On APN and AB Power Functions

Lilya Budaghyan

Selmer Center in Secure Communication
University of Bergen
Norway

ALCOCRYPT 2023
Marseille, February 23

Outline

1. Optimal cryptographic functions
   - Introduction
   - Preliminaries
   - APN and AB functions
2. Equivalence relations of cryptographic functions
   - EAI-equivalence and known APN and AB monomials
   - CCZ-equivalence and its applications
3. Constructions and properties of APN functions
   - Classes of APN polynomials CCZ-inequivalent to monomials
   - Properties of APN monomials
   - Dobbertin conjecture on APN monomials

Vectorial Boolean functions

For n and m positive integers
Boolean functions: $F : \mathbb{F}_2^n \to \mathbb{F}_2$
Vectorial Boolean (n, m)-functions: $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

Modern applications of Boolean functions:

- reliability theory, multicriteria analysis, mathematical biology, image processing, theoretical physics, statistics;
- voting games, artificial intelligence, management science, digital electronics, propositional logic;
- algebra, coding theory, combinatorics, sequence design, cryptography.

Cryptographic properties of functions

Functions used in block ciphers, S-boxes, should possess certain properties to ensure resistance of the ciphers to cryptographic attacks.

Main cryptographic attacks on block ciphers and corresponding properties of S-boxes:

- Linear attack – Nonlinearity
- Differential attack – Differential uniformity
- Algebraic attack – Existence of low degree multivariate equations
- Higher order differential attack – Algebraic degree
- Interpolation attack – Univariate polynomial degree

Optimal cryptographic functions

Optimal cryptographic functions

- are vectorial Boolean functions optimal for primary cryptographic criteria (APN and AB functions);
- are UNIVERSAL - they define optimal objects in several branches of mathematics and information theory (coding theory, sequence design, projective geometry, combinatorics, commutative algebra);
- are "HARD-TO-GET" - there are only a few known constructions (12 AB, 19 APN);
- are "HARD-TO-PREDICT" - most conjectures are proven to be false.

Outline

Univariate representation and algebraic degree of functions

The univariate representation of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ for $m|n$:

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$

The binary expansion of $0 \leq k < 2^n$:

$$k = \sum_{s=0}^{n-1} 2^s k_s,$$

where k_s, $0 \leq k_s \leq 1$. Then binary weight of k:

$$w_2(k) = \sum_{s=0}^{n-1} k_s.$$

Algebraic degree of F:

$$d^\circ(F) = \max_{0 \leq i < 2^n, c_i \neq 0} w_2(i).$$

Special functions

- F is linear if

$$F(x) = \sum_{i=0}^{n-1} b_i x^{2^i}.$$

- F is affine if it is a linear function plus a constant.
- F is quadratic if for some affine A

$$F(x) = \sum_{i,j=0}^{n-1} b_{ij} x^{2^i+2^j} + A(x).$$

- F is power function or monomial if $F(x) = x^d$.
- The inverse F^{-1} of a permutation F is s.t. $F^{-1}(F(x)) = F(F^{-1}(x)) = x$.

Trace and component functions

Trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ for $m|n$:

$$\mathrm{tr}_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}.$$

Absolute trace function:

$$\mathrm{tr}_n(x) = \mathrm{tr}_n^1(x) = \sum_{i=0}^{n-1} x^{2^i}.$$

For $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $v \in \mathbb{F}_{2^n}^*$

$$\mathrm{tr}_n(vF(x))$$

is a component function of F.

Outline

1. Optimal cryptographic functions
   - Introduction
   - Preliminaries
   - APN and AB functions
2. Equivalence relations of cryptographic functions
   - EAI-equivalence and known APN and AB monomials
   - CCZ-equivalence and its applications
3. Constructions and properties of APN functions
   - Classes of APN polynomials CCZ-inequivalent to monomials
   - Properties of APN monomials
   - Dobbertin conjecture on APN monomials

Differential uniformity and APN functions

- Differential cryptanalysis of block ciphers was introduced by Biham and Shamir in 1991.
- $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is differentially δ-uniform if

$$F(x+a) + F(x) = b, \qquad \forall a \in \mathbb{F}_{2^n}^*, \quad \forall b \in \mathbb{F}_{2^n},$$

  has at most δ solutions.
- Differential uniformity measures the resistance to differential attack [Nyberg 1993].
- F is almost perfect nonlinear (APN) if $\delta = 2$.
- APN functions are optimal for differential cryptanalysis.

