Cryptography and Communications
https://doi.org/10.1007/s12095-023-00651-5

RESEARCH

An infinite family of 0-APN monomials with two parameters

Nikolay Kaleyski[1] · **Kjetil Nesheim**[1] · **Pantelimon Stănică**[2]

Received: 19 October 2022 / Accepted: 11 May 2023

Abstract
We consider an infinite family of exponents $e(l, k)$ with two parameters, l and k, and derive sufficient conditions for $e(l, k)$ to be 0-APN over $\mathbb{F}_{2^n}$. These conditions allow us to generate, for each choice of l and k, an infinite list of dimensions n where $x^{e(l,k)}$ is 0-APN much more efficiently than in general. We observe that the Gold and Inverse exponents, as well as the inverses of the Gold exponents can be expressed in the form $e(l, k)$ for suitable l and k. We characterize all cases in which $e(l, k)$ can be cyclotomic equivalent to a representative from the Gold, Kasami, Welch, Niho, and Inverse families of exponents. We characterize when $e(l, k)$ can lie in the same cyclotomic coset as the Dobbertin exponent (without considering inverses) and provide computational data showing that the Dobbertin inverse is never equivalent to $e(l, k)$. We computationally test the APN-ness of $e(l, k)$ for small values of l and k over $\mathbb{F}_{2^n}$ for $n \leq 100$, and sketch the limits to which such tests can be performed using currently available technology. We conclude that there are no APN monomials among the tested functions, outside of the known classes.

Keywords APN function · 0-APN function · Power function · Cyclotomic equivalence

Mathematics Subject Classification (2010) 11T06

1 Introduction

We consider vectorial Boolean functions, i.e. mappings over the vector space $\mathbb{F}_2^n$ or, equivalently, the finite field $\mathbb{F}_{2^n}$, where n is some positive integer. The differential uniformity is

Some of the results in this paper were partially presented at Boolean Functions and Their Applications (BFA) 2022. In particular, all results from Section 4 onwards are completely new.

✉ Nikolay Kaleyski
Nikolay.Kaleyski@uib.no

Kjetil Nesheim
kjetil.nesheim@protonmail.com

Pantelimon Stănică
pstanica@nps.edu

[1] Department of Informatics, University of Bergen, 5020 Bergen, Norway

[2] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5212, USA

Published online: 10 July 2023

one of the most important properties of vectorial Boolean functions from a cryptographic point of view since it measures their resistance to attacks such as differential cryptanalysis. More precisely, the differential uniformity Δ_F of a vectorial Boolean function F is desired to be as low as possible. It is simple to see that $\Delta_F \geq 2$ for any vectorial Boolean function F. The best possible functions are thus the ones with $\Delta_F = 2$, which are called almost perfect nonlinear (APN). These functions are of interest since they also correspond to optimal objects and constructions in other fields of mathematics and computer science, including combinatorics, algebra, and coding theory. For instance, APN functions can be related to linear codes with prescribed parameters [1]. The study of APN and PN functions, including finding new instances of such functions and investigating their properties, is thus interesting and relevant from multiple points of view.

Unfortunately, APN functions are generally difficult to find and analyze. To date, we know many instances of APN functions (see e.g. [2, 3]) but very little can be said about their structure in general. We refer the reader to [4, 5] for a detailed overview of cryptographic Boolean functions.

Some of the oldest known instances of APN functions are monomials, or power functions, i.e. functions that can be expressed as polynomials of the form $F(x) = x^d$ over $\mathbb{F}_{2^n}$ for some positive integer d. Due to their relatively simple structure, these are some of the most studied and best understood vectorial Boolean functions, although the area is still riddled with open questions and unsolved problems.

Due to the general difficulty of constructing and analyzing APN functions, weaker notions of APN-ness have been introduced, such as that of partial APN-ness (pAPN-ness) [6] which we focus on in this paper. This means that any APN function is pAPN, but not necessarily vice-versa; and so this weaker notion can be used as a "stepping stone" in formulating constructions of APN functions and analyzing their properties. In particular, one of the motivations behind the notion of partial APN-ness is the possibility of learning more about the structure of APN permutations. We note that the existence of APN permutations over $\mathbb{F}_{2^n}$ with even n (typically referred to as the "big APN problem") is one of the oldest and most important questions in the field of cryptographic Boolean functions; and that, while APN permutations over $\mathbb{F}_{2^n}$ with odd n are known (for instance, all monomial APN functions are of this form), we still know very few examples and constructions of such functions.

In addition to the "big APN problem", one of the most important open questions in the area is the existence of APN monomials inequivalent to the six known families [7]. In the aforementioned paper, it is conjectured that these six known families exhaust all possible cases up to equivalence. According to [4], this conjecture has been computationally verified over $\mathbb{F}_{2^n}$ for all n up to 34, and also up to 42 in the case of even n. Computationally searching for new APN monomials becomes very difficult for large values of n, since not only does the verification of the APN property require more effort, but the number of exponents that need to be checked grows exponentially with n. Finding constructions of 0-APN monomials can thus also be useful for approaching this conjecture, since instead of examining all exponents over $\mathbb{F}_{2^n}$, only a smaller (and more promising set) has to be considered.

While certainly more tractable than APN functions, the behavior of 0-APN monomials is far from trivial, too. In the case of monomials, it is known that x^d is 0-APN over $\mathbb{F}_{2^n}$ for infinitely many dimensions n, and that the set of dimensions can be characterized by computing the factorization of the polynomial $x^d + (x+1)^d + 1$ over $\mathbb{F}_2[x]$ [8]. This is, however, difficult to do theoretically, and computationally, it is only feasible for relatively small values of d; for instance, the *Magma* algebra system [9] that we use for most of our computations struggles with computing such a factorization already for $d \geq 10^7$. While this number may seem large, we recall that if APN exponents distinct from representatives of

the known families exist, they must be over finite fields $\mathbb{F}_{2^n}$ with $n \geq 35$, which involves exploring exponents much larger than this.

In this paper, we define an infinite family of exponents $e(l,k) = \sum_{j=0}^{l-1} 2^{jk}$ with two parameters l and k (that can take any positive integers as values), and give sufficient conditions that n has to satisfy in order for $x^{e(l,k)}$ to be 0-APN over $\mathbb{F}_{2^n}$. For every choice of l and k, our conditions produce infinitely many dimensions n for which the exponent is 0-APN. Furthermore, we discuss how, with the help of some very simple computations, we can characterize the set of all dimensions n for which $x^{e(l,k)}$ is 0-APN. Generating dimensions that satisfy our conditions requires minimal computational effort and amounts to computing the greatest common divisors of some integers. This is possible even for very large exponents of the form $e(l,k)$, e.g. a list of 24242 dimensions n between 1 and 100000 for which $e(100,100) \approx 10^{2980}$ is 0-APN can be computed in a few seconds on *Magma*. One of the advantages of our construction is that it becomes very easy to find dimensions where $x^{e(l,k)}$ is 0-APN; and, as remarked above, only a bit of additional computation is needed in order to characterize the set of all such dimensions.

Another advantage is that the algebraic degree of $e(l,k)$ is easily predictable, e.g. $\deg(e(l,k)) = l$ when $\gcd(k,n) = 1$ and $l < n$, which allows us to characterize with relative ease when the exponents $e(l,k)$ are cyclotomic equivalent to representatives from the known monomial APN families. We mathematically treat all cases, except that of the Dobbertin inverse, where the computations are too technical: the method that we use in our inequivalence proofs depends on the application of Lemma 4.1 to a set of integers describing the binary decomposition of the exponent of the monomial. Part of the lemma's hypothesis is that all these integers are distinct modulo n, and this requires the degenerate cases when two or more of them are congruent modulo n to be treated separately before the lemma can be applied. Handling these cases is conceptually straightforward, but quite lengthy and technical in practice, especially when the number of cases that need to be considered is large. In the case of the inverse Dobbertin exponent, there is a substantial blowup in the number of cases than need to be handled, which would require a lengthy proof spanning tens of pages or even more. Instead of supplying a heavy and technical proof of this form, we provide computational data for $n \leq 200$ showing that $e(l,k)$ can never be equivalent to the inverse of the Dobbertin function except in trivially small dimensions. The range $n \leq 200$ covers all dimensions where the problem of finding new APN monomials can be handled in practice using our current knowledge and resources. Furthermore, we note that the "missing" case of the Dobbertin inverse only concerns odd dimensions n that are multiples of 5, while the theoretical characterizations from the remaining theorems give a complete description of the equivalence to the known families for all other values of n.

We show that the Gold and Inverse APN functions can always be represented in the form $e(l,k)$ for suitable choices of l and k. Moreover, via [10], the inverse of the Gold function $x \mapsto x^{2^r+1}$ over $\mathbb{F}_{2^n}$, n odd, $\gcd(n,r) = 1$, is given by $e(2r, \frac{n+1}{2}) = \sum_{i=0}^{\frac{n-1}{2}} 2^{2ir}$. Furthermore, we show that representatives from the remaining families are never cyclotomic equivalent to $e(l,k)$ except for small dimensions.

Finally, we consider the exponents $e(l,k)$ for small values of l and k, and computationally check for which dimensions n below 100 they are APN. We do not find any new APN exponents, but we see that the computation load needed to test APN-ness grows very quickly with the size of the exponent $e(l,k)$, even more so than with the dimension n. We provide more detailed comments about our computational experiments in Section 5.

Unfortunately, our current computational methods are insufficient to check APN-ness of the exponents in high dimensions. We leave the computational exploration of the $e(l,k)$ exponents as a problem for future work.

2 Preliminaries

Let n be a natural number. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, and by $\mathbb{F}_2^n$ the vector space of dimension n over $\mathbb{F}_2$. The set of non-zero elements of $\mathbb{F}_{2^n}$ is denoted by $\mathbb{F}_{2^n}^*$. A **vectorial Boolean function**, or (n,m)-function, is any mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. We concentrate on the case $n = m$. Any (n,n)-function can be uniquely represented as a univariate polynomial over $\mathbb{F}_{2^n}$ of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

with $a_i \in \mathbb{F}_{2^n}$. This is called the **univariate representation** of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. A **monomial** function, or power function, is any (n,n)-function with univariate representation $F(x) = x^d$ for some natural number d. The **algebraic degree** of F, denoted $\deg(F)$, is the largest (Hamming) weight of i (that is, $\mathrm{wt}(i)$, which is the number of nonzero bits in the binary representation of i), where $a_i \neq 0$.

The **differential uniformity** of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as

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

that is, as the largest number of solutions x to $F(a+x) + F(x) = b$ for any choice of a, b with $a \neq 0$. The differential uniformity is a measurement of the resistance provided by the function to differential cryptanalysis [11], and should be as low as possible. The number of solutions x to any equation of the form $F(a+x)+F(x) = b$ is even, and so the optimal value of the differential uniformity is 2. If $\Delta(F) = 2$, we say that F is **almost perfect nonlinear (APN)**.

The large number of vectorial Boolean functions makes it necessary to consider e.g. APN functions up to some suitable notion of equivalence in order to reduce the number of instances that have to be treated. Such an equivalence relation should leave the differential uniformity invariant, and should be as general as possible (in the sense that its equivalence classes should be as large as possible) in order to leave a small number of representatives that have to be considered. At present, the most general known equivalence relation used in practice is Carlet-Charpin-Zinoviev (CCZ) equivalence. Two (n,n)-functions F and G are said to be **CCZ-equivalent** if there is an affine permutation A of $\mathbb{F}_{2^n}^2$ mapping the graph $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph Γ_G of G. CCZ-equivalence is, in general, difficult to test computationally.

In the particular case of monomial functions, however, CCZ-equivalence reduces to a much simpler notion of equivalence. We say that $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $F(x) = x^d$ and $G(x) = x^e$ are **cyclotomic equivalent** if there exists a natural number a such that either $2^a d$ is in the cyclotomic coset of e modulo $2^n - 1$, i.e.

$$2^a \cdot d \equiv e \pmod{2^n - 1},$$

or the inverse of d modulo $2^n - 1$ is in the cyclotomic coset of e, i.e.

$$2^a \cdot d^{-1} \equiv e \pmod{2^n - 1},$$

provided of course that $\gcd(d, 2^n - 1) = 1$ so that the inverse d^{-1} exists. We know that two monomials are CCZ-equivalent if and only if they are cyclotomic equivalent [12, 13]. Testing cyclotomic equivalence, in contrast to the more general CCZ-equivalence, is quite simple, and amounts to checking whether a small number of modular equations hold.

For natural numbers n, k, we will denote by n Mod k the least positive residue of n modulo k, e.g. 11 Mod $3 = 2$.

At present, we know of six infinite families of APN monomials; these are summarized in Table 1. In [7], it is conjectured that no other APN monomials exist over $\mathbb{F}_{2^n}$ up to cyclotomic equivalence. In [4], it is reported that this has been computationally verified for $n \leq 34$, and for $n \leq 42$ in the case of even n. Despite this, the question of whether the list in Table 1 is exhaustive up to cyclotomic equivalence remains open, and is one of the oldest and hardest unresolved questions in the area of APN functions. It is sometimes referred to as **Dobbertin's conjecture**.

Finding new instances of APN functions is challenging, especially when APN-ness is combined with other desirable properties, e.g. being bijective or being a monomial function. For this reason, various weaker notions of APN-ness have been defined in the literature (see [8, 20], for example). Following [8], we say that a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is **$\mathbf{x_0}$-APN** for some $x_0 \in \mathbb{F}_{2^n}$ if any $y, z \in \mathbb{F}_{2^n}$ satisfying

$$F(x_0) + F(y) + F(z) + F(x_0 + y + z) = 0$$

necessarily satisfy $(x_0 + y)(x_0 + z)(y + z) = 0$. It is straightforward to verify that a function is APN if and only if it is x_0-APN for all $x_0 \in \mathbb{F}_{2^n}$.

