ON THE EXponents OF APN POWER FUNCTIONS AND SIDON SETS, SUM-FREE SETS, AND DICKSON POLYNOMIALS

CLAude CARLET
Department of informatics, University of Bergen
Norway and LAGA, University of Paris 8, France

STJEPAN PiceK*
Delft University of Technology, The Netherlands and LAGA
University of Paris 8, France

(Communicated by Sihem Mesnager)

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 what extent these new conditions may speed up the search for new APN exponents $d$. We summarize all the necessary conditions that an exponent must satisfy for having a chance of being an APN, including the new conditions presented in this work. Next, we give results up to $n = 48$, providing the number of exponents satisfying all the conditions for a function to be APN.

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 $\{y \in \mathbb{F}_2^n; \text{tr}_n(y) = 0\}$ 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

There is a significant number of works investigating APN Almost Perfect Nonlinear functions (see, e.g., [3]) and, in particular, APN power functions, i.e., functions of the form $F(x) = x^d$ where $d \in \mathbb{Z}/(2^n-1)\mathbb{Z}$. 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 $\left\{ \begin{array}{l} x + y + z + t = 0 \\ F(x) + F(y) + F(z) + F(t) = 0 \end{array} \right.$ has for only solutions quadruples $(x, y, z, t)$ whose elements are not all distinct (i.e., are pairwise equal).

While we know several exponent values $d$ that result in APN power functions (see Table 1), there has been no substantial progress (e.g., new exponent values) for a number of years. One of the core reasons for this lack of new results is the...
computational complexity required to test many large values $d$ in $\mathbb{F}_{2^n}$. While new APN functions would not have immediate use in cryptography (in cryptography, one commonly uses small functions, e.g., up to $n = 8$, making the results of a search with large $n$ less directly applicable), finding new APN exponents or confirming there are no new APN exponents for a certain value $n$ would significantly impact the APN research. Informally, we can divide the research on the new APN power functions into two directions.

1. **Reducing the number of possible APN exponents.** For a value $n$, there is a number of values (trivially, $2^n - 2$ values as we do not need to consider the exponent values 0 and $2^n - 1$) that are possible APN exponents. Thus, the goal is to efficiently recognize those values that will not result in an APN function.

2. **Speed-up the evaluation if a power function is APN.** This direction concentrates on actually checking if the equation $F(x) + F(x + a) = b$ has at most two solutions (thus, making the power function APN).

In this paper, we concentrate on the first direction. More precisely, 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 APN.

Recall that changing $d$ into one of its conjugates $2^jd$ corresponds to changing $F(x)$ into a linearly equivalent APN function, which preserves APNness. Given such $d$, the set of all the elements $2^jd$ (mod $2^n - 1$) equals by definition the cyclotomic class of 2 mod $2^n - 1$ containing $d$. The APN exponents then constitute 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, 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 book [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. What is more, $\gcd(d, 2^n - 1)$ equals 1 if and only if the function $F$ is a permutation. 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

| Functions | Exponents $d$ | Conditions |
|-----------|--------------|------------|
| Gold      | $2^i + 1$    | $\gcd(i, n) = 1$ |
| Kasami    | $2^{2i} - 2^i + 1$ | $\gcd(i, n) = 1$ |
| Welch     | $2^i + 3$    | $n = 2t + 1$ |
| Niho      | $2^t + 2^t - 1$, $t$ even | $n = 2t + 1$ |
|           | $2^t + 2^{3t+1} - 1$, $t$ odd |
| Inverse   | $2^{2t} - 1$ | $n = 2t + 1$ |
| Dobbertin | $2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$ | $n = 5t$ |
other property cannot be that \( \gcd(d, 2^n - 1) = 1 \) for every \( j = 0, \ldots, n-1 \). Note that for Gold and Kasami exponents, we use the notation \((n; i)\) to show all the values \( i \) such that \( \gcd(i, n) = 1 \) for a specific \( n \) that result in the APN exponent \( d \) fulfilling the condition \( \gcd(d - 2^j, 2^n - 1) = 1 \) for every \( j = 0, \ldots, n-1 \).

