On the exponents of APN power functions and Sidon sets, sum-free sets, and Dickson polynomials

Claude Carlet[1] and Stjepan Picek[1, 2]

[1]LAGA, Department of Mathematics, University of Paris 8 (and Paris 13 and CNRS), France
[2]Cyber Security Research Group, Delft University of Technology, Mekelweg 2, Delft, The Netherlands

Abstract

We derive necessary conditions related to the notions, in additive combinatorics, of Sidon sets and sum-free sets, on those exponents $d \in \mathbb{Z}/(2^n-1)\mathbb{Z}$ which are such that $F(x) = x^d$ is an APN function over $\mathbb{F}_{2^n}$ (which is an important cryptographic property). We study to which extent these new conditions may speed up the search for new APN exponents d. We also show a new connection between APN exponents and Dickson polynomials: $F(x) = x^d$ is APN if and only if the reciprocal polynomial of the Dickson polynomial of index d is an injective function from $\{y \in \mathbb{F}_{2^n}^*; tr_n(y) = 0\}$ to $\mathbb{F}_{2^n} \setminus \{1\}$. This also leads to a new and simple connection between Reversed Dickson polynomials and reciprocals of Dickson polynomials in characteristic 2 (which generalizes to every characteristic thanks to a small modification): the squared Reversed Dickson polynomial of some index and the reciprocal of the Dickson polynomial of the same index are equal.

1 Introduction

In this paper, we study the so-called *APN exponents* in fields $\mathbb{F}_{2^n}$, that is, those values $d \in \mathbb{Z}/(2^n-1)\mathbb{Z}$ such that the corresponding *power function* $F(x) = x^d$ over $\mathbb{F}_{2^n}$ is *Almost Perfect Nonlinear* (APN). A function from $\mathbb{F}_{2^n}$ to itself is called APN [11, 2, 10] if, for every nonzero $a \in \mathbb{F}_{2^n}$ and every $b \in \mathbb{F}_{2^n}$, the equation $F(x) + F(x+a) = b$ has at most two solutions. Equivalently, the system of equations $\begin{cases} x+y+z+t = 0 \\ F(x)+F(y)+F(z)+F(t) = 0 \end{cases}$ has for only solutions quadruples (x, y, z, t) whose elements are not all distinct (i.e., are pairwise equal). Recall that changing d into one of its conjugates $2^j d$ corresponds to changing $F(x)$ into a linearly equivalent APN function, which preserves APNness. The APN exponents constitute then a union of cyclotomic classes of 2 mod $2^n - 1$. The known APN exponents (Gold, Kasami, Welch, Niho, Inverse, and Dobbertin) are all those exponents which are the conjugates of those given in Table 1 below,

Table 1: Known APN exponents on $\mathbb{F}_{2^n}$ up to equivalence and to inversion.

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
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	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

or of their inverses when they are invertible in $\mathbb{Z}/(2^n - 1)\mathbb{Z}$. Note that i (in the definitions of Gold and Kasami exponents) can always be taken lower than $n/2$ (thanks to conjugacy).

It has been proved by Dobbertin (as described in the survey chapter [3], to which we refer for more information on APN functions) that an exponent can be APN only if $gcd(d, 2^n - 1)$ equals 1 if n is odd and 3 if n is even. We shall show in Section 2 that for all exponents given in Table 1, we have $gcd(d - 1, 2^n - 1) = 1$. This corresponds to the fact that the related functions F have 0 and 1 as only fixed points, since $x \in \mathbb{F}_{2^n}$ is a nonzero fixed point of function $F(x) = x^d$ if and only if $x^{d-1} = 1$.

It happens for some cyclotomic classes that the property $gcd(d-1, 2^n-1) = 1$ be true for any element in the cyclotomic class, or equivalently that $gcd(d - 2^j, 2^n - 1) = 1$ for every $j = 0, \dots, n-1$. We list in Table 2, for the (known) APN exponents of Table 1 up to $n = 32$, when $gcd(d - 2^j, 2^n - 1) = 1$ is true for every $j = 0, \dots, n-1$. The proportion of such exponents is large. Since such property is unlikely for random exponents satisfying Dobbertin's observation recalled above, we can hope that some other property can be found, which would explain such large proportion, and could maybe ease the search for APN exponents outside the main classes. This other property cannot be that $gcd(d-1, 2^n-1) = 1$ for all APN exponents d, which would imply $gcd(d - 2^j, 2^n - 1) = 1$ for all j, since we see in Table 2 that some cyclotomic classes do not satisfy this.

In this paper, we find a new property relating APN exponents to Sidon sets and sum-free sets (two well-known notions in additive combinatorics [1, 6, 12]; see the definitions in Section 3): for every APN exponent d and every integer j, the multiplicative subgroup of $\mathbb{F}_{2^n}$ of order $gcd(d - 2^j, 2^n - 1)$ is a Sidon set and a sum-free set.

The relationship between APN functions and Sidon sets is not new: by definition, an (n, n)-function is APN if and only if its graph is a Sidon set (see Section 3). But the relationship we establish in this paper is different and gives more insight on APN exponents.

We study the consequences on the search for new APN exponents, which is a sensitive open question on which the research is being stuck since almost 20 years. We do not find new APN exponents, but we show that d is an APN exponent if and only if the function equal to the reciprocal of the Dickson polynomial $D_d(X, 1)$ is injective from $\{y \in \mathbb{F}_{2^n}^*; tr_n(y) = 0\}$ to $\mathbb{F}_{2^n} \setminus \{1\}$, where $tr_n(x) = x + x^2 + \cdots + x^{2^{n-1}}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Finally, we show a very simple new relationship (which generalizes to every characteris-

Table 2: $gcd(d-2^j, 2^n-1)=1$ for every $j=0,\dots,n-1$.

Class name	Value
	$(n\|i)$; $i \le n/2$
Gold	$(3\|1), (5\|1,2), (6\|1), (7\|1,2,3), (9\|1,2,4), (11\|2,4,5)$ $(13\|1,2,3,4,5,6), (14\|1,3,5), (15\|1,2,4,7), (17\|1,2,3,4,5,6,7,8),$ $(19\|1,2,3,4,5,6,7,8,9), (21\|1,2,4,5,8,10), (22\|5,7,9),$ $(23\|2,5,7,8,9,10), (25\|1,2,3,4,6,7,8,9,11,12), (26\|1,3,5,7,9,11)$ $(27\|1,2,4,5,7,8,10,11,13), (29\|1,2,3,4,5,6,7,8,9,10,11,12,14)$ $(31\|1,2,3,4,5,6,7,8,9,10,11,12,13,14,15)$
Kasami	$(3\|1), (5\|1,2), (6\|1), (7\|1,2,3), (9\|1,2,4), (11\|3,4), (13\|1,2,3,4,5,6)$ $(14\|1,3), (15\|1,2,4,7), (17\|1,2,3,4,5,6,7,8), (19\|1,2,3,4,5,6,7,8,9),$ $(21\|1,4,5,8,10), (22\|3,7), (23\|2,3,6,8,9,11), (25\|1,2,3,4,6,7,8,9,11,12),$ $(26\|1,3,5,7,9,11), (27\|1,2,4,5,7,8,10,11,13),$ $(29\|1,2,3,5,6,7,8,9,10,11,12,13,14),$ $(31\|1,2,3,4,5,6,7,8,9,10,11,12,13,14,15)$
	n
Welch	$3, 5, 7, 9, 13, 15, 17, 19, 23, 25, 27, 31$
Niho	$3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31$
Dobbertin	$5, 15, 25$
Inverse	$3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31$

tic after a small modification) between Reversed Dickson polynomials and the reciprocals of Dickson polynomials: for every positive integer d, the Reversed Dickson polynomial $D_{2d}(1,X)$ of index $2d$ and the reciprocal of the Dickson polynomial $D_d(X,1)$ of index d are equal.

2 On the exponents of Table 1

The value $gcd(d-1, 2^n-1)$ for a power function $F(x)=x^d$ is an important parameter. The number of fixed points of F equals $2^{gcd(d-1,2^n-1)}$.

