On a Relationship between Gold and Kasami Functions and other Power APN Functions

Lilya Budaghyan, Marco Calderini, Claude Carlet,
Diana Davidova and Nikolay Kaleyski

Department of Informatics
University of Bergen
Bergen, Norway

{lilya.budaghyan,marco.calderini,diana.davidova,nikolay.kaleyski}@uib.no,

claude.carlet@gmail.com

Abstract

A well-known conjecture that the classification of power APN functions is complete up to equivalence dates back to 2000. The present paper finds that, in some cases for n odd, both the Kasami APN function and its inverse can be described, up to EA-equivalence, via the composition of a Gold function and the inverse of a Gold function with a certain linear polynomial in between. We study whether a similar approach can be used to obtain other APN functions by combining power functions with linear polynomials. We experimentally find all APN functions over $\mathbb{F}_{2^n}$ that can be expressed by composing two power functions with a linear polynomial with coefficients in $\mathbb{F}_2$ for $4 \leq n \leq 9$, and verify that the cases described in our constructions exhaust all possibilities of this form.

1 Introduction

Let n be a positive integer, and let $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements. An (n,n)-function, or vectorial Boolean function, is any mapping F from $\mathbb{F}_{2^n}$ to itself. Any (n,n)-function can be uniquely represented as a univariate polynomial of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, for $a_i \in \mathbb{F}_{2^n}$. We say that an (n,n)-function F is a *power, or monomial, function*, if its univariate representation is of the form $F(x) = x^d$ for some positive integer d.

Given a positive integer i, its *binary weight* is the number of ones in its binary notation. More precisely, if $i = \sum_{j=0}^{K} c_i 2^i$ for some positive integer K and for $c_i \in \{0,1\}$ for $0 \leq j \leq K$, then the binary weight of i is $\mathrm{w}(i) = \sum_{j=0}^{K} c_i$. The largest binary weight of any exponent i in the univariate representation of an (n,n)-function F with $a_i \neq 0$ is called the *algebraic degree* of F. A function of algebraic degree 1, resp, 2, resp. 3 is called *affine*, resp. *quadratic*, resp. *cubic*. An affine function F with $F(0) = 0$ is called *linear*.

Vectorial Boolean functions are widely applied to the design of block ciphers in cryptography, where they are used to represent so-called substitution boxes, or S-boxes, whose input and output are both sequences of bits. This is made possible by the identification of $\mathbb{F}_{2^n}$ with the n-dimensional vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2 = \{0, 1\}$, which implies that any element of $\mathbb{F}_{2^n}$ can be interpreted as an n-dimensional binary vector, i.e. a vector consisting of zeros and ones. A prominent example is the AES, or Rijndael, block cipher, which contains an $(8, 8)$-function at its core [8].

It is clearly important to analyze the resistance of any given vectorial Boolean function against various kinds of cryptanalytic attacks. One of the most powerful attacks against block ciphers is differential cryptanalysis [2], which exploits statistical dependencies between the difference $a = x - y$ of two inputs and the difference $b = F(x) - F(y)$ of their corresponding outputs under $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$; if, for some input difference $a \in \mathbb{F}_{2^n}$, the probability of obtaining some output difference $b \in \mathbb{F}_{2^n}$ is greater than uniform, this correlation can be used to mount an attack on the corresponding block cipher. Furthermore, the efficiency of the attack is directly related to the largest probability among all pairs $(a, b) \in \mathbb{F}_{2^n}^2$ of input and output differences.

The notion of the differential uniformity of a function is introduced in [15] as a measurement of the resistance to this kind of attack. More precisely, the *differential uniformity* Δ_F of an (n, n)-function F is defined as the largest number of solutions $x \in \mathbb{F}_{2^n}$ to any equation of the form $F(x) + F(a + x) = b$ for $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$, i.e.

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \#\{x \in \mathbb{F}_{2^n} : F(a + x) + F(x) = b\}.$$

Since $a + x$ is a solution to $F(x) + F(a + x) = b$ whenever x is, Δ_F must be even for any F, and hence can be no lower than 2. The (n, n)-functions attaining this lower bound with equality are called *almost perfect nonlinear (APN)* and provide the best possible resistance to differential cryptanalysis.

