On the minimal value set size of APN functions

Ingo Czerwinski
Karlsruhe, Germany
ingo@czerwinski.eu

June 12, 2020

Abstract

We give a lower bound for the size of the value set of almost perfect nonlinear (APN) functions $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. For n even it is $\frac{2^n+2}{3}$ and sharp as the simple example $F(x) = x^3$ shows. The sharp lower bound for n odd has to lie between $\frac{2^n+1}{3}$ and 2^{n-1}. Sharp bounds for the cases $n = 3$ and $n = 5$ are explicitly given.

Keywords Boolean functions, Cryptographic S-boxes, Almost perfect nonlinear (APN), Value set size

Mathematics Subject Classification (2020) 94A60, 06E30, 11T71

1 Introduction

Almost perfect nonlinear (APN) functions are quite important in cryptography. Due to their optimal resistance to differential attacks [6] they are used as S-boxes of block ciphers. An introduction to the topic can be found in the book [4] and in the survey [1]. In general, a better understanding of APN functions could be helpful to find new APN functions. Therefore, we will have a closer look on the minimal value set size of APN functions.

In Section 2 we will introduce some basic definitions and have a look on some preimage properties of APN functions. Afterwards in Section 3 we will state our main theorem about the minimal value set size of APN functions and present beside theoretical results also some results based on computations for dimension 5.

2 Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements with $n \geq 2$. A (vectorial Boolean) function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear (APN)* if, for every nonzero $c \in \mathbb{F}_{2^n}$ and every $d \in \mathbb{F}_{2^n}$, the equation $F(x+c)+F(x)=d$ has at most two solutions.

A set $P=\{x_1,x_2,x_3,x_1+x_2+x_3\}$ with $x_1,x_2,x_3 \in \mathbb{F}_{2^n}$ pairwise different is called *affine sub-plane* (or affine subspace of dimension 2) of $\mathbb{F}_{2^n}$ and a function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *affine on P* if $F(x_1+x_2+x_3)=F(x_1)+F(x_2)+F(x_3)$. It is easy to see that F is APN if and only if F is not affine on every affine sub-plane of $\mathbb{F}_{2^n}$.

The *value set* of a function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by $V_F=\{F(x) : x \in \mathbb{F}_{2^n}\}$, its size (or cardinality) is denoted by $|V_F|$ and $F^{-1}(y)=\{x \in \mathbb{F}_{2^n} : F(x)=y\}$ is the *preimage* of $y \in \mathbb{F}_{2^n}$ of F.

There are several equivalence relations on functions which preserve properties like APN or value set size. Two functions $F,G\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called:

1. *affine equivalent* if $G=T_1\circ F\circ T_2$ where the functions $T_1,T_2\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
2. *extended affine (EA) equivalent* if $G=T_1\circ F\circ T_2+A$ where the functions $T_1,T_2\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations and $A\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an affine function.

It is clear that affine equivalence is included in EA equivalence. The APN property of a function is preserved by EA equivalence. The value set size is preserved by affine equivalence but not in general by EA equivalence. Because of its importance we mention also the *Carlet-Charpin-Zinoviev (CCZ) equivalence* (see [3], [5] for more details).

Let us take a closer look on some preimage properties of APN functions. We define

$$S_2(M)=\{m_1+m_2 : m_1,m_2 \in M \text{ and } m_1 \neq m_2\}$$

for $M \subseteq \mathbb{F}_{2^n}$.

Proposition 2.1. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function. If F is APN then*

$$\biguplus_{y\in\mathbb{F}_{2^n}} S_2(F^{-1}(y)) \subseteq \mathbb{F}_{2^n} \setminus \{0\}$$

and for each $y \in \mathbb{F}_{2^n}$ it holds

$$|S_2(F^{-1}(y))| = \binom{|F^{-1}(y)|}{2}.$$

Proof. It follows immediately from the definition that $0 \notin S_2(F^{-1}(y))$ for $y \in \mathbb{F}_{2^n}$.

