Journal of Algebraic Combinatorics (2022) 55:43–59
https://doi.org/10.1007/s10801-020-00988-7

On those multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are Sidon sets and/or sum-free sets

Claude Carlet[1,2,3] · **Sihem Mesnager**[1,2,4]

Received: 31 January 2020 / Accepted: 30 October 2020 / Published online: 10 November 2020

Abstract
We study those multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are Sidon sets and/or sum-free sets in the group $(\mathbb{F}_{2^n}, +)$. These Sidon and sum-free sets play an important role relative to the exponents of APN power functions, as shown by a paper co-authored by the first author.

Keywords Sidon sets · Sum-free sets · APN exponents · APN functions · Symmetric cryptography

1 Introduction

The notions of Sidon set and of sum-free set are well known in combinatorics [1,6,8].

Definition 1.1 [1] A subset of an additive group $(G, +)$ is a *Sidon set* if it does not contain elements x, y, z, t, three of which are distinct and such that $x + y = z + t$.

Definition 1.2 [6,8] A subset S of an additive group $(G, +)$ is a *sum-free set* if it does not contain elements x, y, z such that $x + y = z$ (i.e. if $S \cap (S + S) = \emptyset$).

Note that these definitions are also relevant in characteristic 2, which will be our framework; they simplify then: *S is a Sidon set (resp. a sum-free set) in $\mathbb{F}_2^n$ (or in*

✉ Sihem Mesnager
sihem.mesnager@univ-paris8.fr

Claude Carlet
claude.carlet@univ-paris8.fr

1 Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France

2 University of Paris XIII, CNRS, UMR 7539 LAGA, Sorbonne Paris Cité, 93430 Villetaneuse, France

3 Department of Informatics, University of Bergen, Bergen, Norway

4 Telecom Paris, 91120 Palaiseau, France

$\mathbb{F}_{2^n}$ since it is always possible to endow $\mathbb{F}_2^n$ with the structure of a field) if it does not contain 4 distinct elements (resp 3 elements) whose sum is null.

Denoting z by $x + a$, a set S is a Sidon set if for every nonzero element a of G, the condition "$x \in S, x + a \in S, y \in S, y + a \in S$" implies that $x = y$ or $x = y + a$.

There exists a natural connection between those (n, n)-functions (from $\mathbb{F}_2^n$ to itself) in cryptography which are almost perfect nonlinear (in brief, APN; see the definition, e.g. in [5]) and Sidon sets: by definition, an (n, n)-function 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 the group $(\mathbb{F}_2^n \times \mathbb{F}_2^n, +)$. In [5] is shown another connection, between the exponents of APN power functions $F(x) = x^d$ over $\mathbb{F}_{2^n}$ (called APN exponents) and those multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are at the same time Sidon sets and sum-free sets in the group $(\mathbb{F}_2^n, +)$:

Theorem 1.3 [5] *If d is an APN exponent, then for every integer j, the multiplicative subgroup of order* $\gcd(d - 2^j, 2^n - 1)$ *is a Sidon set and a sum-free set.*

In this paper, we make a study of those multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are Sidon sets (resp. sum-free sets). The motivation for this work is twofold: it is theoretically interesting to see how the structure of the field can help in finding new Sidon sets and sum-free sets (of course, these notions are purely additive, but the determination of Sidon sets and sum-free sets may benefit from the richer structure of the field[1]); it is also practically useful to have as much information as possible on Sidon–sum-free multiplicative subgroups of $\mathbb{F}_{2^n}^*$, for selecting candidates for a search of new infinite classes of APN power functions (see [5]). Indeed, the result recalled from [5] and such knowledge may allow discriminating better those exponents which are likely to be new APN exponents. To this aim, we need to be able to determine the Sidon–sum-free (SSF) multiplicative subgroups of $\mathbb{F}_{2^n}^*$ for n larger than 34 (since for $n \leq 34$, all APN exponents are known) and it begins to be very difficult to obtain them with a computer for $n \geq 32$. In [5] is then defined and used the notion of approximate Sidon–sum-free (ASSF) multiplicative subgroups of $\mathbb{F}_{2^n}^*$; such a subgroup is called ASSF (resp. AS, ASF) if none of the results in the present paper show that it is not Sidon–sum-free (resp. not Sidon, not sum-free). This allows going further than $n = 32$. It is then important to find not only sufficient but also necessary conditions for some multiplicative subgroup of $\mathbb{F}_{2^n}^*$ to be SSF, for as many orders of such subgroups as possible (i.e. for as many divisors of $2^n - 1$ as possible) and this is what the present paper produces. The paper is organized as follows. In Sect. 2, we study the characterization of Sidon and sum-free sets by the Fourier transform of their indicator functions. In Sect. 3, we derive Sidon–sum-free sets from the known classes of APN power functions. Sections 4 and 5 are devoted to the study of Sidon and sum-free multiplicative subgroups of $\mathbb{F}_{2^n}^*$. Next, in Sect. 6, we exhibit more Sidon and sum-free multiplicative subgroups of $\mathbb{F}_{2^n}^*$. Finally, in Sect. 1, we present some computation results related to our study.

[1] The same is true, in an extreme way, for APN functions in cryptography: the notion is purely additive, but no construction of an APN function is known which does not use the field structure.

2 Characterizations by the Fourier transform

For any set E, we shall denote $E^\star = E \setminus \{0\}$ and $|E|$ will denote the cardinality of E.

In this section, we study the characterization of Sidon and sum-free sets by the Fourier transform of their indicator functions (or equivalently by the Walsh transforms of their indicator functions). We are not yet able to deduce significant results on Sidon and sum-free sets from these characterizations, but since many cryptographic parameters can be characterized this way (and more and more are, see e.g. [3,4]), it is important for further works to make such a study.

Let some inner product "$\cdot$" be chosen in $\mathbb{F}_2^n$. In this paper, we shall endow $\mathbb{F}_2^n$ with the structure of the field $\mathbb{F}_{2^n}$; the usual inner product in this field is defined as $a \cdot x = tr(ax)$, where tr is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by $tr(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Given a numerical (i.e. $\mathbb{R}$-valued) function f over $\mathbb{F}_2^n$, the Fourier transform of f is defined as $\widehat{f}(a) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x}$. The Fourier transform of the indicator function 1_S of a subset S of $\mathbb{F}_{2^n}$ equals then

$$\widehat{1_S}(a) = \sum_{x \in S} (-1)^{a \cdot x}.$$

It is possible to characterize Sidon sets by the Fourier transform; we restrict ourselves to $\mathbb{F}_2^n$ but this characterization can be made more general:

Proposition 2.1 *For every subset S of $\mathbb{F}_2^n$, we have:*

$$\sum_{a \in \mathbb{F}_2^n} \widehat{1_S}^4(a) \geq 3 \cdot 2^n |S|^2 - 2^{n+1}|S|, \tag{1}$$

or equivalently:

$$\sum_{a \in \mathbb{F}_2^n; a \neq 0} \widehat{1_S}^4(a) \geq 3 \cdot 2^n |S|^2 - 2^{n+1}|S| - |S|^4, \tag{2}$$

and

$$\sum_{a \in \mathbb{F}_2^n} \widehat{1_S}^3(a) \geq 0, \tag{3}$$

or equivalently

$$\sum_{a \in \mathbb{F}_2^n; a \neq 0} \widehat{1_S}^3(a) \geq -|S|^3, \tag{4}$$

and S is a Sidon set (resp. a sum-free set) in the additive group $(\mathbb{F}_2^n, +)$ if and only if (1) or (2) is an equality (resp (3) or (4) is an equality).