In the case of monomials, it is shown [6] that if a monomial is x_0-APN for some $x_0 \neq 0$, then it is also x_1-APN for any $x_1 \neq 0$, and that 1-APN-ness implies 0-APN-ness for monomials. This means that a monomial can be either: APN; 0-APN but not 1-APN; not 0-APN. In this sense, 0-APN-ness is a natural intermediate step towards constructions of APN monomials.

One potential strategy for approaching Dobbertin's conjecture is to describe constructions of 0-APN monomials over fields $\mathbb{F}_{2^n}$ of high dimension n. As outlined in the introduction, in this work we introduce an infinite family of exponents which are particularly tractable from the point of view of 0-APN-ness and cyclotomic equivalence to the known families.

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

Family	Exponent	Conditions	Algebraic degree	Source
Gold	$2^i + 1$	$\gcd(i, n) = 1$	2	[10, 14]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[15, 16]
Welch	$2^t + 3$	$n = 2t + 1$	3	[17]
Niho	$2^t + 2^{t/2} - 1$, t even	$n = 2t + 1$	$(t + 2)/2$	[18]
	$2^t + 2^{(3t+1)/2} - 1$, t odd		$t + 1$	
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[10, 19]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[7]

3 An infinite family of 0-APN exponents with two parameters

In this section, we introduce the exponents $e(l,k)$ and provide sufficient conditions on n in order for $x^{e(l,k)}$ to be 0-APN over $\mathbb{F}_{2^n}$. We recall that any monomial x^d is 0-APN over infinitely many dimensions n, but in general it can be difficult to characterize these dimensions n without doing computations such as factorizing the polynomial $x^d+(x+1)^d+1$ over $\mathbb{F}_2$ (see [21]), which can be a computationally hard task for large values of d. The class of exponents $e(l,k)$ has the advantage of being significantly more tractable in this sense. As outlined in the introduction, we are able to find 24242 dimensions n for which $e(100,100) \approx 10^{2980}$ is 0-APN in a few seconds on *Magma*, while factorizing $x^d+(x+1)^d+1$ is computationally infeasible already for $d \geq 10^7$.

The sufficient conditions can be formulated in two ways. In the proof of Theorem 3.2, we show that if the expression $F(x)+F(1+x)+F(1)$ for $F(x)=x^{e(l,k)}$ vanishes for some $x \in \mathbb{F}_{2^n}$, then x is in $\mathbb{F}_{2^{\gcd(lk,n)}}$, or it satisfies $(x/(x+1))^{e(l-1,k)}=1$. Consequently, if $\gcd(lk,n)=1$ and $\gcd(e(l-1,k),2^n-1)=1$, then both of these cases imply that x is a trivial solution, i.e. $x \in \mathbb{F}_2$.

The second condition, viz. $\gcd(e(l-1,k),2^n-1)=1$, can be replaced by requiring that $\gcd(jk,n)=1$ for all $j \in \{2,\ldots,l\}$ as explained in the remark following the theorem. This "cascading" condition is less general in the sense that it is not satisfied by all dimensions n for which $x^{e(l,k)}$ is 0-APN according to Theorem 3.2. Nonetheless, it is somewhat simpler to evaluate and allows us to easily construct an infinite sequence of dimensions n over which $x^{e(l,k)}$ is 0-APN even more easily.

Definition 3.1 Let l,k be natural numbers. We define the exponent $e(l,k)$ as

$$e(l,k)=\sum_{j=0}^{l-1} 2^{jk}.$$

The exponent $e(l,k)$ can also be expressed as

$$e(l,k)=\frac{2^{lk}-1}{2^k-1}$$

from the formula for the sum of a geometric progression.

Theorem 3.2 *Let n,l,k be natural numbers such that* $\gcd(kl,n)=1$ *and* $\gcd(e(l-1,k),2^n-1)=1$. *Then $x^{e(l,k)}$ is 0-APN over $\mathbb{F}_{2^n}$.*

Proof Denote $e=e(l,k)$. Suppose that $x \in \mathbb{F}_{2^n}$ satisfies $x^e+(x+1)^e+1=0$. For natural numbers $a \leq b$, let $[a,b]=\{a,a+1,\ldots,b\}$, and let $\mathcal{P}I$ denote the power set of a discrete set I. Furthermore, let $x^{2^{kI}}$ denote $\prod_{i\in I} x^{2^{ki}}$. Then $x^e+(x+1)^e+1=0$ can be written as

$$x^e+\sum_{I\in\mathcal{P}[0,l-1]} x^{2^{kI}}+1=\sum_{\substack{I\in\mathcal{P}[0,l-1]\\ I\neq\emptyset,[0,l-1]}} x^{2^{kI}}=0. \tag{1}$$

Raising this to the power 2^k yields

$$\sum_{\substack{I\in\mathcal{P}[1,l]\\ I\neq\emptyset,[1,l]}} x^{2^{kI}}=0.$$

Summing the two expressions causes all terms $x^{2^{kI}}$ corresponding to subsets I that contain neither 0 nor l to cancel out, leaving us with

$$\sum_{\substack{I\in\{x\cup\{0\}|x\in\mathcal{P}[1,l-1]\}\\ I\neq[1,l-1]}} x^{2^{kI}} + \sum_{\substack{I\in\{x\cup\{l\}|x\in\mathcal{P}[1,l-1]\}\\ I\neq[1,l-1]}} x^{2^{kI}} = 0.$$

This then becomes

$$x\left(\sum_{\substack{I\in\mathcal{P}[1,l-1]\\ I\neq[1,l-1]}} x^{2^{kI}}\right) + x^{2^{lk}}\left(\sum_{\substack{I\in\mathcal{P}[1,l-1]\\ I\neq[1,l-1]}} x^{2^{kI}}\right) = \left(x + x^{2^{lk}}\right)\left(\sum_{\substack{I\in\mathcal{P}[1,l-1]\\ I\neq[1,l-1]}} x^{2^{kI}}\right) = 0.$$

If $x + x^{2^{lk}} = 0$, then we must have $x \in \mathbb{F}_{2^{\gcd(n,lk)}}$. However, by assumption, $\gcd(n, lk) = 1$, and so $x \in \mathbb{F}_2$. If $x \neq x^{2^{lk}}$, then we must have

$$\left(\sum_{\substack{I\in\mathcal{P}[1,l-1]\\ I\neq[1,l-1]}} x^{2^{kI}}\right) = \left(\sum_{\substack{I\in\mathcal{P}[0,l-2]\\ I\neq[0,l-2]}} x^{2^{kI}}\right)^{2^k} = 0,$$

instead. Comparing this with (1), we see that this is simply

$$(x^{e(l-1,k)} + (x+1)^{e(l-1,k)})^{2^k} = 0,$$

and hence

$$x^{e(l-1,k)} + (x+1)^{e(l-1,k)} = 0. \tag{2}$$

Clearly $x \neq 0, 1$, and so the above implies $(\frac{x}{x+1})^{e(l-1,k)} = 1$. If the second condition of the hypothesis is satisfied, i.e. $\gcd(e(l-1,k), 2^n - 1) = 1$, then we immediately have $\frac{x}{x+1} = 1$, i.e. $x = x + 1$, which is impossible. Therefore, $x^{e(l,k)}$ is 0-APN. □

Remark 3.3 The proof above could have also been continued by adding (2) to its 2^k-th power; this would have produced the same equation as if we had added the derivative $x^{e(l-1,k)} + (x+1)^{e(l-1,k)} + 1$ to its 2^k-th power since the extra term 1 would have canceled out. By induction on l, we would have obtained the condition that if $\gcd(ik, n) = 1$ for $i = 2, 3, \ldots, l$, then $x^{e(l,k)}$ must be 0-APN. We have tested these conditions computationally, and, as expected, we observed that the condition in the statement of Theorem 3.2 always produces a set of dimensions n that subsumes those given by the alternative condition described in this remark. This is why we have formulated the theorem only in terms of this more general condition, but we state the second condition as a corollary.

Corollary 3.4 *Let n, l, k be natural numbers. Then, if $x^{e(l,k)} + (x+1)^{e(l,k)} + 1$ vanishes for some $x \in \mathbb{F}_{2^n}$, we must have $x \in \mathbb{F}_{2^{\gcd(jk,n)}}$ for some $j \in \{2, 3, \ldots, l\}$.*

In particular, if $\gcd(jk, n) = 1$ for all $j \in \{2, 3, \ldots, l\}$, then $x^{e(l,k)}$ is 0-APN over $\mathbb{F}_{2^n}$.

Remark 3.5 The sufficient conditions of Corollary 3.4 allow us to explicitly determine the set of dimensions n such that $x^{e(l,k)}$ over $\mathbb{F}_{2^n}$ is 0-APN. We can see that for any choice of l and k, there are only finitely many dimensions $m = \gcd(jk, n)$ such that $x^{e(l,k)} + (x+1)^{e(l,k)} + 1$ vanishes on $\mathbb{F}_{2^m}$ but on no proper subfield of $\mathbb{F}_{2^m}$. Consequently, $e(l, k)$ is a 0-APN exponent over $\mathbb{F}_{2^n}$ for any n that is not a multiple of one of these dimensions m.

For instance, the exponent $e(3,2) = 21$ can only violate the 0-APN-ness on $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^4}$ or $\mathbb{F}_{2^2}$ (or any extension field thereof). Hence, x^{21} is 0-APN over $\mathbb{F}_{2^n}$ for any n that is not divisible by 2, 4 and 6. Furthermore, we can computationally verify that x^{21} is 0-APN over $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^4}$, and that it is not 0-APN over $\mathbb{F}_{2^6}$. Thus, x^{21} is 0-APN over $\mathbb{F}_{2^n}$ whenever n is not a multiple of 6. We remark that a proof of the same fact is given for x^{21} in [8] using the factorization of $x^{21}+(x+1)^{21}+1$. The framework described in this remark allows this proof to be easily generalized to any function of the form $x^{e(l,k)}$, and allows us to characterize the values of n for which $x^{e(l,k)}$ is 0-APN for large values of d for which it is not computationally feasible to factor $x^d + (x+1)^d + 1$.

The conditions $\gcd(kl, n) = 1$ and $\gcd(e(l-1,k), 2^n - 1) = 1$ are sufficient for $x^{e(l,k)}$ to be 0-APN over $\mathbb{F}_{2^n}$ but are not necessary in general. The same is true for the "cascading" conditions formulated in Corollary 3.4. In particular, we can observe that the particular statement of the corollary can never be applied to finite fields $\mathbb{F}_{2^n}$ of even extension degree n since $\gcd(2k, n) = 2$, and this violates the conditions in the corollary whenever $l > 1$.

The conditions of the corollary can be refined for instance as follows. Let $d = e(l,k)$. If $\gcd(kl, n) = 2$, then we can see that $x^d + (x+1)^d + 1 = 0$ can only have $x \in \mathbb{F}_4$ as a root, and x^d is not 0-APN only in the case when $x \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Clearly, this happens precisely when $3 \nmid d$. If the exponent is a multiple of 3, therefore, the restriction $\gcd(kl, n) = 1$ can be relaxed to $\gcd(kl, n) \leq 2$.

A similar approach can be applied in general for $\gcd(kl, n) = m$ by imposing the restriction that $x^d + (x+1)^d + 1$ does not vanish on $\mathbb{F}_{2^{\gcd(m,n)}}$. For a fixed m, this essentially means that $d \pmod{2^m - 1}$ must be a 0-APN exponent in $\mathbb{F}_{2^m}$.

A trivial case is when the exponent d satisfies $d \pmod{2^m - 1} \equiv 0$ for some $m > 2$ dividing n. When this happens, the function x^d coincides with the indicator function $1_0(x) = x^{2^m-1}$ over $\mathbb{F}_{2^m}$, and so it is always 0-APN but can never be an APN function (except if $m = 2$). Since the primary motivation for our study is the possibility of identifying new APN monomials, all such cases can be excluded from consideration.

Remark 3.6 To see how discriminating the condition in Theorem 3.2 is, we can perform a simple computational experiment as follows: pick some values of k and l, and generate all dimensions n in some range that satisfy the conditions in Theorem 3.2; by computing the number of roots of $x^e + (x+1)^e + 1 = 0$ for $e = e(l,k)$, we check whether x^e is 0-APN over $\mathbb{F}_{2^n}$ for all n in the range, then compare the two sets. Generating all $e(l,k)$ satisfying the conditions of Theorem 3.2 with $l, k \leq 6$, we found that all 0-APN monomials of the form $e(l,k)$ were covered by our theorem in dimensions $2 \leq n \leq 100$.

Another consideration that we should take into account is the size of the image set of $x^{e(l,k)}$. It is known that any APN monomial x^d over $\mathbb{F}_{2^n}$ is a bijection if n is odd, and is 3-to-1 on $\mathbb{F}_{2^n}^*$ if n is even. Furthermore, we know that this occurs if and only if $\gcd(d, 2^n - 1) = 1$ and $\gcd(d, 2^n - 1) = 3$, respectively. Thus, exponents of the form $e(l,k)$ that do not satisfy this condition can be discarded when searching for new APN monomials. This is the motivation for the following proposition.

Proposition 3.7 *Let l, k, n be natural numbers such that* $\gcd(k, n) = 1$. *Then*

$$\gcd(e(l,k), 2^n - 1) = 2^{\gcd(l,n)} - 1.$$

In particular, $x^{e(l,k)}$ is a permutation if and only if $\gcd(l, n) = 1$, *and it is a* 3*-to-*1 *function if and only if* $\gcd(l, n) = 2$.

