Walsh zero spaces of APN functions

Petr Lisoněk

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada

Abstract

We report on work in progress that is motivated by the "Big APN Problem" that concerns the existence of APN permutations of $\mathbb{F}_{2^n}$ for even $n \geq 8$. Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. We define a Walsh zero space (WZ space) of f to be any $\mathbb{F}_2$-linear n-dimensional space of Walsh zeros of f. This definition is motivated by the fact that a function is CCZ-equivalent to a permutation if and only if it possesses a pair of WZ spaces that intersect trivially. We discuss characterization of Walsh zeros and construction of WZ spaces for quadratic functions, and we include examples and results for Gold functions and for the function $f(x) = x^3 + \mathrm{Tr}(x^9)$.

1 Background

Let $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements. A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *almost perfect nonlinear (APN)* if for all $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, the equation $f(x + a) - f(x) = b$ has at most two solutions $x \in \mathbb{F}_{2^n}$. Without loss of generality, we can normalize any APN function such that $f(0) = 0$, and we will assume this throughout.

APN functions, and more generally functions with low differential uniformity, have been extensively studied due to their importance in the design of S-boxes of block ciphers in cryptography, where they offer the best possible protection against the differential cryptanalysis attack. In some block cipher designs, such as substitution-permutation networks (SPN), it is required that S-boxes are invertible mappings. Of special interest are therefore APN functions which are invertible, that is, they are *permutations* of $\mathbb{F}_{2^n}$. Many APN permutations of $\mathbb{F}_{2^n}$ are known for odd n. It is known that APN permutations of $\mathbb{F}_{2^n}$ do not exist for $n = 2, 4$. An APN permutation of $\mathbb{F}_{2^6}$ was discovered in 2009 [2]. We will briefly describe the method by which it was found. Our description is somewhat different from [2] but it is equivalent.

Let Tr_s^n denote the trace function from $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^s}$. The absolute trace Tr_1^n will be denoted simply as Tr. Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. For $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ we define the Walsh transform of f at (a, b) as $\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax + bf(x))}$. We say that (a, b) is a *Walsh zero* of f if $\mathcal{W}_f(a, b) = 0$. The *Walsh spectrum* of f is the set $\{\mathcal{W}_f(a, b) : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$.

Definition 1.1 *Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Suppose that S is an $\mathbb{F}_2$-linear subspace of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\dim_{\mathbb{F}_2} S = n$ and each element of S except $(0, 0)$ is a Walsh zero of f. We say that S is a* WZ space *of f.*

Note that $\mathbb{F}_{2^n} \times \{0\}$ is a WZ space of any function on $\mathbb{F}_{2^n}$. We say that two WZ spaces S, T of the same function *intersect trivially* if $S \cap T = \{(0, 0)\}$.

The *CCZ-equivalence* of functions was introduced by Carlet, Charpin and Zinoviev in [4]. It has many important features, in particular it preserves the APN property. The construction of APN permutation of $\mathbb{F}_{2^6}$ in [2] consists of choosing a certain APN function κ on $\mathbb{F}_{2^6}$, and then finding a permutation of $\mathbb{F}_{2^6}$ that is CCZ-equivalent to κ. For the latter task, the following characterization is used in [2], which we present in a different but equivalent form.

Proposition 1.2 *[2] Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ such that $f(0) = 0$. Then f is CCZ-equivalent to a permutation of $\mathbb{F}_{2^n}$ if and only if there exist two WZ spaces of f that intersect trivially.*

The existence of APN permutations of $\mathbb{F}_{2^n}$ for even $n \geq 8$ is an important open problem, and it is called "The Big APN Problem" in [2].

Keeping in mind the approach of [2], one can attack this problem by considering a known APN function and using Proposition 1.2 to determine if it is CCZ-equivalent to a permutation. The first general results in this direction (i.e., involving infinite families of functions) were announced by Göloğlu (joint work with Langevin) in 2015 at the conference Fq12 [6]. Their work presently exists as preprint [7]. According to [7], Gold APN functions $f(x) = x^{2^k+1}$, where $\gcd(k, n) = 1$, are never CCZ-equivalent to permutations of $\mathbb{F}_{2^n}$ when n is even, and Kasami APN functions $f(x) = x^{2^{2k}-2^k+1}$, where $\gcd(k, n) = 1$, are never CCZ-equivalent to permutations of $\mathbb{F}_{2^n}$ when n is divisible by 4 (with the case $n \equiv 2 \pmod 4$ remaining open).