First examples of APN functions [Nyberg 1993]:

- Gold function x^{2^i+1} on $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$;
- Inverse function x^{2^n-2} on $\mathbb{F}_{2^n}$ with n odd.

Quadratic and Power APN Functions

- $F(x) = x^d$ on $\mathbb{F}_{2^n}$, then F is APN iff $D_1F(x) = F(x+1) + F(x)$ is a two-to-one mapping. Indeed, for any $a \neq 0$

$$F(x+a) + F(x) = (x+a)^d + x^d = a^d D_1 F(x/a).$$

- If F is quadratic then F is APN iff $F(x+a) + F(x) = F(a)$ has 2 solutions for any $a \neq 0$.

Nonlinearity of functions

- Linear cryptanalysis was discovered by Matsui in 1993.
- Distance between two Boolean functions:

$$d(f,g) = |\{x \in \mathbb{F}_{2^n} : f(x) \neq g(x)\}|.$$

- Nonlinearity of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$:

$$N_F = \min_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_2, v \in \mathbb{F}_{2^n}^*} d(\mathrm{tr}_n(v\, F(x)), \mathrm{tr}_n(ax) + b)$$

- Nonlinearity measures the resistance to linear attack [Chabaud and Vaudenay 1994].

Walsh transform of an (n,n)-function F

$$\lambda_F(u,v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_n(v\ F(x)) + \mathrm{tr}_n(ax)}, \qquad u \in \mathbb{F}_{2^n},\ v \in \mathbb{F}_{2^n}^*$$

- Walsh coefficients of F are the values of its Walsh transform.
- Walsh spectrum of F is the set of all Walsh coefficients of F.
- The extended Walsh spectrum of F is the set of absolute values of all Walsh coefficients of F.
- F is APN iff

$$\sum_{u,v \in \mathbb{F}_{2^n}, v \neq 0} \lambda_F^4(u,v) = 2^{3n+1}(2^n - 1).$$

Almost bent functions

The nonlinearity of F via Walsh transform:

$$N_F = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_{2^n}, v \in \mathbb{F}^*_{2^n}} |\lambda_F(u, v)| \leq 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Functions achieving this bound are called almost bent (AB).

- AB functions are optimal for linear cryptanalysis.
- F is AB iff $\lambda_F(u, v) \in \{0, \pm 2^{\frac{n+1}{2}}\}$.
- AB functions exist only for n odd.
- F is maximally nonlinear if n is even and $N_F = 2^{n-1} - 2^{\frac{n}{2}}$ (conjectured optimal).

Almost bent functions II

- If F is AB then it is APN.
- If n is odd and F is quadratic APN then F is AB.
- Algebraic degrees of AB functions are upper bounded by $\frac{n+1}{2}$ [Carlet, Charpin, Zinoviev 1998].

First example of AB functions:

- Gold functions x^{2^i+1} on $\mathbb{F}_{2^n}$ with $\gcd(i,n)=1$, *n odd*;
- Gold APN functions with n even are not AB;
- Inverse functions are not AB.

Almost Bent Power Functions

- In general, checking Walsh spectrum for power functions is sufficient for $a \in \mathbb{F}_2$ and $b \in \mathbb{F}_{2^n}^*$.
  - $F(x) = x^d$ is AB on $\mathbb{F}_{2^n}$ iff $\lambda_F(a, b) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for $a \in \mathbb{F}_2$, $b \in \mathbb{F}_{2^n}^*$, since $\lambda_F(a, b) = \lambda_F(1, a^{-d}b)$ for $a \in \mathbb{F}_{2^n}^*$.
- In case of power permutation, sufficient for $b = 1$ and all a.
  - If $F = x^d$ is a permutation, F is AB iff $\lambda_F(a, 1) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ for $a \in \mathbb{F}_{2^n}$, since $\lambda_F(a, b) = \lambda_F(ab^{-\frac{1}{d}}, 1)$.

