A lower bound on the total number of CCZ-inequivalent APN functions

Christian Kaspers

joint work with Yue “Joe” Zhou (Changsha)

Otto von Guericke University Magdeburg

Paderborn, November 9, 2019

Vectorial boolean functions

A vectorial boolean function is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. We are interested in functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

A function f on $\mathbb{F}_2^4$ represented by its graph:

$\mathbf{x}$	0000	1000	0100	1100	0010	1010	0110	1110
$f(\mathbf{x})$	0000	0100	0100	0100	1000	1110	1101	1111

$\mathbf{x}$	0001	1001	0101	1101	0011	1011	0111	1111
$f(\mathbf{x})$	1000	1101	1111	1110	1000	1111	1110	1101

Representations of vectorial boolean functions

The same function f in

- coordinate function representation:

$$f\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}x_3x_4+x_3+x_4\\x_1x_2+x_1+x_2\\x_1x_3+x_2x_4\\x_1x_4+x_2x_3+x_2x_4\end{pmatrix}$$

  - algebraic degree of f: largest degree of all the coordinate functions
  - f has algebraic degree 2. The function is quadratic.

Representations of vectorial boolean functions

The same function f in

- coordinate function representation:

$$f\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}x_3x_4+x_3+x_4\\x_1x_2+x_1+x_2\\x_1x_3+x_2x_4\\x_1x_4+x_2x_3+x_2x_4\end{pmatrix}$$

  - algebraic degree of f: largest degree of all the coordinate functions
  - f has algebraic degree 2. The function is quadratic.

- univariate representation on $\mathbb{F}_{2^4}$, where u is primitive in $\mathbb{F}_{2^4}$:

$$f(x)=ux^{12}+u^{14}x^9+u^8x^8+u^9x^6+u^5x^5+u^{10}x^3+u^8x^2+ux$$

Representations of vectorial boolean functions

The same function f in

- coordinate function representation:

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_3x_4 + x_3 + x_4 \\ x_1x_2 + x_1 + x_2 \\ x_1x_3 + x_2x_4 \\ x_1x_4 + x_2x_3 + x_2x_4 \end{pmatrix}$$

  - algebraic degree of f: largest degree of all the coordinate functions
  - f has algebraic degree 2. The function is quadratic.

- univariate representation on $\mathbb{F}_{2^4}$, where u is primitive in $\mathbb{F}_{2^4}$:

$$f(x) = ux^{12} + u^{14}x^9 + u^8x^8 + u^9x^6 + u^5x^5 + u^{10}x^3 + u^8x^2 + ux$$

- bivariate representation on $\mathbb{F}_{2^2} \times \mathbb{F}_{2^2}$, where u' is primitive in $\mathbb{F}_{2^2}$:

$$f(x,y) = \left(x^3 + u'y^3,\ xy\right)$$

Almost perfect nonlinear (APN) functions

Definition

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

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

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

Why are people interested in APN functions?

- Cryptography: APN functions offer the best resistance possible to the differential attack
- Applications in coding theory, projective geometry, semifield theory

For more background, see the survey by Pott (2016).

(Open) problems regarding APN functions

1. Find another APN permutation on $\mathbb{F}_{2^n}$, where n is even.
   - So far, only one is known: for $n = 6$ (Dillon 2009).

2. Establish a lower bound on the number of inequivalent APN functions.
   - Several infinite families are known, however it is often not clear if APN functions
     - within one class or
     - from different classes

     are mutually inequivalent.

3. Find more non-quadratic APN functions.
   - No progress since 2006.

(Open) problems regarding APN functions

2. Establish a lower bound on the number of inequivalent APN functions.
   - Several infinite families are known, however it is often not clear if APN functions
     - within one class or
     - from different classes

     are mutually inequivalent.