### Table 2. \( \gcd(d - 2^j, 2^n - 1) = 1 \) for every \( j = 0, \ldots, n-1 \) \( n; i \) such that \( i \leq n/2 \)

| Class name | Value |
|------------|-------|
| 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, 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, 7, 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) |
| 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 |

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 \( \gcd(d - 1, 2^n - 1) = 1 \) is true for any element in the cyclotomic class, or equivalently that \( \gcd(d - 2^j, 2^n - 1) = 1 \) for every \( j = 0, \ldots, n-1 \). We list in Table 2, for the (known) APN exponents \( d \) of Table 1 up to \( n = 31 \), when \( \gcd(d - 2^j, 2^n - 1) = 1 \) is true for every \( j = 0, \ldots, n-1 \). 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 \( \gcd(2^n-jd - 1, 2^n - 1) = \gcd(d - 2^j, 2^n - 1) \), and 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. Note that 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). The relationship we establish in this paper is different and gives more insight into APN exponents.
We study the consequences of searching for new APN exponents, which is a sensitive, open question on which the research is being stuck for almost 20 years. We do not find new APN exponents, but we show that 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 characteristic 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 EXONENTS 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 $F(x) = x^{2^t + 1}$, where $\gcd(i, n) = 1$, we have $\gcd(d - 1, 2^n - 1) = \gcd(2i, 2^n - 1) = 1$.

In the case of Kasami functions $F(x) = x^{2^{2^i} - 2^i + 1}$, 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 $F(x) = x^{2^i + 3}$, we have according to the Gauss theorem (which states that if $a$ divides $bc$ and is co-prime with $b$ then it divides $c$): $\gcd(d - 1, 2^n - 1) = \gcd(2^{t - 1} + 1, 2^{2^i + 1} - 1) = \frac{\gcd(2^{2t - 1} - 1, 2^{2^i + 1} - 1)}{\gcd(2^{2t - 1} - 1, 2^{2i + 1} - 1)} = 1$.

In the case of Niho functions:

$-F(x) = x^{2^t + 2^{t - 1} - 1}$, $t$ even, we have, applying the Euclidean algorithm: $\gcd(d - 1, 2^n - 1) = \gcd(2^{t^2} + 2^t - 2, 2^{2^t + 1} - 1) = \gcd(2 + 2^t - 2, 5 \cdot 2^{2^t + 1} + 11) = \gcd(2^2 \cdot 5 \cdot (2^t + 2^t - 2), 5 \cdot 2^{2^t + 1} - 11) = \gcd(5 \cdot 2^{2^t + 1} - 11, 31) = 1$, since 31 divides $2^{2t + 1} - 1$ if and only if $2t + 1 = 0 \mod 5$ and the only possibility for that $t = 2 \mod 5$, $\frac{t^2 + 1}{2} \equiv 1 \mod 5$ and $2^t + 2^{t/2} - 2 = 4 \not\equiv 0 \mod 31$.

$-F(x) = x^{2^t + 2^{t - 1} - 1}$, $t$ odd, we have $\gcd(d - 1, 2^n - 1) = \gcd(2^t + 2^t - 2, 2^{2t + 1} - 1) = \gcd(2^{t^2} + 2^t - 2, 2^t + 2^{t/2} - 3) = \gcd(2^t + 2^{t/2} - 3, 9 \cdot 2^{t/2} - 11) = \gcd(9 \cdot 2^{t/2} - 11, 31) = 1$, since, again, 31 divides $2^{2t + 1} - 1$ if and only if $2t + 1 = 0 \mod 5$ and the only possibility for that $t = 2 \mod 5$, $\frac{t^2 + 1}{2} \equiv 1 \mod 5$ and $2^t + 2^{t/2} - 2 = 4 \not\equiv 0 \mod 31$.

In the case of the APN Inverse function $F(x) = x^{2^{t - 1} - 1}$, we have, by the Euclidean algorithm:

$\gcd(d - 1, 2^n - 1) = \gcd(2^{2t - 1} - 1, 2^{2t + 1} - 1) = 2^{\gcd(2^{2 - 1} - 1, 2^{2t + 1} - 1)} - 1 = 1$.

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 $d - 1 = 2 \mod 3$).
Then \( \gcd(d - 1, 2^n - 1) = 1 \) in all cases. 

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

**Remark 1.** 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 permutation has the same number of fixed points as its compositional inverse.

3. **Sidon sets and sum-free sets**

In Section 2, we saw that the known APN exponents might have a property not covered by the Dobbertin observation (recalled in Section 1). We also saw in Section 1 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 this section, we show that every APN exponent (known or unknown) satisfies a property that 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 S. Sidon \(^1\). 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 2.** By definition, an \((n, n)\)-function \( F \) is APN if and only if its graph \( G_F = \{(x, F(x)) ; x \in \mathbb{F}_{2^n}\} \) is a Sidon set in \((\mathbb{F}_{2^n}, +)\). 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.** 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 3.2.** [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 P. Erdős.

\(^1\)His last name is often also spelled as Szidon.
Remark 4. 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 5. 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 $G \backslash S$. 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.