APN functions are typically classified with respect to CCZ-equivalence, which is currently the most general known equivalence relation that preserves the differential uniformity [7]. Two (n, n)-functions F and G are said to be *Carlet-Charpin-Zinoviev-equivalent, or CCZ-equivalent*, if their graphs $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $\Gamma_G = \{(x, G(x)) : x \in \mathbb{F}_{2^n}\}$ are affine equivalent, i.e. if there is an affine permutation $\mathcal{A} : \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}^2$ such that $\mathcal{A}(\Gamma_F) = \Gamma_G$. Another equivalence relation preserving differential uniformity is the so-called extended affine equivalence, or EA-equivalence. Two functions F and G are said to be *EA-equivalent* if there exist affine permutations A_1, A_2 of $\mathbb{F}_{2^n}$ and an affine function $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $A_1 \circ F \circ A_2 + A = G$. EA-equivalence is a particular case of CCZ-equivalence, with the latter being strictly more general than EA-equivalence and taking inverses of permutations [6].

In the case of power functions, CCZ-equivalence coincides with cyclotomic equivalence. Two power functions $F(x) = x^d$ and $G(x) = x^e$ over $\mathbb{F}_{2^n}$, where d, e, n are positive integers, are said to be *cyclotomic equivalent* if $d \equiv 2^k e \mod (2^n - 1)$ for some positive integer k, or if $d^{-1} \equiv 2^k e \mod (2^n - 1)$ for some positive integer k in the case that $\gcd(d, 2^n - 1) = 1$, with d^{-1} being the multiplicative inverse of d modulo $2^n - 1$. Cyclotomic equivalence has the advantage of being significantly simpler to test than both EA- and CCZ-equivalence.

Table 1: Known infinite families of APN power functions over $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	$2^i + 1$	$\gcd(i, n) = 1$	2	[13, 15]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[14, 16]
Welch	$2^t + 3$	$n = 2t + 1$	3	[9]
Niho	$2^t + 2^{t/2} - 1$, t even $2^t + 2^{(3t+1)/2} - 1$, t odd	$n = 2t + 1$	$(t + 2)/2$ $t + 1$	[10]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[1, 15]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[11]

APN functions have been studied since the 90's, and only around 16 infinite families of such functions are known to date. In particular, this illustrates that it is quite challenging to construct such functions, which should come as no surprise, as cryptographically strong functions exhibit no clear patterns or regularities by design. Among the known APN functions, the power APN functions play a particularly prominent role. For one, the earliest known examples of APN functions and of infinite families of APN functions are power functions. For another, all known APN functions (including both instances of infinite families and unclassified sporadic examples) are CCZ-equivalent to power functions or quadratic functions (that is, functions of algebraic degree 2), with only one known exception in $\mathbb{F}_{2^6}$ [12].

The six known infinite families of APN monomials are given in Table 1. It is conjectured that this classification is complete up to CCZ-equivalence [11], i.e. any APN power function is CCZ-equivalent to an instance from one of the families in Table 1. The conjecture is verified computationally for $n \leq 24$ by Anne Canteaut according to [11] and later by Edel for $n \leq 34$ and $n = 36, 38, 40, 42$ (unpublished).

The present paper is dedicated to possible constructions of power APN functions. We study the composition of two power functions $P_i(x) = x^i$ and $P_j(x) = x^j$ with a linear polynomial L of the form $P_i \circ L \circ P_j$. In particular, we focus on the possibility of obtaining an APN function by this construction. We discover that in some cases, a function EA-equivalent to the inverse of a Kasami APN function can be described via the composition of a Gold function and the inverse of a Gold function with certain linear maps. Further, we experimentally find all APN functions over $\mathbb{F}_{2^n}$ that can be expressed by composing two power functions with a linear polynomial with coefficients in $\mathbb{F}_2$ for $4 \leq n \leq 9$, and verify that the cases described in our constructions exhaust all possibilities of this form.

2 Composition of power functions with linear functions

To facilitate the discussion, we introduce the following notation:

1. $P_i(x) = x^i$ for any positive integer i;

2. $G_i(x) = x^{2^i+1}$ is the Gold function with parameter i;

3. $K_i(x) = x^{2^{2i}-2^i+1}$ is the Kasami function with parameter i;

4. $W(x) = x^{2^t+3}$ is the Welch function, where $n = 2t+1$;

5. $N(x) = x^{2^t+2^{t/2}-1}$ and $N(x) = x^{2^t+2^{(3t+1)/2}-1}$ is the Niho function for t even and for t odd, respectively, where $n = 2t+1$;

6. $I(x) = x^{2^n-2}$ is the inverse function;

7. $D(x) = x^{2^{4i}+2^{3i}+2^{2i}+2^i-1}$ is the Dobbertin function, where $n = 5i$.

