On those Boolean functions having only one Walsh zero

Claude Carlet[1], Pierrick Méaux[2] and Marek Broll[3]

[1] Universities of Paris 8, France and Bergen, Norway
[2] University of Luxembourg, Luxembourg
[3] Independent researcher, Germany
claude.carlet@gmail.com,pierrick.meaux@uni.lu,marekbroll@protonmail.com

Abstract. Boolean functions having only one Walsh zero (or equivalently up to a translation, balanced functions whose sums with non-constant affine Boolean functions are all unbalanced) have been constructed for every $n \geq 10$, by Mesnager and the first author, twenty years ago. This same paper had checked (partly mathematically and partly thanks to computer investigations) that no such function exists for $n \leq 6$ but left open the question of constructing them for $7 \leq n \leq 9$. Since then, functions in 7, 8 and 9 variables having one Walsh zero have been found by Lou and Wang, thanks to ad hoc methods combined with computer searches, but not as elements in infinite classes of functions having this property. In the present paper, we provide such infinite classes for $n \geq 8$. For $n = 7$, we provide one more function (found by a computer investigation thanks to an algorithm) but we leave open the possibility of finding an infinite class valid for $n \geq 7$. We also provide a secondary construction of functions with one Walsh zero in $n + 2$ variables from such functions in n variables, which does not need particular conditions on the latter for being successful (and which provides then a systematic way to obtain functions in $n + 2$ variables from functions in n variables). We investigate mathematical proofs of non-existence of such functions in $n \leq 6$ variables.

Keywords: Boolean function, Walsh support.

1 Introduction

The question of determining the possible algebraic structure of the Walsh supports of Boolean functions is important, from theoretical and practical viewpoints. For example, understanding the structure of the Walsh support is necessary to build functions with optimal algebraic immunity and high resilience, a problem studied in [DMR23] that would address an open question raised both in [AL16] and in [Car21]. Such functions would define the limits for the security of Goldreich's pseudorandom generator [Gol00]. This primitive has far reaching implications in cryptology such as the construction of indistinguishability obfuscation [JLS21], and its security has been the focus of multiple works *e.g.* [AL16,CDM+18,YGJL22,Üna23]. The structure of the Walsh support is also a key parameter to characterize plateaued functions [HPWZ19] and functions with spectra with only a few distinct values [HHP21,WF22]. The structure of the Walsh support has been studied in [CM04]. Since then, the most significant advance has been made by the paper [JM25].

An important subproblem is to study the existence of functions whose Walsh supports are the complements of singletons $\{a\}$ (i.e. having only one Walsh zero), constructing them when they exist, and finding infinite classes if possible. Such functions are equivalently the Boolean functions f such that the 2^n-length binary vector associated to $f(x + a)$ is the only balanced vector in the coset of the Reed-Muller code of order 1 to which it belongs. They were constructed for every $n \geq 10$ in [CM04], where was also checked (partly mathematically and partly thanks to computer investigations) that no such function exists for $n \leq 6$. After this paper, the questions of determining their existence for $7 \leq n \leq 9$ and of constructing them remained open. In [LW24], a function in 7 variables having one Walsh zero has been obtained by observing that such a function can be built from a pair of functions in fewer variables whose Walsh absolute values coincide except at one point, and then deriving an ad hoc method to find such a pair. Then, examples of functions having one Walsh zero in 8 variables and one in 9 variables have been provided. These approaches do not provide infinite classes.

In the present paper, by adapting a method introduced by Dobbertin in [Dob95], we provide such infinite

classes for $n \geq 8$. We are not able to provide an infinite class also valid for $n = 7$, and for such a number of variables, all we can do is to exhibit one more function (found by a computer investigation thanks to an algorithm that we provide). We also design a secondary construction (the first one providing, in a systematic way, $(n+2)$-variable functions having the desired property from n-variable functions having it).
We try to find mathematical proofs of non-existence for $n \leq 6$ and we succeed for $n \leq 5$ (several papers have addressed this question but none did this entirely without computer investigations). For this, we study three approaches: one essentially using the Parseval relation, one essentially based on error correcting codes, and one dealing with the values of the Walsh transform reduced modulo a power of 2. More precisely, for $n = 1$, all functions have a unique Walsh zero. For $n = 2$, the non-existence is easily proved in [DMR23]. It can also be proved by the Parseval approach developed here. For $n = 3$, another approach by the Parseval relation worked in [JM25] and the approach by coding theory developed here allows to show the non-existence. [PQ00] also deals with the cases $n = 2$ and $n = 3$ without computer investigations, but the proofs are not written in a completely checkable way. For $n = 4$, only Parseval's relation (and a related property) allows us to prove that complements of singletons cannot be the Walsh supports of n-variable Boolean functions. For $n = 5$, it is the reduction of the Walsh transform modulo a power of 2 which works. And for $n = 6$, we have no method working without any use of a computer, and we leave then the question open.

