On the Cardinality of the Walsh Support

Maxence Jauberty, Pierrick Méaux

September 1, 2025

University of Luxembourg, Luxembourg

Our Study in Short

What are the possible cardinalities of the Walsh supports?

Basic Definitions

Definition

$$\textbf{Walsh Transform:} \quad W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus u \cdot x}$$

$$\textbf{Walsh support:} \ \mathrm{Wsupp}_f = \{u \mid W_f(u) \neq 0\}$$

Definition

We consider the following set: $\mathcal{C}_n = \{|\mathrm{Wsupp}_f| \mid f \in \mathcal{B}_n\}$.

Basic Definitions

Definition

$$\textbf{Walsh Transform:} \quad W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus u \cdot x}$$

$$\textbf{Walsh support:} \ \mathrm{Wsupp}_f = \{u \mid W_f(u) \neq 0\}$$

Definition

We consider the following set: $\mathcal{C}_n = \{|\mathrm{Wsupp}_f| \mid f \in \mathcal{B}_n\}$.

Main Objective

Determine the sets $\mathcal{C}_n$ for $n \in \mathbb{N}$.

Motivations and Prior Works

Why do we study the Walsh support (cardinality)?

- Cryptographic criteria: balancedness, resilience.
- Plateaued functions [HPW18] and "$2^n - p \in^? \mathcal{C}_n$".
- Dahu functions [DMR21] (optimal AI and highest resilience).

Motivations and Prior Works

Why do we study the Walsh support (cardinality)?

- Cryptographic criteria: balancedness, resilience.
- Plateaued functions [HPW18] and "$2^n - p \in^? \mathcal{C}_n$".
- Dahu functions [DMR21] (optimal AI and highest resilience).

What do we know? Not so much:

- No Walsh support of cardinality $s \in \{2, 3, 5, 6, 7\}$ [PQ00].
- If $s \in \{1, 4, 8\}$, Wsupp_f is an affine space [PQ00].
- Properties and classification ($n = 5$) [CM04].
- $s = 2^m$ [CM04,HPW18], $s = 2^m - 1$ [CM04,LW24].

Main Contributions

Contribution 1

Characterization of the Walsh supports of cardinalities 10 and 13.

Contribution 2

No Walsh support of cardinality $s \in \{9, 11, 12, 14, 15, 17, 19\}$.

Contribution 3

For $n \geq 7$, $\mathcal{C}_n = [1, 2^n] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19\}$.

Table of Contents

Table of Contents

Siegenthaler's Construction

Definition

Let $f, g \in \mathcal{B}_n$, we define $h = \text{Sieg}[f, g] \in \mathcal{B}_{n+1}$ by

$$\text{for } x \in \mathbb{F}_2^n,\ h(x,0) = f(x) \quad \text{and} \quad h(x,1) = g(x)$$

Concatenation of truth tables:

$$\overbrace{\underbrace{01010101}_{f\in\mathcal{B}_3}\underbrace{11110000}_{g\in\mathcal{B}_3}}^{h\in\mathcal{B}_4}$$

Any $(n+1)$-variable function can be seen as a Siegenthaler's construction.

From Wsupp_f and Wsupp_g to Wsupp_h

Property

$$W_h(u,0) = W_f(u) + W_g(u) \quad \textit{and} \quad W_h(u,1) = W_f(u) - W_g(u)$$

How to Compute Wsupp_h

Let $u \in \mathsf{Wsupp}_f \cup \mathsf{Wsupp}_g$

1- If $|W_f(u)| \neq |W_g(u)|$: $(u,0),(u,1) \in \mathsf{Wsupp}_h$.

2- If $W_f(u) = (-1)^v W_g(u)$: $(u,v) \in \mathsf{Wsupp}_h$ and $(u,1+v) \notin \mathsf{Wsupp}_h$.

Seems promising to compute the cardinality of Wsupp_h!