Below, we study the composition of two power functions $P_i(x) = x^i$ and $P_j(x) = x^j$ with a linear polynomial L of the form

$$P_i \circ L \circ P_j \tag{1}$$

over the finite field $\mathbb{F}_{2^n}$ for some positive integer n. In particular, we focus on the possibility of obtaining an APN function by this construction. We consider the case of n odd and n even separately, and then present our computational findings.

2.1 The case of odd dimension

Our study is motivated by an initial observation that, over any finite field $\mathbb{F}_{2^n}$ with n odd, composing the Gold function $G_i(x) = x^{2^i+1}$ with its inverse $G_i^{-1}(x)$ (where i is any positive integer with $\gcd(i,n) = 1$) and the linear polynomial $L(x) = x^{2^{2i}} + x$ in between gives a function EA-equivalent to the Kasami function $K_i(x) = x^{2^{2i}-2^i+1}$ with the same parameter i. More precisely, we observe that

$$G_i \circ L \circ G_i^{-1}(x) = K_i(x) + x^{2^{2i}} + x^{2^i} + x,$$

where $x \mapsto x^{2^{2i}} + x^{2^i} + x$ is a linear function. In fact, taking $L_\mu(x) = x^{2^{2i}} + \mu x$, we have

$$G_i \circ L_\mu \circ G_i^{-1}(x) = \mu K_i(x) + x^{2^{2i}} + \mu^{2^i} x^{2^i} + \mu^{2^i+1} x$$

for any $\mu \in \mathbb{F}_{2^n}^*$.

We thus see that in certain cases, a function CCZ-equivalent to a Kasami function can be obtained by combining a Gold function and the inverse of a Gold function with a linear polynomial. A formal treatment of this observation is provided in the following proposition. This suggests that functions CCZ-inequivalent to P_i and P_j can be obtained as $P_i \circ L \circ P_j$. We contrast this with EA-equivalence, in which an (n,n)-function F is combined with two linear permutations L_1, L_2 in the form $L_1 \circ F \circ L_2$. We note that all linear polynomials L that we compose with in Propositions 1 and 2 are 2-to-1 over $\mathbb{F}_{2^n}$, while the linear functions L_1 and L_2 in the definition of EA-equivalence are necessarily bijective. In particular, this shows that while the Kasami functions (and their inverses) are always 1-to-1 functions for odd dimensions, the addition of certain linear functions can make them 2-to-1 functions.

Proposition 1. *Let $n = 2m+1$, and denote $L_i^\mu(x) = \mu x^{2^i} + x$. Then, for any $1 \le i \le n-1$, we have*

$$G_i \circ L_{2i}^\mu \circ G_i^{-1}(x) = A_i^\mu(x) + \mu^{2^i} K_i(x), \tag{2}$$

where $A_i^\mu(x) = \mu^{2^i+1} x^{2^{2i}} + \mu x^{2^i} + x$.

Similarly, for any $1 \le i \le n-1$, we have

$$G_i \circ L_{n-2i}^\mu \circ G_i^{-1}(x) = \mu K_i(x^{2^{-2i}}) + C_i^\mu(x^{2^{-2i}}), \tag{3}$$

where $C_i^\mu(x) = \mu^{2^i+1} x + \mu^{2^i} x^{2^i} + x^{2^{2i}}$.

Proof. Denoting $x = y^{2^i+1}$, we obtain

$$\begin{aligned} G_i \circ L_{2i}^\mu \circ G_i^{-1}(x) &= \left(\mu y^{2^{2i}} + y\right)^{2^i+1} \\ &= \mu^{2^i+1} y^{2^{2i}(2^i+1)} + \mu^{2^i} y^{2^{3i}+1} + \mu y^{2^i(2^i+1)} + y^{2^i+1} \\ &= \mu^{2^i+1} x^{2^{2i}} + \mu^{2^i} x^{(2^{3i}+1)/(2^i+1)} + \mu x^{2^i} + x \\ &= A_i^\mu(x) + \mu^{2^i} K_i(x) \end{aligned}$$

due to $K_i(x) = x^{2^{2i}-2^i+1} = x^{(2^{3i}+1)/(2^i+1)}$. The proof in the case of L_{n-2i}^μ is similar. □

A natural question is whether APN functions other than the Kasami function can be obtained in the same manner. The following two propositions demonstrate two ways in which we can reach the EA-equivalence class of the inverse of the Kasami function by composing a Gold function and the inverse of a Gold function (with different parameters) with a linear polynomial in between. We note that the polynomial expression of the inverse of the Kasami APN function in odd dimension (that is, the expression of its exponent as a power function) can be quite complex [18]. The expression of K_i^{-1} in Proposition 2 is therefore rather interesting in this sense. We note that explicit formulas for the inverses of the Dobbertin and Welch exponents have previously been studied in [17].