Lemma 2.1 *All the exponents d in Table 1 satisfy $gcd(d-1,2^n-1)=1$.*

Proof. In the case of Gold functions $F(x)=x^{2^i+1}$, where $(i,n)=1$, we have $gcd(d-1,2^n-1)=gcd(2^i,2^n-1)=1$.
In the case of Kasami functions $F(x)=x^{2^{2i}-2^i+1}$, where $(i,n)=1$, we have $gcd(d-1,2^n-1)=gcd(2^i-1,2^n-1)=2^{gcd(i,n)}-1=1$.
In the case of Welch function $F(x)=x^{2^t+3}$, we have according to the Gauss theorem (which states that if a divides bc and is co-prime with b then it divides c): $gcd(d-1,2^n-1)=gcd(2^{t-1}+1,2^{2t+1}-1)=\frac{gcd(2^{2t-2}-1,2^{2t+1}-1)}{gcd(2^{t-1}-1,2^{2t+1}-1)}=\frac{2^{gcd(2t-2,2t+1)}-1}{2^{gcd(t-1,2t+1)}-1}=\frac{2^{gcd(t-1,2t+1)}-1}{2^{gcd(t-1,2t+1)}-1}=1$.
In the case of Niho functions:
- $F(x)=x^{2^t+2^{\frac{t}{2}}-1}$, t even, we have, applying the Euclidean algorithm: $gcd(d-1,2^n-1)=gcd(2^t+2^{\frac{t}{2}}-2,2^{2t+1}-1)=gcd(2^t+2^{\frac{t}{2}}-2,-5\cdot 2^{t/2+1}+11)=gcd(2^2\cdot 5^2\cdot(2^t+2^{\frac{t}{2}}-2),5\cdot 2^{t/2+1}-11)=gcd(5\cdot 2^{t/2+1}-11,31)=1$, since 31 divides $2^{2t+1}-1$ if and only if $2t+1\equiv 0$ [mod 5] and the only possibility for

that is $t \equiv 2$ [mod 5], $\frac{t}{2} \equiv 1$ [mod 5] and $2^t + 2^{t/2} - 2 \equiv 4 \not\equiv 0$ [mod 31];
- $F(x) = x^{2^t+2^{\frac{3t+1}{2}}-1}$, t odd, we have $gcd(d-1, 2^n-1) = gcd(2^{\frac{3t+1}{2}} + 2^t - 2, 2^{2t+1}-1) = gcd(2^{\frac{3t+1}{2}} + 2^t - 2, 2^t + 2^{\frac{t+3}{2}} - 3) = gcd(2^t + 2^{\frac{t+3}{2}} - 3, 9 \cdot 2^{\frac{t+1}{2}} - 11) = gcd(2 \cdot 9^2 \cdot (2^t + 2^{\frac{t+3}{2}} - 3), 9 \cdot 2^{\frac{t+1}{2}} - 11) = gcd(9 \cdot 2^{\frac{t+1}{2}} - 11, 31) = 1$, since, again, 31 divides $2^{2t+1} - 1$ if and only if $2t + 1 \equiv 0$ [mod 5] and the only possibility for that is $t \equiv 2$ [mod 5], $\frac{3t+1}{2} \equiv 1$ [mod 5] and $2^t + 2^{\frac{3t+1}{2}} - 2 \equiv 4 \not\equiv 0$ [mod 31].
In the case of the APN Inverse function $F(x) = x^{2^{2t}-1}$, we have, by the Euclidean algorithm: $gcd(d-1, 2^n-1) = gcd(2^{2t-1}-1, 2^{2t+1}-1) = 2^{gcd(2t-1,2t+1)} - 1 = 1$.
In the case of Dobbertin APN function $F(x) = x^d$, where $d = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$ and $n = 5t$, we could calculate $gcd(d-1, 2^n-1)$ by applying again the Euclidean algorithm but more simply we have $gcd(d-1, 2^n-1) = gcd(d-1, (2^t-1)(d+2))$, and since $d \equiv 3$ [mod (2^t-1)], and $d-1$ is then co-prime with $2^t - 1$, we obtain then $gcd(d-1, 2^n-1) = gcd(d-1, d+2) = gcd(d-1, 3)$, which equals 1 if n is odd (because we know that 3 does not divide $2^n - 1$ in this case) and which equals $gcd(2, 3) = 1$ if n is even (since, t being then even, we have $2^{4t}, 2^{3t}, 2^{2t}, 2^t$ all congruent with 1 mod 3 and then $d - 1 \equiv 2$ [mod 3]). Then $gcd(d-1, 2^n-1) = 1$ in all cases. □

Hence, all the corresponding APN functions have 0, 1 as only fixed points.

Remark 2.2 *If d is invertible mod $2^n - 1$ and d' is its inverse, then $gcd(d-1, 2^n-1)$ equals 1 if and only if $gcd(d'-1, 2^n-1)$ equals 1, since a permutaton has the same number of fixed points as its compositional inverse.*

3 Sidon sets and sum-free sets

We saw in Section 2 that the known APN exponents may have a property not covered by the Dobbertin observation (recalled in introduction). We also saw in introduction that such property (to be found) cannot be that $gcd(d-1, 2^n-1) = 1$, since this would imply $gcd(d-2^j, 2^n-1) = 1$ for every $j \in \mathbb{Z}/n\mathbb{Z}$, which is already not true (for some n) for the simplest known APN exponent 3. In the present section, we show that every APN exponent (known or unknown), satisfies a property which deals with the numbers $gcd(d-2^j, 2^n-1)$, $j \in \mathbb{Z}/n\mathbb{Z}$, in a more subtle way. We first need to recall two definitions from additive combinatorics.

Definition 3.1 *[1] A subset of an additive group $(G, +)$ is called a* Sidon set *if it does not contain elements x, y, z, t, at least three of which are distinct, and such that $x + y = z + t$.*

This notion is due to the mathematician Sidon. It is preserved by (additive) equivalence, that is, if S is a Sidon set in $(G, +)$ and A is a permutation of G such that $A(x + y) = A(x) + A(y)$, then $A(S)$ is a Sidon set. The notion is also preserved by translation. Of course, any set included in a Sidon set is a Sidon set.
This definition is also relevant in characteristic 2. In such characteristic, we have more simply: *A subset of an additive group of characteristic 2 is a Sidon set if it does not contain four distinct elements x, y, z, t such that $x + y + z + t = 0$.*

Indeed, if two elements are equal, then there cannot be three distinct elements among x, y, z, t such that $x + y + z + t = 0$.

Remark 3.2 *By definition, an (n, n)-function F is APN if and only if its graph $\mathcal{G}_F = \{(x, F(x)); x \in \mathbb{F}_{2^n}\}$ is a Sidon set in $(\mathbb{F}_{2^n}^2, +)$. Hence, APN functions correspond to a subclass of Sidon sets in $(\mathbb{F}_{2^n}^2, +)$: those S such that, for every $x \in \mathbb{F}_{2^n}$, there exists a unique $y \in \mathbb{F}_{2^n}$ such that $(x, y) \in S$.*

Remark 3.3 *A subset S of an additive group $(G, +)$ is a Sidon set if and only if, denoting by P_S the set of pairs in S, the mapping $\{x, y\} \in P_S \mapsto x+y$ is one-to-one. The size $|S|$ is then (see e.g. [1]) such that $\binom{|S|}{2} = \frac{|S|\,(|S|-1)}{2} \leq |G| - 1$, since otherwise the number of pairs $\{x, y\}$ included in S would be strictly larger than the number of nonzero elements of G; at least two different pairs $\{x, y\}$ and $\{x', y'\}$ would then have the same sum and these two pairs would in fact be disjoint (if, for instance $x = x'$, then $y \neq y'$ and $x+y \neq x'+y'$, a contradiction).*

Definition 3.4 *[6, 12] A subset S of an additive group $(G, +)$ is called a* sum-free set *if it does not contain elements x, y, z such that $x + y = z$ (i.e., if $S \cap (S + S) = \emptyset$).*

This notion is due to Erdös. It is also preserved by (additive) equivalence and by translation; any set included in a sum-free set is a sum-free set and no sum-free set contains 0.

Remark 3.5 *A subset S of an additive group $(G, +)$ is sum-free if and only if, denoting again by P_S the set of pairs in S, the mapping $\{x, y\} \in P_S \mapsto x + y$ is valued outside S. The size $|S|$ is then (see e.g. [6, 12]) smaller than or equal to $\frac{|G|}{2}$, because the size of $S + S$ is at least the size of S (since G is a group), and if $|S| > \frac{|G|}{2}$ then the two sets $S + S$ and S have sizes whose sum is strictly larger than the order of the group, and they necessarily have a non-empty intersection. A basic example of a sum-free set in $\mathbb{F}_{2^n}$, which achieves this bound $|S| \leq \frac{|G|}{2}$ with equality, is any affine hyperplane (i.e., the complement of any linear hyperplane).*

Remark 3.6 *The size $|S|$ of a sum-free Sidon set satisfies $\frac{|S|\,(|S|+1)}{2} \leq |G| - 1$, since otherwise, the number of pairs $\{x, y\} \in P_S$ would be strictly larger than the number of nonzero elements of $G \setminus S$. Note that, in characteristic 2, if S is a Sidon-sum-free set, then $S \cup \{0\}$ is a Sidon set, which gives again the same bound by using Remark 3.3.*

4 APN exponents, Sidon sets, and sum-free sets

We give now the new property valid for all APN exponents which is related to Sidon sets and sum-free sets.