Outline

Cyclotomic, EA- and EAI- equivalences

- F and F' are *extended affine equivalent* (EA-equivalent) if

$$F' = A_1 \circ F \circ A_2 + A$$

  for some affine permutations A_1 and A_2 and some affine A. If $A = 0$ then F and F' are called affine equivalent.

- F and F' are EAI-equivalent if F' is obtained from F by a sequence of applications of EA-equivalence and inverses of permutations.

- Functions x^d and $x^{d'}$ over $\mathbb{F}_{2^n}$ are cyclotomic equivalent if $d' = 2^i \cdot d \mod (2^n - 1)$ for some $0 \leq i < n$ or, $d' = 2^i / d \mod (2^n - 1)$ in case $\gcd(d, 2^n - 1) = 1$.

Invariants and Relation Between Equivalences

- Linear equivalence $\subset$ affine equivalence $\subset$ EA-equivalence $\subset$ EAI-equivalence.
- Cyclotomic equivalence $\subset$ EAI-equivalence.
- APNness, ABness are preserved by EAI-equivalence.
- Algebraic degree is preserved by EA-equivalence but not by EAI-equivalence.
- Permutation property is preserved by cyclotomic and affine equivalences (not by EA- or EAI-equivalences).

Known AB power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions on n odd
Gold (1968)	$2^i + 1$	$\gcd(i, n) = 1$, $1 \leq i < n/2$
Kasami (1971)	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$, $2 \leq i < n/2$
Welch (conj.1968)	$2^m + 3$	$n = 2m + 1$
Niho (conjectured in 1972)	$2^m + 2^{\frac{m}{2}} - 1$, m even $2^m + 2^{\frac{3m+1}{2}} - 1$, m odd	$n = 2m + 1$

Welch and Niho cases were proven by Canteaut, Charpin, Dobbertin (2000) and Hollmann, Xiang (2001), respectively.

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

Functions	Exponents d	Conditions
Gold	2^i+1	$\gcd(i,n)=1$, $1\leq i<n/2$
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$, $2\leq i<n/2$
Welch	2^m+3	$n=2m+1$
Niho	$2^m+2^{\frac{m}{2}}-1$, m even $2^m+2^{\frac{3m+1}{2}}-1$, m odd	$n=2m+1$
Inverse	$2^{n-1}-1$	$n=2m+1$
Dobbertin	$2^{4m}+2^{3m}+2^{2m}+2^m-1$	$n=5m$

- Power APN functions are permutations for n odd and 3-to-1 for n even [Dobbertin 1999].
- This list is up to cyclotomic equivalence and is conjectured complete [Dobbertin 1999].
- For n even the Inverse function is differentially 4-uniform and maximally nonlinear and is used as S-box in AES with $n=8$.

Open problems in the beginning of 2000

- All known APN functions were power functions up to EA-equivalence.
- Power APN functions are permutations for n odd and 3-to-1 for n even.

Open problems:

1. Existence of APN polynomials (EA-)inequivalent to power functions.
2. Existence of APN permutations over $\mathbb{F}_{2^n}$ for n even.

Outline

CCZ-equivalence

The *graph of a function* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the set

$$G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}.$$

F and F' are CCZ-equivalent if $\mathcal{L}(G_F) = G_{F'}$ for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ [Carlet, Charpin, Zinoviev 1998].

CCZ-equivalence

- preserves differential uniformity, nonlinearity and extended Walsh spectrum.
- is more general than EAI-equivalence [B., Carlet, Pott 2005].
- was used to disprove two conjectures of 1998:
  - On nonexistence of AB functions EA-inequivalent to any permutation [disproved by B., Carlet, Pott 2005];
  - On nonexistence of APN permutations for n even [disproved for $n = 6$ by Dillon et al. 2009].

First classes of APN and AB maps EAI-inequivalent to monomials

APN functions CCZ-equivalent to Gold functions and EAI-inequivalent to power functions on $\mathbb{F}_{2^n}$; they are AB for n odd [B., Carlet, Pott 2005].