Proposition 2. *Let $n = 3s \pm r$, $3s \ge r$ and $\gcd(3s, r) = 1$, n odd, and let $L_i^\mu(x) = \mu x^{2^i} + x$. Then*

$$G_s \circ L_{2s}^\mu \circ G_r^{-1}(x) = \begin{cases} A^\mu \circ K_s^{-1}(x^{2^{3s}}) + \mu^{2^s} x^{2^{3s}} & n = 3s + r \\ A^\mu \circ K_s^{-1}(x) + \mu^{2^s} x^{2^s} & n = 3s - r, \end{cases} \tag{4}$$

where $A^\mu(x) = \mu^{2^s+1} x^{2^{2s}} + \mu x^{2^s} + x$ is a linear permutation.

Similarly, we have

$$G_s \circ L_{n-2s}^\mu \circ G_r^{-1}(x) = \begin{cases} B_s^\mu \circ K_s^{-1}(x) + \mu x^{2^{-2s}} & n = 3s - r \\ B_s^\mu \circ K_s^{-1}(x^{2^{3s}}) + \mu x^{2^s} & n = 3s + r, \end{cases} \tag{5}$$

where $B_s^\mu(x) = x + \mu^{2^s} x^{2^{n-s}} + \mu^{2^s+1} x^{2^{n-2s}}$ is a linear permutation.

Proof. Denoting by $y = x^{1/(2^r+1)}$ the inverse of $G_r(x)$, we obtain by straightforward manipulation

$$\begin{aligned} G_s \circ L^\mu_{2s} \circ G_r^{-1}(x) = G_s \circ L^\mu_{2s}(y) &= \left(\mu y^{2^{2s}} + y\right)^{2^s+1} \\ &= \mu^{2^s+1} y^{2^{2s}(2^s+1)} + \mu^{2^s} y^{2^{3s}+1} + \mu y^{2^s(2^s+1)} + y^{2^s+1} \\ &= A^\mu\left(y^{2^s+1}\right) + \mu^{2^s} y^{(2^{3s}+1)}. \end{aligned}$$

Suppose now that $n = 3s + r$. Then

$$\frac{1}{2^r+1} \equiv \frac{2^n}{2^r+2^n} \equiv \frac{2^{3s+r}}{2^r(2^{3s}+1)} \equiv \frac{2^{3s}}{2^{3s}+1} \mod (2^n-1),$$

so that $y^{2^s+1} = x^{(2^s+1)/(2^r+1)} = x^{2^{3s}(2^s+1)/(2^{3s}+1)}$, which is precisely $K_s^{-1}(x^{2^{3s}})$ since $K_s(x) = x^{2^{2s}-2^s+1}$; equivalently, $K_s(x) = x^{(2^{3s}+1)/(2^s+1)}$, whence $K_s^{-1}(x) = x^{(2^s+1)/(2^{3s}+1)}$. Similarly, $\mu y^{2^{3s}+1} = \mu x^{(2^{3s}+1)/(2^r+1)} = \mu x^{2^{3s}}$, which concludes the proof in the case of $n = 3s + r$.

When $n = 3s - r$, we have

$$\frac{1}{2^r+1} \equiv \frac{1}{2^{n+r}+1} \equiv \frac{1}{2^{3s}+1} \mod (2^n-1),$$

so that $y^{2^s+1} = x^{(2^s+1)/(2^{3s}+1)} = K_s^{-1}(x)$, and $\mu y^{2^{3s}+1} = \mu x^{2^{3s}+1} 2^r + 1 = x$, concluding the proof for L^μ_{2s}.