Theorem 4.1 *For every positive integers n and d and for every $j \in \mathbb{Z}/n\mathbb{Z}$, let $e_j = gcd(d - 2^j, 2^n - 1) \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$, and let G_{e_j} be the multiplicative subgroup $\{x \in \mathbb{F}_{2^n}^*; x^{d-2^j} = 1\} = \{x \in \mathbb{F}_{2^n}^*; x^{e_j} = 1\}$ of order e_j. If function $F(x) = x^d$ is APN over $\mathbb{F}_{2^n}$, then, for every $j \in \mathbb{Z}/n\mathbb{Z}$, G_{e_j} is a Sidon set in the additive group $(\mathbb{F}_{2^n}, +)$ and is also a sum-free set in this same group. Moreover, for every $k \neq j$, if $x \in G_{e_k}$, $y \in G_{e_j}$, $x \neq y$ and $x \neq y^{-1}$, then we have $(x+1)^{d-2^k} \neq (y+1)^{d-2^j}$.*

Proof. Using the same idea as the one used by Dobbertin for showing the observation recalled in introduction, for every $x \in G_{e_j} \setminus \{1\}$, we introduce the unique $s \in \mathbb{F}_{2^n}^* \setminus \{1\}$ such that $x = \frac{s}{s+1}$, that is, $s = \frac{x}{x+1}$. Then $x^{d-2^j} = 1$ implies $s^{d-2^j} + (s+1)^{d-2^j} = 0$, which implies after multiplication by $s^{2^j} + 1 = (s+1)^{2^j}$ that $s^d + (s+1)^d = s^{d-2^j} = (s+1)^{d-2^j} = \frac{1}{(x+1)^{d-2^j}}$. Note that if $s = \frac{x}{x+1}$ and $s' = \frac{x'}{x'+1}$, with $x \neq 1$ and $x' \neq 1$, then we have $s = s'$ if and only if $x = x'$ (since function $\frac{x}{x+1}$ is bijective, being involutive) and we have $s = s' + 1$ if and only if $x' = x^{-1}$, since $\frac{x}{x+1} + 1 = \frac{x^{-1}}{x^{-1}+1}$.
Suppose that G_{e_j} is not a Sidon set, then let x, y, z, t be distinct elements of G_{e_j} such that $x + y = z + t$. Making the changes of variables $x \to xt, y \to yt, z \to zt$ and dividing the equality by t, we obtain distinct elements x, y, z of $G_{e_j} \setminus \{1\}$ such that $x + y + z = 1$. Making now the change of variable $y \to zy$, we obtain elements x, y, z in $G_{e_j} \setminus \{1\}$ such that $x + 1 = z(y + 1)$, $x \neq y$ and $x \neq y^{-1}$ (indeed, the condition $y = 1$ in the new setting corresponds to the condition $y = z$ in the former setting, the condition $x = y$ in the new setting is equivalent (thanks to $x+1 = z(y+1)$) to $z = 1$ in both settings, and the condition $x = y^{-1}$ in the new setting, that is (thanks to $x+1 = z(y+1)$ again), $zy = 1$, is equivalent to $y = 1$ in the former setting). We have then $\frac{1}{(x+1)^{d-2^j}} = \frac{1}{(y+1)^{d-2^j}}$ and since $x \neq y$ and $x \neq y^{-1}$, we have $\frac{x}{x+1} \neq \frac{y}{y+1}$ and $\frac{x}{x+1} \neq \frac{y}{y+1} + 1$ and this gives 4 distinct solutions to the equation $s^d + (s+1)^d = \frac{1}{(x+1)^{d-2^j}}$, a contradiction with the APNness of F.
Suppose that G_{e_j} is not sum-free, that is, $G_{e_j} \cap (G_{e_j} + G_{e_j}) \neq \emptyset$, that is without loss of generality since G_{e_j} is a multiplicative group, $G_{e_j} \cap (G_{e_j} + 1) \neq \emptyset$, then let $x \in G_{e_j} \cap (G_{e_j} + 1)$ (which implies $x \neq 0, 1$) and $s = \frac{x}{x+1}$ (with $s \neq 0, 1$ as well), we have then $\frac{1}{(x+1)^{d-2^j}} = 1$ and $s^d + (s+1)^d = 1$ and the equation $z^d + (z+1)^d = 1$ has four solutions $0, 1, s$, and $s + 1$ in $\mathbb{F}_{2^n}$, a contradiction.
The last assertion is a direct consequence of the observations made in the first paragraph of the present proof. □

Remark 4.2 *Since for $s = \frac{x}{x+1}$, $x \neq 1$, we have $s^d + (s+1)^d = \frac{x^d+1}{(x+1)^d}$ and since $\frac{x^d+1}{(x+1)^d} = \frac{(x^{-1})^d+1}{(x^{-1}+1)^d}$, the condition "$G_{e_j}$ is sum-free" is in fact a weaker version of the condition "the equation $x^d + 1 = (x+1)^d$ has at most one solution in $\mathbb{F}_{2^n}$, up to the replacement of x by x^{-1}" which is implied by the condition "the equation $x^d + (x+1)^d = 1$ has at most two solutions in $\mathbb{F}_{2^n}$". We shall say more in Subsection 4.1. Note that every element of G_{e_j} satisfies $x^d + 1 = (x+1)^d$ since this equation in G_{e_j} is equivalent to $x^{2^j} + 1 = (x+1)^{2^j}$ which is always true, and this is why G_{e_j} plays an interesting role.*

Remark 4.3 *Denoting $e = gcd(d, 2^n - 1)$, we have that G_e itself is a Sidon set since, as recalled above, we have $e = 1$ if n is odd and $e = 3$ if n is even, and $G_1 = \{1\}$, $G_3 = \mathbb{F}_4^*$ are Sidon sets (since they do not contain 4 distinct elements). But G_e is a sum-free set only for n odd, since $\mathbb{F}_4^*$ is not sum-free.*

Remark 4.4 *An APN function is APN in any subfield where the function makes sense (i.e., such that $F(x)$ belongs to this subfield when x does). In particular, an APN power function is APN in any subfield. Applying Theorem*

4.1 with a divisor r of n in the place of n replaces e_j by $gcd(d-2^j, 2^r-1)$ and G_{e_j} by $G_{e_j} \cap \mathbb{F}_{2^r}^*$, so it gives no additional information since if G_{e_j} is a Sidon-sum-free set in $\mathbb{F}_{2^n}$, then $G_{e_j} \cap \mathbb{F}_{2^r}^*$ is also a Sidon-sum-free set in $\mathbb{F}_{2^r}$.

Remark 4.5 *The condition that G_{e_j} is sum-free for every $j \in \mathbb{Z}/n\mathbb{Z}$ implies that, for every divisor k of n larger than 1, the integer e_j is not divisible by 2^k-1, because otherwise G_{e_j} would contain $\mathbb{F}_{2^k}^*$, and this is contradictory with the condition. For $k>2$, the fact that e_j is not divisible by 2^k-1 is also a consequence of the fact that G_{e_j} is a Sidon set, since it is straightforward that for $k>2$, $\mathbb{F}_{2^k}^*$ is not a Sidon set and any superset is then not one either. In fact, the property of being a Sidon-sum-free set is rather restrictive, and this explains the observations made in the introduction.*

Remark 4.6 *We observed that, in characteristic 2, the size $|S|$ of a Sidon-sum-free set S not containing 0 cannot be such that $\binom{|S|+1}{2} = \frac{|S|\,(|S|+1)}{2} > 2^n-1$. We deduce then from the theorem that, if d is an APN exponent, then for every divisor λ of 2^n-1 such that $\binom{\lambda+1}{2} > 2^n-1$ and every $j \in \mathbb{Z}/n\mathbb{Z}$, this number λ does not divide $d-2^j$. Take for instance $n=8$ and $\lambda = \frac{2^8-1}{3} = 85$, we have $\binom{\lambda+1}{2} > 255$ and for every APN exponent d, we have that 85 does not divide $d-1$, $d-2$, $d-4$, $d-8$, $d-16$, $d-32$, $d-64$ nor $d-128$ (all these numbers being taken modulo 255). We can also take $\lambda = \frac{2^8-1}{5} = 51$, we have $\binom{\lambda+1}{2} > 255$ and 51 does not divide $d-1$, $d-2$, $d-4$, $d-8$, $d-16$, $d-32$, $d-64$ nor $d-128$ as well. For this value of n, there are only two possible values for λ, but for some larger values of n, the number of possible λ may be much larger and the condition discriminates then better the candidates d.*

4.1 A general framework for deriving results similar to Theorem 4.1

In the proof of Theorem 4.1, we have used that, if $x \in G_{e_j} \setminus \{1\}$ and $s = \frac{x}{x+1}$, then $s^d+(s+1)^d = \frac{1}{(x+1)^{d-2^j}}$. In fact, when relaxing the condition $x \in G_{e_j} \setminus \{1\}$, we still have an interesting identity, which leads to a new characterization of APN exponents:

Proposition 4.7 *Let n be any positive integer and $F(x) = x^d$ be any power function over $\mathbb{F}_{2^n}$. If $x \neq 1$ and $s = \frac{x}{x+1}$ then $s^d + (s+1)^d = \frac{x^d+1}{(x+1)^d}$, and F is APN if and only if the function $x \mapsto \frac{x^d+1}{(x+1)^d}$ is 2-to-1 from $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ to $\mathbb{F}_{2^n} \setminus \{1\}$.*

Proof. The first identity is straightforward. Hence, function $x \mapsto \frac{x^d+1}{(x+1)^d}$ is 2-to-1 from $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ to $\mathbb{F}_{2^n} \setminus \{1\}$ if and only if any equation $s^d+(s+1)^d = b \neq 1$ has at most 2 solutions s in $\mathbb{F}_{2^n}$ (indeed, it has no solution in $\mathbb{F}_2$) and equation $s^d+(s+1)^d = 1$ has only 2 solutions s in $\mathbb{F}_{2^n}$ (which are 0 and 1), that is, F is APN. □

Note that function $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \mapsto \frac{x^d+1}{(x+1)^d}$ is invariant under the transformation $x \mapsto x^{-1}$. Note also that instead of $s = \frac{x}{x+1}$, we could take $s = \frac{x}{x+1} + 1 = \frac{1}{x+1}$.