Proof For every subset S of $\mathbb{F}_2^n$, the number of $(x, y, z, t) \in S^4$ such that $x+y+z+t = 0$ equals $\sum_{(x,y,z) \in (\mathbb{F}_2^n)^3} 1_S(x)1_S(y)1_S(z)1_S(x+y+z)$. If $x = y \in S$ and $z \in S$, or $x = z \in S$ and $y \in S$, or $y = z \in S$ and $x \in S$, then we have $1_S(x)1_S(y)1_S(z)1_S(x+$

$y+z)=1$. We deduce the inequality $\sum_{(x,y,z)\in(\mathbb{F}_2^n)^3} 1_S(x)1_S(y)1_S(z)1_S(x+y+z) \geq 3|S|^2-2|S|$ and that S is a Sidon set if and only if this inequality is an equality. The sum $\sum_{(x,y,z)\in(\mathbb{F}_2^n)^3} 1_S(x)1_S(y)1_S(z)1_S(x+y+z)$ is equal to $2^{-n}\sum_{a\in\mathbb{F}_2^n}\sum_{(x,y,z,t)\in(\mathbb{F}_2^n)^4} 1_S(x)1_S(y)1_S(z)1_S(t)(-1)^{a\cdot(x+y+z+t)}$, that is, to $2^{-n}\sum_{a\in\mathbb{F}_2^n}\widehat{1_S}^4(a)$. This proves the first part of the statement, since $\widehat{1_S}(0)=|S|$ Similarly, we have $\sum_{(x,y)\in(\mathbb{F}_2^n)^2} 1_S(x)1_S(y)1_S(x+y)\geq 0$, which is equivalent to $2^{-n}\sum_{a\in\mathbb{F}_2^n}\widehat{1_S}^3(a)\geq 0$, and S is sum-free if and only if this inequality is an equality. □

Remark 2.2 As recalled in [5], it is well known that the size $|S|$ of a Sidon set S in a group $(G,+)$ cannot be such that $\binom{|S|}{2}=\frac{|S|(|S|-1)}{2}>|G|-1$, because the number of pairs $\{x,y\}$ included in S would then be strictly larger than the number of nonzero elements of G. We deduce from the relation $|S|^2-|S|-2|G|+2\leq 0$ that $|S|\leq\frac{1+\sqrt{8|G|-7}}{2}$. In the case of $G=\mathbb{F}_2^n$, this gives $|S|\leq\lfloor\frac{1+\sqrt{2^{n+3}-7}}{2}\rfloor$.

It is also well known that the size $|S|$ of a sum-free set S in a group $(G,+)$ cannot be strictly larger than $\frac{|G|}{2}$, because the two sets $S+S$ and S would have sizes whose sum is strictly larger than the order of the group. As observed in [5], the size $|S|$ of a sum-free–Sidon set satisfies $\frac{|S|(|S|+1)}{2}\leq|G|-1$, that is, $|S|^2+|S|-2|G|+2\leq 0$, which implies that $|S|\leq\frac{-1+\sqrt{8|G|-7}}{2}$. In the case of $G=\mathbb{F}_2^n$, this gives $|S|\leq\lfloor\frac{-1+\sqrt{2^{n+3}-7}}{2}\rfloor$.

For every subset S, we have the inverse Fourier transform formula:

$$\sum_{a\in\mathbb{F}_2^n}\widehat{1_S}(a)=2^n 1_S(0),$$

and Parseval's relation:

$$\sum_{a\in\mathbb{F}_2^n}\widehat{1_S}^2(a)=2^n\sum_{a,x,y\in\mathbb{F}_2^n}1_S(x)1_S(y)(-1)^{a\cdot(x+y)}=2^n\sum_{x\in\mathbb{F}_2^n}1_S(x)=2^n|S|,$$

or equivalently:

$$\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^2(a)=2^n|S|-|S|^2.$$

Note that, for every Sidon–sum-free set S, we know then the precise values of the four first power moments of the Fourier transform.

When S is a Sidon set, we have $\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^4(a)=3\cdot 2^n|S|^2-2^{n+1}|S|-|S|^4$, according to Proposition 2.1. Using the Cauchy–Schwartz inequality, we have

$$\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^4(a)\geq\frac{\left(\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^2(a)\right)^2}{|\{a\in\mathbb{F}_2^n;\,a\neq 0,\,\widehat{1_S}(a)\neq 0\}|}\tag{5}$$

$$\geq\frac{\left(\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^2(a)\right)^2}{2^n-1}=\frac{(2^n|S|-|S|^2)^2}{2^n-1}$$

and we deduce $3\cdot 2^n\,|S|^2-2^{n+1}|S|-|S|^4\geq\frac{(2^n|S|-|S|^2)^2}{2^n-1}$, that is:

$$|S|^3-2|S|^2-(2^{n+1}-3)\,|S|+2\cdot(2^n-1)\leq 0.\tag{6}$$

Observe that one has

$$|S|^3-2|S|^2-(2^{n+1}-3)\,|S|+2\cdot(2^n-1)=(|S|-1)\big(|S|^2-|S|-2\cdot(2^n-1)\big).$$

The roots of $X^2-X-2\cdot(2^n-1)$ are $\frac{1-\sqrt{2^{n+3}-7}}{2}$ and $\frac{1+\sqrt{2^{n+3}-7}}{2}$. Thus, $|S|^3-2|S|^2-(2^{n+1}-3)|S|+2(2^n+1)\leq 0$ if and only if $|S|\in\left[1,\left\lfloor\frac{1+\sqrt{2^{n+3}-7}}{2}\right\rfloor\right]$. We obtain then the same bound as the one obtained at the previous section (for the size of Sidon sets in $\mathbb{F}_2^n$). Moreover, Relation (5) gives a stronger inequality, but which depends on the size of the Fourier transform support of 1_S.