From Wsupp_f and Wsupp_g to Wsupp_h

Property

$$W_h(u,0) = W_f(u) + W_g(u) \quad \textit{and} \quad W_h(u,1) = W_f(u) - W_g(u)$$

How to Compute Wsupp_h

Let $u \in \mathrm{Wsupp}_f \cup \mathrm{Wsupp}_g$

1- If $|W_f(u)| \neq |W_g(u)|$: $(u,0),(u,1) \in \mathrm{Wsupp}_h$.

2- If $W_f(u) = (-1)^v W_g(u)$: $(u,v) \in \mathrm{Wsupp}_h$ and $(u,1+v) \notin \mathrm{Wsupp}_h$.

Seems promising to compute the cardinality of Wsupp_h!

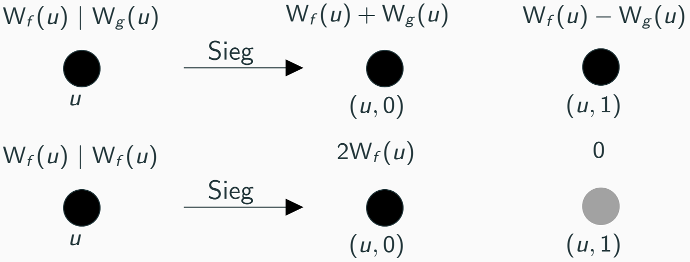
Definition

$K = \mathrm{Wsupp}_f \cap \mathrm{Wsupp}_g$ and $\Xi = \{u \in K |\ W_f(u) = \pm W_g(u)\}$

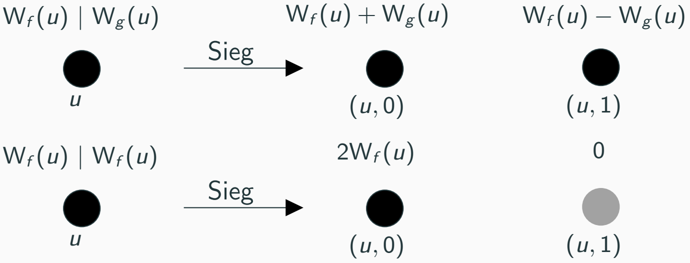
Theorem

$|\mathrm{Wsupp}_h| = 2(|\mathrm{Wsupp}_f| + \left|\mathrm{Wsupp}_g\right| - |K|) - |\Xi|$.

Geometrical Visualization



Geometrical Visualization

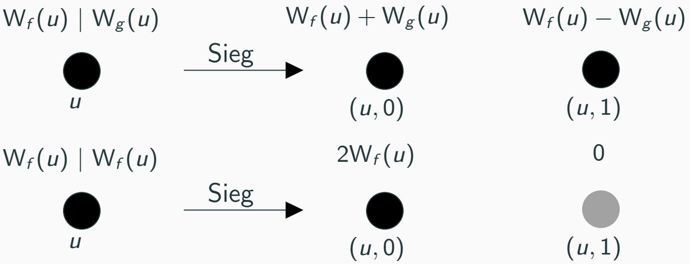


Construction (Walsh Support of Cardinality 4)

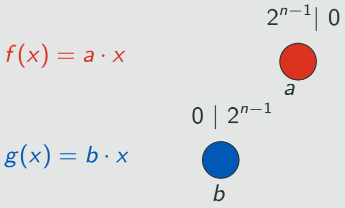
$f(x) = a \cdot x$

$g(x) = b \cdot x$

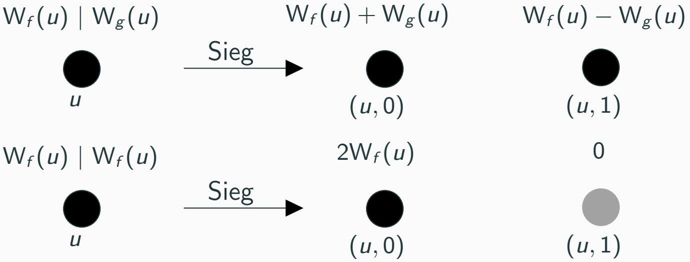
Geometrical Visualization



Construction (Walsh Support of Cardinality 4)