Let j be a positive integer. We will prove that $\mu^{2^j+1} x^{2^{2j}} + \mu x^{2^j} + x$ permutes $\mathbb{F}_{2^n}$ whenever $3 \nmid n$ by showing that it has a trivial kernel. Suppose that $\mu^{2^j+1} x^{2^{2j}} + \mu x^{2^j} + x = 0$. Raising both sides to the power 2^j and multiplying by μ, we obtain $\mu^{2^{2j}+2^j+1} x^{2^{3j}} + \mu^{2^j+1} x^{2^{2j}} + \mu x^{2^j} = 0$. Summing both of these identities, we have $x = \mu^{2^{2j}+2^j+1} x^{2^{3j}}$, and hence, assuming $x \neq 0$, $x^{2^{3j}-1} = (1/\mu)^{2^{2j}+2^j+1}$. Since $2^{3j} - 1 = (2^{2j} + 2^j + 1)(2^j - 1)$, and $\gcd(2^{2j} + 2^j + 1, 2^n - 1) = 1$ for $3 \nmid n$, this implies $x^{2^j-1} = 1/\mu$, whence $x^{2^j} = x/\mu$ and $x^{2^{2j}} = x/\mu^{2^j+1}$. Substituting this into $\mu^{2^j+1} x^{2^{2j}} + \mu x^{2^j} + x = 0$, we obtain $x/\mu = 0$, implying $x = 0$ and contradicting our assumption that $x \neq 0$.

The proof for B^μ_s follows the same logic. Denoting once again $y = x^{1/(2^r+1)}$, we obtain

$$\begin{aligned} G_s \circ L^\mu_{n-2s} \circ G_r^{-1}(x) &= \left(y + \mu y^{(2^{n-2s})}\right)^{2^s+1} \\ &= y^{2^s+1} + \mu y^{2^{n-2s}+2^s} + \mu^{2^s} y^{2^{n-s}+1} + \mu^{2^s+1} y^{2^{n-2s}+2^{n-s}} \\ &= B^\mu_s(y^{2^s+1}) + \mu y^{2^{n-2s}+2^s}. \end{aligned}$$

We have already seen that y^{2^s+1} becomes $K_s^{-1}(x^{2^{3s}})$, resp. $K_s^{-1}(x)$ when $n = 3s + r$, resp. $n = 3s - r$. When $n = 3s + r$, the term $\mu y^{2^{n-2s}+2^s}$ becomes

$$\mu y^{2^{s+r}+2^s} = \mu x^{2^s(2^r+1)/(2^r+1)} = \mu x^{2^s};$$

when $n = 3s - r$, we have

$$\mu y^{2^{n-2s}+2^s} = \mu y^{2^{s-r}+2^s} = \mu x^{2^{s-r}(2^r+1)/(2^r+1)} = \mu x^{2^{s-r}} = \mu x^{2^{-2s}}.$$

Finally, showing that $B^\mu_s(x)$ is a permutation is done in the same way as for $\mu^{2^j+1} x^{2^{2j}} + \mu x^{2^j} + x$. □

While Proposition 2 explicitly describes only compositions of the form $G_s \circ L \circ G_r^{-1}$ over $\mathbb{F}_{2^n}$, where $n = 3s \pm r$, we can observe that G_s and G_{n-s} yield equivalent functions, and so the parameters s and r can be freely replaced with $n - s$ and $n - r$, respectively, thereby allowing for a wider range of compositions. Furthermore, if $s \equiv s' \mod n$, then G_s and $G_{s'}$ correspond to the same function, and so arbitrary multiples of the dimension n can be added or subtracted, allowing us even more freedom. We thus have the following general principle.

Remark 3. Assuming the notation of Proposition 2, the following compositions are all equivalent for any linear function L:

$$\begin{aligned} G_i \circ L \circ G_j^{-1}, \\ G_{n-i} \circ L \circ G_j^{-1}, \\ G_i \circ L \circ G_{n-j}^{-1}, \\ G_{n-i} \circ L \circ G_{n-j}^{-1}. \end{aligned}$$

For instance, the composition $G_1 \circ L \circ G_3^{-1}$ over $\mathbb{F}_{2^7}$ cannot be directly expressed using Proposition 2; but taking $s = n - 1 = 6$, and $r = 11 \equiv 4 \mod n$ so that $n - 3 = 4$, we have $n = 3 \cdot s - r$, and we obtain the case $G_1 \circ L \circ G_3^{-1}$.

Corollary 4. *Let $n = 2m + 1$ be odd with $3 \nmid n$, and let i be a positive integer in the range $1 \leq i \leq n - 1$ such that $\gcd(i, n) = 1$. Let $\mu \in \mathbb{F}_{2^n}^*$ be arbitrary, and denote $L_i^\mu(x) = \mu x^{2^i} + x$ as before. Then the functions*

$$G_i \circ L_{2i}^\mu \circ G_{3i}^{-1}$$

and

$$G_i \circ L_{n-2i}^\mu \circ G_{3i}^{-1}$$

are APN, and EA-equivalent to the inverse K_i^{-1} of the Kasami function with parameter i.