If S is also sum-free, then we have $\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^3(a)=-|S|^3$, according to Proposition 2.1, which implies by the Cauchy–Schwartz inequality that $|S|^6=(\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^3(a))^2\leq(\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^2(a))(\sum_{a\in\mathbb{F}_2^n;a\neq 0}\widehat{1_S}^4(a))=(2^n|S|-|S|^2)(3\cdot 2^n\,|S|^2-2^{n+1}|S|-|S|^4)$ and then

$$|S|^3+3|S|^2-(3\cdot 2^n+2)|S|+2^{n+1}\leq 0.$$

The polynomial $f(X)=X^3+3X^2-(3\cdot 2^n+2)X+2^{n+1}$ has three distinct real roots since its discriminant is $108\cdot 2^{3n}-135\cdot 2^{2n}-180\cdot 2^n+68>0$ for $n\geq 1$. Let us denote by $\lambda_1<\lambda_2<\lambda_3$ these three distinct roots. Now, the derivative $f'(X)$ of this polynomial has two distinct real roots $\mu_1=-\frac{1}{3}\sqrt{9\cdot 2^n+15}-1<0$ and $\mu_2=\frac{1}{3}\sqrt{9\cdot 2^n+15}-1>0$. Now, since $f(0)=2^{n+1}>0$ and $f(1)=2-2^n<0$, one has necessarily $\lambda_1<\mu_1<\lambda_2<1<\mu_2<\lambda_3$. Let us now compute $f\left(\frac{\sqrt{8\cdot 2^n-7}-1}{2}\right)=-\frac{1}{2}\sqrt{8\cdot 2^n-7}\cdot 2^n+\frac{13}{2}\cdot 2^n-3\sqrt{8\cdot 2^n-7}-1=-\frac{1}{2}\sqrt{8\cdot 2^n-7}\cdot\left(2^n+6\right)+\frac{13}{2}\cdot 2^n-1<0$ when $n\geq 3$ and is equal to 0 for $n\in\{1,2\}$ proving that $\lambda_3>\frac{\sqrt{8\cdot 2^n-7}-1}{2}$ when $n\geq 3$.

Remark 2.3 Denoting by W_f the Walsh transform of a Boolean function f: $W_f(a)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}$, we have, for every $a\neq 0$ that $\widehat{1_S}(a)=-\frac{1}{2}W_{1_S}(a)$ (and for $a=0$ that $\widehat{1_S}(0)=2^{n-1}-\frac{1}{2}W_{1_S}(0)$).

Relation (2) is then equivalent to $\sum_{a\in\mathbb{F}_2^n,a\neq 0}W_{1_S}^4(a)\geq 3\cdot 2^{n+4}\,|S|^2-2^{n+5}|S|-2^4|S|^4$ and Relation (4) to $\sum_{a\in\mathbb{F}_2^n,a\neq 0}W_{1_S}^3(a)\leq 2^3|S|^3$.

Remark 2.4 In this paper, S will always be the multiplicative subgroup of $\mathbb{F}_{2^n}^*$ of order $e = |S|$ and then invariant under multiplication by any element of S. We deduce that for every $s \in S$, and every $a \in \mathbb{F}_{2^n}^*$, we have $\widehat{1_S}(sa) = \sum_{x\in S}(-1)^{tr(asx)} = \sum_{x\in S}(-1)^{tr(ax)} = \widehat{1_S}(a)$. Hence, the Fourier transform of the indicator of S will be constant on every coset of S in $\mathbb{F}_{2^n}^*$. Let U be a set of size $\frac{2^n-1}{e}$ such that $\mathbb{F}_{2^n}^* = US$, then according to Proposition 2.1, S is a Sidon set if and only if $\sum_{a\in U}\widehat{1_S}^4(a) = 3\cdot 2^n \cdot e - 2^{n+1} - e^3$. Note that since every element of S can be written in $\frac{2^n-1}{e}$ ways as $x^{\frac{2^n-1}{e}}$, we have $\widehat{1_S}(a) = \frac{e}{2^n-1}\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{tr\left(ax^{\frac{2^n-1}{e}}\right)}$.

3 The Sidon–sum-free sets deduced from the known classes of APN power functions

The result from [5] recalled in the introduction and the knowledge of classes of APN power functions (see e.g. [2,4]) give directly orders of multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are at the same time Sidon sets and sum-free sets; these orders depend on an integer j, which can be any integer (concretely $j = 0, \ldots, n-1$):

- $\gcd(2^i + 1 - 2^j, 2^n - 1)$, where i is co-prime with n (related to the so-called Gold APN functions $F(x) = x^{2^i+1}$),
- $\gcd(2^{2i} - 2^i + 1 - 2^j, 2^n - 1)$, where i is co-prime with n (related to the so-called Kasami APN functions $F(x) = x^{2^{2i}-2^i+1}$),
- $\gcd(2^{\frac{n-1}{2}} + 3 - 2^j, 2^n - 1)$, where n is odd (related to the so-called Welch APN functions $F(x) = x^{\frac{n-1}{2}+3}$),
- $\gcd(2^{(n-1)/2} + 2^{(n-1)/4} - 1 - 2^j, 2^n - 1)$, where $n \equiv 1 \pmod 4$ (related to the so-called Niho APN functions $F(x) = x^{2^{(n-1)/2}+2^{(n-1)/4}-1}$),
- $\gcd(2^{(n-1)/2} + 2^{(3n-1)/4} - 1 - 2^j, 2^n - 1)$, where $n \equiv 3 \pmod 4$ (related to the so-called Niho APN functions $F(x) = x^{2^{(n-1)/2}+2^{(3n-1)/4}-1}$),
- $\gcd(2^n - 2 - 2^j, 2^n - 1)$, where n is odd (related to the so-called inverse APN functions $F(x) = x^{2^n-2}$),
- $\gcd(2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1 - 2^j, 2^n - 1)$, where $n = 5m$ (related to the so-called Dobbertin APN functions $F(x) = x^{2^{4m}+2^{3m}+2^{2m}+2^m-1}$).

We need to see if these classes are included in larger classes of Sidon (resp. sum-free) sets (for instance, if the condition "i is co-prime with n" is necessary).

Remark 3.1 When d is invertible modulo $2^n - 1$, for every positive integer j, we have $\{x \in \mathbb{F}_{2^n}^*; x^{d-2^j} = 1\} = \{x \in \mathbb{F}_{2^n}^*; x^d = x^{2^j}\} = \{x \in \mathbb{F}_{2^n}^*; x = x^{2^j d'}\} = \{x \in \mathbb{F}_{2^n}^*; x^{2^{n-j}} = x^{d'}\} = \{x \in \mathbb{F}_{2^n}^*; x^{d'-2^{n-j}} = 1\}$ where d' stands for the inverse of d modulo $2^n - 1$.

4 Study of Sidon multiplicative subgroups of $\mathbb{F}_{2^n}^*$

In this section, we visit some infinite classes of exponents d for which we are able to determine whether the multiplicative subgroup of $\mathbb{F}_{2^n}^*$ equal to $\{x \in \mathbb{F}_{2^n}^*; x^d = 1\}$ of order $e = \gcd(d, 2^n - 1)$ (and so equal to $\{x \in \mathbb{F}_{2^n}^*; x^e = 1\}$) is a Sidon set in $(\mathbb{F}_{2^n}, +)$. Note that when dealing with a value d, we deal in fact with a whole equivalence class: if two exponents d and d' are conjugate mod $2^n - 1$ (i.e. if $d' \equiv 2^i d \pmod{2^n - 1}$ for some i), or if more generally $d' \equiv kd \pmod{2^n - 1}$ where k is any number co-prime with $2^n - 1$, then $\gcd(d', 2^n - 1) = \gcd(d, 2^n - 1)$.