2 Preliminaries

Throughout this paper, n denotes a positive integer. For a and b positive integers such that $a \leq b$, we denote by $[a, b]$ the interval $\{a, a+1, \ldots, b-1, b\}$ of integers between a and b (including both a and b). The set of binary vectors of length n is denoted by $\mathbb{F}_2^n$, with zero vector written as 0_n. The coordinates of a binary vector $x \in \mathbb{F}_2^n$ are denoted by $x_1, \ldots, x_n$. The Hamming weight $|\{i \in [1, n] \mid x_i = 1\}|$ of a binary vector $x \in \mathbb{F}_2^n$ is denoted by $\mathsf{w_H}(x)$. When there will be no ambiguity, we shall denote by $+$ instead of $\oplus$ the addition over $\mathbb{F}_2$, for better readability. Similarly, we will write $\sum$ instead of $\bigoplus$ for summations over sets.

2.1 Boolean functions and cryptographic criteria

In this part we provide definitions on Boolean functions and their cryptographic parameters, we refer to *e.g.* [Car21] for more details.

Definition 1 (Boolean Function). *A Boolean function f in n variables (an n-variable Boolean function) 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 (Algebraic Normal Form (ANF)). *We call Algebraic Normal Form of a Boolean function f its n-variable polynomial representation over $\mathbb{F}_2$ (i.e. belonging to $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 \oplus x_1, \ldots, x_n^2 \oplus x_n)$):*

$$f(x) = \bigoplus_{I \subseteq [n]} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{I \subseteq [n]} a_I x^I,$$

where $a_I \in \mathbb{F}_2$. The ANF is unique and we denote it by ANF(f). The algebraic degree of f equals the global degree of its ANF: $\deg(f) = \max_{\{I \mid a_I = 1\}} |I|$ (with the convention that $\deg(0) = 0$).

Definition 3 (Numerical Normal Form (NNF)). *We call Numerical Normal Form (NNF) of a pseudo-Boolean function f (i.e. real-valued function over $\mathbb{F}_2^n$) the representation in the quotient ring $\mathbb{R}[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$ (respectively, $\mathbb{Z}[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$ for integer-valued functions, among*

which we shall consider Boolean functions).

$$f(x) = \sum_{I \subseteq [n]} \lambda_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq [n]} \lambda_I x^I; \quad \lambda_i \in \mathbb{R} \, (\textit{resp, } \lambda_i \in \mathbb{Z}).$$

Definition 4 (Balancedness). *A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if $w_H(f) = |\mathsf{supp}(f)| = 2^{n-1} = |\mathsf{supp}(f+1)|$, where $\mathsf{supp}(f)$ denotes the support of f, the set $\{x \in \mathbb{F}_2^n \mid f(x) = 1\}$.*

Definition 5 (Walsh transform and Walsh support). *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:*

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

where $a \cdot x$ denotes an inner product. The Walsh support is the set $\mathsf{Wsupp}_f = \{a \in \mathbb{F}_2^n \,|\, \mathsf{W}_f(a) \neq 0\}$.

We recall Parseval's identity, for any $f \in \mathcal{B}_n$:

$$\sum_{a \in \mathbb{F}_2^n} \mathsf{W}_f(a)^2 = 2^{2n}. \tag{1}$$

Definition 6 (Bent functions). *Let n be an even integer, $f \in \mathcal{B}_n$ is called a bent function if and only if $\max_{a \in \mathbb{F}_2^n} |\mathsf{W}_f(a)| = 2^{n/2}$ (equivalently, if $\forall a \in \mathbb{F}_2^n, |\mathsf{W}_f(a)| = 2^{n/2}$).*

Bent functions are the Boolean functions at maximal distance from the space of affine functions. Due to their broad applications and importance, they have been the focus of multiple works *e.g.* [Rot76,Dob95] and surveys *e.g.* [Tok15,Mes16,Car21]. Bentness is preserved by the so-called extended affine (EA) equivalence. Two Boolean functions are called EA-equivalent if there exists an affine permutation A and an affine Boolean function ℓ such that $g = f \circ A + \ell$ (and if $\ell = 0$, then we speak of affine equivalence).