4. APN exponents, sidon sets, and sum-free sets

We now give the new property valid for all APN exponents 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 $e_j = \gcd(d - 2j, 2^n - 1) \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$, and let $G_{e_j}$ be the multiplicative subgroup 
\{ $x \in \mathbb{F}_{2^n} : x^{d-2j} = 1$ \} = \{ $x \in \mathbb{F}_{2^n} : x^j = 1$ \} 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 $(x + 1)^{d-2j} \neq (y + 1)^{d-2j}$.

**Proof.** Using the same idea as the one used by Dobbertin for showing the observation recalled in Section 1, for every $x \in G_{e_j} \backslash \{1\}$, we introduce the unique $s \in \mathbb{F}_{2^n} \backslash \{1\}$ such that $x = \frac{s}{s+1}$, that is, $s = \frac{x}{x+1}$. Then $x^{d-2j} = 1$ implies $s^{d-2j} + (s+1)^{d-2j} = 0$, which implies after multiplication by $s^{d-2j} + 1 = (s+1)^{d-2j}$ that $s^d + (s+1)^d = s^{d-2j} = (s+1)^{d-2j} = \frac{1}{(x+1)^{d-2j}}$. 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 $\frac{x}{x+1} + 1 = \frac{x-1}{x}$.

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 $x \rightarrow xt$, $y \rightarrow yt$, $z \rightarrow zt$ and dividing the equality by $t$, we obtain distinct elements $x, y, z$ of $G_{e_j} \backslash \{1\}$ such that $x + y + z = 1$. Making now the change of variable $y \rightarrow zy$, we obtain elements $x, y, z$ in $G_{e_j} \backslash \{1\}$ 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 $\frac{1}{(x+1)^{d-2j}} = \frac{1}{(y+1)^{d-2j}}$ 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 $s^d + (s+1)^d = \frac{1}{(x+1)^{d-2j}}$, a contradiction with the APNess 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 \(\frac{1}{(x+1)^{d-2^r}} = 1\) 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 6.** 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 \(\frac{x^d + 1}{(x+1)^d} = \frac{(x-1)^d + 1}{(x+1)^d}\), the condition “\(G_e\) 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 \(G_e\) satisfies \(x^d + 1 = (x + 1)^d\) since this equation in \(G_e\) is equivalent to \(x^{2^d} + 1 = (x + 1)^{2^d}\) which is always true, and this is why \(G_e\) plays an interesting role.

**Remark 7.** 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 \(G_1 = \{1\}\), \(G_3 = \mathbb{F}_2^*\) are Sidon sets (since they do not contain 4 distinct elements). But \(G_e\) is a sum-free set only for \(n\) odd, since \(\mathbb{F}_2^*\) is not sum-free.

**Remark 8.** 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 \(\gcd(d - 2^j, 2^n - 1)\) 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 9.** 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. The property of being a Sidon-sum-free set is rather restrictive, and this explains the observations made in Section 1.

**Remark 10.** We observed that, in characteristic 2, the size \(|S|\) of a Sidon-sum-free set \(S\) not containing 0 cannot be such that \((\frac{|S|+1}{2}) = \frac{|S|(|S|+1)}{2} > 2^n - 1\). We deduce then from the theorem that, if \(d\) is an APN exponent, then for every divisor \(\lambda\) of \(2^n - 1\) such that \((\frac{\lambda+1}{2}) > 2^n - 1\) and every \(j \in \mathbb{Z}/n\mathbb{Z}\), this number \(\lambda\) does not divide \(d - 2^j\). Take for instance \(n = 8\) and \(\lambda = \frac{2^8 - 1}{3} = 85\), we have \((\frac{\lambda+1}{2}) > 255\) 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 \(\lambda = \frac{2^8 - 1}{15} = 51\), we have \((\frac{\lambda+1}{2}) > 255\) 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 \(\lambda\), but for some larger values of \(n\), the number of possible \(\lambda\) 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 \(s^d + (s + 1)^d = \frac{1}{(x+1)^{d-2^r}}\). 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 1.** 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 $s^d + (s+1)^d = \frac{x^{d+1}+1}{(x+1)^d}$, and $F$ is APN if and only if the function $x \mapsto \frac{x^{d+1}+1}{(x+1)^d}$ 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 $x \mapsto \frac{x^{d+1}+1}{(x+1)^d}$ 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 $\mathbb{F}_2$ (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. \hfill \square

