A doubly-infinite family of 0-APN monomials

Nikolay Kaleyski[1], Kjetil Nesheim[1], and Pantelimon Stănică[2]

[1]Department of Informatics, University of Bergen, Norway
[2]Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA, USA

Abstract

We give an infinite family of power functions, each of which is 0-APN over infinitely many finite fields $\mathbb{F}_{2^n}$. We computationally observe that our construction covers the majority of cases. We observe that representatives from the Gold and Inverse family of functions can be represented in this form. Finally, we discuss how our method can naturally be generalized to a necessary condition for perfect nonlinear (PN) functions over finite fields of odd characteristic.

1 Introduction

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements, where n is a natural number. An (n, m)**-function** is a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. These functions play a crucial role in many areas of mathematics and computer science, including symmetric cryptography, where the non-linear parts of virtually all modern block ciphers are represented as (n, m)-functions. The security of the cipher then directly depends on the properties of the (n, m)-functions. Characterizing and analyzing (n, m)-functions with good cryptographic properties is an active and important field of research. We mostly focus on the case $n = m$, which is arguably the most natural. We refer the reader to [4] for an excellent detailed survey of the topic.

One of the most important cryptographic properties of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is its **differential uniformity** $\Delta_F = \max\{\#\delta_F(a, b) : 0 \neq a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}\}$, where $\delta_F(a, b)$ is the set of solutions to $F(a + x) + F(x) = b$ for some $0 \neq a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$. A low differential uniformity indicates a good resistance to differential cryptanalysis [2]. The optimal value when $n = m$ is $\Delta_F = 2$; the functions attaining it are called **almost perfect nonlinear (APN)**. Equivalently, F is APN if and only if any $x, y, z \in \mathbb{F}_{2^n}$ with $F(x) + F(y) + F(z) + F(x + y + z) = 0$ satisfy $(x + y)(x + z)(y + z) = 0$.

Constructing APN functions is very difficult in practice. This makes it natural to investigate weaker, necessary conditions that any APN function needs to satisfy. One such condition is the notion of x_0-APN-ness (partial APNess) introduced in [3]. We say that F is x_0-APN for some $x_0 \in \mathbb{F}_{2^n}$ if any $y, z \in \mathbb{F}_{2^n}$ with $F(x_0) + F(y) + F(z) + F(x_0 + y + z) = 0$ (called the Janwa-Wilson-Rodier equation) satisfy $(x_0 + y)(x_0 + z)(y + z) = 0$. Clearly, F is APN if and only if it is x_0-APN for all $x_0 \in \mathbb{F}_{2^n}$.

Any (n, n)-function F can be uniquely represented as a polynomial $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$ with $a_i \in \mathbb{F}_{2^n}$; this is the **univariate representation** of F. We say that F is a **power function**, or a **monomial** if its univariate representation is of the form $F(x) = x^e$ for some natural number e. Monomial APN functions are the oldest known APN functions, and are among the most interesting APN functions in many senses. In the case of monomials, it can be shown that $F(x) = x^e$ is APN if and only if it is 1-APN; and that if it is 1-APN, then it is also 0-APN. Thus, a monomial can be either APN, 0-APN but not 1-APN, or not 0-APN. In the case of polynomials, the situation is much more varied, and the size of the set of $x_0 \in \mathbb{F}_{2^n}$ for which a function is x_0-APN can take many different values.

At present, we know of six infinite families of APN monomials [8, 11, 9, 10, 5, 6, 1, 7]. A table giving their exact form (which we omit here due to lack of space) can be found in e.g. [4]. One of the oldest and most resilient conjectures in the field is known as *Dobbertin's conjecture*; it states that the six families cover all possible APN monomials up to equivalence, i.e. any APN monomial over any finite field $\mathbb{F}_{2^n}$ must be cyclotomic equivalent to a representative from one of these six families [7]. Two monomials x^e and x^d are called **cyclotomic equivalent** if $e \equiv 2^k d \pmod{2^n - 1}$ or $e^{-1} \equiv 2^k d \pmod{2^n - 1}$ for some natural number k. Dobbertin's conjecture has been verified computationally up to dimension $n = 34$, and for all even n up to $n = 42$ (see e.g. [4]).

One of the reasons that the conjecture is difficult to verify is that the number $2^n - 1$ of possible exponents grows exponentially with n, and this makes it computationally difficult to check all exponents for large values of n. On the other hand, characterizing the APN-ness of (n, n)-functions theoretically (even in the case of monomials) is a difficult problem in itself, and even then, is only possible if one knows the approximate form of the exponents that need to be characterized.

In this paper, we introduce an infinite family of exponents of the form $e(l, k) = \sum_{j=0}^{l-1} 2^{jk}$ for some natural numbers l, k. For any choice of l and k, we give infinitely many dimensions n for which $x^{e(l,k)}$ is 0-APN over $\mathbb{F}_{2^n}$. In this sense, we define a "doubly infinite" family of 0-APN monomials. We observe that representatives from two of the known infinite families can be represented in this form which suggests that $e(l, k)$ are good candidates for APN monomials that might disprove Dobbertin's conjecture. Finally, we show that our approach naturally generalizes to perfect nonlinear (PN) monomials over finite fields of odd characteristic, and suggest some directions for future work.