Functions	Conditions
$x^{2^i+1} + (x^{2^i} + x + \mathrm{tr}_n(1) + 1)\mathrm{tr}_n(x^{2^i+1} + x\,\mathrm{tr}_n(1))$	$n \geq 4$ $\gcd(i,n) = 1$
$[x + \mathrm{tr}_n^3(x^{2(2^i+1)} + x^{4(2^i+1)}) + \mathrm{tr}_n(x)\mathrm{tr}_n^3(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1}$	$6 \mid n$ $\gcd(i,n) = 1$
$x^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + x^{2^i}\mathrm{tr}_n^m(x) + x\,\mathrm{tr}_n^m(x)^{2^i}$ $+[\mathrm{tr}_n^m(x)^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + \mathrm{tr}_n^m(x)]^{\frac{1}{2^i+1}}(x^{2^i} + \mathrm{tr}_n^m(x)^{2^i} + 1)$ $+[\mathrm{tr}_n^m(x)^{2^i+1} + \mathrm{tr}_n^m(x^{2^i+1}) + \mathrm{tr}_n^m(x)]^{\frac{2^i}{2^i+1}}(x + \mathrm{tr}_n^m(x))$	$m \neq n$ n odd $m \mid n$ $\gcd(i,n) = 1$

CCZ-construction of APN permutation for n even

Big APN problem: Do APN permutations exist for n even?

- No quadratic APN permutations for n even [Nyberg 1993].

The only known APN permutation for n even [Dillon et al 2009]:

- Applying CCZ-equivalence to quadratic APN on $\mathbb{F}_{2^n}$ with $n = 6$ and c primitive

$$F(x) = x^3 + x^{10} + cx^{24}$$

obtain a nonquadratic APN permutation

$$c^{25}x^{57}+c^{30}x^{56}+c^{32}x^{50}+c^{37}x^{49}+c^{23}x^{48}+c^{39}x^{43}+c^{44}x^{42}+c^{4}x^{41}+c^{18}x^{40}+c^{46}x^{36}+c^{51}x^{35}+c^{52}x^{34}+c^{18}x^{33}+c^{56}x^{32}+c^{53}x^{29}+c^{30}x^{28}+cx^{25}+c^{58}x^{24}+c^{60}x^{22}+c^{37}x^{21}+c^{51}x^{20}+cx^{18}+c^{2}x^{17}+c^{4}x^{15}+c^{44}x^{14}+c^{32}x^{13}+c^{18}x^{12}+cx^{11}+c^{9}x^{10}+c^{17}x^{8}+c^{51}x^{7}+c^{17}x^{6}+c^{18}x^{5}+x^{4}+c^{16}x^{3}+c^{13}x$$

Relation between equivalences for monomials and the problem of APN permutations

Two power functions are CCZ-equivalent iff they are cyclotomic equivalent [Dempwolff 2018].

Conjecture: For non-quadratic power APNs CCZ- and EAI-equivalences coincide [B., Calderini, Villa 2020].

- confirmed for $n \leq 9$ [B., Calderini, Villa 2020];
- confirmed for inverse functions [Koelsch 2021].

This problem can be reduced to studying permutations $L'(x^d) + L(x)$ for linear L, L'.

Related problems on APN permutations:

- Are there APN permutations of the form $x^d + L(x)$ where d is Kasami, Welch, Niho or Dobbertin exponent and $L(x) \neq 0$ linear.

Relation between equivalences for APN polynomials

- For quadratic APN functions CCZ-equivalence is more general than EAI-equivalence [B., Carlet, Pott, Leander 2005-2009].
- Two quadratic APN functions are CCZ-equivalent iff they are EA-equivalent [Yoshiara 2017].
- For non-power non-quadratic APN functions CCZ-equivalence is more general than EAI-equivalence [B., Calderini, Villa, 2020].