Note that function $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \mapsto \frac{x^{d+1}+1}{(x+1)^d}$ 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 2-to-1 over $\mathbb{F}_{2^n}$, is 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 since we have $x^2 + x \neq y^2 + y$ for every two inputs $x$ and $y$ such that $x + y \notin \mathbb{F}_2$ (or in other words, the function $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \mapsto x^2+x$ is injective), $x^d + (x+1)^d$ equals $\phi_d(x^2+x)$ for some polynomial $\phi_d$ and $F(x) = x^d$ is APN if and only if $\phi_d$ 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 $\phi_d$ 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 $\frac{x^{d+1}+1}{(x+1)^d}$ 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, $\frac{x^{d+1}+1}{(x+1)^d}$ equals $\psi_d(x + x^{-1})$ for some function $\psi_d$, which is here characterized by $(\psi_d(y))^2 = \frac{D_d(y, 1)}{y^d}$, since

$$\left(\frac{x^{d+1}+1}{(x+1)^d}\right)^2 = \frac{x^{2d} + x^-d}{(x+2x^{-1})^d}.$$  

According to Proposition 1, function $F$ is then APN if and only if $\psi_d$ 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 $\frac{D_d(y^{-1}, 1)}{y^d}$ equals the value at $y$ of the reciprocal polynomial of $D_d(X, 1)$. Hence:

**Proposition 2.** For every positive integers $n$ and $d$, function $F(x) = x^d$ is APN if and only if the reciprocal polynomial $D_d(X, 1) = X^dD_d(X^{-1}, 1)$ 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 $\frac{x^{d+1}+1}{(x+1)^d} = s^d + (s+1)^d$. We have then $x + x^{-1} = \frac{s+1}{s} + \frac{s}{s+1} = \frac{1}{s^2+s}$.
and therefore \( \frac{x^{d+1}}{(x+1)^d} = \psi_d(x+x^{-1}) = \psi_d \left( \frac{1}{x^{d+1}} \right) = s^d + (s+1)^d = \phi_d(s^2 + s) \). Hence, for every \( z \in H^* \), \( \phi_d(z) = \psi_d(z^{-1}) \) and squaring gives \( (\phi_d(z))^2 = D_d(z, 1) \). 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 3.** 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\(^2\). For every \( z \neq 0 \) such that \( t_1^2(z) = 0 \), we have then \( (\phi_d(z))^2 = D_d(z, 1) \), where \( D_d \) is the reciprocal 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 \( \widetilde{D}_{2^i+1}(X^2 + X, 1) = 1 + \sum_{j=1}^{i} X^{2^j} \), \( D_{2^i+1}(X, 1) = 1 + \sum_{j=1}^{i} X^{2^j} \). 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 3 also allows to obtain the explicit expressions of other Dickson polynomials; for instance with so-called Kasami indices:

**Corollary 1.** 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):

\[
x^{4^i-2^i+1} + (x+1)^{4^i-2^i+1} = \frac{x^{4^i+1}(x+1)^{2^i} + (x+1)^{4^i+1}x^{2^i}}{(x^2 + x)^{2^i}} = \frac{x^{4^i+1} + x^{4^i+2^i} + x^{2^i+1} + x^{2^i}}{(x^2 + x)^{2^i}} = 1 + \frac{\left( \sum_{j=0}^{i-1} (x^2 + x)^{2^j} \right)^{2^i+1}}{(x^2 + x)^{2^i}},
\]

and therefore, after squaring and denoting \( X = x^2 + x \), we obtain:

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

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

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

This completes the proof. \( \square \)

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

The same method applies more generally to \( D_{2^{i}-2^{i+1}} \) but without the nice factorization above.

**Remark 11.** The Müller-Cohen-Matthews (MCM) polynomial (see [5]) equals \( \sum_{i=0}^{k-1} X(2^{k}+1)2^{i} \) 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 \( \phi(X) = \sum_{i=0}^{k-1} X^{2^{i}} = 1 + \left( \widetilde{D}_{2^{k+1}}(X,1) \right)^{2^{n-i}} \).

5. **Experimental results**

This section discusses how to use Sidon and sum-free conditions in a computer search for possibly new APN exponents. Afterward, we provide results for \( n \) up to 48 showing the number of possibly new APN exponents.

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:

1. Consider all the elements in \( \mathbb{Z}/(2^{n} - 1)\mathbb{Z} \), discard (because of Dobbertin’s observation recalled in Section 1) 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
2. 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 \( \mathbb{F}_{2^{r}} \)”.

The progress made by Edel over Canteaut and Dobbertin is impressive because the complexity of the search is exponential in \( n \). More precisely, checking the possible APN exponents has complexity \( 2^{n} \), after which one needs to evaluate if each of those exponents results in an APN function. For finding a contradiction to APN (i.e., showing a function is not APN) one needs on average about \( c\sqrt{2^{n-1}} \) tests per exponent. Still, his computer investigation concentrated on smaller values of \( n \) or such values that have a structure allowing easier investigation. Our search includes all values up to and including \( n = 48 \).

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 when discussing the subfield condition in the rest of the paper, we mean the condition implemented by Yves Edel in his investigation.