Theorem 4.1 can then be revisited as follows: we use the facts that if a function is 2-to-1 over some set, then it is at most 2-to-1 over any subset, and that the expression of $\frac{x^d+1}{(x+1)^d}$ is simplified when $x \in G_{e_j}$, because $x^{d-2^j} = 1$

implies $\frac{x^d+1}{(x+1)^d} = \frac{x^{2^j}+1}{(x+1)^d} = \frac{(x+1)^{2^j}}{(x+1)^d} = \frac{1}{(x+1)^{d-2^j}}$. The nice thing here is that we obtain an expression with the same exponent $d - 2^j$ as in the definition of G_{e_j} and this is what leads to the Sidon-sum-free property.

4.2 On the relationship between APN exponents and Dickson polynomials

Recall that, for every positive integer d, functions $x^d + (x+1)^d$ and $x^2 + x$ being invariant by the translation $x \mapsto x + 1$ and the latter one being 2-to-1, $x^d + (x+1)^d$ equals $\phi_d(x^2 + x)$ for some polynomial ϕ_d and $F(x) = x^d$ is APN if and only if function ϕ_d is injective over the hyperplane $H = \{x^2 + x; x \in \mathbb{F}_{2^n}\} = \{y \in \mathbb{F}_{2^n}; tr_n(y) = 0\}$, where $tr_n(x) = x + x^2 + \cdots + x^{2^{n-1}}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. This polynomial ϕ_d is called the *Reversed Dickson polynomial* [8] and equals $D_d(1, X)$ (see e.g. [8]), where D_d is classically defined by $D_d(X + Y, XY) = X^d + Y^d$.

Similarly, functions $\frac{x^d+1}{(x+1)^d}$ and $x + x^{-1}$ over $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ being invariant under the transformation $x \mapsto x^{-1}$ and the latter one being 2-to-1, $\frac{x^d+1}{(x+1)^d}$ equals $\psi_d(x + x^{-1})$ for some function ψ_d, which is here characterized by $(\psi_d(y))^2 = \frac{D_d(y,1)}{y^d}$, since $\left(\frac{x^d+1}{(x+1)^d}\right)^2 = \frac{x^d+x^{-d}}{(x+x^{-1})^d}$. According to Proposition 4.7, function F is then APN if and only if ψ_d is injective over $\{x + x^{-1}; x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\}$, that is, over $\{y \in \mathbb{F}^*_{2^n}; tr_n(y^{-1}) = 0\}$ and does not take value 1. Note that $\frac{D_d(y^{-1},1)}{(y^{-1})^d} = y^d D_d(y^{-1}, 1)$ equals the value at y of the reciprocal polynomial of $D_d(X, 1)$. Hence:

Proposition 4.8 *For every positive integers n and d, function $F(x) = x^d$ is APN if and only if the reciprocal polynomial $\widetilde{D_d(X,1)} = X^d D_d(X^{-1}, 1)$ of the Dickson polynomial $D_d(X, 1)$ is injective and does not take value 1 over $H^* = \{y \in \mathbb{F}^*_{2^n}; tr_n(y) = 0\}$.*

We have seen that, for $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, if $s = \frac{x}{x+1}$, that is, $x = \frac{s}{s+1}$ or $s = \frac{1}{x+1}$, that is, $x = \frac{s+1}{s}$, we have $\frac{x^d+1}{(x+1)^d} = s^d + (s+1)^d$. We have then $x + x^{-1} = \frac{s+1}{s} + \frac{s}{s+1} = \frac{1}{s^2+s}$ and therefore $\frac{x^d+1}{(x+1)^d} = \psi_d(x + x^{-1}) = \psi_d\left(\frac{1}{s^2+s}\right) = s^d + (s+1)^d = \phi_d(s^2 + s)$. Hence, for every $z \in H^*$, $\phi_d(z) = \psi_d(z^{-1})$ and squaring gives $(\phi_d(z))^2 = \widetilde{D_d}(z, 1)$. In other words, the squared Reversed Dickson polynomial and the reciprocal of Dickson polynomial of a same index take the same value over H and then, given their common degree, are equal to each other (this can also be easily seen as a consequence of the classical recurrence relations satisfied by these two polynomials [8]). We have then:

Proposition 4.9 *For every positive integer d, the squared Reversed Dickson polynomial of index d (equal to the Reversed Dickson polynomial of index $2d$) and the reciprocal of Dickson polynomial of index d are equal*[1]*. For every $z \neq 0$ such that $tr_1^n(z) = 0$, we have then $(\phi_d(z))^2 = \widetilde{D_d}(z, 1)$, where $\widetilde{D_d}$ is the reciprocal*

[1] Xiang-dong Hou [7], informed of this property by the authors, has observed that it can be generalized to any characteristic: $X^d D_d(\frac{1}{X} - 2, 1) = D_{2d}(1, X)$.

polynomial of the Dickson polynomial D_d of degree d. In particular, we have:

$$x^d + (x+1)^d = \left(\widetilde{D_d}(x^2+x,1)\right)^{2^{n-1}} .$$

This property allows to deduce the expression of Dickson polynomials with so-called Gold indices: for every integer i, we have $D_{2^i+1}(X,1) = X^{2^i+1} + \sum_{j=1}^{i} X^{2^i+1-2^j}$. Indeed, $x^{2^i+1} + (x+1)^{2^i+1} = x^{2^i} + x + 1 = 1 + \sum_{j=0}^{i-1}(x^2+x)^{2^j}$ and therefore $\widetilde{D_{2^i+1}}(X^2+X,1) = 1 + \sum_{j=1}^{i}(x^2+x)^{2^j}$, $\widetilde{D_{2^i+1}}(X,1) = 1 + \sum_{j=1}^{i} X^{2^j}$. The values of $D_{2^i+1}(X,1)$ and $D_{2^i-1}(X,1)$ (which are related by $D_{2^i-1}(X,1) + D_{2^i+1}(X,1) = X^{2^i+1}$) are already known from [5], but Proposition 4.9 also allows to obtain the explicit expressions of other Dickson polynomials; for instance with so-called Kasami indices:

Corollary 4.10 *For every integer i we have:*

$$D_{4^i-2^i+1}(X,1) = X^{4^i-2^i+1} + X^{4^i+2^i+1}\left(\sum_{j=1}^{i} X^{-2^j}\right)^{2^i+1} .$$

Proof. For every $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, we have (as already observed and used by Dobbertin):

$$\begin{aligned} x^{4^i-2^i+1} + (x+1)^{4^i-2^i+1} &= \frac{x^{4^i+1}(x+1)^{2^i} + (x+1)^{4^i+1}x^{2^i}}{(x^2+x)^{2^i}} \\ &= \frac{x^{4^i+1} + x^{4^i+2^i} + x^{2^i+1} + x^{2^i}}{(x^2+x)^{2^i}} \\ &= 1 + \frac{(x^{2^i}+x)^{2^i+1}}{(x^2+x)^{2^i}} \\ &= 1 + \frac{\left(\sum_{j=0}^{i-1}(x^2+x)^{2^j}\right)^{2^i+1}}{(x^2+x)^{2^i}}, \end{aligned}$$

and therefore, after squaring and denoting $X = x^2 + x$, we obtain:

$$\widetilde{D_{4^i-2^i+1}}(X,1) = 1 + \frac{\left(\sum_{j=1}^{i} X^{2^j}\right)^{2^i+1}}{X^{2^{i+1}}},$$

and then:

$$D_{4^i-2^i+1}(X,1) = X^{4^i-2^i+1} + X^{4^i+2^i+1}\left(\sum_{j=1}^{i} X^{-2^j}\right)^{2^i+1} .$$

This completes the proof. □

Of course we can deduce $D_{4^i+2^i+1}(X,1)$ thanks to the relation $D_{4^i-2^i+1}(X,1) + D_{4^i+2^i+1}(X,1) = D_{2^i}(X,1)D_{4^i+1}(X,1) = X^{2^i}D_{4^i+1}(X,1)$.

The same method applies more generally to $D_{2^j-2^i+1}$ but without anymore the nice factorization above.