2.2 Walsh support properties, and functions with studied Walsh support

Property 1 (Walsh transform of affine functions)**.** *Let $n \in \mathbb{N}$, for ℓ affine we represent it as $\ell(x) = b \cdot x + \varepsilon$ where $b \in \mathbb{F}_2^n$ and $\varepsilon \in \mathbb{F}_2$. The Walsh transform of ℓ is given by:*

$$\mathsf{W}_{b \cdot x + \varepsilon}(a) = (-1)^{\varepsilon} 2^n \delta_b(a),$$

where δ_b denotes the indicator function of b, whose value at a equals 1 if $a = b$ and 0 otherwise. That is,

$$\mathsf{W}_f(b) = (-1)^{\varepsilon} 2^n, \textit{ and } \forall a \in \mathbb{F}_2^n \setminus \{b\}, \, \mathsf{W}_f(a) = 0.$$

Accordingly, $\mathsf{Wsupp}_f = \{b\}$. Moreover, Wsupp_f is a singleton if and only if f is an affine function (this is a direct consequence of the Parseval relation, that we shall recall below as Relation (1), and which shows that the unique nonzero value of the Walsh transform equals $\pm 2^n$).

Property 2 (Walsh transform of bent functions)**.** *Let $n \in \mathbb{N}$, n even. Let f be a bent function, the Walsh transform of f is given by:*

$$\forall a \in \mathbb{F}_2^n, \, \mathsf{W}_f(a) = \pm 2^{n/2}, \textit{ and } \sum_{a \in \mathbb{F}_2^n} \mathsf{W}_f(a) = \pm 2^n.$$

That is, the Walsh transform of f takes the value $2^{n/2}$ on $2^{n-1} \pm 2^{n/2-1}$ inputs and $-2^{n/2}$ on the $2^{n-1} \mp 2^{n/2-1}$ remaining inputs. Accordingly, $\mathsf{Wsupp}_f = \mathbb{F}_2^n$.

The Siegenthaler construction is a secondary construction which combines two n-variable functions to obtain an $(n+1)$-variable function:

Definition 7 (Siegenthaler's Construction). *Let $n \in \mathbb{N}$, $f, g \in \mathcal{B}_n$, we call Siegenthaler construction h from components f and g the function:*

$$h \in \mathcal{B}_{n+1}, \quad \forall x \in \mathbb{F}_2^n, \forall y \in \mathbb{F}_2, \; h(x,y) = (1+y)\, f(x) + y\, g(x). \tag{2}$$

Note that any function of $\mathcal{B}_{n+1}$ can be built using this construction, and in a unique way when the variable playing the role of y is fixed.

Property 3 (Siegenthaler's Construction and Walsh transform (*e.g.* [Car21])**.** *Let $n \in \mathbb{N}$, $f, g \in \mathcal{B}_n$, h obtained through Siegenthaler's construction with components f and g. The following property holds on the Walsh transform of h:*

$$\forall a \in \mathbb{F}_2^n, \quad \mathsf{W}_h(a,0) = \mathsf{W}_f(a) + \mathsf{W}_g(a), \;\; \textit{and} \;\; \mathsf{W}_h(a,1) = \mathsf{W}_f(a) - \mathsf{W}_g(a).$$