2 Characterizing WZ spaces

In order to complement the previous work, we envision a different approach, while still employing Proposition 1.2. In [7] the non-existence of two trivially intersecting WZ spaces is argued by assuming the contrary and driving this assumption to a contradiction. Instead, we plan to characterize many (preferably all) WZ spaces for a given APN function, and show the non-existence of two trivially intersecting WZ spaces in that way. This approach has some advantages. Examples of WZ spaces can be found with computer aid, which can inform the theoretical proofs. At the same time, this proof method can also target discovery of a trivially intersecting pair of WZ spaces should it in fact exist, which is something that the proof by contradiction can not target as an objective. Furthermore, computer searches suggest that some APN functions (such as Kasami and Dobbertin functions) may posses *only one* WZ space, namely the space $\mathbb{F}_{2^n} \times \{0\}$. This assertion can be then set as the proof objective instead of the original objective.

2.1 Quadratic functions

We give further details for the case when the APN function is *quadratic,* that is, assuming that the function is expressed in its unique polynomial form, then the exponent of each monomial has binary weight at most 2. We note that the function κ used to construct the APN permutation in dimension 6 is quadratic [2].

To characterize the WZ spaces of an APN function f we first have to characterize the Walsh zeros of f. One possible way to do this is known as the "squaring method" that computes $(\mathcal{W}_f(a, b))^2$, and it is often used to determine the entire Walsh spectrum of f. It associates a certain linear form $\mathcal{L}_b$ to f and (a, b). As the symbol suggests, the linear form depends on b but not on a. Then (a, b) is a Walsh zero of f if $\mathrm{Tr}(f(x))$ does not vanish completely on the kernel of $\mathcal{L}_b$. For the APN function $f(x) = x^3 + \mathrm{Tr}(x^9)$ this computation was carried out in detail by Bracken et al. in Section 2 of [1], see in particular equation (6) there. This computation was further generalized by Budaghyan et al. in [3] to compute Walsh spectra (hence, implicitly, also Walsh zeros) of the more general families of APN functions denoted F_0, F_1 and F_2 in [3]. In order to upper bound the cardinality of the kernel of the linear form, both [1] and [3] apply an ad-hoc method developed earlier by Dobbertin [5].

It is worth noting that for investigations of such kernels one can apply a more systematic theory developed by van der Geer and van der Vlugt [8]. While a more detailed exposition would exceed the size limit of this abstract, we at least survey the results that one obtains in this way for two families of quadratic APN functions.

Proposition 2.1 *Let n be even, $\gcd(k, n) = 1$, and $a, b \in \mathbb{F}_{2^n}$. If $b \neq 0$, then (a, b) is a Walsh zero of the Gold function $f(x) = x^{2^k+1}$ if and only if b is a (2^k+1)th power in $\mathbb{F}_{2^n}$ (equivalently, b is a cube in $\mathbb{F}_{2^n}$) and $\mathrm{Tr}_2^n(az) \neq 0$ for each $z \in \mathbb{F}_{2^n}$ such that $bz^{2^k+1} + 1 = 0$.*

Proposition 2.2 *Let n be even and $a, b \in \mathbb{F}_{2^n}$.*
(i) If $b \neq 0$ and $\mathrm{Tr}(b) = 0$ then (a, b) is a Walsh zero of $f(x) = x^3 + \mathrm{Tr}(x^9)$ if and only if it is a Walsh zero of $f(x) = x^3$.