Proof. Take $s = i + n$ and $r = 3s - n$. We have $3s - r = n$. Furthermore, $s \equiv i \mod n$, and $r \equiv 3i \mod n$. Thus, we only have to show that the pair (s, r) satisfies the hypothesis of Proposition 2 in order to finish the proof. We want to show that $|r| \leq 3s$, i.e. $-3s \leq 3s - n \leq 3s$, which gives the inequalities $n \geq 0$ and $n \leq 6s \leq 6i + 6n$. Both of these are clearly always satisfied. Finally, we need to show that $\gcd(3s, r) = 1$. Clearly, $3 \nmid r$ since $3 \nmid n$ by the hypothesis; thus, we only need to show that $\gcd(s, r) = 1$. Suppose d is a non-trivial common divisor of s and $r = 3s - n$; then d is a non-trivial common divisor of $s = i + n$ and n, and hence of i and n. But since $1 \leq i \leq n - 1$ by assumption, we reach a contradiction, and thus $\gcd(s, r) = \gcd(3s, r) = 1$ as claimed. Now, all conditions on (s, r) from the hypothesis of Proposition 2 are satisfied, and an application of the latter concludes the proof.

□

Remark 5. We note that while Propositions 1 and 2 describe cases in which a composition of the form $P_i \circ L \circ P_j$ is EA-equivalent to a Kasami K_i function (or its inverse), in some cases we obtain K_1 (or its inverse), which is actually the Gold function G_1 (or its inverse). In particular, this happens in Proposition 1 for $i = 1$, and in Proposition 2 for $s = 1$.

In our experimental results, we also observe combinations of the form $G_t^{-1} \circ L \circ G_t$, which are EA-equivalent to G_t^{-1}, and combinations of the form $I \circ L \circ I$, which gives a function EA-equivalent to the inverse function I.

Observation 6. *Let $n = 2t + 1$. Then the compositional inverse of $G_t(x) = x^{2^t+1}$ is $x^{2^{t+1}(2^{t+1}-1)}$. Consequently, the composition $G_t^{-1} \circ L \circ G_t$ becomes*

$$G_t^{-1} \circ L \circ G_t(x) = \left(x^{2^t+1} + x^{2^{2t}+2^t}\right)^{2^{t+1}\cdot(2^{t+1}-1)} \tag{6}$$

for $L = x^{2^t} + x$, and

$$G_t^{-1} \circ L \circ G_t(x) = \left(x^{2^t+1} + x^{2^{2t+1}+2^{t+1}}\right)^{2^{t+1}\cdot(2^{t+1}-1)} \tag{7}$$

for $L = x^{2^{t+1}} + x$. Similarly, we get

$$I \circ L \circ I(x) = \left(x^{2^{2t}-1} + x^{2^{2t+1}-2}\right)^{2^{2t}-1} \tag{8}$$

for $L = x^2 + x$, and

$$I \circ L \circ I(x) = \left(x^{2^{2t}-1} + x^{2^{4t}-2^{2t}}\right)^{2^{2t}-1} \tag{9}$$

for $L = x^{2^{2t}} + x$.

The functions in (6) *and* (7)*, and* (8) *and* (9) *are EA-equivalent to G_t^{-1} and I, respectively. Furthermore, for $n \in \{3, 5, 7, 9\}$, the combinations described in* (6), (7), (8), *and* (9)*, and Propositions 2 and 1 exhaust all APN functions over $\mathbb{F}_{2^n}$ that can be obtained as $P_i \circ L \circ P_j$ for any affine function L with coefficients in $\mathbb{F}_2$.*

Proof. We show that the functions from (6) and (8) are equivalent to the Gold and inverse functions, respectively.

In the Gold case, we have $n = 2t+1$, and $G_t^{-1} \circ L \circ G_t = (x^{2^{t+1}+1} + x^{2^t+1})^{2^{t+1}-1}$. Since $2^{t+1} - 1 = 2^t + 2^{t-1} + \cdots + 1$, we have that this is equal to

$$\prod_{j=0}^{t} (x^{2^{t+1}+1} + x^{2^t+1})^{2^j} = \prod_{j=0}^{t} x^{2^j(2^t+1)} \prod_{j=0}^{t} (x^{2^t} + 1)^{2^j} = x^{2^t} \prod_{j=0}^{t} (x^{2^t} + 1)^{2^j} = x^{2^t} \sum_{j=0}^{2^{t+1}-1} (x^{2^t})^j.$$

The latter function is EA-equivalent to

$$\sum_{j=1}^{2^{t+1}} x^j = \frac{(x^{2^{t+1}+1} + 1)}{x+1} + 1.$$

Using the transformation $x \mapsto x+1$ (and adding 1), we get the function

$$\frac{(x^{2^{t+1}+1} + x^{2^{t+1}} + x)}{x} = x^{2^{t+1}} + x^{2^{t+1}-1} + 1,$$

which is EA-equivalent to G_t^{-1}.