Suppose that $S_2(F^{-1}(y_1)) \cap S_2(F^{-1}(y_2)) \neq \emptyset$ for $y_1, y_2 \in \mathbb{F}_{2^n}$, $y_1 \neq y_2$. Hence there exist $c \in \mathbb{F}_{2^n} \setminus \{0\}$ and $x_1, x_2 \in \mathbb{F}_{2^n}$, $x_1 \neq x_2$ such that $F(x_1) = F(x_1 + c) = y_1$ and $F(x_2) = F(x_2 + c) = y_2$ and therefore $F(x_1) + F(x_2) + F(x_2 + c) = F(x_1 + c)$. Thus, F is not APN.

Suppose that $|S_2(F^{-1}(y))| < \binom{|F^{-1}(y)|}{2}$ for $y \in \mathbb{F}_{2^n}$. Hence there exist $x_1, x_2, x_3, x_4 \in F^{-1}(y)$ pairwise different with $x_1 + x_2 = x_3 + x_4$. Thus, $F(x_1) + F(x_2) + F(x_3) = F(x_1 + x_2 + x_3)$. But then it follows that F is affine on $\{x_1, x_2, x_3, x_1 + x_2 + x_3\}$ and therefore not APN. □

We remark that Proposition 2.1 cannot be used to characterise APN functions since $S_2(F^{-1}(y)) = \emptyset$ for all $y \in \mathbb{F}_{2^n}$ if $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is bijective. But it is quite useful to find a lower bound for the value set size of APN functions.

For a function $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we define

$$k_i = |\{y \in \mathbb{F}_{2^n} : |F^{-1}(y)| = i\}|$$

for $1 \leq i \leq 2^n$ and call the vector $(k_i)_{1 \leq i \leq 2^n}$ the *preimage size distribution* of F. Due to $\mathbb{F}_{2^n} = \uplus_{y \in \mathbb{F}_{2^n}} F^{-1}(y)$ it follows

$$2^n = \sum_{i=1}^{2^n} i k_i. \tag{1}$$

If F is additionally APN then it holds by Proposition 2.1

$$2^n - 1 \geq \sum_{i=1}^{2^n} \binom{i}{2} k_i. \tag{2}$$

Subtracting equation (1) from (2) leads to the following result:

Corollary 2.2. *If F is APN then*

$$k_1 + k_2 \geq 1 + \sum_{i=4}^{2^n} \frac{i(i-3)}{2} k_i. \tag{3}$$

Thus, there always exists $y \in \mathbb{F}_{2^n}$ such that $|F^{-1}(y)|$ equals 1 or 2.

3 Minimal value set size

Theorem 3.1. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function and $n \geq 3$. If F is APN then*

$$|V_F| \geq \begin{cases} \frac{2^n+1}{3} & \textit{for } n \textit{ odd,} \\ \frac{2^n+2}{3} & \textit{for } n \textit{ even.} \end{cases}$$

Proof. The equations (1) and (3) can be translated into a linear programming problem.
Primary Problem: Minimize

$$k_1 + \cdots + k_{2^n}$$

with $k_i \in \mathbb{Q}$ and $k_i \geq 0$ for $1 \leq i \leq 2^n$ such that (1) and (3) holds.
Dual Problem: Maximize

$$-2^n l_1 + l_2$$

with $l_1, l_2 \in \mathbb{Q}$ and $l_2 \geq 0$ such that

$$jl_1 + \frac{j(j-3)}{2} l_2 \geq -1$$

for each $1 \leq j \leq 2^n$.

