Constructions and applications of Walsh zero spaces

Petr Lisoněk
Simon Fraser University
Burnaby, BC, Canada
joint work with Benjamin Chase (SFU)

The 6th International Workshop
on Boolean Functions and their Applications (BFA 2021)
Rosendal, Norway
6 September 2021

Outline

1. APN permutations
2. Walsh zero spaces of Gold APN functions
3. TI pairs of WZ spaces

APN functions

Definition

We say that a function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ 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 $x \in \mathbb{F}_{2^n}$.

More generally such f is called a *differentially 2-uniform function.*

We can use $\mathbb{F}_2^n$ instead of $\mathbb{F}_{2^n}$ in the definition, or other groups can be used as well.

APN functions

Differentially uniform functions are important in symmetric cryptography (block ciphers, message authentication codes, hash functions) where they protect against the differential cryptanalysis attack.

In block ciphers, APN functions find applications in the construction of *S-boxes* (substitution boxes) which are the only non-linear components of the cipher.

In the design of block ciphers it is beneficial if the S-boxes are *invertible,* that is, if they are *permutations* of $\mathbb{F}_{2^n}$.

APN functions: examples

$f(x) = x^3$ is APN for all n (but it is a permutation of $\mathbb{F}_{2^n}$ only when n is odd)

$f(x) = 1/x$ (with $f(0) = 0$) is APN iff n is odd (it is a permutation of $\mathbb{F}_{2^n}$ for all n). This function is used in the S-box of the *Advanced Encryption Standard (AES)* with $n = 8$; it is differentially 4-uniform when n is even.

Infinite families of APN *monomial* functions have been classified, and also several infinite families of *multinomial* APN functions are known.

The question about existence of APN permutations of $\mathbb{F}_{2^n}$ for even $n > 6$ is the Big APN Problem.

Walsh zero space

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

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*.

Walsh zero space

WZ spaces occur implicitly in the famous construction of APN permutation of $\mathbb{F}_{2^6}$ by Dillon et al. (Fq9, 2009, next slide).

Recently the importance of WZ spaces has been recognized more explicitly in several papers. For example, Canteaut and Perrin (2019) prove that the number of EA-classes inside the CCZ-class of f is upper bounded by the number of WZ spaces of f.

Examples of WZ spaces have been obtained numerically. As far as we know, we are providing the first *theoretical (computer-free)* constructions of non-trivial WZ spaces.

Functions CCZ-equivalent to a permutation

Definition

We say that two WZ spaces S, T of the same function *intersect trivially* if $S \cap T = \{(0,0)\}$. Then we say that $\{S, T\}$ is a *TI-pair* (trivially intersecting pair).

Proposition

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. 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.

This was used to construct the APN permutation of $\mathbb{F}_{2^6}$ by Dillon et al. in 2009, using the *Kim function* for f.

WZ spaces of Gold functions

Gold functions $x \mapsto x^{2^i+1}$ where $\gcd(i, n) = 1$ are a well studied class of APN functions on $\mathbb{F}_{2^n}$. In this talk we exclusively deal with Gold functions in odd dimensions n.

Being permutations of $\mathbb{F}_{2^n}$, they possess the trivial WZ spaces $Z_{a0} = \{(a, 0) : a \in \mathbb{F}_{2^n}\}$ and $Z_{0a} = \{(0, a) : a \in \mathbb{F}_{2^n}\}$.

WZ spaces of Gold functions

Theorem (Gold)

Suppose n is odd and $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ with $f(x) = x^{2^i+1}$ such that $\gcd(i, n) = 1$. Then (a, b) is a Walsh zero of f if and only if $\mathrm{Tr}(ab^{-\frac{1}{2^i+1}}) = 0$ or $a \neq 0,\ b = 0$.

This was implicitly proved by Gold in 1968. A full proof given by Lahtonen, McGuire, and Ward (2007) covers the case $b = 1$. A simple substitution in the summation range covers the case $b \neq 1$.