As for the inverse case, the function from (8) can be written as $1/(x+1)+x+1$. Indeed, $I \circ L \circ I = (\frac{1}{x^2} + \frac{1}{x})^{-1} = (\frac{1+x}{x^2})^{-1} = \frac{x^2}{1+x} = \frac{1}{x+1} + x + 1$. □

2.2 The case of even dimension

Our experimental results indicate that the case for even values of n is somewhat less interesting. For $n = 6$, no APN functions can be obtained as $P_i \circ L \circ P_j$ for L with coefficients in $\mathbb{F}_2$, while for $n \in \{4, 8\}$, only APN functions from the equivalence class of P_i can be obtained in this manner, as described in the following proposition.

Proposition 7. *Let $n = 2m$, $l_n = \frac{2^{n-1}+1}{3}$, $L(x) = \sum_{j=1}^t x^{2^{2i_j}}$ be a permutation for some positive integer t and for some non-negative integers i_j for $1 \leq j \leq t$, and let $1 \leq i \leq 2^n-2$ be arbitrary with $3 \mid i$. Then*

$$P_i \circ L \circ P_{l_n}(x) = P_i \circ M, \tag{10}$$

and

$$P_i \circ L \circ P_{2l_n+1} = P_{2i} \circ M' \circ x^2,$$

where $M(x) = \sum_{j=1}^t x^{2^{2i_j-1}}$ and $M'(x) = \sum_{j=1}^t x^{2^{2i_j+1}}$. In particular, both $P_i \circ L \circ P_{l_n}$ and $P_i \circ L \circ P_{2l_n+1}$ are linear equivalent to P_i.

Proof. Let us denote $y = x^{l_n}$. We will prove that

$$L(y)^3 = \left(\sum_{j=1}^t y^{2^{2i_j}}\right)^3 = \left(\sum_{j=1}^t x^{2^{i_j-1}}\right)^3 = M(x)^3;$$

this then implies the case for general i due to $3 \mid i$.

In the following, we use the fact that

$$\frac{2^n+2}{3} 3j \equiv 3j \mod (2^n-1)$$

for any integer j, and, in particular

$$\frac{2^n+2}{3}(2^{2i_j}-1) \equiv 2^{n-k}+1 \mod (2^n-1) \tag{11}$$

for any integer i_j.

Clearly, $(x^{(2^n-1)/3}f(x))^3 = f(x)^3$ for any polynomial $f(x)$ over $\mathbb{F}_{2^n}$ with $f(0) = 0$. We apply this to $L(y)^3 = L(x^{l_n})^3$. The exponent of x in $y^{2^{2i_j}} = x^{2^{2i_j}l_n} = x^{2^{2i_j}(2^{n-1}+1)/3}$ becomes

$$\begin{aligned} &2^{2i_j}\frac{2^{n-1}+1}{3} + \frac{2^n-1}{3} = \frac{2^{n+2i_j-1}+2^{2i_j}+2^n-1}{3} \\ &= \frac{2^n+2}{3}(2^{2i_j-1}+1) - 1 \equiv 2^{2i_j-1} \mod (2^n-1) \end{aligned}$$

for any non-negative integer i_j. Thus, $L(y)^3 = M(x)^3$ as claimed.

The case for $2l_n+1$ follows in the same way, but we multiply the expression by $(x^{(2^n-1)/3})^2$. Denoting $z = x^{2l_n+1}$, the exponent of x in $z^{2^{2i_j}}$ becomes

$$\begin{aligned} &2^{2i_j}\left(\frac{2^n+2}{3}+1\right) + \frac{2^{n+1}-2}{3} \\ &= (2^{2i_j}-1)\left(\frac{2^n+2}{3}\right) + 2^{2i_j} + \frac{2^n+2}{3} + \frac{2^{n+1}-2}{3} \\ &= \frac{2^n+2}{3} + 2^{2i_j} - 1 + 2^{2i_j} + \frac{2^{n+1}-2}{3} \\ &= 2^n - 1 + 2^{2i_j+1} \equiv 2^{2i_j+1} \mod (2^n-1). \end{aligned}$$

The rest follows in the same way as in the previous case. □

We then immediately have the following generalization.