4.1 A characterization

Let us start with a preliminary result which is included in the proof of the main theorem in [5] but not explicitly stated, and which will be useful in the sequel. For making the paper self-contained, we include its proof.

Lemma 4.1 *Let n and d be positive integers and let $e = \gcd(d, 2^n - 1)$. The multiplicative subgroup $G_e = \{x \in \mathbb{F}_{2^n}^\star \mid x^d = 1\} = \{x \in \mathbb{F}_{2^n}^\star \mid x^e = 1\}$ of order e is a Sidon set if and only if the only solutions $(x, y) \in G_e^2$ of equation $(x+1)^d = (y+1)^d$ are the trivial solutions (x, y) such that $x = y$ or $x = \frac{1}{y}$.*

Proof Writing $z = x + a$ in Definition 1.1 shows that G_e is a Sidon set if and only if, for every $a, x, y \in \mathbb{F}_{2^n}^*$,

$$x^d = (x + a)^d = y^d = (y + a)^d = 1 \tag{7}$$

implies $x = y$ or $x = y + a$.

Assume that the condition of Lemma 4.1 is satisfied and write $x = au$ and $y = av$ in (7) with $u \in \mathbb{F}_{2^n}$ and $v \in \mathbb{F}_{2^n}$. Then, (7) becomes:

$$u^d = (u + 1)^d = v^d = (v + 1)^d = \frac{1}{a^d}. \tag{8}$$

According to the equality between the first and the third terms in (8), one gets that $v = uz$ with $z \in G_e$. Considering the equality between the second and the fourth terms in (8), one gets that $uz + 1 = \lambda(u + 1)$ with $\lambda \in G_e$. If $\lambda = z$, we have $\lambda = z = 1$; in this case, $v = u$ and $x = y$. Assume from now on $\lambda \neq z$. Then, we get from $uz + 1 = \lambda(u + 1)$ that $u = \frac{\lambda+1}{\lambda+z}$ from which we deduce that $u + 1 = \frac{z+1}{z+\lambda}$ and $v + 1 = \frac{z(\lambda+1)}{z+\lambda} + 1 = \frac{\lambda(z+1)}{z+\lambda}$. One therefore must have the following equations from $u^d = (v + 1)^d$, the equality between the first and fourth terms in equation (8),

$$\frac{(\lambda + 1)^d}{(\lambda + z)^d} = \frac{(z + 1)^d}{(z + \lambda)^d} \iff (\lambda + 1)^d = (z + 1)^d.$$

That implies that $\lambda = \frac{1}{z}$ (since $\lambda \neq z$), that is,

$$v = \frac{z(\frac{1}{z}+1)}{z+\frac{1}{z}} = \frac{z(z+1)}{z^2+1} = \frac{z}{z+1},$$

from which we deduce that $y = av = au + a = x + a$.
Conversely, assume that G_e is a Sidon set. Let $x \in G_e$ and $y \in G_e$ be such that $(x+1)^d = (y+1)^d$. There exists $\rho \in G_e$ such that $x+1 = \rho(y+1) = \rho y + \rho$. Now, x, 1, ρy and ρ are four elements of G_e which is a Sidon set. Hence, either $\rho = 1$, that is, $x = y$ or $\rho = x$ and $\rho y = 1$, that is $x = \frac{1}{y}$. □

We deduce the following useful corollary, in which the polynomials are viewed in $\mathbb{F}_{2^n}[X]/(X^{2^n} + X)$:

Corollary 4.2 *Let n and d be positive integers and $e = \gcd(d, 2^n - 1)$. The multiplicative subgroup $G_e = \{x \in \mathbb{F}_{2^n}^\star \mid x^d = 1\} = \{x \in \mathbb{F}_{2^n}^\star \mid x^e = 1\}$ of order e is a Sidon set if and only if, for every dth-power u of an element of $\mathbb{F}_{2^n}^*$, the polynomial $\gcd(X^d + 1, (X + 1)^d + u)$ has at most two zeros in $\mathbb{F}_{2^n}$. For $u = a^d$ where $a \in \mathbb{F}_{2^n}^\star$, this condition is equivalent to: the set $\{\frac{x}{a+x}, x \in (a + G_e) \cap G_e\}$ has at most two elements. Still equivalently, the polynomial $\gcd(X^d + 1, (X + 1)^d + u, X^{2^n} + X) = \gcd(X^e + 1, (X + 1)^e + u)$ has degree at most 2.*

Proof According to Lemma 4.1, G_e is a Sidon set if and only if, for every $u \in \mathbb{F}_{2^n}$, there exist in $\mathbb{F}_{2^n}$ at most two common zeros of $X^d + 1$ and $(X + 1)^d + u$ (and if there are two such zeros, they are inverses of each other). Note that u can be taken nonzero, since for $u = 0$ there is exactly one common zero. Furthermore, if u is not the dth-power of an element of $\mathbb{F}_{2^n}$ then $\gcd(X^d + 1, (X + 1)^d + u)$ has no zero in $\mathbb{F}_{2^n}$. Hence, G_e is a Sidon set if and only if, for every dth-power u of an element of $\mathbb{F}_{2^n}^*$, the polynomial $\gcd(X^d + 1, (X + 1)^d + u)$ has as most two zeros in $\mathbb{F}_{2^n}$.

For $u = a^d$ where $a \in \mathbb{F}_{2^n}^\star$, an element y is a zero of $\gcd(X^d + 1, (X + 1)^d + u)$ if and only if $y \in G_e$ and $y = 1 + az$ for some z in G_e. Observe then that $y = \frac{z^{-1}y}{a+z^{-1}y}$ (since $z^{-1}y + a = z^{-1}$) and that $z^{-1}y \in (a + G_e) \cap G_e$.
Conversely, let $y = \frac{x}{a+x}$ with $x \in (a + G_e) \cap G_e$. Then, $y^d = 1$ and $(y + 1)^d = (\frac{a}{a+x})^d = a^d$ proving that y is a zero of $\gcd(X^d + 1, (X + 1)^d + a^d)$.

Hence, the set of zeros of $\gcd(X^d + 1, (X + 1)^d + a^d)$ is $\{\frac{x}{a+x}, x \in (a + G_e) \cap G_e\}$. The rest of the proof is obvious: since $X^{2^n} + X$ splits and its zeros are the elements of $\mathbb{F}_{2^n}$, we have for every polynomial $P(X) \in \mathbb{F}_{2^n}[X]$ that $\gcd(P(X), X^{2^n} + X) = \prod_{v \in V}(X + v)$, where V is the set of zeros of $P(X)$ in $\mathbb{F}_{2^n}$. We have then $\gcd(X^d + 1, X^{2^n} + X) = X^e + 1$ and $\gcd((X + 1)^d + u, X^{2^n} + X) = (X + 1)^e + u$. □

Remark 4.3 Checking the condition on the number of zeros of the equation in Corollary 4.2 has complexity $\mathcal{O}(2^n)$, while checking the last condition has average complexity $\mathcal{O}(n)$, see [7].

