# Constructions and applications of Walsh zero spaces

Benjamin Chase and Petr Lisoněk

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

**Abstract**

A Walsh zero space (WZ space) for $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an $n$-dimensional vector subspace of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ whose all nonzero elements are Walsh zeros of $f$. We provide several theoretical and computer-free constructions of WZ spaces for Gold APN functions $f(x) = x^{2^i+1}$ on $\mathbb{F}_{2^n}$ where $n$ is odd and $\gcd(i, n) = 1$. We also provide several constructions of trivially intersecting pairs of such spaces. We illustrate applications of our constructions that include partitioning of the CCZ class of $f$ to EA classes, and constructing APN permutations that are CCZ equivalent to $f$ but not extended affine equivalent to $f$ or its compositional inverse.

## 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 differential cryptanalysis. 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 $\mathbb{F}_{2^n}$. Constructing new APN permutations of $\mathbb{F}_{2^n}$ is one of the objectives of our work.

Let $\mathrm{Tr}^n_m$ denote the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, and let Tr denote the absolute trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. 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 $\mathcal{W}_f(a, b) = 0$.

**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 $f$.*

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. Dillon et al. introduced in [2] a method that, assuming certain conditions are satisfied, constructs a permutation that is CCZ equivalent to a given APN function. In the following proposition we present this method in a different but equivalent form, using the concept of WZ spaces. We also include a proof of the proposition, which is contained only implicitly in [2], because it allows one to *explicitly construct* an APN permutation CCZ equivalent to the given APN function.

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

**Proof:** Fix a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then the elements of $\mathbb{F}_{2^n}$ can be represented as $n$-dimensional column vectors over $\mathbb{F}_2$, and we will use this representation to associate functions $f, f'$ with matrices $G, G'$ in this proof. Let $G$ be a $(2n) \times (2^n - 1)$ matrix over $\mathbb{F}_2$ whose columns are of the form $\begin{pmatrix} x \\ f(x) \end{pmatrix}$ where $x$ runs through all nonzero elements of $\mathbb{F}_{2^n}$. Since $f$ is assumed to be APN, we know [4, Corollary 1(i)] that the rank of $G$ is $2n$.

Let $S$ and $T$ be the two given trivially intersecting WZ spaces, and let $\{(a_1, b_1), \ldots, (a_n, b_n)\}$ and $\{(a_{n+1}, b_{n+1}), \ldots, (a_{2n}, b_{2n})\}$ be their bases. Let $G'$ be the $(2n) \times (2^n - 1)$ matrix over $\mathbb{F}_2$ defined as follows. The $i$-th row of $G'$ is $(\mathrm{Tr}(a_i x + b_i f(x)))_x$ where $x$ runs through all nonzero elements of $\mathbb{F}_{2^n}$ in the same order as it did when we constructed the matrix $G$ above. Let $G'_1$ be the submatrix of $G'$ formed by its top $n$ rows, and let $G'_2$ be the submatrix of $G'$ formed by its bottom $n$ rows. Since $f(0) = 0$ and each $(a_i, b_i)$ is a Walsh zero of $f$, it follows that each row of $G'$ has Hamming weight $2^{n-1}$. Since $S$ and $T$ are trivially intersecting and each of them has dimension $n$, it follows that $S \oplus T = \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and the rank of $G'$ is $2n$. Hence the binary linear codes generated by $G$ and $G'$ are equal. Further it follows that the binary linear codes generated by $G'_1$ and $G'_2$ are simplex codes, hence columns of $G'_1$ are distinct and columns of $G'_2$ are distinct. Viewing the columns of $G'$ as $\begin{pmatrix} y \\ f'(y) \end{pmatrix}$ defines a new function $f' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ where we additionally let $f'(0) = 0$. The function $f'$ is CCZ equivalent to $f$ [4] and since $f$ is APN, it follows that $f'$ is APN. Since the columns of $G'_2$ are distinct and nonzero, $f'$ is a permutation. □

## 2 Constructions of WZ spaces

In this section we provide constructions of some WZ spaces for the Gold APN functions $f(x) = x^{2^i+1}$ defined on $\mathbb{F}_{2^n}$, where $n$ is odd and $\gcd(i, n) = 1$.