Proof Since $\gcd(A, B) = \gcd(CA, B)$ for C with $\gcd(C, B) = 1$, we have that

$$\gcd(e(l,k), 2^n - 1) = \gcd\left(\frac{2^{lk}-1}{2^k-1}, 2^n - 1\right) = \gcd(2^{lk} - 1, 2^n - 1)$$

due to $\gcd(k, n) = 1$ implying $\gcd(2^k - 1, 2^n - 1) = 1$. Again from $\gcd(k, n) = 1$, we have

$$\gcd(2^{lk} - 1, 2^n - 1) = 2^{\gcd(lk,n)} - 1 = 2^{\gcd(l,n)} - 1,$$

which shows our proposition. □

4 Equivalence to known monomial families

In this section, we study when the exponent $e(l, k)$ can be cyclotomic equivalent to an exponent from one of the known families. Recall that two exponents e and d are cyclotomic equivalent modulo n if either e or e^{-1} is in the cyclotomic coset of d modulo $2^n - 1$. For each of the infinite APN families, we treat the two cases separately. In the case of the Dobbertin family, a characterization using our current techniques is too cumbersome due to the large number of degenerate cases that need to be treated before applying Lemma 4.1, and so we supply computational data instead showing that $e(l, k)$ can not be equivalent to the Dobbertin inverse for $n \leq 200$ except for $n = 5$ and $n = 10$. We refer the reader to the discussion at the end of Section 1 for more details about why we have made this decision.

Below, we shall have arguments dealing with the set (or rather, multiset, since we allow for potential repetitions of elements) of exponents in a sum of powers of 2 and we make the convention that if the set contains two "copies" of the same element j, then the set is *compressed* by replacing the two copies of j by $j+1$. For instance, the expression $2^a+2^b+2^c$, for some natural numbers a, b, c corresponds to the set of exponents $\{a, b, c\}$, and if $a = b$ so that $2^a + 2^b + 2^c = 2^{a+1} + 2^c$, then the set compresses to $\{a + 1, c\}$. If S is a set of integers, we will also used the shorthand notation

$$S \bmod n = \{s \bmod n : s \in S\}.$$

Similarly, we will write $A \equiv B \pmod n$ if $A \bmod n = B \bmod n$ for two sets A, B.

In the sequel, we make use of the following simple observation. It is based on the well-known fact that the binary weight of any two integers in the same cyclotomic coset modulo $2^n - 1$ is the same.

Lemma 4.1 *Let $n, M, a_1, a_2, \ldots, a_M, b_1, b_2, \ldots, b_M$, and n be natural numbers such that all a_i for $1 \leq i \leq M$ are distinct modulo n, and all b_i for $1 \leq i \leq M$ are distinct modulo n. Suppose that*

$$\sum_{i=1}^{M} 2^{a_i} \equiv \sum_{i=1}^{M} 2^{b_i} \pmod{2^n - 1}. \tag{3}$$

Then

$$\{a_i \bmod n : 1 \leq i \leq M\} = \{b_i \bmod n : 1 \leq i \leq M\}.$$

Proof Suppose that (3) holds and consider the left-hand side. Since $2^{a_i} \equiv 2^{a_i \bmod n} \pmod{2^n - 1}$, we can assume that $a_i < n$ for all i. Since by assumption all a_i are distinct modulo n, the weight of the sum on the left-hand side will remain unchanged after this

modulation, and we will once again have M terms. Similarly, we can modulate the sum on the right-hand side, and thus assume that $b_i < n$ for all i. Since all the powers of 2 on the left-hand side are distinct, their sum cannot be greater than $2^n - 1$; the same is true for the right-hand side, and so the assumption that the two sums are congruent in fact implies that they are equal. The claim then follows by the uniqueness of the binary expansion. □

In many of the following proofs, we will use the fact that we know the algebraic weight of an exponent d from one of the known families, and we would like to select a value of l such that $\mathrm{wt}(e(l,k) \bmod (2^n-1)) = \mathrm{wt}(d)$. Following Theorem 3.2, we will focus on the cases when $\gcd(n,k) = 1$ and $\gcd(n,k) = 2$. To begin with, we can observe that if $l < n$ and $\gcd(n,k) = 1$, then $\mathrm{wt}(e(l,k)) = l$ since all of the exponents 2^{jk} in $e(l,k) = \sum_j 2^{jk}$ are distinct modulo n.

Observation 4.2 *Let n, l, k be natural numbers such that $l < k$ and $\gcd(l,k) = 1$. Then $\mathrm{wt}(e(l,k) \bmod (2^n-1)) = l$.*

The situation when $\gcd(k,n) = 2$ is slightly more complicated, and it is addressed by the following Lemma 4.4. Note that in the first few cases we only characterize the weight of $e(l,k)$ modulo $2^n - 1$ since this is what we need in the subsequent characterizations. However, in the last case, we show that $e(3n/2 + m, 2t)$ not only has the same weight, but is in fact congruent to $e(m, 2t)$ modulo $2^n - 1$. This shows that there is no need to consider values of l in $e(l, 2t)$ greater than $3n/2$ up to equivalence.

Before proving Lemma 4.4, we first prove the following auxiliary result. It is useful on its own (by reducing the number of values of k that have to be considered up to equivalence), and is also used in the proof of Lemma 4.4.

Lemma 4.3 *The following are true:*

(i) Let l, k, m be natural numbers with $n = 2m$. Then $e(l, m-k)$ and $e(l, m+k)$ are cyclotomic equivalent modulo $2^n - 1$.

(ii) Let l, k, m be natural numbers with $n = 2m+1$. Then $e(l, m-k+1)$ and $e(l, m+k)$ are cyclotomic equivalent modulo $2^n - 1$.

Proof We show (i) first. Let $X = lk + lm + m - k$. We claim that $2^X e(l, m-k) \equiv e(l, m+k) \pmod{2^n - 1}$. Recall that we can write

$$e(l, K) = \frac{2^{lK} - 1}{2^K - 1}.$$

We now multiply the above for $K = m - k$ by 2^X with the aforementioned X. We use the fact that $2m = n \equiv 0 \pmod{n}$, and obtain

$$2^X \frac{2^{l(m-k)} - 1}{2^{m-k} - 1} \equiv \frac{2^{lm-lk+lk+lm+m-k} - 2^{lk+lm+m-k}}{2^{m-k} - 1} \equiv \frac{2^{m-k} - 2^{lk+lm+m-k}}{2^{m-k} - 2^{2m}}$$
$$\equiv \frac{2^{m-k}(1 - 2^{l(k+m)})}{2^{m-k}(1 - 2^{m+k})} \equiv \frac{1 - 2^{l(k+m)}}{1 - 2^{m+k}} \equiv \frac{2^{l(k+m)} - 1}{2^{m+k} - 1} \pmod{2^n - 1}.$$

The claim (ii) follows similarly, by taking $X = l(m+k) + m - k + 1$. □

Lemma 4.4 *Let $\gcd(n, 2t) = 2$, the following statements are true*:

1. $\mathrm{wt}\,(e\,(m, 2t)) = m$ *for any* $0 < m < \frac{n}{2}$;

2. $\mathrm{wt}\left(e\left(\frac{n}{2}+m, 2t\right)\right) = \frac{n}{2}$ *for any* $0 < m < \frac{n}{2}$;
3. $\mathrm{wt}\left(e\left(n+m, 2t\right)\right) = \frac{n}{2} + m$ *for any* $0 < m < \frac{n}{2}$;
4. $e\left(\frac{3n}{2}+m, 2t\right) \equiv e\left(m, 2t\right) \pmod{2^n-1}$ *for any* $0 < m < \frac{n}{2}$.

Proof 1. The first claim is straightforward.

2. Since $\gcd(n, t) = 1$ then $e\left(\frac{n}{2}+m, 2t\right)$ and $e\left(\frac{n}{2}+m, 2\right)$ have the same weight, so it suffices to find the weight of $e\left(\frac{n}{2}+m, 2\right)$. Assuming $0 < m < \frac{n}{2}$, we notice

$$e\left(\frac{n}{2}+m, 2\right) = \sum_{j=0}^{\frac{n}{2}-1} 2^{2j} + \sum_{j=0}^{m-1} 2^{2\left(\frac{n}{2}+j\right)}.$$

We note that

$$2^{2\left(\frac{n}{2}+j\right)} \equiv 2^{2j} \pmod{2^n-1},$$

and so

$$\begin{aligned} e\left(\frac{n}{2}+m, 2\right) &\equiv \left(\sum_{j=0}^{\frac{n}{2}-1} 2^{2j} + \sum_{j=0}^{m-1} 2^{2j}\right) \pmod{2^n-1} \\ &\equiv \left(\sum_{j=0}^{m-1} 2^{2j+1} + \sum_{j=m}^{\frac{n}{2}-1} 2^{2j}\right) \pmod{2^n-1} \end{aligned}$$

has weight $m + \left(\frac{n}{2} - m\right) = \frac{n}{2}$.

3. Assuming $0 < m < \frac{n}{2}$, we note that

$$e(n+m, 2) = \sum_{j=0}^{n-1} 2^{2j} + \sum_{j=0}^{m-1} 2^{2(n+j)},$$

and that

$$\sum_{j=0}^{n-1} 2^{2j} = \sum_{j=0}^{\frac{n}{2}-1} 2^{2j} + \sum_{j=0}^{\frac{n}{2}-1} 2^{2\left(\frac{n}{2}+j\right)} \equiv \left(\sum_{j=0}^{\frac{n}{2}-1} 2^{2j+1}\right) \pmod{2^n-1},$$

so that

$$e(n+m, 2) \equiv \left(\sum_{j=0}^{\frac{n}{2}-1} 2^{2j+1} + \sum_{j=0}^{m-1} 2^{2j}\right) \pmod{2^n-1}.$$

It follows that $e(n+m, 2)$ has weight $\frac{n}{2} + m$. The general case of $t > 1$ is treated in the following way. Observe that

$$e\left(n+m, 2t\right) = \sum_{j=0}^{n-1} 2^{2tj} + \sum_{j=0}^{m-1} 2^{2t(n+j)} \equiv \sum_{j=0}^{n-1} 2^{2tj} + \sum_{j=0}^{m-1} 2^{2tj} \pmod{2^n-1}.$$

To prove our claim, we will argue that the first sum compresses to precisely $n/2$ terms, all of which have *odd* exponents. For that, we will show that given $0 \le j_1 < n/2$, there is a unique $n/2 \le j_2 < n$ (j_2 cannot be in the interval $[0, n/2)$, as we will see below) such that $2^{2tj_1} \equiv 2^{2tj_2} \pmod{2^n-1}$ (the situation is similar if we start with $n/2 \le j_1 < n$). Via Lemma 4.3, we know that one can take $2t < n/2$, so we will assume that from here on in our argument. Since $\gcd(n, 2t) = 2$, then $\gcd(n, t) = 1$. First, given $0 \le j_1 < n/2$,

we can take $j_2 = n/2 + j_1$. Then $2^{2tj_2} - 2^{2tj_1} = 2^{2tj_1}\left(2^{2t(j_2-j_1)} - 1\right) \equiv 0 \pmod{2^n - 1}$, since $n \mid 2t(j_2 - j_1) = nt$. The existence is shown, and next, we show uniqueness (via a Dirichlet principle type argument). If there exist two values $j_2 < j_3$, say, such that for a given $0 \leq j_1 < n/2$, we have $2^{2tj_1} \equiv 2^{2tj_2} \equiv 2^{2tj_3} \pmod{2^n - 1}$, then $n \mid 2t(j_2 - j_1)$ and $n \mid 2t(j_3 - j_1)$ and consequently, $n \mid 2t(j_3 - j_2)$. However, because $\gcd(n, t) = 1$, it is not possible that both j_2, j_3 belong to the interval $[n/2, n)$, since then $j_3 - j_2 < n/2$ and $n/2$ cannot divide their difference. In the same way, neither j_2, nor j_3 can belong to the interval $[0, n/2)$ since then $n/2$ could not divide the difference $j_2 - j_1$, or, $j_3 - j_1$.

4. Assuming $0 < m < \frac{n}{2}$, we note that

$$e\left(\frac{3n}{2} + m, 2t\right) = \sum_{j=0}^{\frac{3n}{2}-1} 2^{2jt} + \sum_{j=0}^{m-1} 2^{2\left(\frac{3n}{2}+jt\right)}.$$

Recalling $n = 2k$, we see that

$$\sum_{j=0}^{\frac{3n}{2}-1} 2^{2jt} = \frac{2^{3nt} - 1}{2^{2t} - 1} = \frac{2^{6kt} - 1}{2^{2t} - 1},$$

with

$$2^{6kt} - 1 = (2^{2k} - 1)\left(2^{2k(3t-1)} + 2^{2k(3t-2)} + \cdots + 2^{2k} + 1\right).$$

Notice that

$$2^{2k(3t-1)} + \cdots + 2^{2k} + 1 = 4^{k(3t-1)} + \cdots + 4^k + 1 \equiv 3t \equiv 0 \pmod{3},$$

so that

$$\frac{2^{6kt} - 1}{2^{2t} - 1} = \frac{3q\left(2^{2k} - 1\right)}{2^{2t} - 1},$$

for some $q \in \mathbb{N}$. We note that $\gcd(2^{2t} - 1, 2^{2k} - 1) = 3$, and so

$$\frac{3q(2^{2k} - 1)}{2^{2t} - 1} = q'\left(2^{2k} - 1\right) \equiv 0 \pmod{2^{2k} - 1}$$

for some $q' \in \mathbb{N}$. It follows that

$$e\left(\frac{3n}{2} + m, 2t\right) \equiv \sum_{j=0}^{m-1} 2^{2jt} \pmod{2^n - 1}.$$

The lemma is shown. □

We also frequently make use of the following observation which follows from the fact that $1 + 2 + \cdots + 2^{n-1} \equiv 0 \pmod{2^n - 1}$ (see also [22]).

Observation 4.5 *The binary decomposition of $-a$ modulo $2^n - 1$ is the complement of that of a.*

For example, 3 can be written as (000011), i.e. $2^0 + 2^1$ in binary, and $-3 \equiv 60 \pmod{63}$ has the binary expansion (111100), i.e. $2^2 + 2^3 + 2^4 + 2^5$.