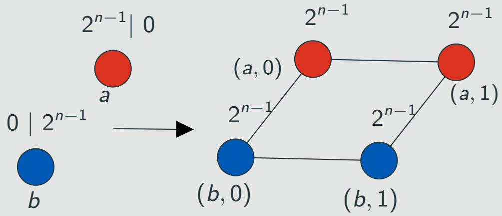
Geometrical Visualization



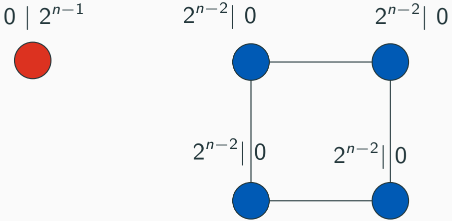
Construction (Walsh Support of Cardinality 4)

$f(x) = a \cdot x$

$g(x) = b \cdot x$



Construction of Wsupp_h of Cardinality 10



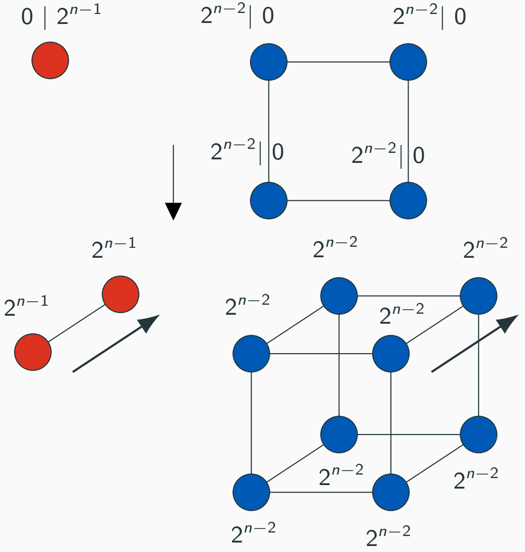
$f \in \mathcal{B}_{n-1,1}$

$g \in \mathcal{B}_{n-1,4}$

$|\Xi| = 0$

$|K| = 0$

Construction of Wsupp_h of Cardinality 10



$f \in \mathcal{B}_{n-1,1}$

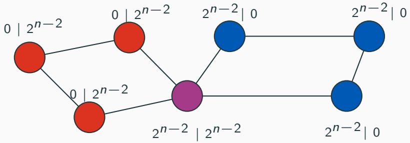
$g \in \mathcal{B}_{n-1,4}$

$|\Xi| = 0$

$|K| = 0$

And we show (see paper) that all Walsh supports of cardinality 10 are equivalent to this one.

Construction of Wsupp_h of Cardinality 13



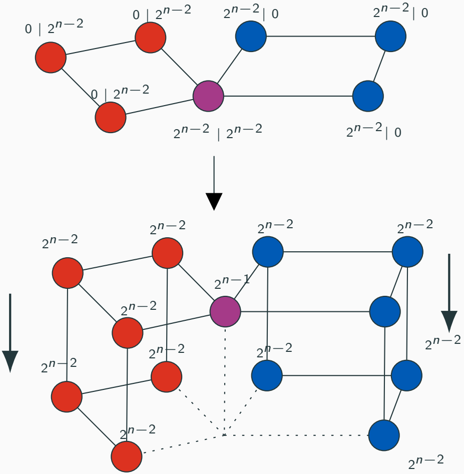
$f \in \mathcal{B}_{n-1,4}$

$g \in \mathcal{B}_{n-1,4}$

$|\Xi| = 1$

$|K| = 1$

Construction of Wsupp_h of Cardinality 13



$f \in \mathcal{B}_{n-1,4}$

$g \in \mathcal{B}_{n-1,4}$

$|\Xi| = 1$

$|K| = 1$

And we show (see paper) that all Walsh supports of cardinality 13 are equivalent to this one.