Notions of equivalence of APN functions

Two functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called

- CCZ-equivalent if there exists an affine permutation C on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ that maps the graph of f onto the graph of g,

- EA-equivalent if there exist affine functions $A_1, A_2, A_3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, where A_1 and A_2 are permutations, such that

$$f(A_1(x)) = A_2(g(x)) + A_3(x).$$

Notions of equivalence of APN functions

Two functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called

- CCZ-equivalent if there exists an affine permutation C on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ that maps the graph of f onto the graph of g,
- EA-equivalent if there exist affine functions $A_1, A_2, A_3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, where A_1 and A_2 are permutations, such that

$$f(A_1(x)) = A_2(g(x)) + A_3(x).$$

in general: EA-equivalence $\implies$ CCZ-equivalence. However:

Theorem (Yoshiara 2012)

For two quadratic APN functions f and g:

$$\text{EA-equivalence} \iff \text{CCZ-equivalence.}$$

Known classes of APN power functions $x \mapsto x^d$ on $\mathbb{F}_{2^n}$

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

- The equivalence problem is well-studied: in general, the APN power functions are inequivalent.

Known classes of APN non-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	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}$ $+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ 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	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$	$3\vert n$, $a\neq 0$	[11]
F6	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$	$3\vert n$, $a\neq 0$	[11]
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v,w\in\mathbb{F}_{2^k}$, $vw\neq 1$, $3\vert(k+s)$ 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]

Table by Budaghyan, Calderini, and Villa (2019)

- It is not much known about the equivalence problem.

Known classes of APN non-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]

Table by Budaghyan, Calderini, and Villa (2019)

- It is not much known about the equivalence problem.

Pott-Zhou APN functions

Theorem (Zhou and Pott 2013)

Let m be even and let k, s be integers, $0 < k < m$ and $0 \leq s \leq m$, such that $\gcd(k, m) = 1$. *Let* $\alpha \in \mathbb{F}_{2^m}^*$.

The function $f_{k,s,\alpha} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ *defined as*

$$f_{k,s,\alpha}(x, y) = \left(x^{2^k+1} + \alpha y^{(2^k+1)2^s},\ xy\right)$$

is APN if s is even and α is a non-cube.

Pott-Zhou APN functions

Theorem (Zhou and Pott 2013 and Anbar, Kalaycı, and Meidl 2019)

Let m be even and let k, s be integers, $0 < k < m$ and $0 \leq s \leq m$, such that $\gcd(k, m) = 1$. Let $\alpha \in \mathbb{F}_{2^m}^*$.

The function $f_{k,s,\alpha} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ defined as

$$f_{k,s,\alpha}(x, y) = \left(x^{2^k+1} + \alpha y^{(2^k+1)2^s},\ xy\right)$$

is APN if and only if s is even and α is a non-cube.

Pott-Zhou APN functions

Theorem (Zhou and Pott 2013 and Anbar, Kalaycı, and Meidl 2019)

Let m be even and let k, s be integers, $0 < k < m$ and $0 \leq s \leq m$, such that $\gcd(k, m) = 1$. Let $\alpha \in \mathbb{F}_{2^m}^*$.

The function $f_{k,s,\alpha} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ defined as

$$f_{k,s,\alpha}(x, y) = \left(x^{2^k+1} + \alpha y^{(2^k+1)2^s},\ xy\right)$$

is APN if and only if s is even and α is a non-cube.

- f from the beginning is the Pott-Zhou APN function $f_{1,0,u'}$ on $\mathbb{F}_{2^4}$:

$$f_{1,0,u'}(x, y) = (x^{2^1+1} + u' y^{(2^1+1)2^0}, xy)$$

- Pott-Zhou functions have two relevant parameters: k and s.
- Pott-Zhou functions are quadratic.

Our goal

Show that there exist many CCZ-inequivalent APN functions on $\mathbb{F}_{2^{2m}}$ by studying for which parameters k, s, α and ℓ, t, β the functions $f_{k,s,\alpha}$ and $f_{\ell,t,\beta}$, where

$$f_{k,s,\alpha}(x,y) = \left(x^{2^k+1} + \alpha y^{(2^k+1)2^s},\ xy\right)$$

and

$$f_{\ell,t,\beta}(x,y) = \left(x^{2^\ell+1} + \beta y^{(2^\ell+1)2^t},\ xy\right),$$

are CCZ-equivalent.