3 Primary constructions of Boolean functions whose Walsh support is the complement of a singleton

In [CM04] is shown that, under some conditions which can be satisfied for every $n \geq 10$, a modified Maiorana-McFarland n-variable Boolean function of the form $f(x,y) = x \cdot \phi(y) + 1_E(x,y)$, where $(x,y) \in \mathbb{F}_2^k \times \mathbb{F}_2^{n-k}$, ϕ is a mapping from $\mathbb{F}_2^{n-k}$ to $\mathbb{F}_2^k$, and $1_E(x,y)$ denotes the indicator function of some set E, can have a Walsh support equal to the complement of a singleton. Such functions are of course of interest from the general point of view of the theory of Boolean functions, and they can also be used as initial functions in secondary constructions of Boolean functions when we want to achieve some specific features for applications. In the present section, we address the values $n = 8, 9$, which were left open by [CM04] (actually, it was not known whether such functions could exist for these values of n). To this end, we first develop other methods to obtain functions having a Walsh support equal to the complement of a singleton. These methods, which are different for n even and n odd, also need $n \geq 10$, but they can be slightly adjusted so as to reach smaller values of n (which was not possible with the method used in [CM04]). They consist as well in adding the indicator of a set to a Boolean function belonging to a classic class (not specifically Maiorana-McFarland's class, contrary to [CM04], but rather the classes of bent functions for n even and of modified bent functions for n odd), because it seems impossible with functions in classic classes to have the desired Walsh support.
In Subsection 3.1 we recall some known results on the Walsh transform of the sum of a function and of the indicator of a set. In Subsection 3.2 we address the case $n \geq 8$ even (with a general construction valid for $n \geq 10$ and slightly modified to address $n = 8$). In Subsection 3.3, we construct the functions in odd dimension $n \geq 9$.

3.1 Altered functions and Walsh support

In this part we consider the impact of altering a function on its Walsh spectrum, which is a classic construction, initiated in [Dob95] and used later in many papers. More precisely we study how modifying a few values in the truth table of a Boolean function affects its Walsh support.

Definition 8 (Altered functions). *Let $f \in \mathcal{B}_n$, and $S \subseteq \mathbb{F}_2^n$, we call f altered on S and denote by f^S the function defined by:*

$$f^S(x) = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_2^n \setminus S, \\ f(x)+1 & \text{if } x \in S. \end{cases}$$

We recall some properties of altered function we will use later on and a proposition for the expression of its Walsh transform.

Property 4 (Altered functions). *Let $f \in \mathcal{B}_n$ and $S \subseteq \mathbb{F}_2^n$, the following holds on f^S*

- $f^{\mathbb{F}_2^n} = f + 1$.
- *ANF expression: The algebraic normal form of f^S is: ANF$(f) + \sum_{u \in S} \prod_{i=1}^{n} x_i^{u_i}(1 + x_i)^{1-u_i}$.*
- *Balancedness. If f is balanced then f^S is balanced if and only if $S \cap \mathsf{supp}(f) = |S|/2$.*

The following proposition is well-known (we give a short proof for our paper to be self-contained).

Proposition 1 (Altered function and Walsh transform). *Let $f \in \mathcal{B}_n$ and $S \subseteq \mathbb{F}_2^n$, for all $a \in \mathbb{F}_2^n$ the Walsh transform at a of f^S is given by $\mathsf{W}_{f^S}(a) = \mathsf{W}_f(a) - 2\sum_{u \in S}(-1)^{f(u)+a\cdot u}$.*

Proof. We rewrite the expression of $\mathsf{W}_{f^S}(a)$ using Definition 8:

$$\begin{aligned}
\mathsf{W}_{f^S}(a) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f^S(x)+a\cdot x} = \sum_{x \in \mathbb{F}_2^n \setminus S} (-1)^{f(x)+a\cdot x} + \sum_{u \in S} (-1)^{f(u)+1+a\cdot u}, \\
&= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} - 2\sum_{u \in S} (-1)^{f(u)+a\cdot u}, \\
&= \mathsf{W}_f(a) - 2\sum_{u \in S} (-1)^{f(u)+a\cdot u}.
\end{aligned}$$

□

3.2 Altered bent functions (in even numbers of variables) with a unique Walsh zero

In this section, we alter bent functions with the aim of obtaining Boolean functions with a limited number of Walsh zeroes. Then, this enables us to construct functions with a unique Walsh zero for all even integers $n \geq 8$. In the next construction, we specify Dobbertin's alteration method (that he introduced in [Dob95] and used to obtain balanced functions with a good nonlinearity iteratively). We use it here for a diffeent purpose (but the nonlinearity of the constructed functions, which is not as high as in the Dobbertin iterative construction, is very good).