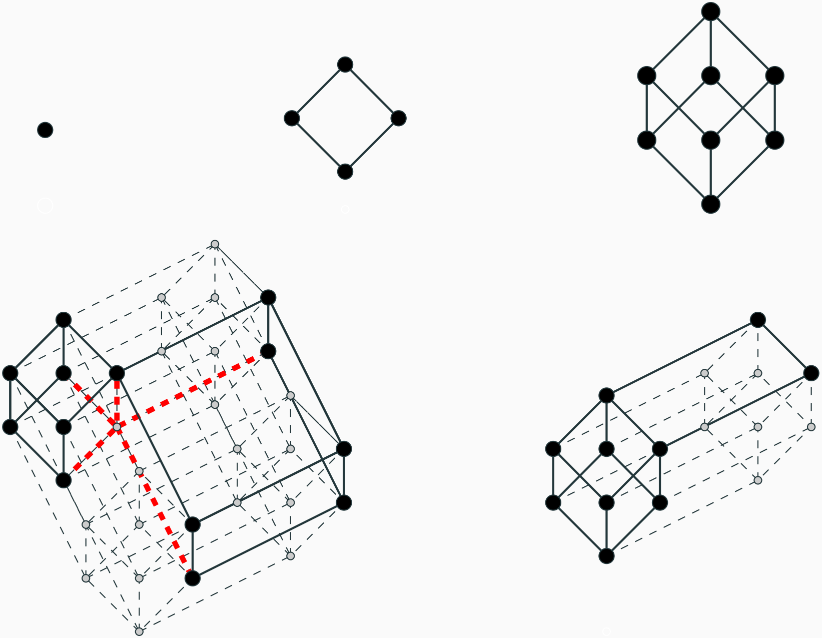


Table of Contents

(s, t, k, ξ)-construction

Recall: $K = \mathrm{Wsupp}_f \cap \mathrm{Wsupp}_g$ and $\Xi = \{u \in K \mid W_f(u) = \pm W_g(u)\}$.

Definition

h such that $|\mathrm{Wsupp}_h| = r$ is a (s, t, k, ξ)-construction if

$$h = \mathrm{Sieg}[f, g]$$

$$|\mathrm{Wsupp}_f| = s, \quad |\mathrm{Wsupp}_g| = t, \quad |K| = k, \quad |\Xi| = \xi$$

(From the previous section: $r = 2(s + t - k) - \xi$)

(s, t, k, ξ)-construction

Recall: $K = \mathrm{Wsupp}_f \cap \mathrm{Wsupp}_g$ and $\Xi = \{u \in K |\ W_f(u) = \pm W_g(u)\}$.

Definition

h such that $|\mathrm{Wsupp}_h| = r$ is a (s, t, k, ξ)-construction if

$$h = \mathrm{Sieg}\,[f, g]$$

$$|\mathrm{Wsupp}_f| = s, \quad |\mathrm{Wsupp}_g| = t, \quad |K| = k, \quad |\Xi| = \xi$$

(From the previous section: $r = 2(s + t - k) - \xi$)

Remark: Impossible (s, t, k, ξ)

Many (s, t, k, ξ)-construction are **not** possible (*e.g.* $(1, 1, 1, 0)$ would give $r = 2$).

How do we keep track of the possible constructions?

Construction Tables

Definition (Construction Table)

$\mathrm{CT}^{s,t}$ is the table such that:

$$\mathrm{CT}^{s,t}_{\xi,k} = 2(s+t-k) - \xi,$$

If the cell (ξ, k) is colored then the (s, t, k, ξ) is not a possible construction.

