ y \\ R(y,x) \end{pmatrix}_{x,y\in\mathbb{F}_2^m} \qquad \in \mathbb{F}_2^{(2n+1,2^n)}$$

is an APN permutation (in code terminology). Browning, Dillon, McQuistan, Wolfe example used

$$R(x,y) = (x+\alpha y)^3 + x^3.$$

This very nice description is due to Perrin, Udovenko, Biryukov (2016). Impossible to generalize **this** function Canteaut, Perrin, Tian (2018).

Partially APN permutations

Budaghyan, Kaleyski, Kwon, Riera, Stanica (2019) studied 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 $x \neq 0, a$. They called these partially APN.

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

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

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

Steiner systems

STEINER quadruple systems:

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

HANANI 1960: Existence if and only if $v \equiv 2$ or 4 modulo 6.

STEINER triple systems:

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

KIRKMAN: Existence if and only if $v \equiv 1$ or 3 modulo 6.

The classical STEINER systems

- triple system on $\mathbb{F}_2^n \setminus \{0\}$: Points and 2-dimensional subspaces.
- quadruple system on $\mathbb{F}_2^n$: Points and 2-dimensional affine subspaces.

Partially APN permutations

Theorem (P. (2019))

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 (1977) 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.

Comments

- Teirlinck's result has a short (1 page) and elementary but non-trivial proof.
- Teirlinck's result is needed only for the classical Steiner triple system.
- Teirlinck's result is not constructive.
- This approach is far away from using finite fields!

Rodier Condition

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

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

for all subsets $\{x, y, z, u\}$ of order 4 with $x + y + z + u = 0$.

- Note that the subsets $\{x, y, z, u\}$ of order 4 with $x + y + z + u = 0$ form the classical Steiner quadruple system.

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 $\mathbb{F}_2^n$.

Interesting Observation:

There is an APN permutation F iff there is a collection of subsets D_i of size 4 on $\mathbb{F}_2^n$ forming the classical Steiner quadruple system of affine subspaces such that none of the D_i is an affine subspace of dimension 2.

The D_i are simply the sets

$$\big\{\{F(x), F(y), F(z), F(u)\} \;:\; x + y + z + u = 0\big\}.$$

APN permutations and quadruple systems

- We tried to generalize the TEIRLINCK result to quadruple systems, without success.
- APN for arbitrary quadruple systems?

Why finite fields?

- APN is an additive property. Why use multiplicative group for the construction?
- Using the mix of additive and multiplicative structure is a common approach in difference set theory. **Nice** multiplicative subsets are difference sets in the additive group, or vice versa.
    - Squares in $\mathbb{F}_q$ form a difference set in the additive group.
    - A hyperplane in $\mathbb{F}_p^n$ gives rise to a Singer cycle in the multiplicative group.
    - $\cdots$
- BUT: The APN permutation is **ugly**; it has no nice finite fields representation.

Why are there (perhaps) no APN permutations?

Try to build an APN function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ from **maximal nonlinear coordinate functions** $f : \mathbb{F}_2^n \to \mathbb{F}_2$, which are called bent functions:

- bent: $x \mapsto f(x + a) + f(x)$ is balanced.
- Bent functions itself are not balanced, so they cannot be used to construct APN permutations. Actually APN permutations have to avoid them.

All APNs x^d on $\mathbb{F}_{2^n}$ before 2006

	d	Condition
Gold	$2^k + 1$	$\gcd(k, n) = 1$
Kasami	$2^{2k} - 2^k + 1$	$\gcd(k, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1,\ t$ even $2^t + 2^{\frac{3t+1}{2}} - 1,\ t$ odd	$n = 2t + 1$
inverse function	-1	$n = 2t + 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

NSA/Magdeburg 2006

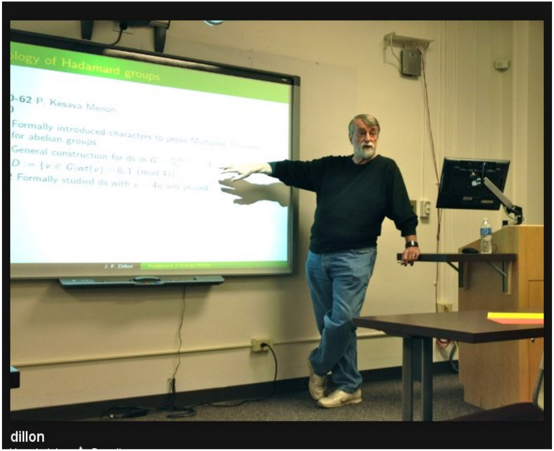
Edel, P., Kyureghyan; Bierbrauer; Dillon, McQuistan, Wolfe), found several new APNs:

Example

- $x \mapsto x^3 + x^{10} + \alpha x^{24}$ on $\mathbb{F}_{2^6}$
- more on $\mathbb{F}_{2^6}$
- $x \mapsto x^3 + \beta x^{2^5+2^2}$ on $\mathbb{F}_{2^{10}}$
- $x \mapsto x^3 + \gamma x^{2^9+2^4}$ on $\mathbb{F}_{2^{12}}$

α, β, γ must be chosen properly.