In this section, we concentrate on utilizing the same methods as well as our newly developed Sidon and sum-free conditions to derive the number of possible new APN exponents to test and see if the Sidon and sum-free conditions contribute to reducing this number. We use the acronym S for Sidon condition, SF for sum-free condition, and SSF for Sidon-sum-free condition. We shall call “S values” (respectively, 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 (respectively, SF, SSF).

Next, we propose two techniques to calculate S and SF values and one additional technique to calculate SF values. The first technique for S/SF has high computational complexity but low memory complexity, while the second one for S/SF has low computational complexity but high memory complexity. A trade-off can be considered concerning 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 (respectively, a sum-free) set if and only if, for every $u \in \mathbb{F}_{2^n}^*$ (respectively, for $u = 1$), the polynomial $(X + 1)^e + u$ has at most two zeros in $G_e$ (respectively, has no zero in $G_e$).

In the first technique (we name it “Memory-efficient calculation”), to determine whether a value $e$ is Sidon (respectively, 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), where each needs to be 2 bits long.

For the second technique (we name it “Time-efficient calculation”), 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 the computational complexity of $e$ and the memory complexity of $2^n$. Since we require two 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. Observe that sum-free condition is somewhat more discriminating and enables us to reduce more values $e$ than the Sidon condition. Calculating the Sidon condition (and possibly the sum-free condition) as we proposed with “Memory-efficient calculation” or “Time-efficient calculation” 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). Indeed, in the cases when a large value $e$ is SSF, and $n$ is large, calculating Sidon (and possibly sum-free) can become too expensive.
Table 3. Divisors of $2^n - 1$ which are Sidon-sum-free, part I.

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

in time and memory complexities. Consequently, we arrive at the situation that checking SSF is potentially 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 but the values we call *Approximate SSF (ASSF)* values. The ASSF
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, 1025 |
|    | SF            | 1, 5, 11, 25, 41, 55, 205, 275, 1025         |
|    | SSF           | 1, 5, 11, 25, 41, 55, 205, 275, 1025         |
| 21 | S             | 1, 337                                      |
|    | SF            | 1, 337                                      |
|    | SSF           | 1, 337                                      |
| 22 | S             | 1, 3, 23, 69, 683, 2049                     |
|    | SF            | 1, 23, 89, 683, 15709                      |
|    | 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, 1205, 4097 |
|    | SF            | 1, 5, 13, 17, 65, 221, 241, 1205, 4097       |
|    | SSF           | 1, 5, 13, 17, 65, 221, 241, 1205, 4097       |
| 25 | S             | 1, 601, 1801                                |
|    | SF            | 1, 601, 1801                                |
|    | SSF           | 1, 601, 1801                                |
| 26 | S             | 1, 3, 2731, 8193                            |
|    | SF            | 1, 2731                                     |
|    | SSF           | 1, 2731                                     |
| 27 | S/SF/SSF      | 1                                           |
| 28 | S             | 1, 3, 5, 29, 43, 87, 113, 129, 145, 215, 339, 565, 1247, 3277, 16385 |
|    | SF            | 1, 5, 29, 43, 113, 145, 215, 565, 1247, 3277, 4859, 6235, 16385, 24295 |
|    | SSF           | 1, 5, 29, 43, 113, 145, 215, 565, 1247, 3277, 16385 |
| 29 | S             | 1, 233, 1103, 2089                          |
|    | SF            | 1, 233, 1103, 2089                          |
|    | SSF           | 1, 233, 1103, 2089                          |
| 30 | S             | 1, 3, 9, 11, 33, 99, 151, 331, 453, 993, 1359, 1661, 2979, 3641, 4983, 10923, 32769 |
|    | SF            | 1, 11, 151, 331, 1661, 3641                 |
|    | SSF           | 1, 11, 151, 331, 1661, 3641                 |
| 31 | S/SF/SSF      | 1                                           |

Values are those values $e$ that 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 $r \equiv 2 \pmod{3}$ 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 obtained from Definition 5.1, conditions 2, 3, 4, and 5.

**Remark 12.** Note that all the SSF values belong to the set of Approximate SSF values, but the ASSF set possibly contains more values.

**Remark 13.** Comparing the results from Tables 3 and 4 with those obtained from the ASSF calculations, there are only a few values of \( n \) where SSF and ASSF sets are not the same. Naturally, this does not necessarily mean that using ASSF for larger \( n \) does not weaken the discriminative power of Sidon and sum-free conditions.

**Remark 14.** It is possible to improve the computation speed for calculating the 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 it is always SSF) and \( 2^n - 1 \) since we know it is never SSF.