Construction Table $\mathrm{CT}^{1,1}$

ξ \ k	0	1
0	4	2
1		1

Sieving Method

Proposition

There exists Wsupp_h of cardinality r if and only if there exists h a (s, t, k, ξ)-construction such that $r = 2(s + t - k) - \xi$ with $s, t < r$.

9 is only in the impossible constructions of $\mathrm{CT}^{1,1}, \mathrm{CT}^{1,4}, \mathrm{CT}^{1,8}, \mathrm{CT}^{4,4}, \mathrm{CT}^{4,8}, \mathrm{CT}^{8,8}$

$\implies |\mathrm{Wsupp}_h| = 9$ is impossible.

How to Color a Construction Table

Construction Table $CT^{4,4}$

ξ \ k	0	1	2	3	4
0	16	14	12	10	8
1		13	11	9	7
2			10	8	6
3				7	5
4					4

How to Color a Construction Table

Construction Table $\mathrm{CT}^{4,4}$

$\xi \backslash k$	0	1	2	3	4
0	16	14	12	10	8
1		13	11	9	7
2			10	8	6
3				7	5
4					4

Recall: Wsupp_f and Wsupp_g are affines planes.

How to Color a Construction Table

Construction Table $\mathrm{CT}^{4,4}$

ξ \ k	0	1	2	3	4
0	16	14	12	10	8
1		13	11	9	7
2			10	8	6
3				7	5
4					4

Conclusion: $9, 11, 12, 14$ cannot be built with $s = t = 4$.

The Impossible Cardinalities

$2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19$ only appear in the colored cells of $\mathrm{CT}^{s,t}$ for $s, t \leq 18$!

Impossible Cardinalities (Contribution 2)

There is no Walsh support of cardinality $s \in \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19\}$.

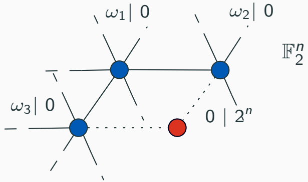
Table of Contents

Our Goal

Objective

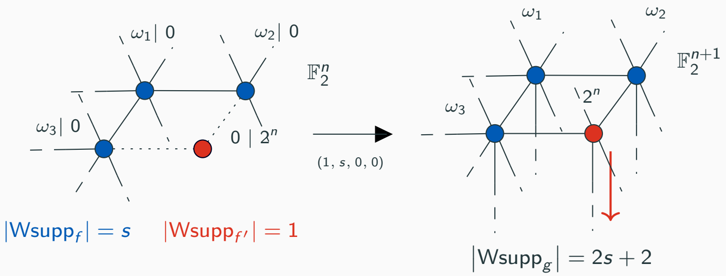
From any Walsh support of cardinality s create a Walsh support of cardinality $ms + \ell$