Outline

1. Optimal cryptographic functions
   - Introduction
   - Preliminaries
   - APN and AB functions
2. Equivalence relations of cryptographic functions
   - EAI-equivalence and known APN and AB monomials
   - CCZ-equivalence and its applications
3. Constructions and properties of APN functions
   - Classes of APN polynomials CCZ-inequivalent to monomials
   - Properties of APN monomials
   - Dobbertin conjecture on APN monomials

First APN and AB classes CCZ-ineq. to monomials

First example of APN polynomial [Edel, Pott, Kyureghyan 2005]:

$$F_{bin}(x) = x^3 + wx^{36}$$

over $\mathbb{F}_{2^{10}}$, where w has the order 3 or 93.

First infinite family of APN and AB [B., Carlet, Leander 2006-2008]:
Let s, k, p be positive integers such that $n = pk$, $p = 3, 4$, $\gcd(k, p) = \gcd(s, pk) = 1$ and α primitive in $\mathbb{F}_{2^n}^*$.

$$x^{2^s+1} + \alpha^{2^k-1} x^{2^{-k}+2^{k+s}}$$

is quadratic APN on $\mathbb{F}_{2^n}$. If n is odd then this function is an AB permutation.
This disproved the conjecture from 1998 on nonexistence of quadratic AB functions inequivalent to Gold functions.

Known APN families CCZ-ineq. to power functions

N°	Functions	Conditions
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}$, $i=sk \bmod p, m=p-i, n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$
C3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m, n=2m, gcd(i,m)=1, c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$
C4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$
C5	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\|n, a\neq 0$
C6	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n, a\neq 0$
C7-C9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}$, $vw\neq 1, 3\|(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$
C10	$(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m, m\geqslant 2$ even, $\gcd(k,m)=1$ and $i\geqslant 2$ even, u primitive in $\mathbb{F}_{2^n}^*, u'\in\mathbb{F}_{2^m}$ not a cube
C11	$L(x)^{2^i}x+L(x)x^{2^i}$	
C12	$ut(x)(x^q+x)+t(x)^{2^{2i}+2^{3i}}+at(x)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$n=2m, q=2^m, \gcd(m,i)=1, t(x)=u^qx+x^qu$, $X^{2^i+1}+aX+b$ has no solution over $\mathbb{F}_{2^m}$
C13	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n=2m=10, (a,b,c)=(\beta,1,0,0), i=3, k=2, \beta$ primitive in $\mathbb{F}_{2^2}$
		$n=2m, m$ odd, $3\nmid m, (a,b,c)=(\beta,\beta^2,1), \beta$ primitive in $\mathbb{F}_{2^2}$, $i\in\{m-2,m,2m-1,(m-2)^{-1} \mod n\}$

- All are quadratic. For *n* odd they are AB otherwise have optimal nonlinearity.
- In general, these families are pairwise CCZ-inequivalent [B., Calderini, Villa, 2020].

APN Polynomial CCZ-Inequivalent to Monomials and Quadratics

Only one known example of APN polynomial CCZ-inequivalent to quadratics and to power functions for n=6:

$$x^3 + c^{17}(x^{17} + x^{18} + x^{20} + x^{24}) +$$
$$c^{14}\left(\mathrm{tr}_6(c^{52}x^3 + c^6x^5 + c^{19}x^7 + c^{28}x^{11} + c^2x^{13}) +\right.$$
$$\left.\mathrm{tr}_3(c^{18}x^9) + x^{21} + x^{42}\right)$$

where c is some primitive element of $\mathbb{F}_{2^6}$ [Brinkmann, Leander; Edel, Pott 2008].

- No infinite families known.
- No AB examples known.

Complete Classification of APN Functions for $n \leq 5$

Brinkmann and Leander 2008:

CCZ-classification finished for:

- APN functions with $n \leq 5$ (there are only power functions).

EA-classification is finished for:

- APN functions with $n \leq 5$ (there are only power functions and the ones constructed by CCZ-equivalence in 2005).

Some Classifications of APN Functions for $6 \leq n \leq 8$

- CCZ-classification of quadratics for $n \leq 8$ by B., Kaleyski, Yu, Dillon, Edel, Kalgin, Idrisova, Pott, Berlier, Leander, Perrin et al 2006-2023:
  13 functions for $n = 6$ and 488 for $n = 7$ and more than 26500 for $n = 8$;
- EA-classification of known APN for $n = 6$ by Calderini 2019:
  - Gold has 3 EA-classes;
  - non-quadratic APN has 23 EA-classes;
  - Dillon permutation has 13 EA-classes, two of them containing permutations; 4 affine classes of permutations;
  - remaining 11 functions have 3,13,19,85,86 or 91 EA-classes.