Remark 4.11 *The Müller-Cohen-Matthews (MCM) polynomial (see [5]) equals* $\sum_{i=0}^{k-1} X^{(2^k+1)2^i-2^k}$ *and is a permutation polynomial when* $gcd(k,n)=1$ *and* k *is odd. Note that it equals* $\frac{\phi(X^{2^k+1})}{X^{2^k}}$, *where* $\phi(X)=\sum_{i=0}^{k-1} X^{2^i} = 1+\left(\widetilde{D_{2^k+1}}(X,1)\right)^{2^{n-1}}$.

5 Experimental Results

5.1 Sidon and sum-free conditions

Hans Dobbertin and Anne Canteaut have checked by computer investigation that no unclassified APN exponent exists for $n \leq 26$. By unclassified APN exponent, we mean an APN exponent not equal to a Gold, Kasami, Dobbertin, Welch, Niho or Inverse APN exponent, with n odd in the three latter cases, nor to its inverse mod 2^n-1 when it is co-prime with 2^n-1 (that is, when n is odd), nor to these exponents multiplied by powers of 2 and reduced modulo 2^n-1.

Yves Edel checked the same for $n \leq 34$ and $n = 36, 38, 40, 42$. The main idea for his computer investigation was to consider all the elements in $\mathbb{Z}/(2^n-1)\mathbb{Z}$, discard (because of Dobbertin's observation recalled in introduction) all those which are not co-prime with 2^n-1 for n odd and do not have gcd equal to 3 with 2^n-1 for n even, and discard (because the restriction to a subfield of an APN power function is an APN power function) all the remaining exponents whose reduction mod 2^r-1 is not an APN exponent in $\mathbb{F}_{2^r}$ for some divisor r of n. Since the checking that no unclassified APN exponent exists had been already done previously for r, the condition "is not an APN exponent in $\mathbb{F}_{2^r}$" could be replaced by "is not a known APN exponent in $\mathbb{F}_{2^r}$". Then, after discarding all known APN exponents in $\mathbb{F}_{2^n}$, the remaining exponents were investigated as possibly new APN exponents; they were gathered in cyclotomic classes and the APNness of one member of each class was investigated. No unclassified APN exponent could be found. Note that in the rest of the paper, when discussing the subfield condition, we mean the condition as implemented by Yves Edel in his investigation.

In this section, we concentrate on utilizing the same method as well as our newly developed Sidon and sum-free conditions in order to derive the number of possibly new APN exponents to test, and to see if the Sidon and sum-free conditions contribute to reducing this number. Note that we use acronym S for Sidon condition, SF for sum-free condition, and SSF for Sidon-sum-free condition. We shall call "S values" (resp. SF, SSF values) those divisors e of 2^n-1 such that $G_e = \{x \in \mathbb{F}_{2^n}^*; x^e = 1\}$ satisfies S (resp. SF, SSF).

We propose here two techniques; the first one has high computational complexity but low memory complexity and the second one has low computational complexity but high memory complexity. A trade-off can be considered with respect to the available resources. In both techniques, we use a result from [4]: for every divisor e of 2^n-1, G_e is a Sidon (resp. a sum-free) set if and only if, for every $u \in \mathbb{F}_{2^n}^*$ (resp. for $u=1$), the polynomial $(X+1)^e+u$ has at most two zeros in G_e (resp. has no zero in G_e).

In the first technique, to determine whether a value e is Sidon (resp. sum-free), we visit all the elements u of $\mathbb{F}_{2^n}^*$ and for each of them we visit all x of G_e (that is, all those powers of a primitive element whose exponents are multiples of $\frac{2^n-1}{e}$) and we:

1. Calculate $(x+1)^e + u$.
2. Increment a counter for value u when $(x+1)^e + u = 0$.
3. Keep e as Sidon (S) if for no value of u, the counter reached more than 2 and as sum-free (SF) if, for $u = 1$, the counter never reached more than 0.

This gives computational complexity equal to $2^n e$. From the memory perspective, at any time we are required only to keep two counters (one for S and one for SF).

For the second technique, we visit all the elements x of G_e (that is, again, all those powers of a primitive element whose exponents are multiples of $\frac{2^n-1}{e}$) and for each, we:

1. Calculate $(x+1)^e$.
2. Increment a counter in a table for value $(x+1)^e$.
3. Keep e as Sidon (S) if we never reached more than 2 in the table and as sum-free (SF) if, for value 1, we never reached more than 0.

This technique gives computational complexity of e and memory complexity of 2^n. Since we require 2 bits to store the value 2 in memory, in total we need up to 2^{n+1} bits.

We show the results for $n \in [3, 31]$ in Tables 3 and 4. Note that sum-free condition is somewhat more discriminating and enables us to reduce more values e than the Sidon condition.

Calculating the SSF conditions as we propose here is efficient only for relatively small values of n or of e or if a value e is not SSF (since then we stop the search relatively fast). In the cases when a large value e is SSF and n is large, calculating SSF can become too expensive in time and space complexities. Consequently, we arrive to the situation that checking SSF is more expensive than checking if a value d is a new APN exponent. To circumvent that problem, for larger values of n, we do not calculate SSF values exactly: we call *Approximate SSF (ASSF)* those values e which are not shown "not SSF" by the results of Carlet and Mesnager given in [4]:

Definition 5.1 *The Approximate Sidon-sum-free (ASSF) set is the set consisting of the divisors e of $2^n - 1$ after discarding the following values:*

1. *$2^r - 1$ where $r \geq 2$ divides n.*
2. *$gcd(2^r + 1, 2^n - 1)$ where r is odd and n is even.*
3. *$gcd(2^r + 3, 2^n - 1)$ where $r \equiv 2 \bmod 3$ and n is a multiple of 3.*
4. *$gcd(2^r - 2^k + 1, 2^n - 1)$ where n, r and $k - 1$ have a common divisor larger than 1.*
5. *Every divisor of $2^n - 1$ which is a multiple of one of the values described in one of the items above.*

Analogous to the definition of ASSF set, we define the *Approximate Sidon* (AS) set and *Approximate sum-free* (ASF) set. More precisely, Approximate Sidon (AS) set is the set consisting of the divisors e of $2^n - 1$ after discarding the values from Definition 5.1, conditions 1 and 5. Approximate sum-free (ASF) set is the set consisting of the divisors e of $2^n - 1$ after discarding the values

Table 3: Divisors of $2^n - 1$ which are Sidon-sum-free, part I.

n	Specification	Values
3	S/SF/SSF	1
4	S	1, 3, 5
	SF	1, 5
	SSF	1, 5
5	S/SF/SSF	1
6	S	1, 3, 9
	SF	1
	SSF	1
7	S/SF/SSF	1
8	S	1, 3, 5, 17
	SF	1, 5, 17
	SSF	1, 5, 17
9	S/SF/SSF	1
10	S	1, 3, 11, 33
	SF	1, 11
	SSF	1, 11
11	S	1, 23
	SF	1, 23, 89
	SSF	1, 23
12	S	1, 3, 5, 9, 13, 39, 65
	SF	1, 5, 13, 65
	SSF	1, 5, 13, 65
13	S/SF/SSF	1
14	S	1, 3, 43, 129
	SF	1, 43
	SSF	1, 43
15	S	1, 151
	SF	1, 151
	SSF	1, 151
16	S	1, 3, 5, 17, 257
	SF	1, 5, 17, 257, 1 285
	SSF	1, 5, 17, 257
17	S/SF/SSF	1
18	S	1, 3, 9, 19, 27, 57, 171, 513
	SF	1, 19
	SSF	1, 19

Table 4: Divisors of $2^n - 1$ which are Sidon-sum-free, part II.

n	Specification	Values
19	S/SF/SSF	1
20	S	1, 3, 5, 11, 25, 33, 41, 55, 123, 205, 275, 1 025
	SF	1, 5, 11, 25, 41, 55, 205, 275, 451, 1 025, 2 255,
	SSF	1, 5, 11, 25, 41, 55, 205, 275, 1 025
21	S	1, 337
	SF	1, 337
	SSF	1, 337
22	S	1, 3, 23, 69, 683, 2 049
	SF	1, 23, 89, 683, 15 709
	SSF	1, 23, 683
23	S	1, 47
	SF	1, 47
	SSF	1, 47
24	S	1, 3, 5, 9, 13, 17, 39, 65, 221, 241, 723, 1 205, 4 097
	SF	1, 5, 13, 17, 65, 221, 241, 1 205, 4 097
	SSF	1, 5, 13, 17, 65, 221, 241, 1 205, 4 097
25	S	1, 601, 1 801
	SF	1, 601, 1 801
	SSF	1, 601, 1801
26	S	1, 3, 2 731, 8 193
	SF	1, 2 731
	SSF	1, 2 731
27	S/SF/SSF	1
28	S	1, 3, 5, 29, 43, 87, 113, 129, 145, 215, 339, 565, 1 247, 3 277, 16 385
	SF	1, 5, 29, 43, 113, 145, 215, 565, 1 247, 3 277, 4 859, 6 235, 16 385, 24 295
	SSF	1, 5, 29, 43, 113, 145, 215, 565, 1 247, 3 277, 16 385
29	S	1, 233, 1 103, 2 089
	SF	1, 233, 1 103, 2 089, 256 999
	SSF	1, 233, 1 103, 2 089
30	S	1, 3, 9, 11, 33, 99, 151, 331, 453, 993, 1 359, 1 661, 2 979, 3 641, 4 983, 10 923, 32 769
	SF	1, 11, 151, 331, 1 661, 3 641
	SSF	1, 11, 151, 331, 1 661, 3 641
31	S/SF/SSF	1

obtained from Definition 5.1, conditions 2, 3, 4, and 5. Due to the large number of possible AS, ASF, ASSF values for n large, we give tables with results up to $n = 40$ in Appendix A, Tables 6 until 10.

