Searching for APN functions by polynomial expansion

Maren Hestad Aleksandersen[1], Lilya Budaghyan[1], and Nikolay Stoyanov Kaleyski[1]

Department of Informatics, University of Bergen
lilya.budaghyan@uib.no, maren.aleksandersen@gmail.com, nikolay.kaleyski@uib.no

Abstract. We investigate how far the approach of searching for APN functions by expanding their univariate representation can be pushed. We present some theoretical tricks that can be used to speed up the search up to EA-equivalence. We conduct systematic experiments over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$ and partition the resulting functions using the differential spectrum of their orthoderivatives. We find one new APN instance over $\mathbb{F}_{2^8}$. We also find 15 APN instances over $\mathbb{F}_{2^8}$ and 19 APN instances over $\mathbb{F}_{2^9}$ that are CCZ-inequivalent to the known infinite APN families. We see that they have differential spectra corresponding to known APN instances, but observe that the representatives that we obtain are significantly simpler than the known ones. We thus conclude that polynomial expansion deserves to be investigated in more detail.

Keywords: APN functions · differential uniformity · polynomial expansion.

1 Introduction

An (n, n)-function is a mapping with n input bits and n output bits. Nonlinear components of block ciphers are typically modeled as (n, n)-functions, and their properties are crucial for the security of the ciphers. One of the most powerful known attacks is differential cryptanalysis [2]. The best resistance to it is provided by APN (almost perfect nonlinear) functions which also have many other connections to mathematics and computer science (see e.g. [6] for a comprehensive survey).

Finding APN functions is difficult and many computational procedures have been developed, e.g. [1], [3], [11]. These typically exploit a representation or some property of the functions, and have produced thousands of CCZ-inequivalent APN instances. A disadvantage is that these procedures (and their implementation) can be complicated. A more serious drawback is that the obtained functions often have a very complicated form, which makes it difficult to e.g. generalize them into infinite constructions.

Some of the earliest known polynomial APN functions (e.g. [7] or [8]) were found by polynomial expansion. This amounts to adding terms to the polynomial

representation of a function F, and checking whether the resulting functions are APN. This method is easy to implement, and produces functions with a simple representation upon success. Despite this, it has not been considered seriously in the literature. In particular, no well-documented results exist showing how far it can be taken, and what searches have been performed.

In this abstract, we report on our computational results of applying polynomial expansion to some known APN functions over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$. We obtain many APN functions in this way, and use the differential spectra of the orthoderivatives [5] to partition them into classes. We find 16 classes in $\mathbb{F}_{2^8}$ and 19 classes in $\mathbb{F}_{2^9}$ of APN functions that are CCZ-inequivalent to representatives from the known infinite families. In the case of $\mathbb{F}_{2^8}$, one of the classes is completely new. The remaining classes match those of known APN instances (found by e.g. the method from [1] or [11]), but our representatives have a significantly simpler representation (for instance, only 5 instead of 44 terms). When the initial function that we expand is a monomial, we introduce some theoretical tricks that can be used to restrict the choice of coefficients (up to EA-equivalence) and significantly speed up the search.

We thus conclude that the polynomial expansion approach can still produce useful results, and deserves to receive more attention that it currently does.

2 Background and notation

An (n, n)**-function**, or vectorial Boolean function, is a map from the finite field $\mathbb{F}_{2^n}$ to itself. Any (n, n)-function can be uniquely represented as a univariate polynomial of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$ for $a_i \in \mathbb{F}_{2^n}$. The largest binary weight of an exponent i with $a_i \neq 0$ is called the **algebraic degree** of F, denoted $\deg(F)$. If $\deg(F) \leq 1$, we say that F is **affine**, and if $\deg(F) = 2$, we say that F is **quadratic**. An affine F with $F(0) = 0$ is called **linear**.