4.2 Study of some classical multiplicative subgroups of $\mathbb{F}_{2^n}^*$

4.2.1 Generalized Gold and Kasami exponents

We study first the exponents $2^j + 1$, which we shall call generalized Gold exponents (Gold exponents being equal to $2^j + 1$ with the additional condition that j is co-prime with n so that $2^j + 1$ can be an APN exponent).

Proposition 4.4 *For every pair of positive integers n and j, let $e = \gcd(2^j+1, 2^n-1)$, then the multiplicative subgroup $G_e = \{x \in \mathbb{F}_{2^n};\ x^{2^j+1} = 1\} = \{x \in \mathbb{F}_{2^n};\ x^e = 1\}$ of order e is a Sidon set.*

Proof It is easily seen by applying the Euclidean algorithm that $\gcd(X^{2^j+1}+1, (X+1)^{2^j+1}+u) = \gcd(X^{2^j+1}+1, X^{2^j}+X+u) = \gcd(X^{2^j}+X+u, X^2+uX+1)$. □

In particular, when j and n are such that $2^j + 1$ divides $2^n - 1$, that is, when $j \geq 2$ divides n and $\frac{n}{j}$ is even, G_{2^j+1} is a Sidon set.

Remark 4.5 Let us see if this property allows the sizes of Sidon sets in $(\mathbb{F}_{2^n}, +)$ to reach values near the upper bound $\lfloor \frac{1+\sqrt{2^{n+3}-7}}{2} \rfloor$. Since $2^j + 1$ and $2^j - 1$ are co-prime, The order of G_e equals $\gcd(2^j + 1, 2^n - 1) = \frac{\gcd(2^{2j}-1, 2^n-1)}{\gcd(2^j-1, 2^n-1)} = \frac{2^{\gcd(2j,n)}-1}{2^{\gcd(j,n)}-1}$, which equals 1 if $\gcd(2j, n) = \gcd(j, n)$ and $2^{\gcd(j,n)} + 1$ otherwise. The largest possible value of $\gcd(2^j + 1, 2^n - 1)$ is then when n is even and $j = \frac{n}{2}$; it equals $2^{\frac{n}{2}} + 1$, which is not far from $\lfloor \frac{1+\sqrt{2^{n+3}-7}}{2} \rfloor$ but not close either.

Let us now study the other well-known class of exponents in symmetric cryptography: the generalized Kasami exponents $4^j - 2^j + 1$. Let n and j be positive integers and let $e = \gcd(4^j - 2^j + 1, 2^n - 1)$. We have: $(4^j - 2^j + 1)(2^j + 1) = (2^{2j} - 2^j + 1)(2^j + 1) = 2^{3j} + 1$, and $4^j - 2^j + 1$ then divides $2^{3j} + 1$, which implies $G_e = \{x \in \mathbb{F}_{2^n}^\star \mid x^d = 1\} \subseteq G_{\gcd(2^{3j}+1, 2^n-1)}$. Any subset of a Sidon set being a Sidon set, we deduce:

Corollary 4.6 *For every pair of positive integers n and j, let $e = \gcd(4^j - 2^j + 1, 2^n - 1)$, then the multiplicative subgroup G_e of order e is a Sidon set.*

Let us briefly study the other divisors of $2^j + 1$, obtained by factorizing $2^j + 1$ in $\mathbb{Z}$ differently from $2^{3j} + 1 = (2^j + 1)(2^{2j} - 2^j + 1)$. They will straightforwardly provide Sidon sets; we mention them because of the possible applications to APN exponents. A first example comes from the so-called Aurifeuillian factorization $2^{4k+2} + 1 = (2^{2k+1} - 2^{k+1} + 1)(2^{2k+1} + 2^{k+1} + 1)$, which shows that:

Corollary 4.7 *For every pair of positive integers n and j, let $e = \gcd(2^{2k+1} - 2^{k+1} + 1, 2^n - 1)$ or $e = \gcd(2^{2k+1} + 2^{k+1} + 1, 2^n - 1)$, then G_e is a Sidon set.*

Recall also that, for every positive integer k, the cyclotomic polynomial ϕ_k is the unitary polynomial over $\mathbb{Z}$ whose zeros are all the primitive kth roots of unity in $\mathbb{C}$. Every ϕ_k is irreducible, and we have $X^j - 1 = \prod_{k \mid j} \phi_k(X)$. If j is odd, then $X^j + 1 = -((-X)^j - 1)$ equals $\pm \prod_{k \mid j} \phi_k(-X)$ and every product of $|\phi_k(-2)|$ for distinct divisors k of j is a divisor of $2^j + 1$. Hence:

Corollary 4.8 *Let j be odd and $e = \prod_{k\in K} |\phi_k(-2)|$, where K is a set of divisors of j, then G_e is a Sidon set.*

Also, every product of $\phi_k(-2^\ell)$ for distinct divisors k of j and some ℓ is a divisor of $2^{j\ell}+1$.

4.2.2 Dillon-like exponents

Starting with $e = 3$ and increasing the value of e, the first value of e which is odd (so that it can be a divisor of $2^n - 1$) and which is not a generalized Gold exponent equals $7 = 2^3 - 1$. Let us study the exponents of the form $2^j - 1$, that we call Dillon-like, because Dillon in his thesis studied the bent functions of the form $f(x) = tr(ax^{2^m-1})$ where $n = 2m$. They behave very differently from the generalized Gold exponents, since we have:

Proposition 4.9 *Let n be a positive integer, let $d = 2^j - 1$ for some j and $e = \gcd(d, 2^n - 1)$. Then, G_e is a Sidon set if and only if $\gcd(j, n) \leq 2$. Equivalently, if r is a divisor of n, then the multiplicative subgroup G_{2^r-1} of order $2^r - 1$ is a Sidon set if and only if $r \leq 2$.*

Proof We have $e = \gcd(2^j - 1, 2^n - 1) = 2^r - 1$ with $r = \gcd(j, n)$, and $G_e = \mathbb{F}_{2^r}^*$. Hence, G_e is a Sidon set if and only if $r \leq 2$. (Indeed, if $r \geq 3$, then G_e contains a 2-dimensional affine subspace not containing 0 and if $r \leq 2$, then it is clear that G_e is a Sidon set.) □

Remark 4.10 Let us see how Corollary 4.2 applies. For every $u \in \mathbb{F}_{2^n}^*$, we have $\gcd(X^{2^j-1} + 1, (X+1)^{2^j-1} + u) = \gcd(X^{2^j-1} + 1, \sum_{k=1}^{2^j-2} X^k + u) = \gcd(\sum_{k=1}^{2^j-2} X^k + u, (u+1)(X+1))$, since $(X+1)(\sum_{k=1}^{2^j-2} X^k + u) = X^{2^j-1} + 1 + (u+1)(X+1)$. If $u \neq 1$ then we deduce that $\gcd(X^{2^j-1} + 1, (X+1)^{2^j-1} + u)$ has at most one zero, whatever is j. If $u = 1$ then $\gcd(X^{2^j-1} + 1, (X+1)^{2^j-1} + 1) = \sum_{k=0}^{2^j-2} X^k = \frac{X^{2^j-1}+1}{X+1}$ has at most two zeros if and only if $\mathbb{F}_{2^j}^* \cap \mathbb{F}_{2^n}^* \setminus \{1\}$ has at most 2 elements, that is, $\gcd(j, n) \leq 2$.