4.1 Gold and inverse case

We can see that representatives from some of the known infinite families of APN monomials can be expressed in the form $e(l,k)$. This can be observed quite easily using the formula for the sum of a geometric progression. In particular, the Gold functions x^{2^k+1} can clearly be expressed as $e(2,k)$. The inverse function can be written as $e(n-1,1) = \sum_{i=0}^{n-2} 2^i = 2^{n-1}-1$. We have also observed that in some cases, e.g. for $l = (n-1)/2$ and $k = 2$, or for $l = (n-1)/2+1$ and $k = 1$, $e(l,k)$ is equivalent to a Gold function, which is not surprising since the inverse of the Gold function x^{2^r+1} over $\mathbb{F}_{2^n}$, n odd, $\gcd(n,r) = 1$, is given by $e(2r, \frac{n+1}{2}) = \sum_{i=0}^{\frac{n-1}{2}} 2^{2ir}$.

4.2 Welch case

We note that the Welch exponent is only defined for odd dimensions n. Since we assume $\gcd(k,n) \leq 2$ for $e(l,k)$ in Theorem 3.2 and the following remark, this leaves us with $\gcd(k,n) = 1$ as the only possibility. By Observation 4.2 we know that $\mathrm{wt}(e(l,k) \bmod (2^n-1)) = l$, and since the weight of the Welch exponent 2^t+2+1 is 3, it is enough to consider $e(3,k)$.

Theorem 4.6 *Let n be a natural number. Let $W = 2^t+2+1$ be the Welch exponent, where $t > 1$ is some natural number. Suppose $t > 2$. Then W and $e(3,i)$ never lie in the same cyclotomic coset modulo 2^n-1 for any $0 < i < n$ with $n = 2t+1$.*

Proof Suppose that there are natural numbers $a, i < n$ such that

$$2^a e(3,i) = 2^a(2^{2i}+2^i+1) \equiv 2^t+2+1 \pmod{2^n-1}. \tag{4}$$

First, we argue that the exponents on the right-hand side are pairwise distinct modulo n. Clearly, we cannot have $1 \equiv 0$, or $t \equiv 0$, or $t \equiv 1$ by the hypothesis. The exponents on the left-hand side of (4) must thus also be distinct modulo n in order for the congruence to hold. By Lemma 4.1, we now have

$$\{2i+a, i+a, a\} \bmod n = \{t, 1, 0\}.$$

We consider several cases depending on which of the three exponents $2i+a$, $i+a$ and a need to be reduced modulo 2^n-1.
Case 1: If $2i+a < n$, then $\{2i+a, i+a, a\} = \{t, 1, 0\}$. Thus, $a = 0$, $i = 1$, $t = 2$.
Case 2: Let $i+a < n$ and $2i+a \geq n$. Write $k = 2i+a-n$. We thus have $\{k, a+i, a\} \bmod n = \{t, 1, 0\}$. We cannot have $a+i = 0$ since this implies $a = i = 0$ and leads to a contradiction. We consider two sub-cases:

1. if $k = 0$, then we have $a+2i = n$. We then have $\{a+i, a\} \bmod n = \{t, 1\}$.
   If $a+i = t$ and $a = 1$, then from $k = 2i+a-n = 0$, we get $2i+1-2t-1 = 0$, i.e. $i = t$. Then $a+i = t$ implies $a \equiv 0$, which contradicts $a = 1$.
   If $a+i = 1$ and $t = a$, then $k = 2i+a-2t-1 = 0$ implies $i = 2t$. Then $a+i = 1$ implies $3t = 1$, which leads to $t = 2$, i.e. $n = 5$.
2. if $k \neq 0$, then $a = 0$, so we have $\{k, a+i\} = \{k, i\} = \{t, 1\}$.
   We have $k = 2i-2t-1$, i.e. $2t+k = 2i-1$. If $k = t$ and $i = 1$, this means that $3t = 1$ as in the previous sub-case. If $k = 1$ and $i = t$, then we get $1 = -1$.

Case 3: If $i + a \geq n$, then let $k = i + a - n$. We thus have $\{k + i, k, a\} = \{t, 1, 0\}$. Surely, only k, a could be 0. Once again, we split into sub-cases:

1. if $k = 0$, then we have $\{i, a\} = \{t, 1\}$. We have two possibilities:
   (a) if $i = 1$ and $a = t$, then $0 = k = a + i - n = t + 1 - 2t - 1 = -t$, so $t = 0$ and thus $n = 1$;
   (b) if $i = t$ and $a = 1$, then we get $0 = k = t - i$, so that $i = t$. But then $k = a + i - n = a + t - 2t - 1 = 1 + t - 2t - 1 = -t$, and so once again $t = 0$.
2. if $a = 0$, then we have $\{k + i, k\} = \{t, 1\}$. We consider two sub-cases:
   (a) if $k + i = t$ and $k = 1$, then we have $k = i - n = i - 2t - 1 = 1$, and so $i = 2t + 2 = n + 1$, which contradicts the choice of i;
   (b) if $k + i = 1$ and $k = t$, then $i = 1 - k = 1 - t$, and since $i \geq 0$, i.e. $1 - t \geq 0$, we have $t \leq 1$, i.e. $n \leq 3$.

The claim is shown.

We now concentrate on the inverse Welch exponent.

Theorem 4.7 *Let $W = 2^t + 2 + 1$ be the Welch exponent for some natural number $t > 2$. Then $W^{-1} \pmod{2^n - 1}$ is never congruent to $e(l, k)$ for any $l < n$ and any k over $\mathbb{F}_{2^n}$ with $n = 2t + 1$.*

Proof We assume that for $n > 5$ and so, $t > 2$, there are some positive integers $a < n, k < n, 1 \leq l < n$ such that

$$e(l, k)(2^t + 2 + 1) \equiv 2^a \pmod{2^n - 1}. \tag{5}$$

If $k = 1$, we get the congruence

$$(2^l - 1)(2^t + 2 + 1) = 2^{l+t} + 2^{l+1} + 2^l - 2^t - 2 - 1 \equiv 2^a \pmod{2^n - 1}.$$

The left-hand side of the above congruence can be written as

$$S = (2^{l+t} - 2^t) + 2^{l+1} + (2^l - 2^2) + 1,$$

and so we have

$$S = 2^{l+t-1} + 2^{l+t-2} + \cdots + 2^t + 2^{l+1} + 2^{l-1} + \cdots + 2^2 + 1 \equiv 2^a \pmod{2^n - 1}. \tag{6}$$

If $l + 1 < t$ (so, $l + t - 1 < n$), we get a contradiction by uniqueness of the binary expansion.

If $l + 1 = t, t + 1$, then $S = 2^{l+t} + 2^{l-1} + \cdots + 2^2 + 1$, respectively, $S = 2^{l+t} + 2^l + 2^{l-1} + \cdots + 2^2 + 1$. If $l + 1 = t + 2$, then (note that $l + t = n$, now) $S = 2^{l+t} + 2^{t+1} + 2^{t+1} + 2^{l-2} + \cdots + 2^2 + 1 \equiv 2^{t+2} + 2^{t-1} + \cdots + 2^2 + 2 \pmod{2^n - 1}$. None of these values of S modulo $2^n - 1$ can have Hamming weight 1.

If $l + 1 \geq t + 3$, arranging the sums to see how the cascading ("merger" of powers of 2) works, we obtain (writing $l + 1 = t + s$, $3 \leq s$, $t + 1 \leq s$, the upper bound comes from $l < n$)

$$\begin{aligned}
S = 2^{l+t-1} + \cdots \quad & +2^{t+s} + 2^{t+s-1} && +2^{t+s-2} + \cdots + 2^t \\
& +2^{l+1} && +2^{l-1} + \cdots + 2^{l+1-s} \\
& && +2^{t-1} + \cdots + 2^2 + 1 \\
= 2^{l+t} + 2^{t+s-1} \quad & +2\left(2^{t+s-2} + \cdots + 2^t\right) && +2^{t-1} + \cdots + 2^2 + 1 \\
= 2^{l+t} + 2^{t+s} \quad & +2^{t+s-2} + \cdots + 2^{t+1} && +2^{t-1} + \cdots + 2^2 + 1 \\
\equiv 2^{l-t-1} + 2^{l+1} \quad & +2^{l-1} + \cdots + 2^{t+1} && +2^{t-1} + \cdots + 2^2 + 1 \pmod{2^n - 1},
\end{aligned}$$

where we used above that $l + t \pmod n = l + t - n = l - t - 1$, and $t + s = l + 1$. Since $t \geq 1, l - t - 1$ falls either in the set of indices $\{0\}$, $\{2, \ldots, t - 1\}$, or $\{t + 1, \ldots, l - 1\}$ and since the gaps between these sets are of length 2, the cascading compression cannot jump into a different set. Thus, the expression $S \pmod{2^n - 1}$ cannot have Hamming weight 1.

We now take $1 < k < n$. Equation (5) is equivalent to

$$B = \sum_{i=0}^{l-1} 2^{ki+t} + \sum_{i=0}^{l-1} 2^{ki+1} + \sum_{i=0}^{l-1} 2^{ki} \equiv 2^a \pmod{2^n - 1}. \tag{7}$$

If $k(l - 1) + t < n$ and $t \not\equiv 0, 1 \pmod k$, we get a contradiction by the uniqueness of the binary expansion, since the exponents are sitting in different residue classes modulo k. We next assume that $k(l - 1) + t < n, t \equiv 0 \pmod k$, say $t = ks, s \geq 1$. Since $k(l - 1) + t < n = 2t + 1$, that is, $k(l - 1) < ks + 1$, then $s > l - 1$, and so, there is no compression in (7), and the claim follows via the uniqueness of the binary decomposition. The case of $k(l - 1) + t < n, t \equiv 1 \pmod k$ follows similarly.

We now let $k(l - 1) + t \geq n$, that is, $k(l - 1) \geq t + 1$. In the same way as above, if $t \not\equiv 0, 1 \pmod k$, reducing all exponents modulo n, we see that they cannot overlap (hence no compression in the sum) since they belong to different residue classes modulo k. We now take $t \equiv 0 \pmod k$ (one treats similarly $t \equiv 1 \pmod k$), $t = ks, s \geq 1$ and, since $k(l - 1) \geq t + 1 = ks + 1$, then $1 \leq s < l - 1$. Thus, recalling that a Mod N denotes the least positive residue of a modulo N,

$$\begin{aligned} B &\equiv 2^{k(l-1+s) \text{ Mod } n} + \cdots + 2^{kl \text{ Mod } n} + \sum_{i=s}^{l-1} 2^{ki+1 \text{ Mod } n} \\ &\quad + 1 + 2^k + \cdots + 2^{k(s-1) \text{ Mod } n} + \sum_{i=0}^{l-1} 2^{ki+1 \text{ Mod } n} \\ &\equiv 2^{k(l-1+s) \text{ Mod } n} + \cdots + 2^{kl \text{ Mod } n} + \sum_{i=s}^{l-1} 2^{ki+2 \text{ Mod } n} \\ &\quad + 2^{k(s-1)(\text{ Mod } n)} + \cdots + 2^k + 1 + \sum_{i=0}^{s-1} 2^{ki+1 \text{ Mod } n}, \end{aligned}$$

and again working modulo k, we see that this cannot have Hamming weight 1.

Thus, the result holds. □

To conclude the discussion, we observe that for $t = 1$ the Welch exponent is $2^t + 3 = 5$, and can be expressed as $e(2, 2)$, while for $t = 2$, the Welch exponent is $2^t + 3 = 7$. Its inverse, $7^{-1} \equiv 9 \pmod{2^5 - 1}$, can be expressed as $e(2, 3)$. As the above theorems demonstrate, these are the only cases in which the Welch exponent can be expressed as $e(l, k)$.

4.3 Kasami case

The Kasami exponents on $\mathbb{F}_{2^n}$ are defined as $2^{2t} - 2^t + 1$ with $\gcd(t, n) = 1$. The algebraic degree of the Kasami exponent is known (and easily shown) to be $t + 1$.

If $\gcd(i, n) = 1$, this means that we need to consider $l = t+1$. Since the Kasami exponents are defined for both even and odd n, it is possible that we have $\gcd(i, n) = 2$ in addition to $\gcd(i, n) = 1$. According to Lemma 4.4, however, even if $\gcd(i, n) = 2$, it is still sufficient to consider $l = t + 1$ due to $t < n/2$ which we can always assume up to equivalence.

Theorem 4.8 *Let t, n be natural numbers such that $t > 2$, $\gcd(t, n) = 1$ and let $K_t = 2^{2t} - 2^t + 1$ be the Kasami exponent for $t < n/2$. Then K_t is never congruent to $e(t+1, i)$ modulo $2^n - 1$ for any $i < n$ such that $\gcd(i, n) = 1$.*

Proof Let us assume that there is some $a < n$ such that

$$2^a \cdot (2^{2t} - 2^t + 1) \equiv e(t+1, i) \tag{8}$$

for some $i < n$. Depending on which of the exponents in $\{2t + a, t + a, a\}$ need to be modulated, we examine several cases, applying Lemma 4.1 in each case.