Remark 5.2 *Note that all the SSF values belong to the set of Approximate SSF values, but this set possibly contains more values.*
By comparing the results from Tables 3 and 4 with those from Tables 6 until 10 we see there are only a few values of n where SSF and ASSF sets are not the same. This does not mean necessarily that using ASSF for larger n does not weaken the techniques.

Remark 5.3 *It is possible to improve the computation speed for calculating SSF set by considering the ASSF set: first, we calculate the ASSF set and then we check if all those values are indeed SSF values. Trivially, we can exclude values 1 from the check (since we know that it is always SSF) and $2^n - 1$ since we know it is never SSF.*

Remark 5.4 *When $2^n - 1$ is a Mersenne prime then there is no need to check SSF since we know value 1 is always SSF and there is no other strict divisor of $2^n - 1$.*

5.2 Calculating the number of possibly new APN exponents

In this section, we employ all constraints on the possibly new APN exponents d in order to investigate the computational effort needed to find new APN exponents or discard all possible values d for a certain value of n. We start by recalling all the conditions a value d needs to fulfill to be a possibly new APN exponent. We list the conditions in the order we apply them.

1. Remove any value d such that $gcd(d, 2^n - 1) \neq 1$ if n is odd and $gcd(d, 2^n - 1) \neq 3$ if n is even.

2. Remove any value d if it is already a known APN exponent.

3. If n is even, keep only one representative of a cyclotomic class with d being an element. Keep the minimal representative of a cyclotomic class. If n is odd, keep only one representative of cyclotomic classes with d and its inverse being the elements. Keep the minimal representative of both cyclotomic classes.

4. Remove any value d such that $gcd(d, 2^r - 1)$ is not an APN exponent in $\mathbb{F}_{2^r}$.

5. Remove any value d such that $gcd(d - 2^j, 2^n - 1)$ is not an SSF value, for some j. If n is too large, replace SSF by ASSF.

6. Remove any value d such that there exists a divisor λ of $2^n - 1$ such that $\binom{\lambda+1}{2} > 2^n - 1$ and there exists $j = 1, \dots, n-1$ such that λ divides $d - 2^j$ (see Remark 4.6).

Remark 5.5 *Note that if n is a prime, then the subfield condition is useless since there are no subfields to explore.*

Table 5: Number of possibly new APN exponents, the total number of values to consider for a certain n equals $2^n - 2$.

n	$gcd(d, 2^n - 1)$	Not known APN	Cyclotomic rep.	Subfield	SSF
3	6	3	1	1	0
4	4	0	0	0	0
5	30	5	1	1	0
6	12	6	1	0	0
7	126	49	4	4	3
8	64	40	5	5	4
9	432	315	19	6	4
10	300	260	26	21	21
11	1 936	1 683	78	78	66
12	576	540	45	21	21
13	8 190	7 839	302	302	301
14	5 292	5 222	373	226	226
15	27 000	26 685	893	365	365
16	16 384	16 272	1 017	377	370
17	131 070	130 475	3 838	3 838	3 837
18	46 656	46 566	2 587	697	697
19	524 286	523 545	13 778	13 778	13 777
20	240 000	239 840	11 992	1 592	1 512
21	1 778 112	1 777 545	42 326	12 923	12 923
22	1 320 352	1 320 154	60 007	7 834	7 824
23	8 210 080	8 208 999	178 458	178 458	178 434
24	2 211 840	2 211 672	92 153	2 153	2 135
25	32 400 000	32 398 875	647 981	539 979	539 966
26	22 358 700	22 358 414	859 939	36 844	36 844
27	113 467 392	113 466 339	2 101 232	569 069	569 010
28	66 382 848	66 382 540	2 370 805	31 349	31 127
29	533 826 432	533 824 721	9 203 878	9 203 878	9 202 166
30	178 200 000	178 199 760	5 939 992	11 212	11 212
31	2 147 483 646	2 147 481 693	34 636 802	34 636 802	34 636 801

Remark 5.6 *Since the SSF condition works for all values of n where $2^n - 1$ is not a Mersenne prime and subfield condition works for all values where n is not prime, we consider SSF condition to be a more general one since Mersenne primes are rarer than primes.*

In Table 5, we give results for the number of values d one needs to examine in order to look for new APN exponents. We note that this list serves only the illustrative purpose how SSF constraint reduces the number of values to check. Previous results by Y. Edel [9] show that there are no new APN exponents for those values of n. We can observe as the values of n become larger and when $2^n - 1$ has many divisors, SSF condition is able to discriminate more values. This gives hope that for even higher values of n, SSF would be more useful and significantly reduce the number of values d to test. This could be especially true for cases when n is prime but $2^n - 1$ has many divisors (e.g. $n = 29$).

6 More properties of APN exponents

In this section, we give more results on APN exponents, which are not so nice to state as in Section 4, but may however be useful for future works.

6.1 Other necessary conditions for an exponent to be APN

Proposition 6.1 *For every positive integers n and d and for every integer j such that $0 \leq j \leq n-1$, let $f_j = gcd(d+2^j, 2^n-1)$. Consider the multiplicative group $G_{f_j} = \{x \in \mathbb{F}_{2^n}^*; x^{d+2^j} = 1\} = \{x \in \mathbb{F}_{2^n}^*; x^{f_j} = 1\}$. If function $F(x) = x^d$ is APN over $\mathbb{F}_{2^n}$, then, for every $j, k \in \mathbb{Z}/n\mathbb{Z}$ and for every elements $x \in G_{f_j} \setminus \{1\}$, $x' \in G_{f_k} \setminus \{1\}$ satisfying $x^{2^j}(x+1)^{d-2^j} = {x'}^{2^k}(x'+1)^{d-2^k}$, we have $x' = x$ or $x' = x^{-1}$.*

Proof. Writing again $x = \frac{s}{s+1}$, $s = \frac{x}{x+1}$, the identity $x^{d+2^j} = 1$ implies $s^{d+2^j} + (s+1)^{d+2^j} = 0$, that is, $s^{d+2^j} + (s+1)^d(s^{2^j}+1) = 0$, that is, $s^d + (s+1)^d = \frac{(s+1)^d}{s^{2^j}} = \frac{1}{x^{2^j}(x+1)^{d-2^j}}$. Hence, if F is APN, every elements $x \in G_{f_j} \setminus \{1\}$, $x' \in G_{f_k} \setminus \{1\}$ such that $\frac{1}{x^{2^j}(x+1)^{d-2^j}} = \frac{1}{{x'}^{2^k}(x'+1)^{d-2^k}}$, or equivalently $x^{2^j}(x+1)^{d-2^j} = {x'}^{2^k}(x'+1)^{d-2^k}$, are such that $x' = x$ or $x' = x^{-1}$. □

Remark 6.2 *The interpretation of Subsection 4.1 is in the present case as follows: if $x^{d+2^j} = 1$ then $\frac{x^d+1}{(x+1)^d} = \frac{x^{-2^j}+1}{(x+1)^d} = \frac{x^{2^j}+1}{x^{2^j}(x+1)^d} = \frac{1}{x^{2^j}(x+1)^{d-2^j}}$.*