**Lemma 2.1** *Suppose $n$ is odd and $\gcd(i, n) = 1$, where $0 < i < n$. Let $f(x) = x^{2^i+1}$ be a Gold APN function. Then $(a, b)$ is a Walsh zero of $f$ if and only if $\mathrm{Tr}(ab^{-\frac{1}{2^i+1}}) = 0$ or $a \neq b = 0$.*

**Proof:** For $b = 1$ the result is proved in [6] by a calculation based on the arguments given in [5]. For $b \neq 1$ it is sufficient to augment the calculation in [6] by a simple substitution in the summation range. □

Theoretical constructions given in this section were partially motivated by examples of WZ spaces in low dimensions that we obtained computationally using the SboxU software package written by Léo Perrin [1, Section 4], [7]. We expect that the constructions given herein are not exhaustive; indeed this is an active project that we are currently pursuing. Proofs of propositions are omitted due to the page limit of this extended abstract; all proofs will be included in the full version of the paper.

**Proposition 2.2** *The space $\mathbb{F}_{2^n} \times \{0\}$ is a WZ space for each function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. The space $\{0\} \times \mathbb{F}_{2^n}$ is a WZ space for $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ if and only if $f$ is a permutation.*

**Proposition 2.3** *Assume that $n = 3k$ where $k$ is odd. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Let $\xi \in \mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and let $\mu \in \mathbb{F}^*_{2^n}$. Then*

$$S = \{ \Big( x \, , \, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x)) \Big) \ : \ x \in \mathbb{F}_{2^n} \}$$

*is a WZ space of $f$.*

While Proposition 2.3 holds for each $\xi \in \mathbb{F}_{2^3}$, one obtains interesting results only when $\xi$ is a primitive element of $\mathbb{F}_{2^3}$. If $\xi = 0, 1$ then $S$ is the trivial WZ space $\mathbb{F}_{2^n} \times \{0\}$.

From now on let us define $0^{-\frac{1}{2^i+1}} = 0$ as this will simplify some of the forthcoming constructions and arguments. Let us note that for testing whether a pair $(a, b)$ is a Walsh zero it is then sufficient to use only the first condition of Lemma 2.1, because for a pair $(a, 0)$ we get $\mathrm{Tr}(a \cdot 0^{-\frac{1}{2^i+1}}) = \mathrm{Tr}(a \cdot 0) = 0$, as desired.

**Definition 2.4** *Let $n$ be odd and $\gcd(i, n) = 1$. Let $S$ be an additive subspace of $\mathbb{F}_{2^n}$. We say that $S$ is $i$-*compatible *if the set $S^{-\frac{1}{2^i+1}} = \{s^{-\frac{1}{2^i+1}} : s \in S\}$ is also an additive subspace of $\mathbb{F}_{2^n}$.*

It is easy to show that if $S$ is $i$-compatible, then it is also $(n-i)$-compatible. This is closely related to the linear equivalence of Gold functions $f(x) = x^{2^i+1}$ and $g(x) = x^{2^{n-i}+1}$.

For $U \subseteq \mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}$ denote $aU = \{au : u \in U\}$.

**Example 2.5**
*(i) If $n$ is odd and $\gcd(i, n) = 1$ then the following subspaces of $\mathbb{F}_{2^n}$ are $i$-compatible: $\{0\}$, $\mathbb{F}_2$ and $\mathbb{F}_{2^n}$.*
*(ii) If $S$ is $i$-compatible subspace of $\mathbb{F}_{2^n}$, then $\mu S$ is also $i$-compatible for each $\mu \in \mathbb{F}_{2^n}$.*

Moreover, when $n$ is a multiple of 3, then $\mathbb{F}_{2^n}$ contains the subfield $\mathbb{F}_{2^3}$ and the following lemma applies.

**Lemma 2.6** *Assume that $n$ is odd and divisible by 3. Let $S$ be the subspace of $\mathbb{F}_{2^n}$ isomorphic to $\mathbb{F}_{2^3}$. Then each additive subspace of $S$ is $i$-compatible whenever $\gcd(i, n) = 1$.*

As any two 2-dimensional subspaces (hyperplanes) of $\mathbb{F}_{2^3}$ can be obtained from each other just by scaling by an element of $\mathbb{F}_{2^3}^*$, it follows that if 3 divides $n$, then Lemma 2.6 along with Example 2.5(ii) provide $2^n - 1$ two-dimensional $i$-compatible subspaces of $\mathbb{F}_{2^n}$ and $(2^n - 1)/7$ three-dimensional $i$-compatible subspaces of $\mathbb{F}_{2^n}$.