Remark 4.11 If $\gcd(n, j) = 2$ then $G_e = \mathbb{F}_4^\star$ and, if $\gcd(n, j) = 1$ then $G_e = \{1\}$. In both cases G_e is a Sidon set.

4.2.3 Generalized Welch exponents

We are now interested in $d = 2^j + 3$, which we shall call generalized Welch exponent, since for n odd and $j = \frac{n-1}{2}$, this is the well-known Welch exponent.

Proposition 4.12 *Let j and n be two positive integers and let $e = \gcd(2^j + 3, 2^n - 1)$. Then:*

- *If $j \equiv 0 \pmod 3$ or $j \equiv 1 \pmod 3$, then G_e is a Sidon set,*
- *If $j \equiv 2 \pmod 3$, then G_e is a Sidon set if and only if n is not a multiple of 3.*

Proof According to Corollary 4.2, G_e is a Sidon set if and only if, for every $u \in \mathbb{F}_{2^n}^*$, $\gcd(X^{2^j+3}+1, (X+1)^{2^j+3}+u)$ has at most two zeros in $\mathbb{F}_{2^n}$. Applying the division process of the Euclidean algorithm, we obtain $\gcd(X^{2^j+3}+1, (X+1)^{2^j+3}+u) = \gcd(X^{2^j+3}+1, X^{2^j+2}+X^{2^j+1}+X^{2^j}+X^3+X^2+X+u) = \gcd(X^{2^j+2}+X^{2^j+1}+X^{2^j}+X^3+X^2+X+u, X^{2^j}+X^4+(u+1)X+u+1) = \gcd(X^{2^j}+X^4+(u+1)X+u+1, X^6+X^5+X^4+uX^3+X^2+X+1)$.
Suppose that $u = 1$. Note that $(X^6+X^5+X^4+X^3+X^2+X+1)(X^2+X) = X^8+X$ and:

$$X^{2^j}+X^4 \pmod{X^8+X} = \begin{cases} X^4+X & \text{if } j \equiv 0 \pmod 3 \\ X^4+X^2 & \text{if } j \equiv 1 \pmod 3 \\ 0 & \text{if } j \equiv 2 \pmod 3. \end{cases}$$

Hence, reducing $X^{2^j}+X^4 \pmod{X^8+X}$ and continuing the Euclidean algorithm one step further gives:

$$\gcd(X^{2^j+3}+1, (X+1)^{2^j+3}+1) = \begin{cases} 1 & \text{if } j \equiv 0 \pmod 3 \\ \gcd(X^4+X^2, X^2+X+1) = 1 & \text{if } j \equiv 1 \pmod 3 \\ X^6+X^5+X^4+X^3+X^2+X+1 & \text{if } j \equiv 2 \pmod 3. \end{cases}$$

By similar calculation, we can show when $u \neq 1$ that

$$\begin{aligned} &\gcd(X^{2^j+3}+1, (X+1)^{2^j+3}+u) \\ &= \begin{cases} \gcd(X^4+uX+u+1, (u+1)X^3+u) & \text{if } j \equiv 0 \pmod 3 \\ \gcd(X^4+X^2+(u+1)X+u+1, (u+1)X^3+X^2+uX+1) & \text{if } j \equiv 1 \pmod 3 \\ \gcd(X^6+X^5+X^4+X^3+X^2+X+1, (u+1)X+u+1) & \text{if } j \equiv 2 \pmod 3 \end{cases} \\ &= \begin{cases} \gcd((u+1)X^3+u, \frac{u^2}{u+1}X+u+1) & \text{if } j \equiv 0 \pmod 3 \\ \gcd((u+1)X^3+X^2+uX+1, \frac{u}{u^2+1}X^2+\frac{u^3+u^2+u}{u^2+1}X+\frac{u^3+u^2+u}{u^2+1}) & \text{if } j \equiv 1 \pmod 3 \\ 1 & \text{if } j \equiv 2 \pmod 3. \end{cases} \end{aligned}$$

Hence, if $j \equiv 0 \pmod 3$ or $j \equiv 1 \pmod 3$, G_e is a Sidon set, and if $j \equiv 2 \pmod 3$, G_e is a Sidon set if and only if the polynomial $X^6+X^5+X^4+X^3+X^2+X+1 = \frac{X^7+1}{X+1}$ has at most two zeros, that is, $|\mathbb{F}_{2^n} \cap \mathbb{F}_8| \leq 4$, that is, 3 does not divide n. □

5 Study of sum-free multiplicative subgroups of $\mathbb{F}_{2^n}^*$

5.1 A characterization

We start with characterizing the sum-free property in a similar way as in Corollary 4.2 (with polynomials viewed in $\mathbb{F}_{2^n}[X]/(X^{2^n}+X)$).

Proposition 5.1 *Let d and n be two positive integers and $e = \gcd(d, 2^n - 1)$. Then, G_e is sum-free if and only if $\gcd(X^d + 1, (X + 1)^d + 1)$ has no zero in $\mathbb{F}_{2^n}$. Equivalently, $\gcd(X^d + 1, (X + 1)^d + 1, X^{2^n} + X) = \gcd(X^e + 1, (X + 1)^e + 1 = 1$.*

Proof We are going to show that G_e is not sum-free if and only if $\gcd(X^d + 1, (X + 1)^d + 1)$ has at least one zero in $\mathbb{F}_{2^n}$. Suppose that G_e is not sum-free. Then, there exists x, y and z in G_e such that $x = y + z$. Observe then that $r = z^{-1}x = 1 + z^{-1}y$ is a zero of $\gcd(X^d + 1, (X + 1)^d + 1)$ because $r^d = 1$ and $(r + 1)^d = 1$. Conversely, suppose that $\gcd(X^d + 1, (X + 1)^d + 1)$ has a zero r. One has $r \in G_e$ and $r + 1 = y$ for some $y \in G_e$, that is, $r = 1 + y \in G_e + G_e$ proving that G_e is not sum-free. The rest of the proof is as in the proof of Corollary 4.2. □

5.2 Study of some classical multiplicative subgroups of $\mathbb{F}_{2^n}^*$

5.2.1 Generalized Gold and Kasami exponents

We apply our characterization to $d = 2^j + 1$. We have seen in the proof of Proposition 4.4 that:

$$\gcd(X^{2^j+1} + 1, (X + 1)^{2^j+1} + u) = \gcd(X^{2^j} + X + u, X^2 + uX + 1).$$

Using that $\gcd(A(X), B(X)) = \gcd(A(X), B(X) \pmod{A(X)})$ for any polynomials A, B and C over $\mathbb{F}_{2^n}$, we have:

$$\begin{aligned}&\gcd(X^{2^j+1} + 1, (X + 1)^{2^j+1} + 1)\\ &\quad = \gcd((X^{2^j} + X + 1) \pmod{X^2 + X + 1}, X^2 + X + 1).\end{aligned}$$