Other similar properties can be derived but they are more complex (and give then less simple ways of discriminating APN exponents).
For instance, for every integers k, j, d such that $0 \leq k < j \leq n-1$, let $e_{k,j} = gcd(d-2^k-2^j, 2^n-1)$, and let $G_{e_{k,j}}$ be the multiplicative subgroup $\{x \in \mathbb{F}_{2^n}^*; x^{d-2^k-2^j} = 1\} = \{x \in \mathbb{F}_{2^n}^*; x^{e_{k,j}} = 1\}$ of order $e_{k,j}$. If function $F(x) = x^d$ is APN over $\mathbb{F}_{2^n}$, then, if $x, y \in G_{e_{k,j}} \setminus \{1\}$, $x \neq y$ and $x \neq y^{-1}$, then we have $\frac{x^d+x^{d-2^k-2^j}+x^{d-2^k+2^j}+x^{d-2^j+2^k}}{(x+1)^d} \neq 1$ and $\frac{x^d+x^{d-2^k-2^j}+x^{d-2^k+2^j}+x^{d-2^j+2^k}}{(x+1)^d} \neq \frac{y^d+y^{d-2^k-2^j}+y^{d-2^k+2^j}+y^{d-2^j+2^k}}{(y+1)^d}$. Indeed, still introducing the unique $s \in \mathbb{F}_{2^n}^* \setminus \{1\}$ such that $x = \frac{s}{s+1}$, we have $s^{d-2^k-2^j} + (s+1)^{d-2^k-2^j} = 0$, and multiplying by $(s+1)^{2^k+2^j}$ we obtain $s^d + (s+1)^d = s^{d-2^k-2^j} + s^{d-2^k} + s^{d-2^j} = \frac{x^{d-2^k-2^j}(x+1)^{2^k+2^j}+x^{d-2^k}(x+1)^{2^j}+x^{d-2^j}(x+1)^{2^k}}{(x+1)^d} = \frac{x^d+x^{d-2^k-2^j}+x^{d-2^k+2^j}+x^{d-2^j+2^k}}{(x+1)^d}$.
The rest of the proof is similar to above.
More generally, let k be any integer and let $x^k = 1$, $x \neq 1$, $x = \frac{s}{s+1}$, we have $s^k + (s+1)^k = 0$ and therefore, by multiplication by $(s+1)^{d-k}$: $s^d + (s+1)^d = \sum_{j=0}^{d-k-1} \binom{d-k}{j} s^{j+k}$, which implies that $x \neq 1$, $y \neq 1$, $x \neq y, x \neq \frac{1}{y}$ and $x^k = y^k = 1$ imply $\sum_{j=0}^{d-k-1} \binom{d-k}{j} \frac{x^j}{(x+1)^{j+k}} \neq 1$ and $\sum_{j=0}^{d-k-1} \binom{d-k}{j} \frac{x^j}{(x+1)^{j+k}} \neq \sum_{j=0}^{d-k-1} \binom{d-k}{j} \frac{y^j}{(y+1)^{j+k}}$.

7 Conclusions

In this paper, we presented necessary conditions related to Sidon sets and sum-free sets for an element $d \in \mathbb{Z}/(2^n-1)\mathbb{Z}$ to be an APN exponent in $\mathbb{F}_{2^n}$ (we call these conditions the Sidon-sum-free, in brief SSF, conditions). This makes a junction between vectorial Boolean functions for cryptography and additive combinatorics. We also gave a new characterization of such exponents, which can be nicely expressed by means of Dickson polynomials, and we proved that Dickson polynomials in characteristic 2 and Reversed Dickson polynomials of the same index are reciprocal of each others, up to squaring the latter. Since Reversed Dickson polynomials are easier to calculate than Dickson polynomials, this allows simplifying the determination of the expressions of the latter (we gave two examples of such determinations). The new conditions related to Sidon sets and sum-free sets in turn enable us to speed up the search for new APN exponents, i.e., to discriminate even more what could be possible new APN exponents. Although our experimental results show the improvements are relatively small, they are nevertheless important from both theoretical and practical perspective. We observe only small improvements with our new SSF condition since we apply it after all the other known conditions and we notice that the Edel's subfield condition removes many of the same exponents as the SSF condition. Finally, our results suggest that SSF condition should become more discriminative as we increase the value n and especially for those values where n is prime and $2^n - 1$ has many divisors.

In future work, we plan to extend our research for new APN exponents for higher values of n, as well as investigate how to calculate SSF values more efficiently. Finally, the discrepancy between the obtained SSF values and the super-class (more easy to determine) of ASSF values points us that additional conditions to recognize ASSF values more precisely should be found.

Acknowledgment

We deeply thank Yves Edel for his very useful indications on the investigation of APN exponents he made (whose results were not published but were reported by Gohar Kyureghyan in [9]). We thank Sihem Mesnager for useful observations and Wolfgang Schmid and Alain Plagne for informations on Sidon sets and on sum-free sets.

References

[1] L. Babai and V. T. Sós. Sidon Sets in Groups and Induced Subgraphs of Cayley Graphs. *European Journal of Combinatorics* Volume 6, Issue 2, pp. 101-114, 1985.

[2] T. Beth and C. Ding, On almost perfect nonlinear permutations. *Proceedings of Eurocrypt' 93, Lecture Notes in Computer Science* 765, pp. 65-76, 1994.

[3] C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 398-469, 2010.

[4] C. Carlet and S. Mesnager. On those subgroups of $\mathbb{F}_{2^n}^*$ which are Sidon sets and/or sum-free sets. Preprint, 2017.

[5] S. D. Cohen and R. W. Matthews. A class of exceptional polynomials. *Trans. Amer. Math. Soc.* 345, pp. 897-909, 1994.

[6] B. Green, I.Z. Ruzsa. Sum-free sets in Abelian groups. *Isr. J. Math.* 147, pp. 157-288, 2005.

[7] X. Hou. Private communication, June 2017.

[8] X. Hou, G. L. Mullen, J. A. Sellers and J. Yucas. Reversed Dickson polynomials over finite fields, *Finite Fields Appl.* 15, pp. 748 - 773, 2009.

[9] G. Kyureghyan. Special Mappings of Finite Fields. *Finite Fields and Their Applications*, Radon Series on Computational and applied mathematics, pp. 117-144, 2013.

[10] K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.

[11] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. *Proceedings of CRYPT0' 92, Lecture Notes in Computer Science* 740, pp. 566-574, 1993.

[12] T. Tao and V. Vu. Sum-free sets in groups: a survey. ArXiv preprint arXiv:1603.03071, 2016 - arxiv.org

A Additional computational results

Tables 6 until 10 give results for AS, ASF, and ASSF sets for values n up to 40.

Table 6: ASSF calculations, part I.

n	Specification	Values
3	AS	1
	ASF	1
	ASSF	1
4	AS	1, 3, 5
	ASF	1, 5
	ASSF	1, 5
5	AS	1
	ASF	1
	ASSF	1
6	AS	1, 3, 9
	ASF	1
	ASSF	1
7	AS	1
	ASF	1
	ASSF	1
8	AS	1, 3, 5, 17, 51, 85
	ASF	1, 5, 17, 85
	ASSF	1, 5, 17, 85
9	AS	1, 73
	ASF	1, 73
	ASSF	1, 73
10	AS	1, 3, 11, 33
	ASF	1, 11
	ASSF	1, 11
11	AS	1, 23, 89
	ASF	1, 23, 89
	ASSF	1, 23, 89
12	AS	1, 3, 5, 9, 13, 39, 65, 117
	ASF	1, 5, 13, 65
	ASSF	1, 5, 13, 65
13	AS	1
	ASF	1
	ASSF	1
14	AS	1, 3, 43, 129
	ASF	1, 43
	ASSF	1, 43
15	AS	1, 151
	ASF	1, 151
	ASSF	1, 151

Table 7: ASSF calculations, part II.

n	Specification	Values
16	AS	1, 3, 5, 17, 51, 85, 257, 771, 1 285, 4 369, 13 107, 21 845
	ASF	1, 5, 17, 85, 257, 1 285, 4 369, 21 845
	ASSF	1, 5, 17, 85, 257, 1 285, 4 369, 21 845
17	AS	1
	ASF	1
	ASSF	1
18	AS	1, 3, 9, 19, 27, 57, 73, 171, 219, 513, 657, 1 387, 1 971, 4 161, 12 483, 37 449
	ASF	1, 19, 73, 1 387
	ASSF	1, 19, 73, 1 387
19	AS	1
	ASF	1
	ASSF	1
20	AS	1, 3, 5, 11, 25, 33, 41, 55, 123, 205, 275, 451, 1 025, 1 353, 2 255, 11 275
	ASF	1, 5, 11, 25, 41, 55, 205, 275, 451, 1 025, 2 255, 11 275
	ASSF	1, 5, 11, 25, 41, 55, 205, 275, 451, 1 025, 2 255, 11 275
21	AS	1, 337
	ASF	1, 337
	ASSF	1, 337
22	AS	1, 3, 23, 69, 89, 267, 683, 2 049, 15 709, 47 127, 60 787, 182 361
	ASF	1, 23, 89, 683, 15 709, 60 787
	ASSF	1, 23, 89, 683, 15 709, 60 787
23	AS	1, 47, 178 481
	ASF	1, 47, 178 481
	ASSF	1, 47, 178 481
24	AS	1, 3, 5, 9, 13, 17, 39, 51, 65, 85, 117, 153, 221, 241, 663, 723, 1 105, 1 205, 1 989, 2 169, 3 133, 4 097, 9 399, 12 291, 15 665, 20 485, 28 197, 36 873, 53 261, 159 783, 266 305, 479 349
	ASF	1, 5, 13, 17, 65, 85, 221, 241, 1 105, 1 205, 3 133, 4 097, 15 665, 20 485, 53 261, 266 305
	ASSF	1, 5, 13, 17, 65, 85, 221, 241, 1 105, 1 205, 3 133, 40 97, 15 665, 20 485, 53 261, 266 305
25	AS	1, 601, 1 801, 1 082 401
	ASF	1, 601, 1 801, 1 082 401
	ASSF	1, 601, 1 801, 1 082 401
26	AS	1, 3, 2 731, 8 193
	ASF	1, 2 731
	ASSF	1, 2 731
27	AS	1, 73, 262 657, 19 173 961
	ASF	1, 73, 262 657, 19 173 961
	ASSF	1, 73, 262 657, 19 173 961