Our goal

Show that there exist many CCZ-inequivalent APN functions on $\mathbb{F}_{2^{2m}}$ by studying for which parameters k, s, α and ℓ, t, β the functions $f_{k,s,\alpha}$ and $f_{\ell,t,\beta}$, where

$$f_{k,s,\alpha}(x, y) = \left(x^{2^k+1} + \alpha y^{(2^k+1)2^s},\ xy\right)$$

and

$$f_{\ell,t,\beta}(x, y) = \left(x^{2^\ell+1} + \beta y^{(2^\ell+1)2^t},\ xy\right),$$

are CCZ-equivalent.

Computational results about the number of inequivalent Pott-Zhou APNs:

m	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
#	1	2	?	?	?	?	?	?	?	?	?	?	?	?	?	?

A first step: some trivial equivalences

Lemma (Zhou and K. (20xx))

Let m be an even integer. Let k, ℓ be integers coprime to m such that $0 < k, \ell < m$, and let s, t be even integers, $0 \leq s, t \leq m$. Let α, β be non-cubes in $\mathbb{F}_{2^m}^*$.

The two Pott-Zhou APN functions $f_{k,s,\alpha}, f_{\ell,t,\beta} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ are CCZ-equivalent

1. *if $k = \ell$ and $s = t$, no matter which non-cubes α and β we choose,*
2. *if $k \equiv \pm\ell \pmod{m}$ and $s \equiv \pm t \pmod{m}$.*

- Since the choice of α does not matter, we write $f_{k,s}$ instead of $f_{k,s,\alpha}$.
- From now on we only consider $k, s \leq \frac{m}{2}$.

Our main theorem: the not so trivial part

Theorem (Zhou and K. (20xx))

Let $m \geq 4$ *be an even integer. Let* k, ℓ *be integers coprime to* m *such that* $0 < k, \ell < \frac{m}{2}$*, and let* s, t *be even integers,* $0 \leq s, t \leq \frac{m}{2}$*.*

The Pott-Zhou APN functions $f_{k,s}, f_{\ell,t} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ *are CCZ-equivalent if and only if* $k = \ell$ *and* $s = t$*.*

Our main theorem: the not so trivial part

Theorem (Zhou and K. (20xx))

Let $m \geq 4$ be an even integer. Let k, ℓ be integers coprime to m such that $0 < k, \ell < \frac{m}{2}$, and let s, t be even integers, $0 \leq s, t \leq \frac{m}{2}$.

The Pott-Zhou APN functions $f_{k,s}, f_{\ell,t} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ are CCZ-equivalent if and only if $k = \ell$ and $s = t$.

- If $m = 2$, up to equivalence, there exists only one function: $f_{1,0}$. It is actually EA-equivalent to the Gold APN function $x \mapsto x^3$.
- Since $f_{k,s}$ is quadratic, it is sufficient to show EA-equivalence.

Sketch of the proof

$f_{k,s}$ and $f_{\ell,t}$ are EA-equivalent if there exist linearized polynomials $L_A(X,Y), L_B(X,Y), M_A(X,Y), M_B(X,Y) \in \mathbb{F}_{2^m}[X,Y]$ and $N_1(X), \ldots, N_4(X) \in \mathbb{F}_{2^m}[X]$ such that

$$\begin{aligned} L_A(x,y)^{2^k+1} + \alpha L_B(x,y)^{(2^k+1)2^s} &= N_1(x^{2^\ell+1} + \alpha y^{(2^\ell+1)2^t}) + N_3(xy) + M_A(x,y), \\ L_A(x,y) L_B(x,y) &= N_2(x^{2^\ell+1} + \alpha y^{(2^\ell+1)2^t}) + N_4(xy) + M_B(x,y) \end{aligned}$$

holds for all $x, y \in \mathbb{F}_{2^m}$.

We show that there only exist such polynomials if $k = \ell$ and $s = t$. Moreover, we show that in this case, L_A and L_B are linearized monomials of the same degree.

1. Show that the equivalence mappings between Gold APN functions are linearized monomials.
2. Show that $f_{k,s}$ and $f_{\ell,t}$ can only be equivalent if $k = \ell$.
3. Show that $f_{k,s}$ and $f_{k,t}$ are equivalent if $s = t$.