**Remark 15.** When \( 2^n - 1 \) is a Mersenne prime, there is no need to check SSF since we know value 1 is always SSF, and there is no other strict divisor of \( 2^n - 1 \).

Finally, there is a technique (Proposition 5.1 in [4]) to calculate SF that is efficient from both computational and memory perspectives. We consider this technique to be preferred for the SF values, but unfortunately, it cannot be used to obtain the Sidon values.

1. Calculate gcd\((x^e + 1, (x + 1)^e + 1)\).
2. If the remainder is 1, then the value is SF.

This technique is efficient as we must calculate in \( \mathbb{F}_2 \) only, and we need only a single bit to store the result.

**Remark 16.** Based on our experiments and the algorithms’ complexities, we recommend the following steps in calculating SSF/ASSF values:

1. Calculate ASSF values.
2. Calculate those values that are SSF in subfield since they are also SSF in the field (which helps by removing some values that are not SSF but also indicating if further reduction is possible - if all the values are covered in subfield then for sure no further reduction is possible).
3. Calculate SF values with the gcd approach (Proposition 5.1 [4]). Here, one needs to check only those values that are ASSF and not covered by the subfield check.
4. Optional: reduce the number of remaining values by running the first or second algorithm (Sidon condition only).

Our results show small differences between ASSF and SSF, and since the sum-free condition is somewhat more discriminative than the Sidon condition, the first three steps should provide similar results compared to when added the final step.

\[^3\text{We assume that } n \text{ is large enough, e.g., larger than } \approx 30, \text{ as, for smaller values, all algorithms are sufficiently efficient.}\]
5.2. Calculating the number of possibly new APN exponents. This section employs all constraints on the possibly new APN exponents \(d\) 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 listing all the constraints a value \(d\) needs to fulfill to be a possibly new APN exponent. The constraints are listed 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. Select one representative per cyclotomic class:
   - if \(n\) is even, keep for a value \(d\) the smallest representative of a cyclotomic class (i.e., the coset leader of the class);
   - if \(n\) is odd, keep for a value \(d\) and its inverse the smallest representative of both cyclotomic classes (i.e., the smallest coset leader of the two 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 \(\lambda\) of \(2^n - 1\) such that \((\lambda^2)^{\lambda + 1} > 2^n - 1\) and there exists \(j = 1, \ldots, n - 1\) such that \(\lambda\) divides \(d - 2^j\) (see Remark 10).

Remark 17. Note that if \(n\) is a prime, then there are no subfields to explore.

Remark 18. 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 the SSF condition a more general one since Mersenne primes are rarer than primes.

We list the results for \(32 \leq n \leq 48\) in Table 5 (\(3 \leq n \leq 31\) values are listed in Appendix A, Table 6). Comparing the results with Table 6, we observe SSF (or, to be more precise, AS and SF criteria) discriminate significantly more exponent values. Indeed, observe that for small \(n\), the improvement of considering SSF is negligible.

For larger \(n\), for odd values, we see that the SSF condition regularly reduces the number of possible exponents, where for some of the values \(n\), the reduction is significant. For example, for \(n = 39\), due to the SSF criterion, we reduce more than 40,000 possible exponent values. Even though the SSF criterion is applied last (and if applied before, e.g., the subfield criterion, it would remove many more exponent values), this represents a significant reduction in the number of possible APN exponents left to test. Indeed, our experiments show it could reduce the time required to check if exponents are APN for several weeks, depending on the computational power available. Simultaneously, for \(n\) even, the SSF criterion does not significantly reduce the possible new APN exponents.

Remark 19. We applied SSF as the last criterion. If applied before (e.g., before the subfield criterion), it would remove significantly more exponent values. Then, the subfield criterion would have only a slight effect.

Remark 20. The exponents removed through SSF are not all the same as exponents removed by any other criterion. Thus, it is impossible to remove any of the criteria and obtain the same results as here.
Table 5. $32 \leq n \leq 48$. Number of possibly new APN exponents, the total number of values to consider for a certain $n$ equals $2^n - 2$. *Cyclotomic rep.* denotes the number of possible APN exponents after keeping only a single representative of a cyclotomic class. *Subfield* denotes the number of possible APN exponents after removing values $d$ such that $\gcd(d, 2^r - 1)$ is not an APN exponent in $\mathbb{F}_2^r$. *SSF* denotes the number of possible APN exponents after removing values $d$ such that $(1) \gcd(d - 2^r, 2^n - 1)$ are not SSF values and $(2)$ there exists a divisor $\lambda$ of $2^n - 1$ such that $(\frac{\lambda + 1}{2}) > 2^{n-l}$ and there exists $j = 1, \ldots, n-1$ such that $\lambda$ divides $d - 2^j$.