2 A doubly infinite family of 0-APN monomials

Let $e(l, k) = \sum_{j=0}^{l-1} 2^{jk}$ for some natural numbers l and k. Recall that, for any natural number e, x^e is 0-APN over $\mathbb{F}_{2^n}$ if and only if $x^e + y^e + (x + y)^e = 0$ implies $xy(x + y) = 0$, i.e. if and only if $x^e + (x + 1)^e + 1 = 0$ is only possible for $x \in \mathbb{F}_2$. Our main theoretical result is the following.

Theorem 1. *Let n, l, k be natural numbers such that $\gcd(kl, n) = 1$ and $\gcd(e(k, l-1), 2^n - 1) = 1$. 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 $a \leq b$ and a set I, let $[a,b] = \{a, a+1, \ldots, b\}$, and let $\mathcal{P}I$ denote the power set of 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

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

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

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

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

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

Assuming $x \neq 0$, 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 1. *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 *cancels out. By induction on* l*, we would have obtained the condition that if* $\gcd(ik, n) = 1$ *for* $i = 2, 3, \ldots, l$*, then* $x^{e(k,l)}$ *must be* 0*-APN. We have tested these conditions computationally, and have seen that the condition in the statement of Theorem* 1 *always produces a set of dimensions* n *that subsumes those given by the alternative condition described in this remark. We have thus formulated the theorem only in terms of this more general condition. The less general condition* $\gcd(ik, n) = 1$ *for* $i = 2, 3, \ldots, l$ *could be useful in some contexts, however, since it does not require the explicit computation of the exponent* $e(l, k)$ *and its GCD with* $2^n - 1$*.*

Remark 2. *To see how discriminating the condition in Theorem* 1 *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* 1*; 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. For* $k = 1$ *and* $l = 7$*, we obtain* 28 *dimensions* n *satisfying the theorem, and* 33 *dimensions for which* $x^{e(7,1)}$ *is* 0*-APN; the ones not covered by the theorem are* $7, 35, 49, 77, 91$*. For* $k = 1$ *and* $l = 5$*, we obtain* 40 *values of* n *satisfying the condition in Theorem* 1*, and* 50 *values of* n *for which* $x^{e(5,1)}$ *is* 0*-APN. The ones that are not covered by Theorem* 1 *are* $n = 5 + 10k$ *for* $k = 0, 1, \ldots, 9$*.*

Remark 3. *We can see that representatives from some of the known infinite families of APN monomials can be expressed in the form* $e(l, k)$*. 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. We leave the characterization of cases when* $e(l, k)$ *is equivalent to the known APN families as a problem for future work.*

3 Possible generalizations and directions for future work

The approach outlined above can easily be generalized to other classes of functions, such as the perfect nonlinear (PN) functions over finite fields of odd characteristic. We recall that a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is PN if all of its derivatives $x \mapsto F(a + x) - F(x) - F(a) + F(0)$ for $0 \neq a \in \mathbb{F}_{p^n}$ are permutations. In the case of a monomial $F(x) = x^e$, this becomes $x \mapsto (a + x)^e - x^e - a^e$, and it clearly enough to consider $a = 1$, i.e. $x \mapsto (x + 1)^e - x^e - 1$. A necessary condition for this to be a permutation is that $(x+1)^e - x^e - 1 = 0$ only has $x = 0$ as a solution. By applying the same approach as in the proof of Theorem 1 for $e = \sum_{j=0}^{l-1} p^{kj}$, i.e. subtracting $(x + 1)^e - x^e - 1 = 0$ from its p^k-th power, we obtain

$$(x^{p^{lk}} - x)((x + 1)^{e'} - x^{e'}) = 0, \text{ with } e' = \sum_{j=0}^{l-2} p^{kj}.$$

Conditions analogous to the ones in Theorem 1 can then be obtained.

Besides exploring the PN case further, the binary case leaves a lot of room for future work as well. Theorem 1 suggests a set of exponents that might potentially be APN and could provide a counterexample to Dobbertin's conjecture, and so it is important to: characterize when $e(l,k)$ is equivalent to a representative from the known infinite families; determine what additional conditions $e(l,k)$ needs to satisfy in order to be APN (instead of merely 0-APN); investigate other exponents with a similar structure. Additionally, finding conditions under which the exponents $e(l,k)$ are not APN, or not 0-APN, would also be a useful result that would facilitate the computational search for new exponents.

References

[1] T. Beth and C. Ding, "On almost perfect nonlinear permutations," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 65–76, Springer, 1993.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, pp. 3–72, Jan 1991.

[3] L. Budaghyan, N. S. Kaleyski, S. Kwon, C. Riera, and P. Stănică, "Partially APN boolean functions and classes of functions that are not APN infinitely often," *Cryptography and Communications*, vol. 12, pp. 527–545, 2020.

[4] C. Carlet, *Boolean functions for cryptography and coding theory*, Cambridge University Press, 2021.

[5] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1271–1275, 1999.

[6] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case," *Information & Computation*, vol. 151, no. 1, pp. 57–72, 1999.

[7] H. Dobbertin, "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] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)," *IEEE Transactions on Information Theory*, vol. 14, no. 1, pp. 154–156, 1968.

[9] H. Janwa and R. M. Wilson, "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.

[10] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes," *Information & Computation*, vol. 18, no. 4, pp. 369–394, 1971.

[11] K. Nyberg, "Differentially uniform mappings for cryptography," *Lecture Notes in Computer Science*, vol. 765, pp. 55–64, 1994.