Now,

$$X^{2^j} + X + 1 \pmod{X^2 + X + 1} = \begin{cases} 1 & \text{if } j \text{ is even} \\ 0 & \text{if } j \text{ is odd} \end{cases}$$

Hence,

$$\gcd(X^{2^j+1} + 1, (X + 1)^{2^j+1} + 1) = \begin{cases} 1 & \text{if } j \text{ is even} \\ X^2 + X + 1 & \text{if } j \text{ is odd} \end{cases} \tag{9}$$

Proposition 5.2 *Let n and j be two positive integers and $e = \gcd(2^j + 1, 2^n - 1)$. Then, G_e is sum-free if and only if n is odd or j is even.*

Proof According to (9), $\gcd(X^{2^j+1} + 1, (X + 1)^{2^j+1} + 1)$ has no zero in $\mathbb{F}_{2^n}$ if and only if j is even or n is odd (since $1 + X + X^2$ is irreducible over $\mathbb{F}_{2^n}$ if and only if n is odd). □

Since, for $e = \gcd(4^j - 2^j + 1, 2^n - 1)$ and $e' = \gcd(2^{3j} + 1, 2^n - 1)$, we have $G_e \subseteq G_{e'}$, and since any subset of a sum-free set is a sum-free set, we deduce that, if n is odd or j is even, then G_e is sum-free. But we shall have a more precise and more general result below in Proposition 6.3.

5.2.2 Dillon-like exponents

The proof of Proposition 4.9 shows that:

Proposition 5.3 *Let n be a positive integer, let $d = 2^j - 1$ for some j and $e = \gcd(d, 2^n - 1)$. Then, G_e is sum-free if and only if $\gcd(j, n) = 1$.*

5.2.3 Generalized Welch exponents

We have made the necessary calculations in Sect. 4.2.3. We have:

$$\gcd(X^{2^j+3} + 1, (X+1)^{2^j+3} + 1) = \begin{cases} 1 & \text{if } j \equiv 0 \pmod 3 \\ & \text{or } j \equiv 1 \pmod 3 \\ X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 & \text{if } j \equiv 2 \pmod 3. \end{cases} \tag{10}$$

Hence, according to Proposition 5.1, if $j \equiv 0 \pmod 3$ or $j \equiv 1 \pmod 3$, G_e is a sum-free set, and if $j \equiv 2 \pmod 3$, G_e is a sum-free set if and only if the polynomial $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = \frac{X^7+1}{X+1}$ has no zero in $\mathbb{F}_{2^n}$, that is, $\mathbb{F}_{2^n} \cap \mathbb{F}_8 = \mathbb{F}_2$, that is, 3 does not divide n:

Proposition 5.4 *Let j and n be two positive integers and $e = \gcd(2^j + 3, 2^n - 1)$. Then,*

- *If $j \equiv 0 \pmod 3$ or $j \equiv 1 \pmod 3$, G_e is sum-free,*
- *If $j \equiv 2 \pmod 3$, G_e is sum-free if and only if n is not a multiple of 3.*

Remark 5.5 Note that the conditions of Proposition 4.12 and Proposition 5.4 are the same. That says that G_e is a sum-free Sidon set or not when e is a generalized Welch exponent.

6 More Sidon and sum-free multiplicative subgroups of $\mathbb{F}_{2^n}^*$ in relation with the result of [5]

Let d, i and n be positive integers such that $d \not\equiv 2^i \pmod{2^n - 1}$ Because of Theorem 1.3, we are now interested in considering multiplicative groups of orders of the form $\gcd(d - 2^i, 2^n - 1)$. To this end, according to Corollary 4.2 and Proposition 4, we need to count the zeros of $\gcd(X^{d-2^i} + 1, (X+1)^{d-2^i} + u)$ (polynomials viewed in $\mathbb{F}_{2^n}[X]/(X^{2^n} + X)$). Now, recall that, if $\gcd(a_1, a_2) = 1$, then $\gcd(b, a_1 a_2) = \gcd(b, a_1)\gcd(b, a_2)$ for every b , where a_1, a_2, b can be integers or polynomials. Hence, if $\gcd(b_1, b_2) = \gcd(a_1, a_2) = 1$, we have $\gcd(b_1 b_2, a_1 a_2) = \prod_{i,j=1,2} \gcd(a_i, b_j)$. We have:

$$X^d + X^{2^i} = (X^{d-2^i} + 1)X^{2^i}$$
$$(X+1)^d + u(X+1)^{2^i} = ((X+1)^{d-2^i} + u)(X+1)^{2^i}$$

and, for $u \neq 0$, $\gcd(X^{d-2^i}+1, X^{2^i}) = \gcd((X+1)^{d-2^i}+u, (X+1)^{2^i}) = 1$, since $d \not\equiv 2^i \pmod{2^n-1}$ Hence, when $u \neq 0$, we have:

$$\begin{aligned}
&\gcd(X^d + X^{2^i}, (X+1)^d + u(X+1)^{2^i}) \\
&\quad = \gcd(X^{d-2^i}+1, (X+1)^{d-2^i}+u)\gcd(X^{d-2^i}+1, (X+1)^{2^i}) \\
&\qquad \times \gcd(X^{2^i}, (X+1)^{d-2^i}+u)\gcd(X^{2^i}, (X+1)^{2^i}) \\
&\quad = \gcd(X^{d-2^i}+1, (X+1)^{d-2^i}+u)\gcd(X^{d-2^i}+1, (X+1)^{2^i}) \\
&\qquad \times \gcd(X^{2^i}, (X+1)^{d-2^i}+u).
\end{aligned}$$

Observe that the set of zeros of $\gcd(X^{d-2^i}+1, (X+1)^{2^i})$ is $\{1\}$ while the unique possible zero of $\gcd(X^{2^i}, (X+1)^{d-2^i}+u)$ is 0 (more precisely, 0 is a zero if $u = 1$ and there is no zero in $\mathbb{F}_{2^n}$ otherwise).