Corollary 8. *Let $n = 2m$ be even, $l_n = \frac{2^{n-1}+1}{3}$, $L(x) = \sum_{j=1}^t x^{2^{2i_j}}$ be a permutation for some positive integer t and for non-negative integers i_j for $1 \le j \le t$, and let $F(x) = G(x^3)$ for some (n,n)-function G. Then*

$$F \circ L \circ P_{l_n}(x) = F \circ M,$$

$$F \circ L_j \circ P_{2l_n+1}(x) = F \circ P_2 \circ L,$$

where $M(x) = \sum_{j=1}^t x^{2^{n-k_j-1}} + x^{2^{n-1}}$. In particular, $F \circ L \circ P_{l_n}$, and $F \circ L \circ P_{2l_n+1}$ are linear equivalent to F.

We note that all APN functions that we obtain as $P_i \circ L \circ P_j$ for L linear with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^n}$ with $n \in \{4, 6, 8\}$ are described by Proposition 7.

2.3 Experimental results

For $\mathbb{F}_{2^n}$ with $4 \le n \le 9$, we consider the function $F = P_i \circ L \circ P_j$ for all possible linear L over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ and for a single i and j from each cyclotomic coset, and record the instances in which F is APN. We confirm that all such cases correspond to one of the cases treated in Sections 2.1 and 2.2.

Acknowledgements

The research of this paper was supported by the Trond Mohn Foundation (TMS).

References

[1] Beth, Thomas, and Cunsheng Ding. “On almost perfect nonlinear permutations.” Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993.

[2] Biham, Eli, and Adi Shamir. “Differential cryptanalysis of DES-like cryptosystems.” Journal of CRYPTOLOGY 4.1 (1991): 3-72.

[3] Blondeau, Céline, Anne Canteaut, and Pascale Charpin. “Differential Properties of $x \mapsto x^{2^t-1}$.” IEEE Transactions on Information Theory 57.12 (2011): 8127-8137.

[4] Brinkmann, Marcus, and Gregor Leander. “On the classification of APN functions up to dimension five.” Designs, Codes and Cryptography 49.1-3 (2008): 273-288.

[5] Budaghyan, Lilya. “The equivalence of Almost Bent and Almost Perfect nonlinear functions and their generalization.” PhD Dissertation, Otto-von-Guericke-University, Magdeburg, Germany, 2005.

[6] Budaghyan, Lilya, Claude Carlet, and Alexander Pott. “New classes of almost bent and almost perfect nonlinear polynomials.” IEEE Transactions on Information Theory 52.3 (2006): 1141-1152.

[7] Carlet, Claude, Pascale Charpin, and Victor Zinoviev. “Codes, bent functions and permutations suitable for DES-like cryptosystems.” Designs, Codes and Cryptography 15.2 (1998): 125-156.

[8] Daemen, Joan, and Vincent Rijmen. “The design of Rijndael: AES-the advanced encryption standard.” Springer Science & Business Media, 2013.

[9] Dobbertin, Hans. “Almost perfect nonlinear power functions on $GF(2^n)$) the Welch case.” IEEE Transactions on Information Theory 45.4 (1999): 1271-1275.

[10] Dobbertin, Hans. “Almost perfect nonlinear power functions on GF (2n): the Niho case.” Information and Computation 151.1-2 (1999): 57-72.

[11] Dobbertin, Hans. “Almost perfect nonlinear power functions on GF (2 n): a new case for n divisible by 5.” Finite Fields and Applications. Springer, Berlin, Heidelberg, 2001. 113-121.

[12] Edel, Yves, and Alexander Pott. “A new almost perfect nonlinear function which is not quadratic.” Adv. in Math. of Comm. 3.1 (2009): 59-81.

[13] Gold, Robert. “Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.).” IEEE transactions on Information Theory 14.1 (1968): 154-156.

[14] Janwa, Heeralal, and Richard M. Wilson. “Hyperplane sections of Fermat varieties in P 3 in char. 2 and some applications to cyclic codes.” International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. Springer, Berlin, Heidelberg, 1993.

[15] Nyberg, Kaisa. “Differentially uniform mappings for cryptography.” Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993.

[16] Kasami, Tadao. “The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes.” Information and Control 18.4 (1971): 369-394.

[17] Kyureghyan, Gohar M., and Valentin Suder. “On inversion in Z_{2n-1}.” Finite Fields and Their Applications 25 (2014): 234-254.

[18] Kölsch, Lukas. “On the inverses of Kasami and Bracken-Leander exponents.” arXiv preprint arXiv:2003.12794 (2020).