| $n$ | $\gcd(d, 2^r - 1)$ | Not known APN | Cyclotomic rep. | Subfield | SSF |
|-----|------------------|---------------|----------------|----------|-----|
| 32  | 1073.741.824    | 1073.741.344  | 33.554.417     | 229.381  | 229.328 |
| 33  | 6.963.536.448   | 6.963.535.629 | 105.508.114    | 6.893.976 | 6.893.986 |
| 34  | 5.726.448.300   | 5.726.447.790 | 168.424.935    | 764.560  | 764.560 |
| 35  | 32.524.632.000  | 32.524.630.145 | 464.637.581    | 236.609.75 | 236.620.012 |
| 36  | 8.707.129.344   | 8.707.128.948 | 241.864.693    | 58.309   | 58.279 |
| 37  | 136.826.65.072  | 136.826.652.297 | 1.848.954.492  | 1.848.954.492 | 1.848.954.380 |
| 38  | 91.625.269.932  | 91.625.269.286 | 2.411.191.297  | 3.407.842 | 3.407.842 |
| 39  | 465.193.834.560 | 465.193.832.571 | 5.964.023.502 | 127.800.480 | 127.759.412 |
| 40  | 236.851.200.000 | 236.851.199.360 | 5.921.279.984 | 1.40.304 | 1.40.210 |
| 41  | 2.198.858.730.832 | 2.198.858.727.429 | 26.815.350.336 | 26.815.350.336 | 26.815.343.652 |
| 42  | 809.240.108.544 | 809.240.108.082 | 19.267.621.621 | 14.85.7 | 14.849 |
| 43  | 8774.777.333.880 | 8774.777.330.139 | 102.032.294.540 | 102.032.294.540 | 102.032.289.465 |
| 44  | 4.417.116.143.616 | 4.417.116.142.780 | 100.389.003.245 | 15.054.317 | 15.054.285 |
| 45  | 28.548.223.200.000 | 28.548.223.197.615 | 317.202.480.005 | 2004.543.425 | 2004.537.282 |
| 46  | 22.957.042.116.160 | 22.957.042.115.194 | 499.066.132.939 | 65.710.726 | 65.710.708 |
| 47  | 9.339.802.874.699 | 9.339.802.877.926 | 1.449.575.966.170 | 1.449.575.966.170 | 1.449.575.962.833 |
| 48  | 36.528.696.852.480 | 36.528.696.851.760 | 761.014.517.745 | 1.096.689 | 1.096.684 |

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 be useful for future works.

6.1. Other necessary conditions for an exponent to be APN.

**Proposition 4.** 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 $x^{2^j}(x + 1)^{d-2^j} = x'^{2^j}(x' + 1)^{d-2^j}$, we have $x' = x$ or $x' = x^{-1}$.

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

**Remark 21.** The interpretation of Subsection 4.1 is in the present case as follows: if $x^{d+2^j} = 1$ then $\frac{x^{d+1}}{(x+1)^d} = \frac{x^{d-1}}{(x+1)^d} = \frac{x^{2^j+1}}{(x+1)^d} = \frac{1}{x^{2^j}(x+1)^{d-2^j}}$. 

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

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 \( \{ x \in \mathbb{F}_{2^{n}}^* ; x^{d-2^{k}-2^{j}} = 1 \} \) 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 \( x^{d} + x^{d-2^{k}-2^{j}} + x^{d-2^{k}+2^{j}} + x^{d-2^{j}+2^{k}} \neq (y^{d})^{(x+1)^{d}} \). Indeed, still introducing the unique \( s \in \mathbb{F}_{2^{n}}^* \setminus \{1\} \) such that \( x = \frac{x}{x+1} \), we have \( s^{d-2^{k}-2^{j}} = (s + 1)^{d-2^{k}-2^{j}} = 0 \), and multiplying by \( (s + 1)^{2k+2j} \) we obtain \( s^{d} + (s + 1)^{d} = s^{d-2^{k}-2^{j}} + s^{d-2^{k}} + s^{d-2^{j}} = x^{d-2^{k}-2^{j}(x+1)^{2k} + x^{d-2^{k}}(x+1)^{2j} + x^{d-2^{j}}(x+1)^{2k} = \frac{(x+1)^{d}}{(x+1)^{d}} } \). The rest of the proof is similar to above.