Lower bound on the number of inequivalent APN functions

Corollary (Zhou and K. (20xx))

On $\mathbb{F}_{2^{2m}}$, where $m \geq 4$ is even, the number of CCZ-inequivalent Pott-Zhou APN functions is

$$\left(\left\lfloor \frac{m}{4} \right\rfloor + 1\right) \frac{\varphi(m)}{2},$$

where φ denotes Euler's phi function.

Lower bound on the number of inequivalent APN functions

Corollary (Zhou and K. (20xx))

On $\mathbb{F}_{2^{2m}}$, where $m \geq 4$ is even, the number of CCZ-inequivalent Pott-Zhou APN functions is

$$\left(\left\lfloor \frac{m}{4} \right\rfloor + 1\right) \frac{\varphi(m)}{2},$$

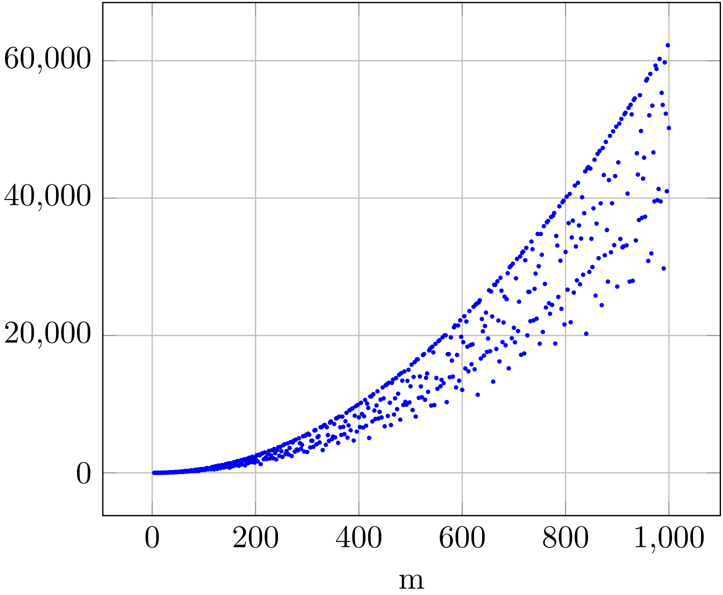
where φ denotes Euler's phi function.

- We have $\left(\left\lfloor \frac{m}{4} \right\rfloor + 1\right)$ choices for s and $\frac{\varphi(m)}{2}$ choices for k.
- Number of functions for small m:

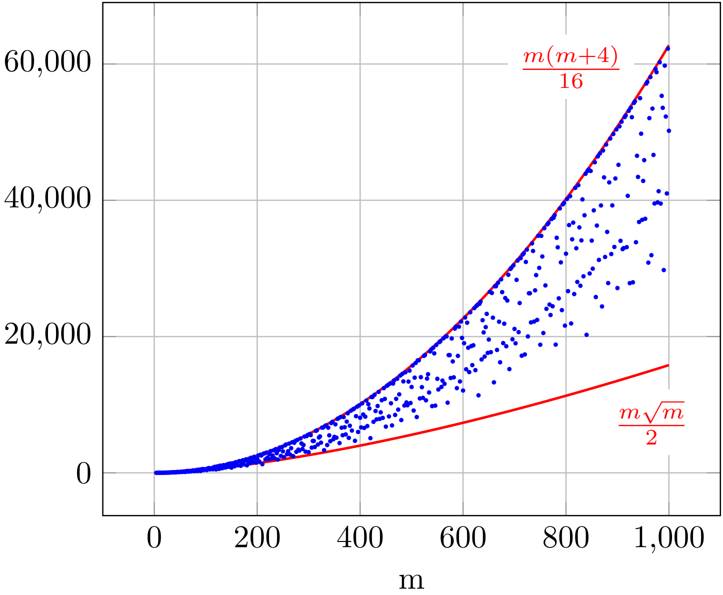
m	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
#	1	2	2	6	6	8	12	20	15	24	30	28	42	48	32	72

(red cases can be checked computationally by computing the Γ-rank)