By using the common convention $0^{-1} = 0$ we can skip the second part of the test.

WZ spaces of Gold functions

Proposition

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

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

is a WZ space of f.

Proof sketch:
Show additive closure (typically follows from linear expressions in the construction).
Show the dimension is n (e.g., count elements).
Verify that each element is Walsh zero (use the trace test from previous slide).

WZ spaces of Gold functions

Definition

Let n be odd, $\gcd(i, n) = 1$ and 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 $\mathbb{F}_{2^n}$.

Example

(i) For each odd n the following subspaces of $\mathbb{F}_{2^n}$ are i-compatible for all admissible i: $\{0\}$, $\mathbb{F}_2$ and $\mathbb{F}_{2^n}$.
(ii) If S is i-compatible subspace of $\mathbb{F}_{2^n}$, then μS is also i-compatible for each $\mu \in \mathbb{F}_{2^n}$.

WZ spaces of Gold functions

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

Each additive subspace of $\mathbb{F}_{2^3}$ is i-compatible when $\gcd(i, n) = 1$.

This is because $x^{-\frac{1}{2^i+1}} = x^{2^i}$ on $\mathbb{F}_{2^3}$ when $\gcd(i, n) = 1$, which is a linear function.

WZ spaces of Gold functions

Problem

For odd n, do there exist i-compatible subspaces of $\mathbb{F}_{2^n}$ other than those described above?

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 $g(x) = x^{2^{n-i}+1}$.

WZ spaces of Gold functions

Proposition

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

The compatibility condition assures that the dimension is n (largest possible).

WZ spaces of Gold functions

Proof.

Let $(0,0) \neq (x,s) \in X \times S$. Then $\mathrm{Tr}(xs^{-\frac{1}{2^i+1}}) = 0$ by construction, hence (x,s) is a Walsh zero of f. Since both X and S are linear spaces, $X \times S$ is also a linear space. Finally, since $s \longmapsto s^{-\frac{1}{2^i+1}}$ is a bijection on $\mathbb{F}_{2^n}$, we get $\dim S^{-\frac{1}{2^i+1}} = \dim S$, and

$$\dim(X \times S) = \dim X + \dim S = (n - \dim S) + \dim S = n.$$

□

TI-pairs of WZ spaces of Gold functions

Recall from earlier that the Dillon-type construction of a permutation CCZ-equivalent to a function f requires two TI-pairs of WZ spaces of f. This motivates the work in this section.

Throughout this section we deal with Gold functions $f(x) = x^{2^i+1}$ and we always assume that $\gcd(i, n) = 1$.

TI-pairs of WZ spaces of Gold functions

Proposition

Let $n = 3k$ where k is odd. Then

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

is a WZ space of f assuming ξ is a fixed primitive element of $\mathbb{F}_{2^3}$ and $\mu \in \mathbb{F}_{2^n}^*$ is fixed. Moreover the pair $\{Z_{0a}, S\}$ intersects trivially.

TI property follows easily as it forces $x = 0$ in the construction.

TI-pairs of WZ spaces of Gold functions

Proof that S is WZ space of f:

The additive closure of S follows from the fact that

$$g(x) = \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i}\mu x))$$

is an $\mathbb{F}_2$-linear function. Suppose $(x, g(x)) \in S\setminus\{(0,0)\}$. Note that $\mu^{2^i+1} g(x) \in \mathbb{F}_{2^3}$. For each $z \in \mathbb{F}_{2^3}^*$ we have $z^{-\frac{1}{2^i+1}} = z^{2^i}$. Then

$$\begin{aligned} \mathrm{Tr}(xg(x)^{-\frac{1}{2^i+1}}) &= \mathrm{Tr}(x\mu(\mu^{2^i+1}g(x))^{-\frac{1}{2^i+1}}) \\ &= \mathrm{Tr}(x\mu\xi^{2^i}\mathrm{Tr}(\mu x)) + \mathrm{Tr}(x\mu \mathrm{Tr}(\xi^{2^i}\mu x)) \\ &= 0 \end{aligned}$$

because $\mathrm{Tr}(x\mu\xi^{2^i}\mathrm{Tr}(\mu x)) = \mathrm{Tr}(x\mu\xi^{2^i})\mathrm{Tr}(\mu x) = \mathrm{Tr}(x\mu\mathrm{Tr}(\xi^{2^i}\mu x))$. By considering the first components of the elements of S it is clear that $\dim S = n$.