Table 8: ASSF calculations, part III.

n	Specification	Values
28	AS	1, 3, 5, 29, 43, 87, 113, 129, 145, 215, 339, 565, 1 247, 3 277, 3 741, 4 859, 6 235, 9 831, 14 577, 16 385, 24 295, 140 911, 422 733, 704 555
	ASF	1, 5, 29, 43, 113, 145, 215, 565, 1 247, 3 277, 4 859, 6 235, 16 385, 24 295, 140 911, 704 555
	ASSF	1, 5, 29, 43, 113, 145, 215, 565, 1 247, 3 277, 4 859, 6 235, 16 385, 24 295, 140 911, 704 555
29	AS	1, 233, 1 103, 2 089, 256 999, 486 737, 2 304 167
	ASF	1, 233, 1 103, 2 089, 256 999, 486 737, 2 304 167
	ASSF	1, 233, 1 103, 2 089, 256 999, 486 737, 2 304 167
30	AS	1, 3, 9, 11, 33, 99, 151, 331, 453, 993, 1 359, 1 661, 2 979, 3 641, 4 983, 10 923, 14 949, 32 769, 49 981, 149 943, 449 829, 549 791, 1 649 373, 4 948 119
	ASF	1, 11, 151, 331, 1 661, 3 641, 49 981, 549 791
	ASSF	1, 11, 151, 331, 1 661, 3 641, 49 981, 549 791
31	AS	1
	ASF	1
	ASSF	1
32	AS	1, 3, 5, 17, 51, 85, 257, 771, 1 285, 4 369, 13 107, 21 845, 65 537, 196 611, 327 685, 1 114 129, 3 342 387, 5 570 645, 16 843 009, 50 529 027, 84 215 045, 286 331 153, 858 993 459, 1 431 655 765
	ASF	1, 5, 17, 85, 257, 1 285, 4 369, 21 845, 65 537, 327 685, 1 114 129, 5 570 645, 16 843 009, 84 215 045, 286 331 153, 1 431 655 765
	ASSF	1, 5, 17, 85, 257, 1 285, 4 369, 21 845, 65 537, 327 685, 1 114 129, 5 570 645, 16 843 009, 84 215 045, 286 331 153, 1 431 655 765
33	AS	1, 23, 89, 599 479, 13 788 017, 53 353 631
	ASF	1, 23, 89, 599 479, 13 788 017, 53 353 631
	ASSF	1, 23, 89, 599 479, 13 788 017, 53 353 631
34	AS	1, 3, 43 691, 131 073
	ASF	1, 43 691
	ASSF	1, 43 691
35	AS	1, 71, 122 921, 8 727 391
	ASF	1, 71, 122 921, 8 727 391
	ASSF	1, 71, 122 921, 8 727 391

Table 9: ASSF calculations, part IV.

n	Specification	Values
36	AS	1, 3, 5, 9, 13, 19, 27, 37, 39, 57, 65, 73, 95, 109, 111, 117, 171, 185, 219, 247, 327, 333, 351, 365, 481, 513, 545, 657, 703, 741, 949, 981, 999, 1 235, 1 387, 1 417, 1 443, 1 971, 2 071, 2 109, 2 223, 2 405, 2 701, 2 847, 2 943, 3 515, 4 033, 4 161, 4 251, 4 329, 4 745, 6 213, 6 327, 6 669, 6 935, 7 085, 7 957, 8 103, 8 541, 9 139, 10 355, 12 099, 12 483, 12 753, 12 987, 13 505, 18 031, 18 639, 18 981, 20 165, 23 871, 24 309, 25 623, 26 923, 27 417, 35 113, 36 297, 37 449, 38 259, 39 785, 45 695, 51 319, 52 429, 54 093, 55 917, 71 613, 72 927, 76 627, 80 769, 82 251, 90 155, 103 441, 105 339, 108 891, 134 615, 151 183, 153 957, 157 287, 162 279, 175 565, 214 839, 229 881, 242 307, 246 753, 256 595, 262 145, 294 409, 310 323, 316 017, 383 135, 453 549, 461 871, 471 861, 486 837, 517 205, 667 147, 689 643, 726 921, 755 915, 883 227, 930 969, 948 051, 996 151, 1 360 647, 1 385 613, 1 415 583, 1 472 045, 1 965 379, 2 001 441, 2 068 929, 2 649 681, 2 792 907, 2 988 453, 3 335 735, 3 827 317, 4 081 941, 4 980 755, 5 593 771, 5 896 137, 6 004 323, 7 949 043, 8 965 359, 9 826 895, 11 481 951, 16 781 313, 17 688 411, 18 012 969, 19 136 585, 26 896 077, 27 968 855, 34 445 853, 50 343 939, 53 065 233, 72 719 023, 103 337 559, 151 031 817, 218 157 069, 363 595 115, 654 471 207, 1 963 413 621
	ASF	1, 5, 13, 19, 37, 65, 73, 95, 109, 185, 247, 365, 481, 545, 703, 949, 1 235, 1 387, 1 417, 2 071, 2 405, 2 701, 3 515, 4 033, 4 745, 6 935, 7 085, 7 957, 9 139, 10 355, 13 505, 18 031, 20 165, 26 923, 35 113, 39 785, 45 695, 51 319, 52 429, 76 627, 90 155, 103 441, 134 615, 151 183, 175 565, 256 595, 262 145, 294 409, 383 135, 517 205, 667 147, 755 915, 996 151, 1 472 045, 1 965 379, 3 335 735, 3 827 317, 4980755, 5 593 771, 9 826 895, 19 136 585, 27 968 855, 72 719 023, 363 595 115
	ASSF	1, 5, 13, 19, 37, 65, 73, 95, 109, 185, 247, 365, 481, 545, 703, 949, 1 235, 1 387, 1 417, 2 071, 2 405, 2 701, 3 515, 4 033, 4 745, 6 935, 7 085, 7 957, 9 139, 10 355, 13 505, 18 031, 20 165, 26 923, 35 113, 39 785, 45 695, 51 319, 52 429, 76 627, 90 155, 103 441, 134 615, 151 183, 175 565, 256 595, 262 145, 294 409, 383 135, 517 205, 667 147, 755 915, 996 151, 1 472 045, 1 965 379, 3 335 735, 3 827 317, 4 980 755, 5 593 771, 9 826 895, 19 136 585, 27 968 855, 72 719 023, 363 595 115
37	AS	1, 223, 616 318 177
	ASF	1, 223, 616 318 177
	ASSF	1, 223, 616 318 177

Table 10: ASSF calculations, part V.

n	Specification	Values
38	AS	1, 3, 174 763, 524 289
	ASF	1, 174 763
	ASSF	1, 174 763
39	AS	1, 79, 121 369, 9 588 151
	ASF	1, 79, 121 369, 9 588 151
	ASSF	1, 79, 121 369, 9 588 151
40	AS	1, 3, 5, 11, 17, 25, 33, 41, 51, 55, 85, 123, 187, 205, 275, 425, 451, 561, 697, 935, 1 025, 1 353, 2 091, 2 255, 3 485, 4 675, 7 667, 11 275, 17 425, 23 001, 38 335, 61 681, 185 043, 191 675, 308 405, 678 491, 1 048 577, 1 542 025, 2 035 473, 2 528 921, 3 145 731, 3 392 455, 5 242 885, 7 586 763, 11 534 347, 12 644 605, 16 962 275, 26 214 425, 27 818 131, 34 603 041, 42 991 657, 57 671 735, 63 223 025, 83 454 393, 128 974 971, 139 090 655, 214 958 285, 288 358 675, 472 908 227, 695 453 275, 1 074 791 425, 1 418 724 681, 2 364 541 135, 11 822 705 675
	ASF	1, 5, 11, 17, 25, 41, 55, 85, 187, 205, 275, 425, 451, 697, 935, 1 025, 2 255, 3 485, 4 675, 7 667, 11 275, 17 425, 38 335, 61 681, 191 675, 308 405, 678 491, 1 048 577, 1 542 025, 2 528 921, 3 392 455, 5 242 885, 11 534 347, 12 644 605, 16 962 275, 26 214 425, 27 818 131, 42 991 657, 57 671 735, 63 223 025, 139 090 655, 214 958 285, 288 358 675, 472 908 227, 695 453 275, 1 074 791 425, 2 364 541 135, 11 822 705 675
	ASSF	1, 5, 11, 17, 25, 41, 55, 85, 187, 205, 275, 425, 451, 697, 935, 1 025, 2 255, 3 485, 4 675, 7 667, 11 275, 17 425, 38 335, 61 681, 191 675, 308 405, 678 491, 1 048 577, 1 542 025, 2 528 921, 3 392 455, 5 242 885, 11 534 347, 12 644 605, 16 962 275, 26 214 425, 27 818 131, 42 991 657, 57 671 735, 63 223 025, 139 090 655, 214 958 285, 288 358 675, 472 908 227, 695 453 275, 1 074 791 425, 2 364 541 135, 11 822 705 675