Definition 9 (Construction 1). *Let $n > 0$ an even integer and $f \in \mathcal{B}_n$ a bent function satisfying:*

$$f(0_n) = 0 \quad \text{and} \quad \mathsf{W}_f(0_n) = 2^{n/2}.$$

Let $s_1, \ldots, s_m$ with $m = 2^{n/2-1}$ be m distinct elements of $\mathbb{F}_2^n$ such that $f(s_i) = 0$. We denote by S the set $S = \{s_1, \ldots, s_m\}$ and define the function g as $g = f^S$. We refer to g as an n-variable function from Construction 1 with seed (f, S).

Note that the condition in this construction is satisfied by any bent function, up to the addition of an affine function, since the addition of 1 allows to change $f(0_n) = 1$ into $f(0_n) = 0$ if necessary, and then the addition of a linear function $a \cdot x$ such that $\mathsf{W}_f(a) = 2^{n/2}$ (which always exists thanks to Property 2) ensures that the new value of $\mathsf{W}_f(0_n)$ equals the former value of $\mathsf{W}_f(a)$.

Proposition 2. *Let $g = f^S$ be a Boolean function obtained from Construction 1 (as in Definition 9) then:*

$$|\mathsf{Wsupp}_g| \in [2^n - 2^{n-t+1}, 2^n - 1],$$

where t is the dimension of $\mathsf{Span}(s_1, \ldots, s_m)$.

Proof. Using Proposition 1, we obtain:

$$\mathsf{W}_g(a) = \mathsf{W}_f(a) - 2\sum_{u\in S}(-1)^{f(u)+a\cdot u} = \mathsf{W}_f(a) - 2\sum_{u\in S}(-1)^{a\cdot u}.$$

Since (by Property 2) $\mathsf{W}_f(a) = \pm 2^{n/2}$ and $|S| = 2^{n/2-1}$, we have $\mathsf{W}_g(a) = 0$ if and only if $a \cdot u$ takes the same value for all u in S and this value equals 0 if $\mathsf{W}_f(a) = 2^{n/2}$ and 1 if $\mathsf{W}_f(a) = -2^{n/2}$. We give an upper bound on the numbers of those elements a that can satisfy this constraint. Note that $a \cdot u = 0$ for all $u \in S$ is equivalent to a being in $\big(\mathsf{Span}(s_1, \ldots, s_m)\big)^{\perp}$, but $a \cdot u = 1$ for all $u \in S$ does not imply that a belongs to a coset of this span, hence we will introduce a matrix to count those elements a. Since t is the dimension of $\mathsf{Span}(s_1, \ldots, s_m)$, we can build a matrix $\mathbf{U}$ of t rows corresponding to t linearly independent elements of S. Then, the numbers of elements a of $\mathbb{F}_2^n$ such that $\mathbf{U}a^T = 0_n^T$ is 2^{n-t}. The same reasoning applies relatively to 1_n^T, hence[4] there are at most 2^{n-t+1} vectors a such that $|\sum_{u\in S}(-1)^{a\cdot u}| = 2^{n/2-1}$. It allows to conclude $|\mathsf{Wsupp}_g| \geq 2^n - 2^{n-t+1}$.

Finally, we prove that there is at least one Walsh zero, leading to $|\mathsf{Wsupp}_g| \leq 2^n - 1$. For $a = 0_n$ using Proposition 1 and the constraints on f we obtain:

$$\mathsf{W}_g(0_n) = \mathsf{W}_f(0_n) - 2\sum_{u\in S}(-1)^{0_n\cdot u} = 2^{n/2} - 2\cdot 2^{n/2-1} = 0.$$

□

In the following we show how Construction 1 enables to build functions with exactly one Walsh zero.

Proposition 3. *Let n be an even integer, $n \geq 10$, there exist functions from Construction 1 such that* $\mathsf{Wsupp}_g = 2^n - 1$.

Proof. This proof uses some intermediate steps from the proof of Proposition 2. First, we will show that for $n \geq 8$ we can choose the elements of S such that $t = n$, which guaranties that $|\mathsf{Wsupp}_g| \in [2^n - 2, 2^n - 1]$ by Proposition 2. Then, using the matrix representation $\mathbf{U}$ of S as in the proof of Proposition 2, we will demonstrate that for $n \geq 10$, there is only one a such that $\mathbf{U}a^T = 0_n^T$ and no a such that $\mathbf{U}a^T = 1_n^T$, allowing to conclude that there is only one Walsh zero.