For an (n, n)-function F, we denote by $\delta_F(a, b)$ the number of solutions $x \in \mathbb{F}_{2^n}$ to $F(a+x)+F(x) = b$ for $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}$. The **differential uniformity** of F is $\delta_F = \max_{a,b \in \mathbb{F}_{2^n}, a \neq 0} \delta_F(a, b)$. The lower the value of δ_F, the more resistant F is to differential attacks. Clearly, $\delta_F \geq 2$ for any (n, n)-function F. If $\delta_F = 2$, we say that F is **almost perfect nonlinear (APN)**.

Two (n, n)-functions F and G are **CCZ-equivalent** (Carlet-Charpin-Zinoviev-equivalent) if there exists an affine permutation A of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ mapping the graph $\{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph of G. CCZ-equivalence is the most general known relation preserving APN-ness, and so APN functions are typically classified up to CCZ-equivalence. A special case of CCZ-equivalence is EA-equivalence. We say that F and G are **EA-equivalent** (extended affine equivalent) if $A_1 \circ F \circ A_2 + A = G$ for some affine A_1, A_2, A with A_1 and A_2 being permutations. Two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [9]. Furthermore, most of the known APN functions are quadratic, or CCZ-equivalent to quadratic (see e.g. [6] for a general survey, or [4] for a survey of the known infinite constructions). Thus, in practice, it is often enough to test EA-equivalence.

The **orthoderivative** π_F is a function uniquely associated with a quadratic APN function F. If F and G are EA-equivalent (and hence also CCZ-equivalent), then so are π_F and π_G [5]. The multiset of the values of $\delta_F(a,b)$ through all $a,b \in \mathbb{F}_{2^n}$ is called the **differential spectrum** of F, and is invariant under EA-equivalence. The differential spectra of the orthoderivatives are a very strong invariant for quadratic APN functions that has almost the same distinguishing power as an EA-equivalence test [5].

3 Polynomial expansion

Consider an initial (n,n)-function F. We conduct an exhaustive search over all functions of the form $F+c_1x^{i_1}+\cdots+c_Kx^{i_K}$ for a natural number K and all possible coefficients c_j and exponents i_j. We restrict the exponents to quadratic ones since we use the orthoderivatives to distinguish between inequivalent functions, and they are only defined for quadratic APN functions; furthermore, most of the known APN functions are quadratic, so the probability of finding non-quadratic ones in this way is very low. For small values of K, we consider all coefficients $c_j \in \mathbb{F}_{2^n}$. When the search becomes too slow, we restrict the coefficients to a subfield of $\mathbb{F}_{2^n}$. We do not perform searches with coefficients restricted to $\mathbb{F}_2$ since all quadratic APN functions with binary coefficients over $\mathbb{F}_{2^n}$ have been classified for $n \leq 9$ [10].

When F is a monomial, we can speed up the search as follows. Let $F(x) = x^d$ and $G(x) = x^d + cx^i$. Composing $L_1 \circ F \circ L_2$ with $L_1(x) = x/a^d$ and $L_2(x) = ax$ for $0 \neq a \in \mathbb{F}_{2^n}$, we obtain the EA-equivalent $G'(x) = x^d + ca^{i-d}x^i$. Thus, the coefficient of the first expansion term can be multiplied by a^{i-d} for $0 \neq a$. Thus, having tried c, we can ignore all coefficients of the form ca^{i-d} for $0 \neq a \in \mathbb{F}_{2^n}$. Similarly, we can take $L_1(x) = x^2$ and $L_2(x) = x^{2^{n-1}}$, and obtain the EA-equivalent $G''(x) = x^d + c^2x^i$. Thus, c can be raised to any power of 2. Restricting the coefficient of the first term in this way significantly reduces the search space, and allows us to perform e.g. searches with $K = 5$ terms in $\mathbb{F}_{2^9}$ when the initial function is a monomial, while in the case of polynomials, we must restrict ourselves to $K = 4$ terms due to long running times.