On the other hand, if $u \neq 0$, then neither 0 nor 1 is a zero of $\gcd(X^{d-2^i}+1, (X+1)^{d-2^i}+u)$. Hence:

Lemma 6.1 *Let d, i and n be positive integers such that $d \not\equiv 2^i \pmod{2^n-1}$ and $u \neq 0$ in $\mathbb{F}_{2^n}$. The zeros of $\gcd(X^{d-2^i}+1, (X+1)^{d-2^i}+u)$ (polynomials viewed in $\mathbb{F}_{2^n}[X]/(X^{2^n}+X)$) are those zeros of $\gcd(X^d+X^{2^i}, (X+1)^d+u(X+1)^{2^i})$ which are not in $\mathbb{F}_2$.*

From Theorem 1.3, Corollary 4.2, Proposition 5.1 and Lemma 6.1, we deduce:

Corollary 6.2 *If d is an APN exponent, then for every integer i and for every $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, the polynomial $\gcd(X^d+X^{2^i}, (X+1)^d+u(X+1)^{2^i})$ has at most two zeros in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$, and for $u = 1$, this same polynomial has no zero in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$.*

Let us take now $d = 2^j+1$ where j is a positive integer. Suppose that $u = 1$. Then, $\gcd(X^{2^j+1}+X^{2^i}, (X+1)^{2^j+1}+(X+1)^{2^i}) = \gcd(X^{2^j+1}+X^{2^i}, X^{2^j}+X) = \gcd(X^{2^i}+X^2, X^{2^j}+X)$. Hence, the set of zeros of $\gcd(X^{2^j+1}+X^{2^i}, (X+1)^{2^j+1}+(X+1)^{2^i})$ is $\mathbb{F}_{2^n} \cap \mathbb{F}_{2^j} \cap \mathbb{F}_{2^{i-1}} = \mathbb{F}_{2^{\gcd(n,j,i-1)}}$. Therefore, according to Proposition 5.1 and to Lemma 6.1, we have:

Proposition 6.3 *Let n and j be positive integers and $e = \gcd(2^j-2^i+1, 2^n-1)$. Then, G_e is sum-free if and only if $\gcd(n, j, i-1) = 1$*

For $j = 2i$, the condition becomes n odd or i even.

The calculations above show that a necessary condition for G_e to be a Sidon set is that $\gcd(n, j, i-1) \leq 2$. Suppose now that $u \notin \mathbb{F}_2$. Then, $\gcd(X^{2^j+1}+X^{2^i}, (X+1)^{2^j+1}+u(X+1)^{2^i}) = \gcd(X^{2^j+1}+X^{2^i}, X^{2^j}+(u+1)X^{2^i}+X+(u+1)) = \gcd(X^{2^j+1}+X^{2^i}, uX^{2^i}+X^2+X+(u+1)) = \gcd(X^{2^j+1}+\frac{1}{u}X^2+\frac{1}{u}X+\frac{u+1}{u}, uX^{2^i}+X^2+X+(u+1))$. A common zero x of $X^{2^j+1}+X^{2^i}$ and $(X+1)^{2^j+1}+u(X+1)^{2^i}$ is then a common zero of $X^{2^j+1}+X^{2^i}$ and $X^{2^j}+(u+1)X^{2^i}+X+(u+1)$, that is, satisfies $x^{2^j+1} = x^{2^i}$ and $x^{2^j}+x = (u+1)(x^{2^i}+1)$. In other words, the function $x \in G_e \setminus \{1\} \mapsto \frac{x^{2^j}+x}{x^{2^i}+1}$ takes each of its values at most 2 times.

7 Conclusions

In this paper, we have characterized by the gcd of polynomials when multiplicative subgroups of $\mathbb{F}_{2^n}^*$ are Sidon sets (resp. sum-free sets) in the group $(\mathbb{F}_{2^n}, +)$. We have deduced the determination of those Sidon (resp. sum-free) multiplicative subgroups whose orders have the so-called Dillon-like form $\gcd(2^i - 1, 2^n - 1)$, Gold-like form $\gcd(2^i + 1, 2^n - 1)$ and Welch-like form $\gcd(2^i + 3, 2^n - 1)$. These characterizations show the interest of using a multiplicative structure when studying an additive property. In the appendix we give two tables, taken from [5], and giving, respectively, the classes of Sidon and sum-free multiplicative subgroups, and the corresponding superclasses (called approximate) which result from the characterizations of the present paper. These tables illustrate for $n \leq 15$ that approximate Sidon–sum-free groups are good approximation of Sidon–sum-free groups. This means that with our results, we cover almost all cases of Sidon–sum-free multiplicative subgroups, for $n \leq 15$.

Appendix

See Tables 1 and 2.

Table 1 Divisors of $2^n - 1$ which are Sidon/sum-free

n	Specification	Values
3	Sidon/sum-free	1
4	Sidon	1, 3, 5
	Sum-free	1, 5
5	Sidon/sum-free	1
6	Sidon	1, 3, 9
	Sum-free	1
7	Sidon/sum-free	1
8	Sidon	1, 3, 5, 17
	Sum-free	1, 5, 17
9	Sidon/sum-free	1
10	Sidon	1, 3, 11, 33
	Sum-free	1, 11
11	Sidon	1, 23
	Sum-free	1, 23, 89
12	Sidon	1, 3, 5, 9, 13, 39, 65
	Sum-free	1, 5, 13, 65
13	Sidon/sum-free	1
14	Sidon	1, 3, 43, 129
	Sum-free	1, 43
15	Sidon	1, 151
	Sum-free	1, 151

Table 2 Approximate Sidon/Sum-free calculations

n	Specification	Values
3	Approximate Sidon	1
	Approximate sum-free	1
4	Approximate Sidon	1, 3, 5
	Approximate sum-free	1, 5
5	Approximate Sidon	1
	Approximate sum-free	1
6	Approximate Sidon	1, 3, 9
	Approximate sum-free	1
7	Approximate Sidon	1
	Approximate sum-free	1
8	Approximate Sidon	1, 3, 5, 17, 51, 85
	Approximate sum-free	1, 5, 17, 85
9	Approximate Sidon	1, 73
	Approximate sum-free	1, 73
10	Approximate Sidon	1, 3, 11, 33
	Approximate sum-free	1, 11
11	Approximate Sidon	1, 23, 89
	Approximate sum-free	1, 23, 89
12	Approximate Sidon	1, 3, 5, 9, 13, 39, 65, 117
	Approximate sum-free	1, 5, 13, 65
13	Approximate Sidon	1
	Approximate sum-free	1
14	Approximate Sidon	1, 3, 43, 129
	Approximate sum-free	1, 43
15	Approximate Sidon	1, 151
	Approximate sum-free	1, 151

References

1. Babai, L., Sós, V.T.: Sidon sets in groups and induced subgraphs of Cayley graphs. Europ. J. Combin. **6**(2), 101–114 (1985)
2. Carlet, C.: Vectorial Boolean functions for cryptography. chapter of the monography. In: Crama, Y., Hammer, P. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Pres, Cambridge (2010)
3. Carlet, C.: Characterizations of the differential uniformity of vectorial functions by the Walsh transform. IEEE Trans. Inf. Theory **64**(9), 6443–6453 (2018). (preliminary version available in IACR Cryptology ePrint Archive, http://eprint.iacr.org/2017/516, 2017)
4. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2020)
5. Carlet, C., Picek, S.: On the exponents of APN power functions and Sidon sets, sum-free sets, and Dickson polynomials. IACR Cryptology ePrint Archive (http://eprint.iacr.org/) 2017/1179, (2017)
6. Green, B., Ruzsa, I.Z.: Sum-free sets in Abelian groups. Israel J. Math. **147**, 157–288 (2005)

7. Ma, K., von zur Gathen, J.: Analysis of Euclidean algorithms for polynomials over finite fields. J. Symb. Comput. **9**(4), 429–455 (1990)
8. Tao, T., Vu, V.: Sum-free sets in groups: a survey. ArXiv preprint arXiv:1603.03071, 2016