From the duality theorem of linear programming (e.g. Corollary 7.1g in [7]) follows now that the feasible solutions

$$k_2 = 1, k_3 = \frac{2^n-2}{3}, k_i = 0 \text{ otherwise}$$
$$l_1 = -\frac{1}{3}, l_2 = \frac{1}{3}$$

are optimal since

$$-2^n(-\frac{1}{3}) + \frac{1}{3} = \frac{2^n+1}{3} = 1 + \frac{2^n-2}{3}.$$

For n odd it follows $k_3 = \frac{2^n-2}{3} \in \mathbb{Z}_{\geq 0}$. For n even the feasible solution

$$k_1 = 1, k_3 = \frac{2^n-1}{3} \in \mathbb{Z}_{\geq 0}, k_i = 0 \text{ otherwise}$$

is optimal since

$$(1 + \frac{2^n-1}{3}) - (1 + \frac{2^n-2}{3}) = \frac{1}{3}.$$

□

For n even the lower bound of Theorem 3.1 is sharp as $F(x) = x^3$ with $|V_F| = \frac{2^n+2}{3}$ and the preimage size distribution $k_1 = 1$, $k_2 = 0$, $k_3 = \frac{2^n-1}{3}$ and $k_i = 0$ for $i > 3$ shows.

For the case n odd the given bound is not sharp as we will show later in Proposition 3.3. But we are able to give the following example which is quite close at the lower bound at least for small dimensions.

Example 3.2. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} : x \mapsto x^4 + x^3$. If n is odd then*

$$|V_F| = 2^{n-1}$$

with a preimage size distribution $k_1 = 0$, $k_2 = 2^{n-1}$ and $k_i = 0$ for $i > 2$.

Proof. It is sufficient to show that for $c \in \mathbb{F}_{2^n}$ the equation

$$x^4 + x^3 + c = 0 \tag{4}$$

has either no solution or two solutions. For $c = 0$ it follows directly that 0 and 1 are the solutions of (4). So let $c \neq 0$ and $\alpha \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ be a solution of (4). Setting $x = z + (\alpha + 1)$ it remains to observe the equation

$$\frac{x^4 + x^3 + c}{x + \alpha} = z^3 + (\alpha + 1)z + \alpha(\alpha + 1) = 0. \tag{5}$$

Let $\mathrm{Tr}\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the *trace* function over $\mathbb{F}_{2^n}$, e.g

$$\mathrm{Tr}\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} : x \mapsto x + x^2 + \cdots + x^{2^{n-1}}.$$

By Theorem 1 of [8] and by

$$\mathrm{Tr}(\frac{(\alpha+1)^3}{(\alpha(\alpha+1))^2}) = \mathrm{Tr}(\alpha^{-2}(\alpha+1)) = \alpha^{-1} + \alpha^{-2^n} = 0$$

it follows now that (5) has exactly one solution and therefore (4) exactly two solutions. □

Next proposition shows that for $n = 3$ the discussed Example 3.2 provides the best possible bound and for $n = 5$ it is almost best possible.

Proposition 3.3. *Let $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function.*

(a) For $n = 3$ it follows $|V_F| \geq 2^2 = 4$.

(b) For $n = 5$ it follows $|V_F| \geq 2^4 - 1 = 15$.

Both lower bounds are sharp.

Proof. (a): By Theorem 3.1 it follows that $|F(\mathbb{F}_{2^3})| \geq 3$. Assume that $|F(\mathbb{F}_{2^3})| = 3$. Using equation (1) and (2) leads straightforward to the situation that the case $k_1 = 0$, $k_2 = 1$, $k_3 = 2$ and $k_i = 0$ for $i > 3$ is the only possible. So, let $F(\mathbb{F}_{2^3}) = \{y_1, y_2, y_3\}$ and $|F^{-1}(y_1)| = |F^{-1}(y_2)| = 3$, $|F^{-1}(y_3)| = 2$. Without restriction we have $F^{-1}(y_1) = \{0, x_1, x_2\}$ with different $x_1, x_2 \in \mathbb{F}_{2^3} \setminus \{0\}$ and therefore $S_2(F^{-1}(y_1)) = \{x_1, x_2, x_1 + x_2\}$. Let $x_3 \in \mathbb{F}_{2^3}$ be linearly independent from x_1, x_2. Then $F^{-1}(y_2) = \{x_3, x_1 + x_2\}$ is the only possible set with more then one element such that $S_2(F^{-1}(y_1)) \cup S_2(F^{-1}(y_2)) = \emptyset$. But this contradicts $|F^{-1}(y_1)| = 3$. Thus, $|F(\mathbb{F}_{2^3})| \geq 4$. The function $F(x) = x^4 + x^3$ reaches this bound. □

The result of Proposition 3.3(b) was found with extensive computations made with a self-written C++ library. Let $G\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function representing an EA equivalence class. It is sufficient to calculate the value set size and preimage size distribution of all $F = G + L$ with $L\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ linear to find the minimal value set size and all its preimage size distributions from the whole EA equivalence class.