For the first part of the proof, since $n \geq 8$ we get that $|S| = 2^{n/2-1} \geq n$. Since $\mathsf{W}_f(0_n) = 2^{n/2}$, there are $2^{n-1} + 2^{n/2-1}$ elements x of $\mathbb{F}_2^n$ such that $f(x) = 0$. This quantity is greater than $2^{n-1} + 1$ and the co-support of f has then rank n, that is, we can choose a subset of n linearly independent elements of this co-support, which then spans $\mathbb{F}_2^n$. Calling this subset S', we build S such that $S' \subset S$, then $t = n$ and applying Proposition 2 we get $|\mathsf{Wsupp}_g| \in [2^n - 2, 2^n - 1]$.

For the second part of the proof, since $n \geq 10$ we get that $|S| > n$. In this case, we can build S' as in the previous part, with n linearly independent elements, and choose S so that it contains 0_n (since $f(0_n) = 0$ from Definition 9). Using the matrix $\mathbf{U} \in \mathbb{F}_2^{n\times n}$ given by the elements of S' as in the proof of Proposition 2, we get that $\mathbf{U}a^T = 0_n^T$ admits only $2^{n-n} = 1$ solution. Only the vector $a = 0_n$ satisfies then $a \cdot u = 0$ for all $u \in S$. And there is no element a such that $a \cdot u = 1$ for all $u \in S$ since $0_n \in S$. This completes the proof. □

Remark 1. Note that the condition $f(0_n) = 0$ of Definition 9 is only used for the proof of Proposition 3. This condition can be relaxed, the role of 0_n inside the proof can be played by another element of the co-support. Specifically, the proof can be adapted by taking any element u such that $f(u) = 0$ and u is a linear combination of an even number of the elements defining the set S' in the proof. Since all the combinations of an odd number of the n elements of S' give only 2^{n-1} vectors, u can be chosen from $\mathsf{supp}(f+1) \setminus \mathsf{Span}(S')$ since this set has a size at least $2^{n-1} + 2^{n/2-1} - 2^{n-1} = 2^{n/2-1}$. In this context, the elements a such that $\mathbf{U}a^T = 1_n$ are such that $u \cdot a^T = 0_n^T$, hence g has no second Walsh zero.

[4] Since $a \cdot u = 1$ for all $u \in S$ implies $\mathbf{U}a^T = 1_n^T$ but the converse is not true.

We present now a result for the special case $n = 8$, since it is not encompassed by Proposition 3 nor by the construction of functions with a unique Walsh zero from [CM04] (that applies for all n greater than or equal to 10).

Proposition 4. *Let $g \in \mathcal{B}_8$ be a function built from Construction 1 with set $S = \{s_1, \ldots, s_8\}$ such that $\dim(\mathsf{Span}(s_1, \ldots, s_8)) = 8$. Let $\mathbf{U}$ be the matrix having the s_i as rows, the following holds on Wsupp_g:*

$$|\mathsf{Wsupp}_g| = \begin{cases} 2^8 - 1 & \text{if } \mathsf{W}_f(\mathbf{U}^{-1}1_8^T) = 2^{n/2}, \\ 2^8 - 2 & \text{if } \mathsf{W}_f(\mathbf{U}^{-1}1_8^T) = -2^{n/2}. \end{cases}$$

Proof. Matrix $\mathbf{U}$ is now square and invertible. Using Proposition 2, we obtain that $|\mathsf{Wsupp}_g| \in [2^8 - 2, 2^8 - 1]$. As already seen, there is only one vector a in the co-support of W_g that satisfies $a \cdot u = 0$ for all $u \in S$; it is $a = \mathbf{U}^{-1}(0_8^T) = 0_8^T$. The only possible vector which can satisfy $a \cdot u = 1$ for all $u \in S$ is $\mathbf{U}^{-1}(1_8^T)$, since the elements of S are all the rows of $\mathbf{U}$. This completes the proof. □

Let us give concrete examples of functions g in 8 variables with Walsh support of size $2^n - 1$ and $2^n - 2$, respectively. As the function f we take the elementary symmetric function $\sigma_{2,8}$ whose ANF consists in all monomials of degree 2. Since it is a symmetric function, $\sigma_{2,8}$ takes the same value on inputs of the same Hamming weight, and its Walsh transform is also identical on inputs with the same Hamming weight. We recall the values of $\sigma_{2,8}$ and its Walsh transform in Table 1.