TI-pairs of WZ spaces of Gold functions

Proposition

Let n be odd. Then

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

is a WZ space described above and the pair $\{Z_{a0}, S\}$ intersects trivially.

Proof.

Suppose $(\mu\alpha, \mu^{2^i+1}\beta) \in Z_{a0} \cap S$. Then $\mu^{2^i+1}\beta = 0$ and since $\mu \neq 0$, we have $\beta = 0$. So $\alpha = \beta + \beta^{\frac{1}{2^i}} = 0$ and the only element in the intersection is $(0, 0)$. □

TI-pairs of WZ spaces of Gold functions

Proposition

Let $n = 3k$ where k is odd. Let

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

and

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

be WZ spaces described above. Suppose also that

$$\mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = 0.$$

Then the pair $\{S, T\}$ intersects trivially.

TI-pairs of WZ spaces of Gold functions

Proof.

Suppose towards a contradiction that $(0,0) \neq (\nu\alpha, \nu^{2^i+1}\beta) \in S \cap T$. It follows that

$$(\mu\nu)^{2^i+1}\beta = \xi \mathrm{Tr}(\mu\nu(\beta + \beta^{\frac{1}{2^i}})) + \mathrm{Tr}(\xi^{2^i}\mu\nu(\beta + \beta^{\frac{1}{2^i}})). \qquad (1)$$

So $(\mu\nu)^{2^i+1}\beta \in \{1, \xi, \xi+1\}$. For each choice of $c \in \{1, \xi, \xi+1\}$, substituting $\beta = c(\mu\nu)^{-2^i-1}$ into (1) and simplifying contradicts the condition $\mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = 0$. □

TI-pairs of WZ spaces of Gold functions

Proposition

Let $n = 3k$ where k is odd. Let

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

and
$T = X \times S_\mu$ where $S_\mu = \mathrm{span}_{\mathbb{F}_2}\{\mu, \xi\mu\}$ for some fixed $\mu \in \mathbb{F}_{2^n}^*$ be WZ spaces described above. Suppose also that

$$\mathrm{Tr}((\xi + \xi^{2^i})\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) = 1.$$

Then the pair $\{R, T\}$ intersects trivially.

The proof is similar to the previous one.

TI-pairs of WZ spaces of Gold functions

We note that conditions

$$\mathrm{Tr}((\xi+\xi^{2^i})(\mu\nu)^{-2^i})=0$$

and

$$\mathrm{Tr}((\xi+\xi^{2^i})\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i})=1$$

are each satisfied with probability close to $1/2$ assuming that $\xi\in\mathbb{F}_{2^3}\setminus\{0,1\}$ and $\mu,\nu\in\mathbb{F}_{2^n}^*$ are sampled uniformly at random from their domains.

Application

By applying the Dillon-type construction introduced earlier with the TI pairs of WZ spaces that we constructed, we have found *many APN permutations* which are not EA-equivalent to the Gold functions and their inverses.

The EA-inequivalence can be proved by computing some simple invariants (e.g., algebraic degree) which are preserved in an EA-class.

We have verified numerically that our theoretical characterizations of WZ spaces and their trivially intersecting pairs are exhaustive in odd dimensions $n \leq 9$.

References

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

Jyrki Lahtonen, Gary McGuire, and Harold N. Ward. Gold and Kasami-Welch functions, quadratic forms, and bent functions. Advances in Mathematics of Communications, 1(2):243, 2007.