Project: On the cardinal of the support of Walsh for functions in a few variables.

Supervisors: Gabor Wiese, Pierrick Méaux

Luxembourg university, Luxembourg
gabor.wiese@uni.lu, pierrick.meaux@uni.lu

Project introduction: The goal of this project is to investigate the possible (or impossible) cardinal of a particular set called the support of Walsh.

First, we introduce the key notions of Boolean function, Walsh transform and Walsh support.

Definition 1 (Boolean Function). *A Boolean function f in n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$.*

Definition 2 (Walsh transform). *Let $f \in \mathcal{B}_n$ be a Boolean function, its Walsh transform W_f at $a \in \mathbb{F}_2^n$ is defined as:*

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

where $\cdot$ denotes the inner product. The values of the Walsh transform belong to $\mathbb{Z}$.

The Walsh transform, or Walsh Hadamard transform, is the Fourier Hadamard transform of the sign function of f. We refer to [Car21] for more context on Boolean functions and their use in cryptography.

Definition 3 (Walsh support). *Let $f \in \mathcal{B}_n$ be a Boolean function, its Walsh support is the set:*

$$\mathsf{Wsupp}_f := \{a \in \mathbb{F}_2^n \,|\, W_f(a) \neq 0\}.$$

The main interest in this project is to determine the possible and impossible values for the cardinal of Wsupp_f (for $f \in \mathcal{B}_n$) and its structure.

Project description:

First, very few is known on the Walsh support. Regarding its cardinal, there are some proven results, such as the existence of functions with support of size 2^ℓ for $\ell \in [0, n] \setminus \{1\}$ [1]. In most of these proven cases the Walsh support is an affine space. There are also examples with $|\mathsf{Wsupp}_f| = 2^n - 1$. These different cases can be found in [CM04], with more properties on the Walsh support. Regarding the impossible cardinal, values such as 2 and 3 have been proven impossible independently in different papers, and there are claims on some other small values. It has been shown experimentally that in 5 variables $|\mathsf{Wsupp}_f|$ belongs to $\{1, 4, 8, 10, 13, 16, 18, 20, 21, 22, 23, 24, 25, 26, 28, 32\}$.

The goal of this project is to study the cardinal of the support of Walsh for functions in n variables with $n \in \{6, 7, 8\}$. It can be done by following one or more of the following directions:

- Finding experimentally possibles values of the cardinal by modifying Boole and functions with known Walsh support.

[1] for a and b in $\mathbb{N}$ we use the notation $[a, b]$ for the set of integers between a and b both included

- Determining experimentally the possible cardinal for $n = 6$ using a list of representative of each affine equivalent class in 6 variables.
- Proving that more values are not possible for the cardinal.
- Building Boolean functions for each different cardinal.

Interests in cryptology:

- Resilience. The criterion of resilience has been an important notion in cryptography to avoid statistical attacks. Its definition is the following:

  Definition 4 (Balancedness and Resilience). *A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$. The function f is called k-resilient if any of its restrictions obtained by fixing at most k of its coordinates is balanced. We denote by $\mathsf{res}(f)$ the maximum resiliency (also called resiliency order) of f and set $\mathsf{res}(f) = -1$ if f is unbalanced.*

  In cryptography the concept has been introduced by Siegenthaler [Sie84], and appears in other domains using Boolean functions. We have the following relation between resilience and Walsh support:

  Property 1 (Walsh Transform and Resilience, *e.g.* [Car21])**.** *Let $f \in \mathcal{B}_n$, f is k-resilient if and only if $W_f(a) = 0$ for all a of Hamming weight at most k. Additionally, f has resilience order k if there exists an $a \in \mathsf{E}_{k+1,n}$ such that $W_f(a) \neq 0$, where $\mathsf{E}_{k+1,n}$ denotes the set $\{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k+1\}$.*

  We also have that $a \in \mathsf{Wsupp}_f$ is equivalent to $f(x) + a \cdot x$ is not balanced. Accordingly the support of Walsh gives information on the resilience of f and its structure could be used to determine if a function in the affine equivalent class of f has a better resilience. There are various equivalent relations defined on Boolean functions, in our context we refer to the following definition:

  Definition 5 (Equivalences Notions (adapted from [Car21], Definition 5)). *Two n-variable Boolean functions f and $g = a_0 + f \circ L$ where:*

  $$L : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n) \times \mathbf{M} + (a_1, \ldots, a_n), \text{ are called:}$$

  affine equivalent if $a_0 \in \mathbb{F}_2$, L is an affine automorphism of $\mathbb{F}_2^n$, $\mathbf{M}$ being an $n \times n$ nonsingular matrix over $\mathbb{F}_2$ and $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$,
  linear equivalent if $a_0 = 0$, L is a linear automorphism of $\mathbb{F}_2^n$, $\mathbf{M}$ being an $n \times n$ nonsingular matrix over $\mathbb{F}_2$ and $(a_1, \ldots, a_n) = 0_n$,
  permutation equivalent if they are linear equivalent with $\mathbf{M}$ having exactly one 1 by row and by column.

- Nonlinearity. The Walsh spectrum (the set of the 2^n values of the Walsh transform) is also used to determine the minimum distance of a function to the n-variable affine function, usually called nonlinearity or first order nonlinearity. The minimum distance considered in this case is the Hamming distance, the truth table of the affine functions correspond to a linear code (Reed Muller code of order 1), and the minimal distance is derived from the maximum value of the absolute value of the Walsh spectrum.

Bibliography:

We recommend the book of Claude Carlet [Car21] for a general introduction (and way more) on Boolean functions and cryptography. For some results on the Walsh support and its properties, the article [CM04] and its references. Regarding the interest in cryptology: [DMR23].

References

Car21. Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

CM04. Claude Carlet and Sihem Mesnager. On the supports of the walsh transforms of Boolean functions. Cryptology ePrint Archive, Report 2004/256, 2004.

DMR23. Aurélien Dupin, Pierrick Méaux, and Mélissa Rossi. On the algebraic immunity - resiliency trade-off, implications for goldreich's pseudorandom generator. *Des. Codes Cryptogr.*, 91(9):3035–3079, 2023.

Sie84. Thomas Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. IT-30(5):776–780, 1984.