For $n = 5$ there exist 7 EA equivalence classes of APN functions as shown in [2]. Our computational results about the minimal value set size and the preimage size distributions are listed in Table 1. It is notable that apart of some functions with minimal value set size and EA equivalent to the inverse function every other APN function with minimal value set size has the same preimage size distribution $k_1 = 0$, $k_2 = 14$, $k_3 = 0$, $k_4 = 1$ and $k_i = 0$ for $i > 4$.

Even for $n = 7$ the complexity of finding the minimal value set size of one EA equivalence class with the given algorithm is exploding.

Table 1: APN functions on $n = 5$ with minimal value set size up to EA equivalence and different preimage size distribution. For $i = 6, \ldots, 32$ it holds $k_i = 0$.

#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	6	11	31	16	8	20	30	4	20	23	21	24	22	4	24
2	0	2	13	9	13	27	25	9	16	8	25	7	10	6	26	16
3	0	10	4	15	10	2	10	3	3	13	15	0	25	21	16	29
4	0	6	31	24	29	25	6	3	20	22	3	0	25	25	11	10
5a	0	17	17	27	8	20	17	4	4	2	18	25	21	21	28	15
5b	0	27	7	7	8	30	7	24	31	19	31	30	14	4	17	8
5c	0	10	28	13	2	5	22	24	29	0	6	22	6	29	2	10
5d	0	0	11	16	23	26	20	16	27	12	23	13	21	4	6	4
5e	0	30	24	29	11	24	27	1	0	9	31	27	18	29	18	14
5f	0	5	5	27	9	1	4	5	4	22	6	25	20	0	9	14
5g	0	2	7	30	21	26	26	28	30	11	30	6	18	1	13	13

5h	0	3	7	31	18	28	29	26	22	2	22	15	29	15	2	3
5i	0	23	29	17	6	28	19	0	17	17	11	6	14	8	11	30
6	0	17	25	18	20	9	22	4	16	24	31	31	16	17	24	4
7	0	28	9	16	29	16	4	19	4	30	15	28	22	9	27	18

#	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	23	13	30	22	0	4	6	16	4	8	21	11	31	13	1	1
2	2	10	0	14	6	26	29	7	14	28	8	28	29	27	2	2
3	25	27	13	14	22	22	4	5	29	27	5	2	10	14	21	16
4	5	11	10	5	29	17	20	25	27	17	24	19	27	19	31	22
5a	14	28	22	8	20	21	11	22	14	20	2	22	4	0	25	15
5b	0	24	14	26	26	17	19	4	27	11	1	31	17	31	26	6
5c	4	13	17	20	20	14	6	0	29	28	28	19	29	2	13	0
5d	25	26	27	20	28	12	25	21	6	13	16	21	19	6	20	19
5e	15	18	30	15	22	24	0	18	11	30	14	21	2	9	22	15
5f	2	4	14	4	25	12	18	27	2	12	26	26	9	25	0	2
5g	0	1	14	3	7	21	14	0	26	19	0	7	13	26	6	3
5h	20	20	26	22	20	7	29	18	6	14	28	26	22	0	29	25
5i	2	22	22	14	22	17	5	30	23	11	23	5	19	17	2	18
6	25	10	10	18	0	20	16	26	26	22	5	16	7	9	7	5
7	29	26	19	27	26	17	10	17	0	18	30	15	0	10	22	0