Case 1: If $2t + a < n$, then all exponents are already less than n. The exponent on the left-hand side of (8) modulo $2^n - 1$ is thus simply $2^{2t+a} - 2^{t+a} + 2^a$, which can be expressed as

$$\left(\sum_{j=a+t}^{2t+a-1} 2^j \right) + 2^a.$$

The set of exponents of this expression is

$$A = \{a\} \cup \{a + t, a + t + 1, \ldots, 2t + a - 2, 2t + a - 1\}.$$

The set of exponents of $e(t + 1, i) = \sum_{j=0}^{t} 2^{ji}$ is

$$B = \{0, i, 2i, \ldots, (t - 1)i, ti\} \text{ Mod } n.$$

Note that all elements in B must be distinct modulo n due to $\gcd(i, n) = 1$, and so we can apply Lemma 4.1. Since $0 \in B$, we must also have $0 \in A$. If $0 = a + t + j$ for some $j > 0$, then we get a contradiction because we would have $a + t < 0$. If $0 = a + t$, then $a = t = 0$, but the Kasami function is only defined for $t > 0$. Thus, we must have $a = 0$ and $t \neq 0$. The set A then becomes

$$A = \{0\} \cup \{t, t + 1, \ldots, 2t - 2, 2t - 1\}.$$

There must be α, β in $0 \leq \alpha, \beta \leq t$ such that $\alpha i \equiv t \pmod{n}$ and $\beta i \equiv t + 1 \pmod{n}$. Then either $\alpha - \beta$ or $\beta - \alpha$ is in the range between 0 and t, so either $(\alpha - \beta)i$ Mod n or $(\beta - \alpha)i$ Mod n belongs to A. But $(\beta - \alpha)i \equiv 1 \notin A$, and so we must have $(\alpha - \beta)i \equiv -1 = n - 1 \in A$, which is impossible under $t < n/2$.

Case 2: If $t + a < n \leq 2t + a$, then let $k = 2t + a - n$. We must have $k < t + a$, otherwise $k = 2t + a - n \geq t + a$, hence $t - n \geq 0$, i.e. $t \geq n$. Similarly, we can assume $k < a$ under $t \leq n/2$. Then $k < a < t + a$. Using Observation 4.5, we have that the Kasami exponent becomes

$$-2^{t+a} + 2^a + 2^k = -(2^{t+a} - 2^a) + 2^k = 2^k + \sum_{j=0}^{a-1} 2^j + \sum_{j=t+a}^{n-1} 2^j = \left(\sum_{j=0}^{k-1} 2^j \right) + 2^a + \left(\sum_{j=t+a}^{n-1} 2^j \right),$$

which gives the set of exponents

$$A = \{0, 1, 2, \ldots, k - 1\} \cup \{a\} \cup \{t + a, t + a + 1, \ldots, n - 1\}.$$

The set of exponents of $e(t + 1, i)$ is still the same as before, i.e.

$$B = \{0, i, 2i, \ldots, (t - 1)i, ti\} \text{ Mod } n.$$

We must have α, β in $0 \le \alpha, \beta \le t$ such that $\alpha i \equiv t + a \pmod{n}$ and $\beta i \equiv a \pmod{n}$. Then either $\alpha - \beta$ or $\beta - \alpha$ is in the range $\{0, 1, \ldots, t\}$, and so we must have either $t \in A$ or $-t \equiv n - t \in A$.

If $t \in A$, then we must have $t = a$ since $t \le k - 1$ means $t \le 2t + a - n - 1$, i.e. $t + a \ge n + 1$ which contradicts $t + a < n$; and $t \ge t + a$ implies $a = 0$ which contradicts that same assumption. If $a = t$, then the set of exponents becomes

$$A = \{0, 1, \ldots, k - 1\} \cup \{t\} \cup \{2t, 2t + 1, \ldots, n - 1\}.$$

Now, take some γ, δ such that $0 \le \gamma, \delta \le t$ and $\gamma i \equiv 1 \pmod{n}$ and $\delta i \equiv t \pmod{n}$. Then either $t - 1$ or $n + 1 - t$ must be in A, and we can verify that this is impossible: if $t - 1 \le k - 1$, then $t \le 3t - n$, i.e. $2t \ge n$ contradicting $t < n/2$; if $t - 1 = t$ or $t - 1 \ge 2t$, then we immediately get a contradiction as well. Similarly, $n + 1 - t \le k - 1$ means $n + 1 - t \le 3t - 1$, i.e. $4t \ge 2n + 2$ contradicting the choice of t; $n + 1 - t = t$ leads to $2t = n + 1$, violating that same hypothesis; and $n + 1 - t \ge t + a$ means $n \ge 3t - 1$, but together with $3t \ge n$ and $\gcd(t, n) = 1$ this leads to $3t = n + 1$ so that $k = 3t - n = 1$. Thus $A = \{0\} \cup \{t\} \cup \{2t, 2t + 1, \ldots, 3t - 2\}$. Then taking $\varepsilon i \equiv 3t - 2 \pmod{n}$, we have either $(3t - 2) - t = 2t - 2 \in A$, or $t - (3t - 2) = n - 2t + 2 \in A$. The former case is clearly impossible except potentially for trivial values of t. In the latter case, we must have $n + 2 - 2t \ge 2t$, i.e. $n + 2 = 3t + 1 \ge 4t$, which again implies a contradiction.

If $n - t \in A$, we derive a contradiction in a similar manner.

Case 3: If $t + a > n$, let $k = t + a - n$. Then

$$2^{2t+a} - 2^{t+a} + 2^a \equiv 2^{k+a} - 2^k + 2^a \pmod{2^n - 1}.$$

Note that $k < a$ since otherwise we get $t + a - n \ge a$, i.e. $t \ge n$. We need to examine two sub-cases depending on whether $k + a$ needs to be modulated or not.

Case 3-1: If $k + a < n$, then the above becomes

$$2^{k+a} + 2^a - 2^k = \left(\sum_{j=k}^{a-1} 2^j\right) + 2^{k+a},$$

giving the set of exponents

$$A = \{k, k + 1, \ldots, a - 1\} \cup \{k + a\}$$

which has to be congruent with

$$B = \{ti, (t - 1)i, \ldots, 2i, i, 0\} \text{ Mod } n.$$

As before, if $0 = k + j$ for some $j > 0$, then we immediately get a contradiction due to $k, j \ge 0$. So $k = 0$, i.e. $t + a = n$. The above sets become

$$A = \{0, 1, 2, \ldots, a - 1, a\}$$

and

$$B = \{ti, (t - 1)i, \ldots, 2i, i, 0\} \text{ Mod } n.$$

Clearly, we must have $a = t$ in order for equality to hold (by comparing the number of terms), but then $t + a > n$ and $k + a < n$ cannot hold simultaneously.

Case 3-2: If $k + a \ge n$, then let $q = k + a - n = t + 2(a - n)$. We have $q < k$ since if $q \ge k$, then $k + a - n \ge k$, i.e. $a \ge n$. Similarly, $k < a$ since if $k \ge a$ then $t + a - n \ge a$,

i.e. $t \geq n$. Thus we have $q < k < a$. The Kasami exponent is thus

$$2^a - 2^k + 2^q = \left(\sum_{j=k}^{a-1} 2^j\right) + 2^q.$$

The set of exponents is

$$A = \{q\} \cup \{k, k+1, k+2, \ldots, a-1\}.$$

Since $0 \in A$ due to $0 \in B$, the only possibility is $q = 0$, i.e. $k + a = n$. Comparing the sizes of A and B, we get $a - 1 - k + 1 + 1 = t + 1$, i.e. $a - k = t$, hence $n = 2t$, which contradicts $\gcd(t, n) = 1$.

This concludes the proof of this case. □

While the inverse of the Kasami power function is known (see [23, Theorem 3.10], as well as [24], for further clarification), it seems complicated to investigate its cyclotomic equivalence to some $e(l, k)$, since the inverse formula depends upon the inverse of the Kasami exponent $2^{2t} - 2^t + 1$ modulo $2^r - 1$, where r is the least positive residue of n modulo $6k$, and that is not explicit.

However, we find a way around that and are able to show the following theorem.

Theorem 4.9 *The inverse of the Kasami exponent $K_t = 2^{2t} + 2^t - 1$ is cyclotomic equivalent to $e(l, i)$ over $\mathbb{F}_{2^n}$, $\gcd(n, t) = 1$, if and only if $t = 1$, or $t = n - 1$, and this happens for $(l, i) = e(2, \frac{n+1}{2})$ (hence K_1^{-1} and K_{n-1}^{-1} are in the same cyclotomic class).*

Proof Suppose that the Kasami exponent $K_t = (2^{2t} - 2^t + 1)$ satisfies $(2^{2t} - 2^t + 1)e(l, i) \equiv 2^a \pmod{2^n - 1}$ for some a, l, i, n satisfying the appropriate hypotheses. This means that

$$\frac{2^{li} - 1}{2^i - 1}(2^{2t} - 2^t + 1) \equiv 2^a \pmod{2^n - 1}. \tag{9}$$

We first make some interesting observations. If $t = 1$, the Kasami function is also a Gold function, and we have already treated that case. If $t = n - 1$ (which is coprime to n), we first observe that the Kasami function is then $2^{2t} - 2^t + 1 = 2^{2n-2} - 2^{n-1} + 1 \equiv 2^{n-2} - 2^{n-1} + 1 \equiv -2^{n-2} \equiv 3 \cdot 2^{n-2} \pmod{2^n - 1}$. Thus, taking $i = 2$, $l = \frac{n+1}{2}$, $a = n - 2$, Equation (9) becomes

$$3 \cdot 2^{n-2} \frac{2^{n+1} - 1}{2^2 - 1} = 2^{n-2} \equiv 2^{n-2} \pmod{2^n - 1}.$$

Thus, the inverse of K_{n-1} is in the cyclotomic class of $e\left(\frac{n+1}{2}, 2\right)$.

We therefore assume that $1 < t < n - 1$. Multiplying both sides of (9) by $2^i - 1$ and regrouping the terms on both sides yields

$$2^{2t+li} + 2^{li} + 2^t + 2^a \equiv 2^{2t} + 2^{li+t} + 2^{a+i} + 1 \pmod{2^n - 1}. \tag{10}$$

We will apply Lemma 4.1 to the exponents on the left-hand and right-hand side of the above identity. In order to do so, we first need to treat the cases when one or more of the integers in the exponent sets

$$A = \{2t + li, li, t, a\}$$

and

$$B = \{2t, li + t, a + i, 0\}$$

are congruent to each other modulo n.

Handling these degenerate cases when some of the exponents in A or B coincide modulo n is generally straightforward but rather technical since each case produce a number of sub-cases that need to be treated as well. For example, if we consider the elements in A, and begin treating the case when $2t + li \equiv t \pmod{n}$, so that A collapses into a three-element set after compression, we would consider several cases depending on which two elements of B coincide modulo n; for each of these cases, we would be left with two three-element sets (corresponding to A and B after compression). We would then apply Lemma 4.1 to these three-element sets, but in order to do so, we would need to first handle the cases where some of the three elements in one of these sets are not distinct modulo n.

Due to the large number of degenerate sub-cases that need to be handled in this proof, we leave out the details here. These sub-cases can be handled in a straightforward way, and they all lead either to contradiction, or to trivial values (say, $t = 1$, which is the Gold function that we have already handled, or very small dimensions such as $n \leq 2$). Furthermore, we use the same principle of ruling out degenerate cases and applying Lemma 4.1 in all of our inequivalence proofs, but for most of them the number of degenerate cases that need to be handled is significantly less, and we feel that they illustrate the principles of applying Lemma 4.1 to solving problems of this type much better due to their relative brevity. The reader can, however, find the full technical proof in the pre-print version of our paper at [25].

In this sketch of the proof, we only demonstrate how to handle the main case, when we know that all elements of A (and, equivalently, B) are distinct modulo n.

Applying Lemma 4.1, we have

$$\{2t + li, t, li, a\} \equiv \{2t, li + t, a + i, 0\} \pmod{n}.$$

- Clearly, $0 \equiv t \pmod{n}$ and $t \equiv 2t \pmod{n}$ is impossible.
- If $t \equiv li + t \pmod{n}$, then $li \equiv 0 \pmod{n}$, and so $A = \{2t, t, 0, a\}$ and $B = \{2t, t, a + i, 0\}$. Then $a \equiv a + i \pmod{n}$ so $i \equiv 0 \pmod{n}$ which can not happen.
- If $t \equiv a + i \pmod{n}$, then $A = \{2t + li, t, li, a\}$ and $B = \{2t, li + t, t, 0\}$.
  - If $li \equiv 0 \pmod{n}$, then $2t + li \equiv 2t \pmod{n}$, so $a \equiv li + t \pmod{n}$ and $a \equiv li + a + i \pmod{n}$ implies $i \equiv 0 \pmod{n}$.
  - If $li \equiv li + t \pmod{n}$, we get $t \equiv 0 \pmod{n}$.
  - If $li \equiv 2t \pmod{n}$, then $A = \{4t, t, 2t, a\}$ and $B = \{2t, 3t, t, 0\}$ which necessarily implies $t \equiv 0 \pmod{n}$.

This completes the proof. □

We can verify that for $n = 3$ (where the Kasami exponents coincide with the Gold exponents) and for $n = 5$, we can express the Kasami using $e(l, k)$. In the case of $n = 5$, the relevant exponents are $5 = e(2, 2)$, $7 = (3, 1)$, $9 = e(2, 3)$, and $25 \equiv e(3, 4) \pmod{2^5 - 1}$. By the above characterizations, the Kasami family never coincides with $e(l, k)$ in any other cases.

4.4 Niho even case

The Niho exponent for $n = 2t + 1$ with t even is $2^t + 2^{t/2} - 1$. The algebraic degree is $(t + 2)/2$.