Outline

Exceptional APN functions

A function F is exceptional APN if it is APN over $\mathbb{F}_{2^n}$ for infinitely many values of n.

Gold and Kasami functions are the only known exceptional APN functions.

It is conjectured by Aubry, McGuire and Rodier (2010) that there are no more exceptional APN functions.

- Proven for power functions [Jedlicka 2007; Hernando, McGuire 2010].
- More partial results confirming this conjecture Jedlika, Hernando, Aubry, McGuire, Rodier, Caullery, Delgado, Janwa, Herbaut, Issa et al (2009-2022).

Nonliniarity properties of known APN families

All known APN families, except inverse and Dobbertin functions, have Gold-like Walsh spectra:

- for n odd they are AB;
- for n even Walsh spectra are $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$.

Walsh spectra of Inverse function: all integers divisible by 4 in the interval $[-2^{n/2+1}+1, 2^{n/2+1}+1]$ [Lachaud, Wolfmann 1990].

Sporadic APN polynomials with Walsh spectra $\{0, \pm 2^{n/2}, \pm 2^{n/2+1}, \pm 2^m\}$ with $m = n/2+2$ or $m = n-1$:

- For $n = 6$ only one case [Dillon et al. 2006]
$$x^3 + a^{11}x^5 + a^{13}x^9 + x^{17} + a^{11}x^{33} + x^{48}.$$
- For $n = 8$ [Yu et al 2014; Beierle, Leander 2022]:
  - more than 500 functions with four different distributions ($\pm 2^{n/2+2}$ taken 16, 48, 32 and 64 times) with $m = n/2+2$;
  - there are cases with $m = n-1$.

Some Problems on Nonlinearity of APN functions

- Find a family of quadratic APN polynomials with non-Gold like nonliniarity.

- The only family of APN power functions with unknown Walsh spectrum is Dobbertin function.
  - All Walsh coefficients are divisible by 2^{2m} but not by 2^{2m+1} implying it is not AB [Canteut, Charpin, Dobbertin 2000].

Walsh Spectrum of Dobbertin Function

Conjecture on the Walsh spectrum of $F(x) = x^d$ with $d = 2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$ over $\mathbb{F}_{2^{5m}}$ [B., Calderini, Carlet, Davidova, Kaleyski 2022]:

- $\{0, 2^{2m}(2^m+1), \pm 2^{5k-2}, \pm s \cdot 2^{2m} \mid 1 \leq s \leq k \cdot (k+1), s \text{ odd}\}$ for $m = 2k-1, k \in \mathbb{N}$;
- $\{0, -2^{2m}(2^m+1), \pm 2^{5k}, \pm 2^{5k+1}, \pm s \cdot 2^{2m} \mid 1 \leq s \leq k \cdot (k+2), s \text{ odd}\}$ for $m = 2k, k \in \mathbb{N}$.

Moreover, $\lambda_F(u, v)$ takes the maximum absolute value $2^{2m}(2^m + 1)$ for $u = v = 1$.
Hence, $N_F = 2^{5m-1} - 2^{2m-1}(2^m + 1)$.

"Optimal" representations for known APN exponents

- Kasami exponent for n odd $2^{2i} - 2^i + 1 = \frac{2^{3i}+1}{2^i+1}$;
- Welch exponent $2^t + 3$, $n = 2t + 1$;
- Niho exponent over $\mathbb{F}_{2^n}$ with $n = 2t + 1$
  - If t is an even then $2^t + 2^{\frac{t}{2}} - 1$ is cyclotomic equivalent to $\frac{3}{2^{t+1}+2^{\frac{t}{2}}+1}$;
  - If t is an odd then $2^{\frac{3t+1}{2}} + 2^t - 1$ is cyclotomic equivalent to $\frac{3}{2^t+2^{\frac{t-1}{2}}+1}$;
- Dobbertin exponent $2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$ over $\mathbb{F}_{2^{5m}}$ is cyclotomic equivalent to $\frac{2^{2m}+2^m+1}{2^m+1}$.