**Problem 2.7** *For odd $n$, do there exist $i$-compatible subspaces of $\mathbb{F}_{2^n}$ other than those described by Example 2.5(i,ii) and Lemma 2.6?*

The next proposition shows an application of $i$-compatible subspaces to the construction of WZ spaces.

**Proposition 2.8** *Assume that $n$ is odd, $\gcd(i, n) = 1$ and $S$ is an $i$-compatible subspace of $\mathbb{F}_{2^n}$. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be given by $f(x) = x^{2^i+1}$. Let*

$$X = \{x \in \mathbb{F}_{2^n} : (\forall a \in S^{-\frac{1}{2^i+1}})\ \mathrm{Tr}(ax) = 0\}.$$

*Then $X \times S$ is a WZ space for $f$.*

**Proposition 2.9** *Suppose $n$ is odd and $m|n$. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$ and let $\mu \in \mathbb{F}_{2^n}^*$ be fixed. Then*

$$S := \{(\mu a, \mu^{2^i+1} b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m} \text{ and } \mathrm{Tr}_m^n(a) = b + b^{\frac{1}{2^i}}\}$$

*is a WZ space of $f$.*

# 3 Constructions of trivially intersecting pairs of WZ spaces

Due to Proposition 1.2 it is of great interest to find APN functions possessing trivially intersecting pairs of WZ spaces, as it allows one to construct APN permutations. In this section we give several constructions of such pairs of WZ spaces of the Gold APN functions. Again we skip the proofs due to the page limit of this extended abstract; all proofs will be included in the full version of the paper.

**Proposition 3.1** *Let $n = 3k$ where $k$ is odd and let $\gcd(i, n) = 1$. Let*

$$S = \{(x, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x))) : x \in \mathbb{F}_{2^n}\}$$

*with $\xi$ a primitive element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and $\mu \in \mathbb{F}_{2^n}^*$, and let $T = \{0\} \times \mathbb{F}_{2^n}$. Then $S$ and $T$ are WZ spaces for $f(x) = x^{2^i+1}$ on $\mathbb{F}_{2^n}$, and the pair $\{S, T\}$ intersects trivially.*

**Proposition 3.2** *Let $n$ be odd and $\gcd(i, n) = 1$. Let*

$$S = \{(\mu a, \mu^{2^i+1} b) : a, b \in \mathbb{F}_{2^n} \text{ and } a = b + b^{\frac{1}{2^i}}\}$$

*and $T = \mathbb{F}_{2^n} \times \{0\}$. Then $S$ and $T$ are WZ spaces for $f(x) = x^{2^i+1}$ on $\mathbb{F}_{2^n}$, and the pair $\{S, T\}$ intersects trivially.*

**Proposition 3.3** *Let $n = 3k$ where $k$ is odd and $\gcd(i, n) = 1$. Let*

$$S = \{(x, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x))) : x \in \mathbb{F}_{2^n}\}$$

*with $\xi$ a primitive element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and $\mu \in \mathbb{F}_{2^n}^*$. Let*

$$T = \{(\nu a, \nu^{2^i+1} b) : a, b \in \mathbb{F}_{2^n} \text{ and } a = b + b^{\frac{1}{2^i}}\}$$

*where $\nu \in \mathbb{F}_{2^n}^*$. Suppose also that $\mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = 0$. Then $S$ and $T$ are WZ spaces for $f(x) = x^{2^i+1}$ on $\mathbb{F}_{2^n}$, and the pair $\{S, T\}$ intersects trivially.*

**Proposition 3.4** *Let $n = 3k$ where $k$ is odd and $\gcd(i, n) = 1$. Let*

$$R = \{(\nu a, \nu^{2^i+1} b) : a, b \in \mathbb{F}_{2^n} \text{ and } a = b + b^{\frac{1}{2^i}}\}$$