J.F. Dillon


logy of Hadamard groups
0-62 P. Kesava Menon
Formally introduced characters to prove Multiplier Theorem
for abelian groups
General construction for ds in G
D := {v ∈ G|wt(v) ≡ 0, 1 (mod 4)}
Formally studied ds with v = 4n and proved
J. F. Dillon

dillon

The race to find more examples

- In 2006 it was easy to check that new examples are really new!
- The first infinite family after 2006 was found by Budaghyan, Carlet, Leander (2008).
- The number of families is decreasing, thanks to Budaghyan, Calderini, Villa (2019): Some families coincide.
- It seems to become more and more difficult to find **provable** new APN functions.

Current status

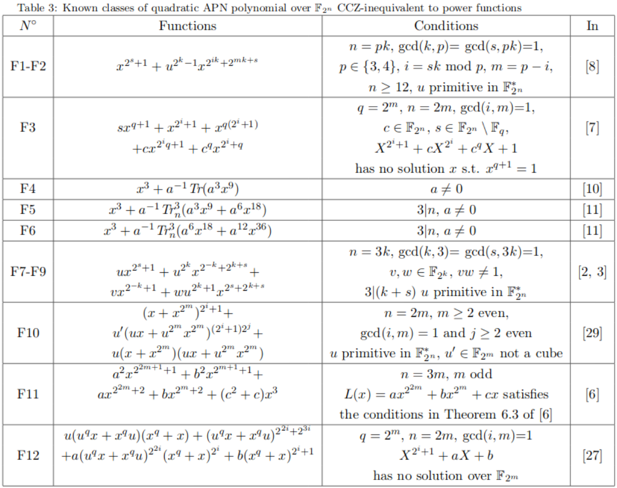


Table 3: Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

$N°$	Functions	Conditions	In
F1-F2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,p)=\gcd(s,pk)=1$, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p - i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[8]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)}$ $+cx^{2^iq+1} + c^q x^{2^i+q}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)=1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ has no solution x s.t. $x^{q+1} = 1$	[7]
F4	$x^3 + a^{-1}\,Tr(a^3x^9)$	$a \neq 0$	[10]
F5	$x^3 + a^{-1}\,Tr_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$	[11]
F6	$x^3 + a^{-1}\,Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$	[11]
F7-F9	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3\|(k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[2, 3]
F10	$(x + x^{2^m})^{2^i+1} +$ $u'(ux + u^{2^m}x^{2^m})^{(2^i+1)2^j} +$ $u(x + x^{2^m})(ux + u^{2^m}x^{2^m})$	$n = 2m$, $m \geq 2$ even, $\gcd(i,m) = 1$ and $j \geq 2$ even u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not a cube	[29]
F11	$a^2x^{2^{2m+1}+1} + b^2x^{2^{m+1}+1} +$ $ax^{2^{2m}+2} + bx^{2^m+2} + (c^2+c)x^3$	$n = 3m$, m odd $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ satisfies the conditions in Theorem 6.3 of [6]	[6]
F12	$u(u^qx + x^qu)(x^q + x) + (u^qx + x^qu)^{2^{2i}+2^{3i}}$ $+a(u^qx + x^qu)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)=1$ $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$	[27]

The Zhou-Kaspers theorem

- One family [F10] is due to Zhou, P. (2013). It is the APN version of a perfect nonlinear function in odd characteristic (two parameter family of semifields, projective planes).
- Now Zhou, Kaspers (2019) investigated inequivalence. Their result provides the best lower bound on the number of inequivalent APNs.

Many more sporadic examples are known

There are many sporadic examples, mostly found by local change techniques. With one exception, none of it has been turned into an infinite family Budaghyan, Carlet, Leander (2009):

$$x^3 + \mathrm{tr}(x^9)$$

is APN on $\mathbb{F}_{2^n}$: Change only one coordinate function.

Other local change approaches: Yu, Wang, Li (2013).

Problem 2

Find more powerful constructions (more parameters to play with) which give pairwise inequivalent examples.

In other words: Beat the ZHOU-KASPERS theorem.

Model: KANTOR's result on commutative semifields (2003).

quadratic vs. non-quadratic

F is called a Dembowski-Ostrom polynomial or quadratic if

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

is affine:

$$F(x) = \sum_{i,j} \alpha_{i,j} x^{p^i + p^j} + \sum_j \beta_j x^{p^j} + \gamma.$$

There are several non-quadratic APN monomials, for instance x^{-1}.

With only one exception, no new non-quadratic APN has been found since 2006, when the race begun.

Quadratic case: Easy proofs

If F is quadratic, then $x \mapsto F(x+a)+F(x)+F(a)+F(0)$ is linear.

We just need to determine the kernels to check the APN property (dimension must be 1).

One sporadic non-quadratic APN

Edel, P. 2009 found some u such that

$$x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) +$$
$$u^{14}(\mathrm{tr}(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) +$$
$$\mathrm{tr}_2^8((u^2x)^9) + \mathrm{tr}_2^4(x^{21}))$$

in $\mathbb{F}_{2^6}$ is APN, where

$$x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24})$$

is APN (local change).

Brinkmann, Leander

Problem 3

Find more non-quadratic APN functions.

Summary

- Definition of APN functions, including crypto motivation.
- BIG open problem: APN permutations if n is even.
  - Problem solved for partially APN.
  - Designs?
- Apparently there are many APN functions. Find nice constructions, perhaps without finite fields, and show inequivalence.
- Non-quadratic APNs: not much progress after 2006.