More generally, let \( k \) be any integer and let \( x^{k} = 1, \ x \neq 1 \), \( x = \frac{x}{x+1} \), we have \( s^{k} + (s + 1)^{k} = 0 \) and therefore, by multiplication by \( (s + 1)^{d-k} \), \( s^{d} + (s + 1)^{d} = \sum_{j=0}^{d-k-1} (d-k) s^{j+k} \), which implies that \( x \neq 1 \), \( y \neq 1 \), \( x \neq y, x \neq \frac{1}{y} \) and \( x^{k} = y^{k} = 1 \) imply \( \sum_{j=0}^{d-k-1} (d-k) \frac{x^{j}}{(x+1)^{j+\tau}} = 1 \) and \( \sum_{j=0}^{d-k-1} (d-k) \frac{x^{j}}{(x+1)^{j+\tau}} = 1 \).

7. Conclusions and future work

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 through Dickson polynomials. We proved that Dickson polynomials in characteristic 2 and Reversed Dickson polynomials of the same index are reciprocal of each other, 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 that the improvements can be relatively small, they are nevertheless important from theoretical and practical perspectives. We observe small improvements with our new SSF condition since we apply it after all the other known conditions, and we notice that Edel’s subfield condition removes many of the same exponents as the SSF condition. Finally, our results show that the SSF condition should become more discriminative as we increase the value \( n \), especially for those values where \( n \) is prime (or even just odd), and \( 2^{n} - 1 \) has many divisors. Our experimental results give all results for possible new APN exponents up to \( n = 48 \). To the best of our knowledge, this is the first time such exhaustive analysis has been done. In future work, we plan to extend our research for new APN exponents for higher \( n \) and investigate how to calculate the Sidon values more efficiently. Finally, we plan to investigate techniques that would enable faster evaluation if a power function is APN.
ACKNOWLEDGMENTS

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 information on Sidon sets and sum-free sets.

REFERENCES

[1] L. Babai and V. T. Sós, Sidon sets in groups and induced subgraphs of cayley graphs, European J. Combin., 6 (1985), 101–114.
[2] T. Beth and C. Ding, On almost perfect nonlinear permutations, Advances in Cryptology–EUROCRYPT ’93 (Loftus, 1993), 765 (1993), 65–76.
[3] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, 2021.
[4] C. Carlet and S. Mesnager, On those multiplicative subgroups of $\mathbb{F}_{2^n}$ which are Sidon sets and/or sum-free sets, Journal of Algebraic Combinatorics, 2020.
[5] S. D. Cohen and R. W. Matthews, A class of exceptional polynomials, Trans. Amer. Math. Soc., 345 (1994), 897–909.
[6] B. Green and I. Z. Ruzsa, Sum-free sets in abelian groups, Isr. J. Math., 147 (2005), 157–188.
[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 (2009), 748–773.
[9] G. Kyureghyan, Special mappings of finite fields, Finite Fields and Their Applications, Radon Ser. Comput. Appl. Math., 11 (2013), 117–144.
[10] K. Nyberg, Differentially uniform mappings for cryptography, Advances in Cryptology–EUROCRYPT’93 (Loftus, 1993), 765 (1993), 55–64.
[11] K. Nyberg and L. R. Knudsen, Provable security against differential cryptanalysis, Advances in Cryptology–CRYPTO ’92 (Santa Barbara, CA, 1992), 740 (1992), 566–574.
[12] T. Tao and V. Vu, Sum-free sets in groups: A survey, J. Comb., 8 (2017), 541–552.

APPENDIX A. NUMBER OF POSSIBLY NEW APN EXONENTS FOR $n < 32$

In Table 6, we give results for the number of values $d$ one needs to examine to look for new APN exponents (considering values up to $n = 32$). We note that this list serves only the illustrative purpose of how the 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, the SSF condition can discriminate more values.

Received June 2021; revised October 2021; early access December 2021.

E-mail address: claude.carlet@gmail.com
E-mail address: s.picek@tudelft.nl
Table 6. $3 \leq n \leq 31$. Number of possibly new APN exponents, the total number of values to consider for a certain $n$ equals $2^n - 2$ as we do not need to consider the values 0 and $2^n - 1$. *Cyclotomic rep.* denotes the number of possible APN exponents after keeping only a single representative of a cyclotomic class. *Subfield* denotes the number of possible APN exponents after removing values $d$ such that gcd($d, 2^n - 1$) is not an APN exponent in $\mathbb{F}_{2^r}$. *SSF* denotes the number of possible APN exponents after removing values $d$ such that (1) gcd($d - 2^j, 2^n - 1$) are not SSF values and (2) there exists a divisor $\lambda$ of $2^n - 1$ such that $(\lambda + 1) > 2^n - 1$ and there exists $j = 1, \ldots, n - 1$ such that $\lambda$ divides $d - 2^j$.

\begin{tabular}{|c|c|c|c|c|c|}
\hline
n & gcd($d, 2^n - 1$) & Not known APN & Cyclotomic rep. & Subfield & SSF \\
\hline
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 \\
\hline
\end{tabular}