*where $\nu \in \mathbb{F}_{2^n}^*$. Suppose $\xi$ is a primitive element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$. Suppose $T = X \times S_\mu$ where $S_\mu = \mathrm{span}_{\mathbb{F}_2}\{\mu, \xi\mu\}$ for some $\mu \in \mathbb{F}_{2^n}^*$ and $T$ is constructed by applying Proposition 2.8. Suppose also that $\mathrm{Tr}((\xi + \xi^{2^i})\mu^{\frac{2^i}{2^i+1}} \nu^{-2^i}) = 1$. Then $R$ and $T$ are WZ spaces for $f(x) = x^{2^i+1}$ on $\mathbb{F}_{2^n}$, and the pair $\{R, T\}$ intersects trivially.*

**Remark 3.5** *The theoretical constructions of WZ spaces for Gold APN functions and of trivially intersecting pairs of such spaces presented above cover all examples existing in odd dimensions $n \leq 9$.*

# 4 Applications

## 4.1 Classifying EA classes of functions

Functions $f$ and $g$ mapping $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ are *extended affine equivalent (EA equivalent)* if there exist affine permutations $A_1, A_2$ of $\mathbb{F}_{2^n}$ and an affine function $A_3$ such that $A_1(f(A_2(x))) + A_3(x) = g(x)$ for all $x \in \mathbb{F}_{2^n}$. It is known that EA equivalent functions are also CCZ equivalent, but partitioning CCZ classes into EA classes is in general a hard problem. This problem was addressed by Canteaut and Perrin [3] by studying the structure of Walsh zeros of functions. WZ spaces play an important role in their investigations.

To bring up a more specific example, in [3, Lemma 12] it is stated that the CCZ class of $f(x) = x^3$ on $\mathbb{F}_{2^5}$ contains three EA classes, and this is based on the classification of 64 WZ spaces that according to [3] were found experimentally. Here we can give a computer-free description of these spaces: 32 of them are obtained from Proposition 2.9 with $m = n = 5$, and the remaining 32 of them are obtained from Proposition 2.8 with $S = \mu\mathbb{F}_2$ where $\mu \in \mathbb{F}_{2^5}$.

### 4.2 Construction of new APN permutations

If we know two trivially intersecting WZ spaces for an APN function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, then Proposition 1.2 allows us to construct an APN permutation $f'$ of $\mathbb{F}_{2^n}$. Then $f'$ is CCZ equivalent to $f$, but in general it need not be EA equivalent to it.

Just for illustration we present a simple numerical example. For $n = 9$, the algebraic degree of $f(x) = x^3$ is 2, and the algebraic degree of its compositional inverse $g(x) = x^{1/3}$, which is also an APN permutation, is 5. By applying Proposition 1.2 along with constructions of trivially intersecting WZ spaces provided in Section 3 above, we found APN permutations of $\mathbb{F}_{2^9}$ of algebraic degrees 2, 4 and 5. Since the algebraic degree is preserved by EA equivalence, the APN permutations of degree 4 are not EA equivalent to $f$ or $g$.

The constructions in Section 3 work in arbitrary odd dimensions and for all Gold APN functions. It will be interesting to investigate how many EA inequivalent APN permutations they provide.

## Acknowledgement

The authors would like to thank Léo Perrin for releasing an updated version of the sboxU software package [7] that is more widely compatible with various computer operating systems.

## References

[1] X. Bonnetain, L. Perrin, S. Tian, Anomalies and vector space search: tools for S-box analysis. In: S. Galbraith, S. Moriai (eds) Advances in Cryptology – ASIACRYPT 2019. Lecture Notes in Computer Science, vol. 11921, pp. 196–223. Springer, Cham, 2019.

[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] A. Canteaut, L. Perrin, On CCZ-equivalence, extended-affine equivalence, and function twisting. Finite Fields Appl. 56 (2019), 209–246.

[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] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Inform. Theory 14 (1968), 154–156.

[6] J. Lahtonen, G. McGuire, H.N. Ward, Gold and Kasami-Welch functions, quadratic forms, and bent functions. Adv. Math. Commun. 1 (2007), no. 2, 243–250.

[7] L. Perrin, SboxU (software library). https://github.com/lpp-crypto/sboxU (accessed 19 April 2021)