4 Computational results

We consider as an initial function F a single representative from each CCZ-class represented by the quadratic infinite APN families. In the case of $n = 8$, we run searches with coefficients in $\mathbb{F}_{2^8}$ for up to 3 terms when F is a monomial, and up to 2 terms otherwise. Restricting the coefficients to $\mathbb{F}_{2^4}$, we attempt to add 4 terms, and with coefficients in $\mathbb{F}_{2^2}$ we are able to go up to 6 terms. All running times are within 100 hours; pushing the search further may be possible, but would require considerable computational effort.

We find 16 classes (according to the orthoderivative's differential spectrum) CCZ-inequivalent to the known infinite families. Among these, the function $x^3 + \beta x^{18} + \beta x^{66} + \beta^2 x^{132}$ (where β is primitive in $\mathbb{F}_{2^2}$) is completely new,

having differential spectrum of the orthoderivative $0^{38196}, 2^{22008}, 4^{4608}, 6^{456}, 8^{12}$ (with the multiplicity of each element written in superscript). The remaining 15 differential spectra match those of known APN instances; however, our representations are significantly shorter and better structured than the known ones in many cases. For instance, one of our representatives, viz. $x^5+x^9+\beta x^{17}+\beta x^{65}+\beta^2 x^{170}x^{80}+\beta x^{96}+x^{144}$, has 7 terms, with coefficients in $\mathbb{F}_{2^2}$. It is equivalent to a known instances obtained in [1] having 36 terms with various coefficients.

For $\mathbb{F}_{2^9}$, the situation is similar. For coefficients in $\mathbb{F}_{2^9}$, we go up to 2 terms, and then restrict the coefficients to $\mathbb{F}_{2^3}$. We can go up to 5 terms for monomials (using the simplification described above) and up to 4 terms when the initial function is a polynomial. The running times are within 600 hours. We find 19 orthoderivative differential spectra that are not represented by the known infinite APN families. All of them correspond to known instances but some of our representatives are significantly simpler. For instance, one of the functions in [1] has 44 terms, while our representative can be written as $x^3+\gamma x^{10}+x^{17}+\gamma x^{66}+x^{80}$, with γ primitive in $\mathbb{F}_{2^3}$.

Due to space limitations, we do not provide a full list of the representatives that we find here; one is available in the first author's master thesis, or online at `https://boolean.h.uib.no/mediawiki/index.php/APN_functions_obtained_via_polynomial_expansion_in_small_dimensions`.

References

1. Beierle C, Leander G. New instances of quadratic APN functions. arXiv preprint arXiv:2009.07204. 2020 Sep 15.
2. Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY. 1991 Jan 1;4(1):3-72.
3. Budaghyan L, Calderini M, Carlet C, Coulter R, Villa I. Generalized isotopic shift construction for APN functions. Designs, Codes and Cryptography. 2021 Jan;89(1):19-32.
4. Calderini M, Budaghyan L, Carlet C. On known constructions of APN and AB functions and their relation to each other. Rad Hrvatske akademije znanosti i umjetnosti: Matematike znanosti. 2021 Aug 25(546= 25):79-105.
5. Canteaut A, Couvreur A, Perrin L. Recovering or Testing Extended-Affine Equivalence. arXiv preprint arXiv:2103.00078. 2021 Feb 26.
6. Carlet C. Boolean functions for cryptography and coding theory. Cambridge University Press, 2021.
7. Dillon JF. APN polynomials and related codes. InBanff Conference, Nov. 2006 2006.
8. Edel Y, Kyureghyan G, Pott A. A new APN function which is not equivalent to a power mapping. IEEE Transactions on Information Theory. 2006 Jan 23;52(2):744-7.
9. Yoshiara S. Equivalences of quadratic APN functions. Journal of Algebraic Combinatorics. 2012 May;35(3):461-75.
10. Yu Y, Kaleyski N, Budaghyan L, Li Y. Classification of quadratic APN functions with coefficients in F2 for dimensions up to 9. Finite Fields and Their Applications. 2020 Dec 1;68:101733.
11. Yu Y, Wang M, Li Y. A matrix approach for constructing quadratic APN functions. Designs, codes and cryptography. 2014 Nov;73(2):587-600.