Theorem 4.10 *Let $t > 2$ be an even natural number, $n = 2t+1$ and i be such that $\gcd(i, n) = 1$. Then the even Niho exponent $2^t + 2^{t/2} - 1$ is never cyclotomic equivalent to $e((t+2)/2, i)$ over $\mathbb{F}_{2^n}$.*

Proof Once again, suppose that

$$2^a(2^t + 2^{t/2} - 1) \equiv e((t+2)/2, i) \pmod{2^n - 1}$$

for some natural number i. We split the proof into several cases, applying Lemma 4.1.
Case 1: If $a + t < n$, the (shifted by a) Niho exponent is then

$$2^{a+t} + 2^{a+t/2} - 2^a = 2^{a+t} + \sum_{j=a}^{a+t/2-1} 2^j,$$

and so the set of its exponents is precisely

$$A = \{a, a+1, a+2, \ldots, a+t/2-1\} \cup \{a+t\}.$$

The set of exponents of $e((t+2)/2, i)$ is

$$B = \{0, i, 2i, 3i, \ldots, (t/2)i\} \bmod n.$$

If $0 = a + j$ for $j > 0$, then we immediately get a contradiction. Thus, we must have $a = 0$ and the set A becomes

$$A = \{0, 1, 2, \ldots, t/2 - 1\} \cup \{t\}.$$

Let $q = t/2$. The sum of all elements in A is

$$t + \sum_{j=1}^{t/2-1} j = 2q + \frac{(q-1)q}{2} = \frac{q^2 + 3q}{2},$$

while the sum of all elements in B is

$$i\frac{q(q+1)}{2} = \frac{(q^2+q)i}{2}$$

modulo n. Since 2, q are invertible modulo n, we must have

$$q + 3 \equiv (q+1)i.$$

Multiplying both sides by 4, we have

$$4q + 12 \equiv (4q+4)i \pmod{n}.$$

Since $n = 2t + 1 = 4q + 1$, the above becomes

$$11 \equiv 3i \pmod{n}.$$

If $q \equiv 2 \pmod 3$, then $3 \mid n$, and so $3i$ does not have an inverse whereas 11 does, which is a contradiction.

If $q \equiv 1 \pmod 3$, then the inverse of 3 modulo $n = 4q + 1$ is $(4q+2)/3$. From the identity $11 \equiv 3i \pmod n$ above, we thus get

$$i \equiv \frac{11(4q+2)}{3} \pmod{n},$$

which becomes

$$i \equiv 3(4q+2) + \frac{2(4q+2)}{3} \equiv 3 + \frac{8q+4}{3} \equiv \frac{8q+13}{3} \equiv \frac{2n+11}{3} \pmod{n}.$$

If $(2n+11)/3 < n$, then no modulation is necessary, and this number belongs to the set A; it must thus either be no greater than $t/2-1$, or it must equal t. In the former case, we have

$$\frac{2n+11}{3} \leq \frac{t-2}{2} \iff 4n+22 \leq 3t-6 \iff 3t \geq 4n+28 \geq 4n,$$

so that $t \geq 4/3n$, which contradicts the choice of t. In the latter case, we have

$$\frac{2n+11}{3} = t \iff 2n+11 = 3t,$$

but since $n = 2t+1$, we have $4t+13 = 3t$, i.e. $t = -13$, which cannot be.

The only remaining case is when $(2n+11)/3 \geq n$, i.e. $n \leq 11$. Since we consider dimensions of the form $n = 2t+1$ for even t with $t/2 \equiv 1 \pmod 3$, this leaves only $n = 5$. In this case, we can see that $e(2,2)$ is exactly the Niho exponent $2^2 + 2^1 - 1 = 5$.

Finally, suppose that $q \equiv 0 \pmod 3$, i.e. $3 \mid q$. The inverse of 3 modulo $n = 4q+1$ is

$$3^{-1} \equiv \frac{8q+3}{3} \pmod n,$$

and so we get

$$\begin{aligned} i &\equiv 11 \cdot 3^{-1} \equiv \frac{11(8q+3)}{3} \equiv 3(8q+3) + \frac{16q+6}{3} \\ &\equiv 3 + \frac{16q+6}{3} \equiv \frac{16q+15}{3} \equiv \frac{n+11}{3} \pmod n. \end{aligned}$$

If $(n+11)/3 < n$, then it must be contained in A. If

$$\frac{n+11}{3} \leq \frac{t}{2} - 1,$$

then we get

$$3t \geq 2n+28,$$

which is clearly impossible.

If $(n+11)/3 = t$, then we get $n+11 = 3t$, i.e. $t = 12$, so that $n = 25$. We can verify by exhaustive search that the Niho exponent for $n = 25$ cannot be expressed using $e(t,i)$ for any choice of the parameters t and i.

Finally, if $(n+11)/3 \geq n$, then we have $2n \leq 11$, and so $n \leq 6$; the only possibility is $n = 1$, i.e. $t = 0$, which is not a valid choice for the Niho family.

Case 2: If $a + t/2 < n \leq a + t$, then let $k = a + t - n$. We have $k < a + t/2$ since if $k = a+t-n \geq a+t/2$, then $t/2 \geq n$. Similarly, we must have $k < a$ since $a+t-n = k \geq a$ means $t \geq n$. The Niho exponent is thus

$$2^{a+t/2} - 2^a + 2^k = \left(\sum_{j=a}^{a+t/2-1} 2^j \right) + 2^k$$

in this case. The set of exponents is

$$A = \{k\} \cup \{a, a+1, a+2, \ldots, a+t/2-1\},$$

while that of $e(t/2, i)$ is once again

$$B = \{0, i, 2i, \ldots, (t/2)i\} \text{ Mod } n.$$

As before, we can only have $0 = a$ or $0 = k$. If $a = 0$, then $k = t - n$, i.e. $n = t - k$ which cannot happen since $t < n$ by the hypothesis. Thus, we must have $k = 0$, i.e. $a + t = n$. From here, we can express $a = t + 1$ due to $n = 2t + 1$. We now have

$$A = \{0, t + 1, t + 2, \ldots, t + t/2\}.$$

There must exist $0 \leq \alpha, \beta \leq t/2$ such that $\alpha i \equiv t + 1 \pmod{n}$ and $\beta i \equiv t + 2 \pmod{n}$. Then either $\alpha - \beta$ or $\beta - \alpha$ is in the range $\{0, 1, \ldots, t/2\}$, and so either $(\alpha - \beta)i \equiv -1 \pmod{n}$ or $(\beta - \alpha)i \equiv 1 \pmod{n}$ must be in A. In other words, either $2t$ or 1 must belong to A, which is clearly impossible for $t > 1$. We have thus reached a contradiction.

Case 3: If $a + t/2 \geq n$, then let $k = a + t/2 - n$. We must have $k + t/2 < a$ since $k + t/2 \geq a$ implies $a + t/2 - n + t/2 \geq a$, i.e. $t \geq n$; and so we have $a > k + t/2 > k$, and the Niho exponent becomes

$$-2^a + 2^{k+t/2} + 2^k = -(2^a - 2^{k+t/2}) + 2^k.$$

Using Observation 4.5, we can see that

$$-(2^a - 2^{k+t/2}) \equiv \sum_{j=0}^{k+t/2-1} 2^j + \sum_{j=a}^{n-1} 2^j \pmod{n},$$

and then

$$-(2^a - 2^{k+t/2}) + 2^k \equiv \left(\sum_{j=0}^{k-1} 2^j\right) + 2^{k+t/2} + \left(\sum_{j=a}^{n-1} 2^j\right) \pmod{n};$$

consequently, we obtain the set of exponents

$$A = \{0, 1, 2, \ldots, k - 1\} \cup \{k + t/2\} \cup \{a, a + 1, \ldots, n - 1\},$$

while, as before, the set of exponents corresponding to $e(t/2, i)$ is

$$B = \{0, i, 2i, \ldots, t/2i\} \pmod{n}.$$

We must have $\alpha i \equiv 1 \pmod{n}$ and $\beta i \equiv n - 1 \pmod{n}$ for some $1 \leq \alpha, \beta \leq t/2$. Then $(\alpha + \beta)i \equiv 0 \pmod{n}$, and since $\gcd(i, n) = 1$ by the hypothesis, we get $\alpha + \beta \equiv 0 \pmod{n}$, i.e. $n \mid \alpha + \beta$. But since $1 \leq \alpha, \beta \leq t/2 = (n - 1)/4$, this is impossible.

We have thus shown our claim (for $n = 5$, we confirmed it computationally). □

We now concentrate on the inverse even Niho exponent.

Theorem 4.11 *Let $t > 2$ be an even natural number, $n = 2t+1$ and i be such that* $\gcd(i, n) = 1$. *Then the inverse of the even Niho exponent $(2^t + 2^{t/2} - 1)^{-1} \pmod{2^n - 1}$ is never cyclotomic equivalent to $e((t + 2)/2, i)$ over $\mathbb{F}_{2^n}$.*

Proof We use [26, Lemma 3], representing the even Niho exponent power function as the composition of x^3 and the inverse of a cubic power function. Precisely,

$$2^t + 2^{t/2} - 1 \equiv 2^{3t/2} \frac{3}{2^{t+1} + 2^{t/2} + 1} \pmod{2^{2t+1} - 1}.$$

To investigate the cyclotomic equivalence of $e(l, k)$, $l < n$ with the even Niho inverse, it is sufficient to consider the congruence ($n = 2t + 1$, t even)

$$3e(l, k) \equiv 2^a(2^{t+1} + 2^{t/2} + 1) \pmod{2^n - 1},$$

for some positive integers $a < n, l < n$. This is equivalent to

$$\sum_{i=0}^{l-1} 2^{ki} + \sum_{i=0}^{l-1} 2^{ki+1} \equiv 2^{a+t+1} + 2^{t/2+a} + 2^a \pmod{2^n - 1}. \tag{11}$$

We start with $k = 1$. Equation (11) becomes

$$1 + \sum_{j=2}^{l-1} 2^j + 2^{l+1} \equiv 2^{a+t+1} + 2^{t/2+a} + 2^a \pmod{2^n - 1}.$$

If $l + 1 = n$, the sets of exponents above are

$$A = \{1, 2, \ldots, l-1\}, \text{ all smaller than } n$$
$$B = \{t + a + 1, t/2 + a, a\} \pmod{n}.$$

Thus, $l \leq 4$. First, we take $l = 4$. If $a = 1$, then $B = \{1, t/2 + 1, t + 2\} = A = \{1, 2, 3\}$, which cannot happen (recall that $t = (n-1)/2 \geq 2$). If $t/2 + a \equiv 1 \pmod{n}$ (recall that $a < n$), then $a = n + 1 - t/2 = n + 1 - (n-1)/4 = (3n+5)/4$. The sets are now $B = \{1, t + a + 1 = \frac{5n+7}{4} \equiv \frac{n+7}{4} \pmod{n}, a = \frac{3n+5}{4}\} = \{1, 2, 3\}$, and that is impossible. The case of $t + a + 1 \equiv 1 \pmod{n}$ implies $t + a \equiv 0 \pmod{n}$, and so, $a = n - t = t + 1 = \frac{n+1}{2}$. Thus, $B = \{1, \frac{n+1}{2}, \frac{3n+1}{4}\} = \{1, 2, 3\}$, which cannot happen. We can theoretically argue it, but to simplify the argument, if $l = 2, 3$ (hence $n = 3, 4$), we checked computationally that our congruence (11) is impossible.

If $l + 1 < n$, then the set $A = \{0, 2, \ldots, l-1, l+1\}$ contains only distinct exponents and so, $l = 3$ and $A = \{0, 2, 4\}$. First, $a = 0$ is impossible. If $t + a + 1 \equiv 0 \pmod{n}$, then $a = n - t - 1 = \frac{n-1}{2} = t$, and so, $B = \{0, a = \frac{n-1}{2}, t/2 + a = \frac{3(n-1)}{4}\}$, which cannot be equal to A. If $t/2 + a \equiv 0 \pmod{n}$, then $a = n - t/2 = \frac{3n+1}{4}$, and so, $B = \{0, a = \frac{3n+1}{4}, t + a + 1 \equiv \frac{n+3}{4} \pmod{n}\}$, which can equal A if and only if $n = 5, a = 4, l = 3$, which is possible and the congruence becomes $3 \cdot (2^2 + 2 + 1) \equiv 2^4 \cdot (2^3 + 2 + 1) \pmod{2^5 - 1}$.

We now let $k > 1$. The set of exponents in the congruence (11) are

$$A = \{0, 1, k, k+1, 2k, 2k+1, \ldots, (l-1)l, (l-1)k + 1\} \text{ Mod } n,$$
$$B = \{a, t + a + 1, t/2 + a\} \text{ Mod } n.$$

For the set A to compress we need to have $s_1 < s_2 < n$ such that either $s_2 k \equiv s_1 k \pmod{n}$, which is impossible since $\gcd(k, n) = 1$, $s_2 k \equiv s_1 k + 1 \pmod{n}$, or $s_2 k + 1 \equiv s_1 k \pmod{n}$. These last two cases are treated similarly, so we only deal with the first one. We take $s_2 k \equiv s_1 k + 1 \pmod{n}$ and s_2 smallest with this property. Thus, $(s_2 - s_1)k \equiv 1 \pmod{n}$, $s_2 - s_1 < n$. Surely, the two elements $s_1 k + 1$, $s_2 k$ compress into $s_1 k + 2$, which occurs by itself in A, since $k > 1$, so no compression occurs. Now, the same will happen for all the remaining exponents above $s_2 k + 1$, since $(s_2 + j)k \equiv (s_1 + j)k + i \pmod{n}$. If $s_1 > 0$, the set A cannot compress to only three exponents as in the set B, so we must have $s_1 = 0, k = n - 1$. It follows that $A = \{0, 1, n-1, n, 2(n-1), 2(n-1)+1\} \pmod{n} = \{0, 2, 3\}$, which renders the case $n = 5, k = 4, l = 3, a = 2$, that is, the congruence $3 \cdot (2^8 + 2^4 + 1) \equiv 2^2(2^3 + 2 + 1) \pmod{2^5 - 1}$.

We thus have our claim (we computationally checked that the two cases do happen for the inverse of the Niho exponent). □

To conclude, we observe that for $t = 2$, i.e. $n = 5$, the Niho exponent or its inverse can be equivalent to $e(l, k)$. These are, in fact, precisely the exponents for $n = 5$ that coincide with the Kasami family.

4.5 Niho odd case

In this case, the exponent is of the form $2^t + 2^{(3t+1)/2} - 1$ for t odd, with $n = 2t + 1$. The algebraic degree is $t + 1$.