(ii) If $\mathrm{Tr}(b) = 1$*, let* x^* *be the unique solution of* $x^9 + x^3 + bx + 1 = 0$ *in* $\mathbb{F}_{2^n}$*. Then* (a, b) *is a Walsh zero of* $f(x) = x^3 + \mathrm{Tr}(x^9)$ *if and only if* x^* *is a cube in* $\mathbb{F}_{2^n}$ *and* $\mathrm{Tr}_2^n(az) \neq 0$ *for each* $z \in \mathbb{F}_{2^n}$ *such that* $z^3 = x^*$*.*

We note that these characterizations are enabled by the fact that in *both* cases the kernels are either trivial or they are cosets of $\mathbb{F}_4$, where z denotes any non-zero element of the kernel in both propositions. This naturally leads to applying trace to $\mathbb{F}_4$. While Proposition 2.1 is likely "folklore" (as remarked in [7]), on the other hand Proposition 2.2 appears to characterize the kernels more explicitly than in [1].

Equipped with the previous two propositions we can construct some non-trivial WZ spaces for the two families of APN functions under consideration.

Proposition 2.3 *Let* n *be even and* $\gcd(k, n) = 1$*. Let* $u \in \mathbb{F}_{2^n}^*$*. The set*

$$G_{k,u} = \{(a, 0) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 0\} \cup \{(a, u^{-(2^k+1)}) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 1\}$$

is a WZ space of the Gold function $f(x) = x^{2^k+1}$ *on* $\mathbb{F}_{2^n}$*.*

Proposition 2.4 *Let* n *be even and* $f(x) = x^3 + \mathrm{Tr}(x^9)$*. Let* $b \in \mathbb{F}_{2^n}^*$*.*
(i) If $\mathrm{Tr}(b) = 0$ *and* b *is a cube in* $\mathbb{F}_{2^n}$*, then* $G_{1,u}$ *is a WZ space of* f *where* u *is any of the cube roots of* $1/b$*.*
(ii) If $\mathrm{Tr}(b) = 1$ *then let* x^* *be the unique solution of* $x^9 + x^3 + bx + 1 = 0$ *in* $\mathbb{F}_{2^n}$*. If* x^* *is a cube in* $\mathbb{F}_{2^n}$ *and* u *is any of the cube roots of* x^**, then the set*

$$S_u = \{(a, 0) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 0\} \cup \{(a, b) \ : \ a \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(ua) = 1\}$$

is a WZ space of f*.*

3 Outlook

This work is currently in progress. We hope that it would lead to an alternative and possibly simpler proof of CCZ-inequivalence of APN Gold functions with permutations in even dimensions. Computer searches suggest that in certain dimensions (e.g., $n = 8$) the spaces $G_{k,u}$ given in Proposition 2.3 and the space $\mathbb{F}_{2^n} \times \{0\}$ are the only WZ spaces of the Gold function. While additional WZ spaces will possibly exist in other dimensions, it seems that a complete classification of WZ spaces should be within reach for the Gold functions. As well, we will study Walsh zero sets of other families of quadratic APN functions with the view of possibly finding functions with richer sets of WZ spaces.

References

[1] C. Bracken, E. Byrne, N. Markin, G. McGuire, On the Walsh spectrum of a new APN function. Cryptography and coding, 92–98, Lecture Notes in Comput. Sci., 4887, Springer, Berlin, 2007.

[2] K.A. Browning, J.F. Dillon, M.T. McQuistan, A.J. Wolfe, An APN permutation in dimension six. Finite fields: theory and applications, 33–42, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

[3] L. Budaghyan, T. Helleseth, N. Li, B. Sun, Some results on the known classes of quadratic APN functions. Codes, cryptology and information security, 3–16, Lecture Notes in Comput. Sci., 10194, Springer, Cham, 2017.

[4] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15 (1998), no. 2, 125–156.

[5] H. Dobbertin, Another proof of Kasami's theorem. Des. Codes Cryptogr. 17 (1999), no. 1–3, 177–180.

[6] F. Göloğlu, Almost perfect nonlinear functions which are not equivalent to permutations. Fq12 conference abstract, July 2015.
Available at https://www.skidmore.edu/fq12/uploads/all-abstracts.pdf

[7] F. Göloğlu, P. Langevin, APN families which are not equivalent to permutations. Preprint, 22 March 2019. (private communication)

[8] G. van der Geer, M. van der Vlugt, Reed-Muller codes and supersingular curves. I. Compositio Math. 84 (1992), no. 3, 333–367.