On the Cardinal of the Support of Walsh for Functions of few Variables

Maxence Jauberty

March 5, 2025

Boolean functions play a crucial role in cryptography and error-correcting codes due to their diverse applications and rich mathematical properties. One such property, the Walsh transform, is a Fourier-Hadamar transform that provides valuable insights into the spectral behavior of Boolean functions. The Walsh support of a Boolean functions, defined as the set of points where the Walsh transform is nonzero, offers further structural information. Despite its signifiance, the Walsh support remains relatively underexplored.

1 Definitions

Definition 1.1. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function and $a \in \mathbb{F}_2^n$, the Walsh transform in a is defined as :

$$\mathsf{W}_f(a) := \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x},$$

and the Walsh support is:

$$\mathsf{W}_{\text{supp}}(f) := \{a \in \mathbb{F}_2^n,\ \mathsf{W}_f(a) \neq 0\}.$$

Proposition 1.2 (Titsworth)**.** Let $f \in \mathcal{BF}_n$. We have for any $a \neq 0$

$$\sum_{b \in \mathbb{F}_2^n} \mathsf{W}(b)\mathsf{W}(a+b) = 0. \tag{1}$$

Proposition 1.3. For any $n \in \mathbb{N}$ and any $f \in \mathcal{BF}_n$,

$$|\mathsf{W}_{\text{supp}}(f)| \neq 3.$$

Proof. Assume that $\mathsf{W}_{\text{supp}}(f) = \{a, b\}$ and denote $c = a + b$. $c \neq 0$, then we can apply Titsworth formula

$$\sum_{u \in \mathbb{F}_2^n} \mathsf{W}_f(u)\mathsf{W}_f(c+u) = 0.$$

$\mathsf{W}_f(u)\mathsf{W}_f(c+u) \neq 0$ if and only $\mathsf{W}_f(u) \neq 0$ and $\mathsf{W}_f(c+u) \neq 0$. This only happens if both quantities are in the support, i.e. $u = a$ or $u = b$, then

$$\sum_{u \in \mathbb{F}_2^n} \mathsf{W}_f(u)\mathsf{W}_f(c+u) = 2\mathsf{W}_f(a)\mathsf{W}_f(b).$$

Hence, we have $2\mathsf{W}_f(a)\mathsf{W}_f(b) = 0$. This leads to $\mathsf{W}_f(a) = 0$ or $\mathsf{W}_f(b) = 0$ which contradicts the definition of a and b. $\square$

Proposition 1.4. For any $n \in \mathbb{N}$ and any $f \in \mathcal{BF}_n$,

$$|\mathsf{W}_{\text{supp}}(f)| \neq 5.$$

Proof. Assume that $\mathsf{W}_{\text{supp}}(f) = \{a_1, a_2, a_3, a_4, a_5\}$. Set $v = a_1 + a_2$. We can then apply Titsworth formula, we have then

$$\sum_{u \in \mathbb{F}_2^n} \mathsf{W}_f(u)\mathsf{W}_f(v+u) = 0.$$

There are then two cases. Either $\sum_{u \in \mathbb{F}_2^n} \mathsf{W}_f(u)\mathsf{W}_f(v+u) = 2\mathsf{W}_f(a_1)\mathsf{W}_f(a_2) + 2\mathsf{W}_f(a_3)\mathsf{W}_f(a_4)$ (w.l.o.g.) or $\sum_{u \in \mathbb{F}_2^n} \mathsf{W}_f(u)\mathsf{W}_f(v+u) = 2\mathsf{W}_f(a_1)\mathsf{W}_f(a_2)$. In the latter case, we would have $\mathsf{W}_f(a_1)\mathsf{W}_f(a_2) = 0$, which contradicts the definition of a_1, a_2. If $\sum_{u \in \mathbb{F}_2^n} \mathsf{W}_f(u)\mathsf{W}_f(v+u) = 2\mathsf{W}_f(a_1)\mathsf{W}_f(a_2) + 2\mathsf{W}_f(a_3)\mathsf{W}_f(a_4)$, then it means that

$$a_1 + a_2 + a_3 + a_4 = 0.$$

Indeed, there exists u in the spectrum such that $u + v$ is also in the spectrum, we only chose to name a_3, a_4 such that $u + v = a_4$ and $a_3 = u$. Therefore $a_4 = a_1 + a_2 + a_3$.

Then, we do the same procedure with $w = a_1 + a_5$. We deduce that for some $i, j \in \{2, 3, 4\}$, we have

$$a_1 + a_i + a_j + a_5 = 0.$$

However, by the first equation, for any i, j there is some $k \in \{2, 3, 4\}$ such that

$$a_1 + a_k = a_i + a_j.$$

Finally, we get $a_1 + a_1 + a_k + a_5 = 0$, hence $a_5 = a_k$. That is a contradiction. □

Definition 1.5. Denote $\mathcal{WS}_n$ the set of Walsh supports of $n-$dimensional Boolean functions, i.e.

$$\mathcal{WS}_n := \{\text{Supp}(\mathsf{W}_f),\ f \in \mathcal{BF}_n\}.$$

It has been shown that $\mathcal{WS}_n$ has some structure.

Proposition 1.6. Let $n, m \in \mathbb{N}$, we have

1. $\mathcal{WS}_n$ is globally invariant under affine transformations,
2. $\mathcal{WS}_n \times \mathcal{WS}_m \subset \mathcal{WS}_{n+m}$.

Definition 1.7. Let $\mathcal{S}_n$ the set defined as

$$\mathcal{S}_n = \{s \in \mathbb{N},\ \exists f \in \mathcal{BF}_n, |\text{Supp}(\mathsf{W}_f)| = s\}.$$

Proposition 1.8. Let $n \in \mathbb{N}$. We have $\mathcal{S}_n \subset \mathcal{S}_{n+1}$.

Proof. According to the assertion 2, $\mathcal{WS}_n \times \mathcal{WS}_m \subset \mathcal{WS}_{n+m}$. In particular, we have

$$\mathcal{WS}_n \times \mathcal{WS}_1 \subset \mathcal{WS}_{n+1}.$$

Consider then f such that $|\text{Supp}(\mathsf{W}_f)| = s$ and let g be an affine function of $\mathcal{BF}_1$. We have $\text{Supp}(\mathsf{W}_g) = \{a\}$. Then, $\text{Supp}(\mathsf{W}_f) \times \text{Supp}(\mathsf{W}_g) \in \mathcal{WS}_{n+1}$ and $|\text{Supp}(\mathsf{W}_f) \times \text{Supp}(\mathsf{W}_g)| = s$. □