Theorem 4.12 *Let $t > 1$ be an odd natural number, $n = 2t+1$ and k be such that $\gcd(k, n) = 1$. Then the odd Niho exponent $2^t + 2^{\frac{3t+1}{2}} - 1$ can never be in the cyclotomic coset of $e(l, k)$ over $\mathbb{F}_{2^n}$.*

Proof Suppose that there exists some $a \leq n - 1$ such that $2^t + 2^{\frac{3t+1}{2}} - 1$ is congruent with $2^a e(l, k)$ for some $l < n, 1 \leq k$. From Lemma 4.3, we can assume that $1 \leq k \leq \frac{n+1}{2}$. Writing $e(l, k) = \frac{2^{lk}-1}{2^k-1}$ and multiplying throughout by $2^k - 1$, we get

$$2^{k+t} + 2^{\frac{3t+1}{2}+k} - 2^k - 2^t - 2^{\frac{3t+1}{2}} + 1 \equiv 2^{lk+a} - 2^a \pmod{2^n - 1},$$

that is

$$2^{\frac{3t+1}{2}+k} + 2^{k+t} + 2^a + 1 \equiv 2^{lk+a} + 2^k + 2^t + 2^{\frac{3t+1}{2}} \pmod{2^n - 1}. \tag{12}$$

If $a = 0$, the sets of exponents are

$$A = \left\{1, k + t, \frac{3t + 1}{2} + k\right\} \text{ Mod } n, B = \left\{k, t, \frac{3t + 1}{2}, lk\right\} \text{ Mod } n.$$

We know that $k + t \leq n$ (since $k \leq \frac{n+1}{2}$ and $t = \frac{n-1}{2}$). If $k + t = n$, that is, $k = \frac{n+1}{2}$, then $A = \{0, 1, \frac{n+1}{4}\}$ and $B = \{\frac{n-1}{2}, \frac{n+1}{2}, \frac{3n-1}{4}, \frac{l(n+1)}{2}\}$. It follows that $l(n + 1) \equiv l \equiv 0 \pmod{n}$, but that is impossible, since $1 < l < n$.

Next, let $k+t < n$ and assume that A does not compress modulo n (that ultimately means that $\frac{3t+1}{2} + k \not\equiv 1 \pmod{n}$, since $n > k + t > 1$). If $k = 1$, the two sets of exponents are $\{1, t + 1, \frac{3t+3}{2}\}$ and $\{1, t, \frac{3t+1}{2}, l\}$, which cannot possibly be equal. If $t = 1, k > 1$, then the two sets become $A = \{1, k + 1, k + 2\}$, $B = \{1, k, 2, l\}$, which is not possible. If $lk \equiv 1 \pmod{n}$, the two sets become $\{1, \frac{3n-1}{4}, 0\}$ and $\{\frac{n+1}{4}, \frac{n-1}{2}, 1\}$, which yet again is not possible (since 0 cannot be equated to anything in B).

Next, we assume that A compresses, that is, $\frac{3t+1}{2} + k \equiv 1 \pmod{n}$. Thus, $k = \frac{n+5}{4}$, $k + t \geq 3$ and so, $A = \{2, \frac{3(n+1)}{4}\}$, $B = \{\frac{n+5}{4}, \frac{n-1}{2}, \frac{3n-1}{4}, l\frac{n+5}{4} \text{ Mod } n\}$. Going through the possibilities (for $n > 3$), we see that there are no values of n for which the two sets match.

We next assume that $a > 0$. If $lk+a < n$ and $\frac{3t+1}{2}+k < n$, then the sets of exponents must be the same (without modulation), but that is impossible since 0 cannot be any of the exponents $k, t, \frac{3t+1}{2}, lk+a$. Therefore, either $lk+a \geq n$ or $\frac{3t+1}{2}+k \geq n$. If $\frac{3t+1}{2}+k < n$, but $lk+a \geq n$, then $lk + a \equiv 0 \pmod{n}$ (observe that A cannot remove 0 by possible compression, since $k + t < \frac{3t+1}{2} + k < n$ and either of the cases $a = k + t = n - 2$, $\frac{3t+1}{2} + k = n - 1$, when $2^a + 2^{k+t} + 2^{\frac{3t+1}{2}+k} = 2^n \equiv 2^0 \pmod{2^n - 1}$, or $a = \frac{3t+1}{2} + k = n - 2, k + t = n - 1$, or $a = \frac{3t+1}{2} + k = n - 1$, or $a = k + t = n - 1$, will all render contradictions) and the sets of exponents become

$$A = \left\{0, a, k + t, \frac{3t + 1}{2} + k\right\}, B = \left\{0, k, t, \frac{3t + 1}{2}\right\}.$$

Surely, the only possibility is for k to be equal to a, and the same is true for t, so that $k = a = t$, but then $\frac{3t+1}{2} + k \geq 2t + 1$, a contradiction.

If $\frac{3t+1}{2}+k \geq n$ and $lk+a < n$, since $k \leq \frac{n+1}{2}$, then $\frac{3t+1}{2}+k \leq \frac{5n+1}{4} = n+\frac{n+1}{4}$, and so, we must have $\frac{3t+1}{2}+k = n$ (otherwise, 0 remains in A, and that should not be the case as B cannot contain 0), that is, $k = \frac{n+1}{4}$ (so, $k+t < n$). The sets of exponents become now (the two copies of 0 in A compress to a 1)

$$A = \left\{1, a, k+t = \frac{3n-1}{4}\right\}, B = \left\{k, t, \frac{3t+1}{2} = \frac{3n-1}{4}, lk+a\right\}.$$

If $a = 1$ (recall that $n > 3$ and $3 \leq k+t < n$), then $A = \{1, 1, \frac{3n-1}{4}\} = \{2, \frac{3n-1}{4}\}$ and (since all of its elements are smaller than n, then $k = t = 1$) $B = \{1, 1, \frac{3n-1}{4}, l+1\} = \{2, \frac{3n-1}{4}, l+1\}$ (by compression and taking modulo 2^n-1). Surely, that is not possible. If $1 < a < n$, then only $k, t, lk \pmod n$ can be 1, but they all lead to contradiction.

It remains to look at the case $\frac{3t+1}{2}+k \geq n$ and $lk+a \geq n$. As remarked before, we must have $lk+a \equiv 0 \pmod n$, so the two sets of exponents become

$$A = \left\{0, a, k+t, \left(\frac{3t+1}{2}+k\right) \text{ Mod } n\right\}, B = \left\{0, k, t, \frac{3t+1}{2}\right\}.$$

We observe that k, t are both smaller than $k+t$ and $\frac{3t+1}{2}+k \leq \frac{3n-1}{4}+\frac{n+1}{2} = n+\frac{n-1}{4}$. Thus, $\left(\frac{3t+1}{2}+k\right) \pmod n = \frac{3t+1}{2}+k-n = k-\frac{n+1}{4}$. The two sets become

$$A = \left\{0, a, k-\frac{n+1}{4}, k+\frac{n-1}{2}\right\}, B = \left\{0, k, \frac{n-1}{2}, \frac{3n-1}{4}\right\},$$

and so, $k = a$ is the only possibility, as well as, $k+\frac{n-1}{2} = \frac{3n-1}{4}$, and so, $k = \frac{n+1}{4}$. Thus,

$$A = \left\{0, \frac{n+1}{4}, 0, \frac{3n-1}{4}\right\}, B = \left\{0, \frac{n+1}{4}, \frac{n-1}{2}, \frac{3n-1}{4}\right\}.$$

This is only possible for $n = 3$, when the sets compress to $A = B = \{0\}$.

The proof is done. □

Theorem 4.13 *Let $t > 1$ be an odd natural number, $n = 2t+1$ and k be such that $\gcd(k, n) = 1$. Then the inverse of the odd Niho exponent $(2^t + 2^{\frac{3t+1}{2}} - 1)^{2^n-1}$ can never be cyclotomic equivalent to $e(l, k)$ over $\mathbb{F}_{2^n}$.*

Proof We use [26, Lemma 6], namely, for t odd, we have

$$2^{\frac{3t+1}{2}} + 2^t - 1 \equiv 2^{\frac{3t-1}{2}} \frac{3}{2^t + 2^{\frac{t-1}{2}} + 1} \pmod{2^{2t+1}-1}.$$

As such, it will be sufficient to investigate the congruence (for positive integers $a, k, l < n$),

$$3e(l, k) \equiv 2^a(2^t + 2^{\frac{t-1}{2}} + 1) \pmod{2^n-1}. \tag{13}$$

We are going to use some computations done for the inverse even Niho case. If $k = 1$, we need to check

$$\sum_{i=0}^{l-1} 2^{ki} + \sum_{i=0}^{l-1} 2^{ki+1} \equiv 2^{a+t} + 2^{\frac{t-1}{2}+a} + 2^a \pmod{2^n-1}.$$

If $k = 1$, the equation becomes

$$1 + \sum_{j=2}^{l-1} 2^j + 2^{l+1} \equiv 2^{a+t} + 2^{\frac{t-1}{2}+a} + 2^a \pmod{2^n-1}.$$

If $l + 1 = n$ (recall that $l < n$), then the corresponding sets of exponents in the congruence are

$$A = \{1, 2, \ldots, l-1\}, \text{ all smaller than } n,$$
$$B = \{a, (t-1)/2 + a, t + a\} \text{ Mod } n,$$

which implies that $l \leq 4$, and $A = \{1, 2, 3\}$ (if $A = \{1, 2\}$, or $A = \{1\}$, we quickly see that it is not possible). If $a = 1$, then $(t-1)/2 = 1$ and $t = 2$, or, $(t-1)/2 = 2$ and $t = 1$, which are both impossible. The other cases can not happen either, since we are dealing with positive integers.

If $l + 1 < n$, then, as argued before, the set A contains only distinct exponents and so, $l = 3$ and $A = \{0, 2, 4\}$. Thus, $a = 0$, $B = \{0, (t-1)/2, t\}$, which cannot match A.

We next assume that $k > 1$. As in the even Niho case,

$$A = \{0, 1, k, k+1, 2k, 2k+1, \ldots, (l-1)l, (l-1)k + 1\} \text{ Mod } n,$$
$$B = \{a, (t-1)/2 + a, t + a\} \text{ Mod } n.$$

This congruence can be handled using a similar method based on compressing the exponent sets. In all cases, we obtain contradictions or trivial results only.

We thus have the proof of our theorem. □

Once again, we can see that for $t = 1$, i.e. $n = 3$, the odd Niho exponents coincide with the Gold exponents, and this is the only case in which they can be expressed as $e(l, k)$.

4.6 Dobbertin case

The Dobbertin exponent is $D_t = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$ for $n = 5t$. Note that in this case we have to consider k with $\gcd(k, n) = 2$ in addition to $\gcd(k, n) = 1$ since the Dobbertin exponent can be defined for even as well as odd dimensions. Nonetheless, by Lemma 4.4, it suffices to consider $l = \text{wt}(D_t)$.

Theorem 4.14 *Let $t > 2$ be a natural number and $n = 5t$. Then the Dobbertin exponent $D_t = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$ over $\mathbb{F}_{2^n}$, can never be cyclotomic equivalent to $e(l, k)$ for $t > 2$ and any k with $\gcd(k, n) \leq 2$.*

Proof Let us assume that the Dobbertin exponent is cyclotomic equivalent to $e(t + 3, i)$ for some i. Then there exists some $a < n$ such that

$$2^{4t+a} + 2^{3t+a} + 2^{2t+a} + 2^{t+a} - 2^a \equiv e(t + 3, i) \pmod{n}.$$

As before, we divide the proof into several cases depending on which of the exponents of the terms of the Dobbertin exponent need to be modulated.

Case 1: If $4t + a < n$, then no modulation is necessary, and the Dobbertin exponent is of the form

$$2^{4t+a} + 2^{3t+a} + 2^{2t+a} + \sum_{j=a}^{t+a-1} 2^j,$$

giving the set of exponents

$$A = \{a, a+1, a+2, \ldots, a+t-1\} \cup \{2t + a, 3t + a, 4t + a\}.$$

The set of exponents of $e(t+3, i)$ is of course

$$B = \{0, i, 2i, \ldots, (t+3)i\} \text{ Mod } n.$$

Since $0 \in B$, then $0 \in A$, and we can only have $a = 0$ unless $t = 0$. Thus, the set A becomes

$$A = \{0, 1, 2, \ldots, t-1\} \cup \{2t, 3t, 4t\}.$$

Since $A \equiv B \pmod{n}$, we must have some $1 \leq \alpha, \beta \leq t+3$ such that $\alpha i \equiv 1 \pmod{n}$ and $\beta i \equiv 4t \pmod{n}$. Now, $(\beta - \alpha)i \equiv 4t - 1 \pmod{n}$, and $4t - 1$ is clearly not in A unless $t \leq 2$. Thus, we must have $\beta - \alpha \notin \{0, 1, \ldots, t+3\}$. Since $\alpha, \beta \leq t+3$, this can only happen if $\alpha > \beta$. In this case, $\alpha - \beta \in \{0, 1, \ldots, t+3\}$, and $(\alpha - \beta)i \equiv 1 - 4t \equiv 1 - 4t + 5t \equiv t + 1 \pmod{n}$, which is also not in A. We have thus obtained a contradiction.

Case 2: If $3t + a < n \leq 4t + a$, let $k = 4t + a - n$. The Dobbertin exponent becomes

$$2^{3t+a} + 2^{2t+a} + 2^{t+a} - 2^a + 2^k = 2^{3t+a} + 2^{2t+a} + \left(\sum_{j=a}^{t+a-1} 2^j \right) + 2^k,$$

since $k < a$, or, equivalently $4t + a - n < a$, i.e. $4t < n$. The set of exponents is

$$A = \{a, a+1, a+2, \ldots, a+t-1\} \cup \{k, 2t+a, 3t+a\}.$$

Once again, $0 \in B$, and we can not have $a = 0$ since then $4t + a$ is always less than n. Consequently, we must have $k = 0$, i.e. $4t + a = n = 5t$, i.e. $a = t$. The set A becomes

$$\{t, t+1, t+2, \ldots, 2t-1\} \cup \{0, 3t, 4t\}.$$

We must have $\alpha, \beta \in \{0, 1, \ldots, t+3\}$ such that $\alpha i \equiv t + 1 \pmod{n}$ and $\beta i \equiv 4t \pmod{n}$. Then $(\beta - \alpha)i \equiv 3t - 1 \pmod{n}$ and $(\alpha - \beta)i \equiv 1 - 3t \equiv 2t + 1 \pmod{n}$, with either $\alpha - \beta$ or $\beta - \alpha$ being in $\{0, 1, 2, \ldots, t+3\}$, and neither of $2t + 1$ and $3t - 1$ being in A. We have thus reached a contradiction.