Example with Construction $s \to 4s + 3$

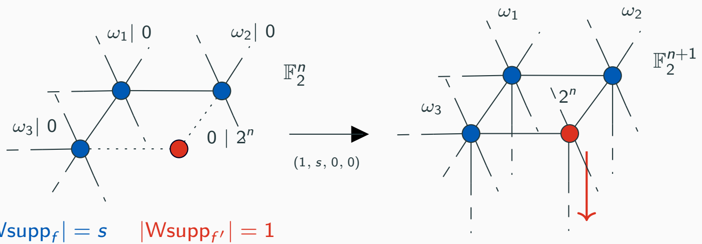


$|\mathrm{Wsupp}_f| = s$ $|\mathrm{Wsupp}_{f'}| = 1$

Example with Construction $s \to 4s + 3$

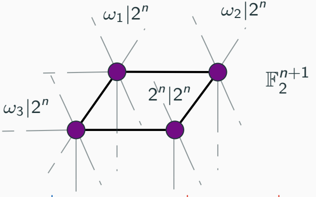


Example with Construction $s \to 4s + 3$



$|\mathrm{Wsupp}_f| = s$ $|\mathrm{Wsupp}_{f'}| = 1$

$|\mathrm{Wsupp}_g| = 2s + 2$

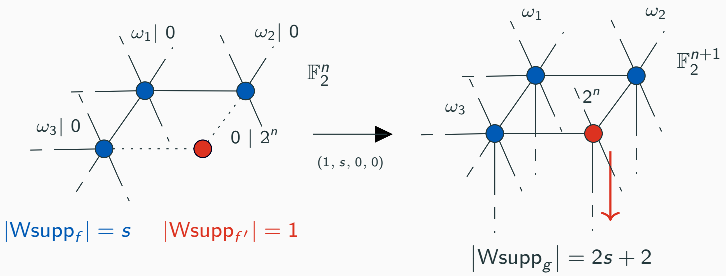


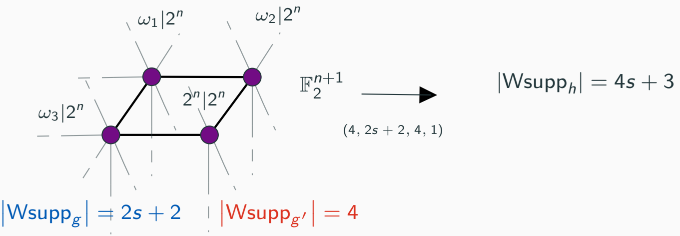
$|\mathrm{Wsupp}_g| = 2s + 2$ $|\mathrm{Wsupp}_{g'}| = 4$

$k = 4$

$\xi = 1$

Example with Construction $s \to 4s + 3$





Generic Constructions

Construction ($s \to 4s$)

If $s \in \mathcal{C}_n$, then $4s \in \mathcal{C}_{n+2}$

Construction ($s \to 4s+3$)

If $s \in \mathcal{C}_n$, then $4s+3 \in \mathcal{C}_{n+2}$

Construction ($s \to 4s+2$)

If $s \in \mathcal{C}_n$, then $4s+2 \in \mathcal{C}_{n+2}$

Construction ($s \to 4s+5$)

If $s \in \mathcal{C}_n$, then $4s+5 \in \mathcal{C}_{n+2}$

Lemma: Induction

We denote by P_n: "$\mathcal{C}_n = [1, 2^n] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19\}$", then

$$P_n \text{ and } P_{n+1} \text{ are true } \implies P_{n+2} \text{ is true.}$$

$\mathcal{C}_n$ for $n \geq 7$

Property

For $n = 7$ and $n = 8$, we have
$\mathcal{C}_n = [1, 2^n] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19\}$

Cardinalities of the Walsh Support (Contribution 3)

Let $n \geq 7$, then

$$\mathcal{C}_n = [1, 2^n] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19\}$$

($\mathcal{C}_n$ for $n \leq 6$ can be computed by exhaustive search through EA equivalent classes thanks to Langevin's online classification)

Table of Contents

Summary and Consequence

- (s, t, k, ξ)-construction to aim precise Walsh support cardinalities
  e.g. plateaued functions or $|\text{Wsupp}_f| = 2^n - 1$

- *e.g.* 5 EA-ineq $f \in \mathcal{B}_7$ s.t. $|\text{Wsupp}_f| = 2^7 - 1$ (1 in [LW24])

- Preneel and Logachev's open question ("$\mathcal{C}_n =$?") [PL08].

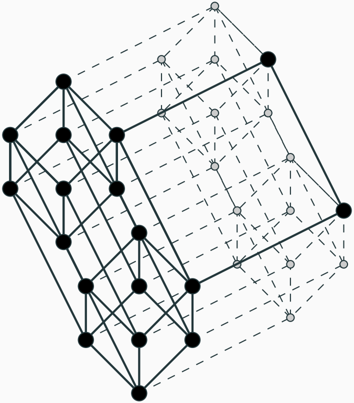
Also from the paper:

Plateaued functions with non-affine Walsh support

Tools to study Walsh supports structure

and more!

Thank you for your attention!



(... and that is the unique Walsh support of cardinality 18)