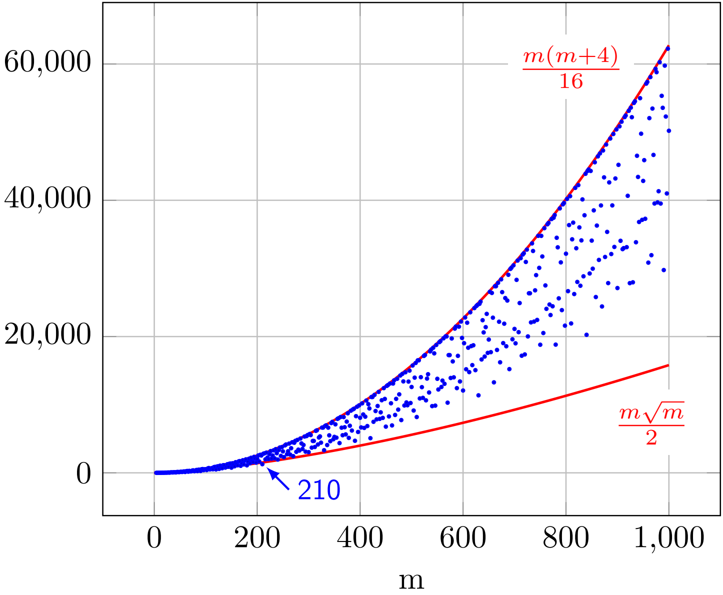
Number of Pott-Zhou APN functions in $\mathbb{F}_{2^{2m}}$, m even



Number of Pott-Zhou APN functions in $\mathbb{F}_{2^{2m}}$, m even



Number of Pott-Zhou APN functions in $\mathbb{F}_{2^{2m}}$, m even



Automorphism group of the Pott-Zhou APN functions

Corollary (Zhou and K. (20xx))

Let $f_{k,s}$ be a Pott-Zhou APN function on $\mathbb{F}_{2^{2m}}$. If $m \geq 4$, then

$$|\mathrm{Aut}(f_{k,s})| = \begin{cases} 3m2^{2m}(2^m - 1) & \text{if } s \in \{0, \frac{m}{2}\}, \\ 3m2^{2m-1}(2^m - 1) & \text{otherwise.} \end{cases}$$

- If $m = 2$, then
$$|\mathrm{Aut}(f_{1,0})| = |\mathrm{Aut}(x^3)| = 5760$$
which was first shown by Berger and Charpin (1996).
- Count the possible equivalence mappings of $f_{k,s}$.

Outlook

We have established a first lower bound on the total number of CCZ-inequivalent APN functions on $\mathbb{F}_{2^{2m}}$, where m is even. However, there is still work to be done:

- Improve this lower bound.
- Establish a lower bound for functions on $\mathbb{F}_{2^n}$ where $n \nmid 4$.
- Clean up the known constructions.
- And, of course, find another APN permutation on $\mathbb{F}_{2^n}$ where n is even.

References I

N. Anbar, T. Kalaycı, and W. Meidl. Determining the Walsh spectra of Taniguchi's and related APN-functions. In: Finite Fields and Their Applications 60 (2019), p. 101577. URL: http://www.sciencedirect.com/science/article/pii/S1071579719300802.

T. P. Berger and P. Charpin. The permutation group of affine-invariant extended cyclic codes. In: IEEE Trans. Inform. Theory 42.6, part 2 (1996), pp. 2194–2209. URL: https://doi.org/10.1109/18.556607.

L. Budaghyan, M. Calderini, and I. Villa. On equivalence between known families of quadratic APN functions. Cryptology ePrint Archive, Report 2019/793. 2019. URL: https://eprint.iacr.org/2019/793.

References II

A. Pott. Almost Perfect and Planar Functions. In: Des. Codes Cryptography 78.1 (2016), pp. 141–195. URL: http://dx.doi.org/10.1007/s10623-015-0151-x.

S. Yoshiara. Equivalences of quadratic APN functions. In: Journal of Algebraic Combinatorics 35.3 (2012), pp. 461–475. URL: https://doi.org/10.1007/s10801-011-0309-1.

Y. Zhou and A. Pott. A new family of semifields with 2 parameters. In: Advances in Mathematics 234 (2013), pp. 43–60. URL: http://www.sciencedirect.com/science/article/pii/S0001870812004057.