Outline

Composition of monomials with linear functions

For $3 \leq s, t \leq n-1$ and some linear function L study $F(x) = x^s \circ L \circ x^t$ for APN property, in particular, for equivalent to APN monomials [B., Calderini, Carlet, Davidova, Kaleyski 2022].

- $F(x) = x^{2^{2i}-2^i+1} + x^{2^{2i}} + x^{2^i} + x$ if $s = 2^i + 1$, $t = \frac{1}{2^i+1}$ and $L(x) = x^{2^{2i}} + x$.
- F is EA-equivalent to the inverse of Kasami $x^{\frac{1}{2^{2i}-2^i+1}}$ for $s = 2^i + 1$, $t = \frac{1}{2^r+1}$ and $L(x) = x^{2^i} + x$ when $n = 3s \pm r$ is odd, $3s \geq r$, $\gcd(3s, r) = 1$.
- F is affine equivalent to $x^{\frac{1}{2^i+1}}$ when $s = \frac{1}{2^i+1}$, $t = 2^i + 1$ for $L(x) = x^{2^i} + x$
- These are the only nontrivial cases for $n \leq 9$ odd and $L \in \mathbb{F}_2[x]$.

Some Particular Exponents

Consider over $\mathbb{F}_{2^{mk}}$ exponents

$$d = \sum_{i=1}^{k-1} 2^{im} - 1$$

[B. 2005; B., Calderini, Carlet, Davidova, Kaleyski 2022].

- For $m = 1$ and $k = 5$ it gives Inverse and Dobbertin exponent - the only two APN monomials which are not AB for n odd.
- Not AB.
- Not APN if $k = 2^l + 2$ for some positive integer l, or when $k = 2$ and $m > 2$.
- Not APN for $k = 3$ it is $2^{2m} - 2^m + 1$ over $\mathbb{F}_{2^{3m}}$ with derivatives 2^m-to-1.
- Not APN for $k = 4$: its derivatives are "almost" 2-to-1 with exceptions taking high values.

Sidon Sets and Sum-Free Sets

- A subset of $\mathbb{F}_{2^n}$ is a Sidon set if it does not contain four different elements whose sum is 0.
- A subset S of $\mathbb{F}_{2^n}$ is a sum-free set if there exist no $a, b, c \in S$ that $a + b = c$.
- If x^d is APN over $\mathbb{F}_{2^n}$ then for every $0 \leq j \leq n-1$ $\{a \in \mathbb{F}_{2^n}^* \ : \ a^{d-2^j} = 1\}$ is a Sidon sum-free set in $\mathbb{F}_{2^n}$ [Carlet, Picek 2017].

Dobbertin conjecture on APN monomials

Search for new APN and AB Monomials:

- No new APN for $n \leq 26$ [Dobbertin, Canteaut 2000];
- No new AB for $n \leq 33$ [Leander, Langevin 2008];
- No new APN for $n \leq 34$ and $n = 36, 38, 40, 42$ [Edel];
  - $gcd(d, 2^n - 1)$ is either 1 or 3;
  - excluding known APN;
  - choosing only one representative from cyclotomic coset;
  - an APN monomial stays APN on subfields.
- Adding Sidon and sum-free sets does not exclude sufficient cases for further progress.

Open problems on APN monomials since 2000

- For d Kasami, Welch, Niho or Dobbertin exponent:
  - does CCZ-equivalence coincide with EAI-equivalence for x^d?
  - find permutations of the form $x^d + L(x)$ where $L(x) \neq 0$ linear.
- Find Walsh spectrum of Dobbertin function:
  - use the conjecture for representation of Walsh coefficients (2022);
  - use "optimal" representation for the Dobbertin exponent.
- Find new APN monomials:
  - study $x^s \circ L \circ x^t$;
  - study known special exponents or find and study other special exponents;
  - find new properties of APN monomials to facilitate computer search.