#	$\lvert F(\mathbb{F}_{2^5})\rvert$	k_1	k_2	k_3	k_4	k_5	$D(x)$	EA	CCZ
1	15	0	14	0	1	0	$6x^8 + x^{16}$	x^5	can.
2	15	0	14	0	1	0	$2x^4 + x^{16}$	x^3	can.
3	15	0	14	0	1	0	$9x + 28x^2 + 23x^4 + 17x^8 + 25x^{16}$	[3]	1
4	15	0	14	0	1	0	$24x + 10x^2 + 7x^4 + 11x^8 + 24x^{16}$	[3]	2
5a	15	3	7	5	0	0	$28x + 15x^2 + 2x^4 + x^8$	x^{15}	can.
5b	15	3	8	3	1	0	$22x + 11x^2 + 6x^4 + x^8$	x^{15}	can.
5c	15	6	3	4	2	0	$8x + 10x^2 + 9x^4 + x^8 + x^{16}$	x^{15}	can.
5d	15	2	9	4	0	0	$25x + 18x^2 + 9x^4 + 2x^8 + x^{16}$	x^{15}	can.
5e	15	4	6	4	1	0	$15x + 13x^2 + 30x^4 + 2x^8 + x^{16}$	x^{15}	can.
5f	15	5	4	5	1	0	$16x + 17x^2 + 12x^4 + 8x^8 + x^{16}$	x^{15}	can.
5g	15	5	5	3	2	0	$6x + 11x^2 + 7x^4 + 8x^8 + x^{16}$	x^{15}	can.
5h	15	4	7	2	2	0	$16x + 28x^2 + 2x^4 + 13x^8 + x^{16}$	x^{15}	can.
5i	15	4	7	3	0	1	$21x + 16x^2 + 20x^4 + 6x^8 + x^{16}$	x^{15}	can.
6	15	0	14	0	1	0	$27x + 2x^2 + 8x^4 + x^{16}$	x^{11}	2
7	15	0	14	0	1	0	$11x + 30x^2 + 9x^4 + x^{16}$	x^7	1

4 Conclusion

We have shown the lower bound $\frac{2^n+2}{3}$ for the value set size of APN functions for even dimension n which is sharp as the simple example $F(x) = x^3$ shows. Furthermore we have proved that for odd dimension n the sharp lower bound has to lie between $\frac{2^n+1}{3}$ and 2^{n-1}. The theoretical result for dimension 3 and the computational result for dimension 5 suggest that for odd dimension greater than 5 the given lower bound is not sharp and has to be close to 2^{n-1}. Further work has to be done to sharpen the lower bound for higher odd dimensions.

References

[1] Blondeau, C., Nyberg, K.: *Perfect nonlinear functions and cryptography.* Finite Fields Appl. 32, 120–147 (2015)

[2] Brinkmann, M., Leander, G.: *On the classification of APN functions up to dimension five.* Des. Codes Cryptogr. 49, 273–288 (2008)

[3] Budaghyan, L., Carlet, C., Pott, A.: *New classes of almost bent and almost perfect nonlinear polynomials.* IEEE Trans. Inform. Theory 52(3), 1141–1152 (2006)

[4] Carlet, C.: *Vectorial boolean functions for cryptography. Boolean Models and Methods in Mathematics, Computer Science, and Engineering 134*, 398–469 (2010)

[5] Carlet, C., Charpin, P., Zinoviev, V.A.: *Codes, bent functions and permutations suitable for des-like cryptosystems.* Des. Codes Cryptogr. 15(2), 125–156 (1998)

[6] Nyberg, K, Knudsen,L.R.: *Provable security against differential cryptanalysis.* In: Brickell E.F. (eds) Advances in Cryptology — CRYPTO' 92. CRYPTO 1992. Lecture Notes in Computer Science, vol 740. Springer, Berlin, Heidelberg (1993)

[7] Schrijver, A.: *Theory of Linear and Integer Programming.* John Wiley & Sons, Inc., New York (1986)

[8] Williams, K. S.: *Note on cubics over $GF(2^n)$ and $GF(3^n)$.* J. Number Theory 7, 361-365 (1975)