Case 3: If $2t + a < n < 3t + a$, then let $k = 3t + a - n$. The exponent $4t + a = 3t + a + t$ is congruent with $k + t$ modulo n, and $k + t < n$ since $k + t = 4t + a - n < n$, i.e. $a < 2n - 4t = n + t$. The Dobbertin exponent thus becomes

$$2^{a+2t} + 2^{a+t} - 2^a + 2^{k+t} + 2^k,$$

giving the set of exponents

$$A = \{a, a+1, a+2, \ldots, a+t-1\} \cup \{k, k+t, a+2t\}.$$

The only possible element in A that can be equal to $0 \in B$ is $k = 0$, so that $a + 3t = n = 5t$, i.e. $a = 2t$. Then the set A becomes

$$A = \{2t, 2t+1, 2t+2, \ldots, 3t-1\} \cup \{0, 3t, 4t\}.$$

Now, $\alpha i \equiv 2t + 1 \pmod{n}$ and $\beta i \equiv 3t \pmod{n}$ for some $1 \leq \alpha, \beta \leq t + 3$, and so $(\beta - \alpha)i \equiv t - 1$, which is not in A; $(\alpha - \beta)i \equiv 1 - t \equiv 4t - 1$ which is also not in A, and since one of $\alpha - \beta$ and $\beta - \alpha$ must lie in $\{0, 1, 2, \ldots, t+3\}$, we have reached a contradiction.

Case 4: If $a + t < n < a + 2t$, then let $k = a + 2t - n$. As before, the Dobbertin exponent modulo n becomes

$$2^{a+t} - 2^a + 2^{k+2t} + 2^{k+t} + 2^k,$$

and it is easy to verify that $k + 2t < n$ and that $k + 2t < a$. The exponent thus becomes

$$\left(\sum_{j=a}^{a+t-1} 2^j\right) + 2^{k+2t} + 2^{k+t} + 2^k,$$

and hence

$$A = \{a, a+1, a+2, \ldots, a+t-1\} \cup \{k, k+t, k+2t\}.$$

As before, we must necessarily have $k = 0$, so we get $a + 2t = n = 5t$, i.e. $a = 3t$. The set A becomes

$$A = \{a, a+1, \ldots, a+t-1\} \cup \{0, t, 2t\}.$$

Taking α and β such that $\alpha i \equiv 3t + 1 \pmod{n}$ and $\beta i \equiv t \pmod{n}$ then leads to a contradiction as before.

Case 5: If $a + t > n$, then let $k = a + t - n$. We can see that $4t + a \equiv 3t + k \pmod{n}$, and $3t + k < n$, so that the exponent becomes

$$-2^a + 2^{3t+k} + 2^{2t+k} + 2^{t+k} + 2^k = -(2^a - 2^{3t+k}) + 2^{2t+k} + 2^{t+k} + 2^k.$$

Using Observation 4.5, the above becomes

$$\left(\sum_{j=0}^{3t+k-1} 2^j\right) + \left(\sum_{j=a}^{n-1} 2^j\right) + 2^{2t+k} + 2^{t+k} + 2^k.$$

This becomes

$$\left(\sum_{j=0}^{k-1} 2^j\right) + 2^{3t+k} + \left(\sum_{j=a}^{n-1} 2^j\right) + 2^{2t+k} + 2^{t+k},$$

giving the set of exponents

$$A = \{0, 1, \ldots, k-1\} \cup \{a, a+1, \ldots, n-1\} \cup \{k+t, k+2t, k+3t\}.$$

We now find α, β in $\{1, 2, \ldots, t+3\}$ such that $\alpha i \equiv 1 \pmod{n}$ and $\beta i \equiv n - 1 \pmod{n}$ so that $(\alpha + \beta)i \equiv 0 \pmod{n}$. Assuming $\gcd(i, n) = 1$ this implies $n \mid \alpha + \beta$, which is impossible. If $\gcd(i, n) = 2$, then either $n \mid \alpha + \beta$, or $n \mid 2(\alpha + \beta)$ implying $n = 5t < 4t + 12$, i.e. $t < 12$, and it can be verified computationally that no equivalence is possible in this case except for $t = 1$.

The proof is done. □

We note that $e(4, 4) \equiv 29 \pmod{2^5 - 1}$ and $e(9, 2) \equiv 426 \pmod{2^{10} - 1}$, and these are the only two cases in which the Dobbertin exponent can be cyclotomic equivalent to $e(l, k)$.

One can attempt to treat the inverse Dobbertin exponent with the same method that we have used for the other families. Using [26, Lemma 9], since the inverse Dobbertin exponent D_t^{-1} is in the cyclotomic coset of $\frac{2^t+1}{2^{2t}+2^t+1}$ modulo $2^{5t} - 1$, it would be sufficient to investigate the congruence

$$(2^{2t} + 2^t + 1)e(l, k) \equiv 2^a(2^t + 1) \pmod{2^{5t} - 1}.$$

However, applying Lemma 4.1 requires a very large number of degenerate cases to be treated (significantly more that even in the proof of Theorem 4.9) and would require multiple pages just to write down. On the other hand, the cases that such a proof would handle on top of our other theorems and characterizations is quite modest: Dobbertin exponents only exist for n that are multiples of 5, while inverses only exist for odd n; and so, the only dimensions n

that the lack of such a proof would leave untouched are the odd integers n divisible by 5. In ordet to handle this subset of dimensions from the point of view of searching for new APN monomials in practice, we simply ran some computer experiments using SageMath on an i7 MacOS with 16GB of RAM. For $n \leq 200$ and $k, l \leq n-1$, the only possible value of t for which we can have equivalence is $t = 1$, when $D_1 = 29 \equiv -2 \pmod{2^5 - 1}$, so $D_1^{-1} \equiv 15 \pmod{2^5 - 1} = e(1, 4)$. We note that the interval $n \leq 200$ should all dimensions n where the investigation of APN-ness can be performed computationally using the currently available methods and computational resources.

5 Computationally testing APN-ness for the 0-APN exponents

We ran experiments to check whether the monomials of the form $x^{e(l,i)}$ with $3 \leq l \leq 9$ and $1 \leq k \leq 8$ are APN over the field $\mathbb{F}_{2^n}$ for $2 \leq n \leq 100$. Our results are presented in Table 2 where the entries list the dimensions n for which $e(l, k)$ is an APN exponent over $\mathbb{F}_{2^n}$. The experiments were run on a server with around 500 GB of RAM and 55 Intel Xeon E5-2690 CPU's using the *Magma* Computational Algebra System [9]. We tested APN-ness by checking whether the polynomial $F(x) = x^{e(l,i)} + a^{e(l,i)} + (x + a + 1)^{e(l,i)} + 1$ has more than two roots for all possible choices of $a \in \mathbb{F}_{2^n} \setminus \{0, a\}$. In our table, the empty cells denote experiments on monomials which did not finish due to time or memory constraints. All APN monomials encountered in our experiment were cyclotomic equivalent to representatives from the known families found in Table 1.

From the table we can observe that the difficulty of testing APN-ness for an exponent d over $\mathbb{F}_{2^n}$ grows not only with the dimension n, but also with d itself. Indeed, for small values of $d = e(l, i)$, we were able to test APN-ness for all $n \leq 100$, while for values as small as $e(6, 6) \approx 10^9$, this was no longer possible. This also illustrates the advantage of using 0-APN monomials as an intermediate step in the search of APN monomials, since it is significantly easier to characterize 0-APN-ness or to test it computationally.

6 Conclusion

We introduced an infinite class of exponents $e(l, k)$ with two parameters $l, k \in \mathbb{N}$, and showed how to easily find infinitely many dimensions n for which $x^{e(l,k)}$ is 0-APN for any choice

Table 2 Dimensions $n = 2$ to 100 where $x^{e(l,i)}$ is APN over $\mathbb{F}_{2^n}$

l \ i	1	2	3	4	5	6	7	8
3	5	2,4,5	3,5	2,4,5,8	5	2,3,4,5,6,12	5,7	2,4,5,8,16
4	2,5,7	5,7	2,5,7	5,7	2,7	5,7	2,5	
5	3,9	3,9	3	3,9	3,5,9			
6	2,4,7,11	2,7,11	2,3,4,7,11	2,4,7,11				
7	5,13	5,13	5,13					
8	2,3,5,6,9,15	3,5,9,15	2,5					
9	5,7,17	2,4,5,7,10,17						

of l and k. We discussed how our theoretical results can be extended with the help of some computations in order to characterize the set of all dimensions n over which $x^{e(l,k)}$ is 0-APN. The introduced class of exponents is significantly more tractable (both from a computational and a mathematical point of view) than in general, and provides a promising set of exponents that may lead to new APN monomials.

Taking advantage of this tractable structure of the exponents $e(l, k)$, we characterized precisely when they are cyclotomic equivalent to the known APN families (except in the case of the inverse of the Dobbertin exponents where the proof using our current methods is too technical, so we provided computational data for $n \leq 200$ instead). We observed that the Gold functions, their inverses, and the inverse APN function can all be expressed in the form $e(l, k)$ for suitable choices of l and k.

We have also provided some computational data on the APN-ness of this class of exponents and outlined the limits of the available computational equipment when it comes to verifying APN-ness.

We hope that further investigations into the structure and properties of the exponents $e(l, k)$ can provide us with additional conditions that might help us to overcome these technical limitations, and to potentially identify new instances of APN monomials over finite fields of large extension degree.

Acknowledgements We would like to thank the editor and the referees for their helpful comments and advice which has helped us to greatly improve the quality of the paper. The paper was started during an enjoyable visit of P. S. at the Selmer Center of University of Bergen in Spring of 2022. He would like to thank the institution for the invitation and the excellent working conditions.

Funding Open access funding provided by University of Bergen (incl Haukeland University Hospital)

References

1. Carlet, C., Charpin, P., Zinoviev, V.A.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Crypt. **15**(2), 125–156 (1998)
2. Yu, Y., Wang, M., Li, Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Crypt. **73**(2), 587–600 (2014)
3. Beierle, C., Leander, G.: New instances of quadratic APN functions. IEEE Trans. Inf. Theory **68**(1), 670–678 (2022)
4. Carlet, C.: Boolean functions for cryptography and coding theory. Cambridge University Press (2021)
5. Cusick, T.W., Stănică, P.: Cryptographic Boolean Functions and Applications (Ed. 2). Academic Press, San Diego, CA (2017)
6. Budaghyan, L., Kaleyski, N.S., Kwon, S., Riera, C., Stănică, P.: Partially APN Boolean functions and classes of functions that are not APN infinitely often. Cryptogr. Commun. **12**, 527–545 (2020)
7. Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5. International Conference on Finite Fields and Applications, pp. 113–121. (2001)
8. Budaghyan, L., Kaleyski, N., Riera, C., Stănică, P.: Partially APN functions with APN-like polynomial representations. Des. Codes Crypt. **88**, 1159–1177 (2020)
9. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)

10. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) Advances in Cryptology-EUROCRYPT '93 (Berlin, Heidelberg), pp. 55–64. Springer, Berlin (1994)
11. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
12. Dempwolff, U.: CCZ equivalence of power functions. Des. Codes Crypt. **86**(3), 665–692 (2018)
13. Yoshiara, S.: Equivalences of quadratic APN functions. J. Algebraic Combin. **35**(3), 461–475 (2012)
14. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)
15. Janwa, H., Wilson, R.M.: Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In: International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, pp. 180–194. Springer (1993)
16. Kasami, T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Inf. Comput. **18**(4), 369–394 (1971)
17. Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. IEEE Trans. Inf. Theory **45**(4), 1271–1275 (1999)
18. Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. Inf. Comput. **151**(1), 57–72 (1999)
19. Beth, T.H., Ding, C.: On almost perfect nonlinear permutations. In: Workshop on the Theory and Application of Cryptographic Techniques, pp. 65–76. Springer (1993)
20. Charpin, P., Kyureghyan, G.M.: On sets determining the differential spectrum of mappings. Internat. J. Inf. Coding Theory **4**(2–3), 170–184 (2017)
21. Budaghyan, L., Kaleyski, N.S., Kwon, S., Riera, C., Stănică, P.: Partially APN Boolean functions. Proceedings of Sequences and Their Applications (SETA 2018), Hong Kong (2018)
22. Cusick, T.W., Li, Y., Stănică, P.: On a combinatorial conjecture. Integers **11**, 185–203 (2011); see also, Electronic Journal of Combinatorial Number Theory **11**, Art. #17 (2011)
23. Kyureghyan, G.M., Suder, V.: On inversion in $\mathbb{Z}_{2^n-1}$. Finite Fields Appl. **25**, 234–254 (2014)
24. Kölsch, L.: On the inverses of Kasami and Bracken-Leander exponents. Des. Codes Crypt. **88**, 2597–2621 (2020)
25. Kaleyski, N., Nesheim, K., Stănică, P.: A doubly-infinite family of 0-APN monomials. Preprint at http://arxiv.org/abs/2211.13485. Accessed 24 Nov 2022
26. Budaghyan, L., Calderini, M., Carlet, C., Davidova, D., Kaleyski, N.S.: On two fundamental problems on APN power functions. IEEE Trans. Inf. Theory **68**(5), 3389–3403 (2022)