Weight of x	0	1	2	3	4	5	6	7	8
$\sigma_{2,8}(x)$	0	0	1	1	0	0	1	1	0
$\mathsf{W}_{\sigma_{2,8}}(x)$	16	-16	-16	16	16	-16	-16	16	16

Table 1: Values of $\sigma_{2,8}$ and its Walsh transform

The function $\sigma_{2,8}$ is bent, and satisfies the constraints of Definition 9, we consider two sets S_1 and S_2 to demonstrate the two cases of Proposition 4. We identify the vectors of $\mathbb{F}_2^8$ with the integers between 0 and 255 through the bijection $(x_1, \ldots, x_8) \mapsto \sum_{i=1}^{8} x_i 2^{i-1}$. We take $S_1 = \{1, 2, 4, 8, 16, 32, 64, 128\}$, which corresponds to the canonical basis ($\sigma_{2,8}$ gives 0 on the elements of Hamming weight one), hence $\mathbf{U}$ is the identity matrix and $\mathbf{U}^{-1}1_8^T = 1_8^T$ and $\mathsf{W}_{\sigma_{2,8}}(1_8^T) = 2^4$ from Table 1. Accordingly, $|\mathsf{Wsupp}_{\sigma_{2,8}^{S_1}}| = 2^8 - 1$.

We take $S_2 = \{1, 2, 4, 8, 23, 39, 71, 143\}$, these elements have Hamming weight 1, 4 and 5 for the last one, which correspond to 0 of $\sigma_{2,8}$. In this case $\mathbf{U}$ is a lower triangular matrix and $\mathbf{U}^{-1} = \mathbf{U}$, hence $\mathbf{U}^{-1}1_8^T = (1, 1, 1, 1, 0, 0, 0, 1)^T$ (we use that $u \cdot 1_8^T$ gives the parity of the the Hamming weight of u). Since $(1, 1, 1, 1, 0, 0, 0, 1)$ has Hamming weight 5, from Table 1 we can conclude that $|\mathsf{Wsupp}_{\sigma_{2,8}^{S_2}}| = 2^8 - 2$.

3.3 Constructions with a unique Walsh zero in an odd number of variables

In this part we extend the results of the previous part to the case of n odd. In this case, the construction we consider starts from a function with no Walsh zero, obtained from Siegenthaler's construction (2) with a bent function and an affine function in $n - 1$ variables. It allows us to build functions with a unique Walsh zero for all n odd at least 9.

Definition 10 (Construction 2). *Let $r > 2$ be an even integer, $f \in \mathcal{B}_r$ a bent function, $b \in \mathbb{F}_2^r$, and denoting $n = r + 1$, let $h \in \mathcal{B}_n$ be obtained through Siegenthaler's construction (2) with components f*

and $g = b \cdot x$ satisfying:

$$h(0_n) = 0 \quad \textit{(that is, } f(0_r) = 0\textit{)} \quad \textit{and} \quad \mathsf{W}_h(0_n) = 2^{r/2} \quad \textit{(that is, } \mathsf{W}_f(0_r) + \mathsf{W}_g(0_r) = 2^{r/2},$$

i.e. $\mathsf{W}_f(0_r) = 2^{r/2}$ *and* $b \neq 0_r$*)*.

Let $s_1, \ldots, s_m$ with $m = 2^{r/2-1}$ be m distinct elements of $\mathbb{F}_2^n$ such that $h(s_i) = 0$. We denote by S the set $S = \{s_1, \ldots, s_m\}$ and define the n-variable function ψ as $\psi = h^S$. We refer to ψ as an n-variable function from Construction 2 with seed (f, b, S).

Proposition 5. *Let $\psi = h^S$ be a Boolean function obtained from Construction 2 (as in Definition 10) then ψ is balanced and:*

$$|\mathsf{Wsupp}_\psi| \in [2^n - 2^{n-t+1}, 2^n - 1],$$

where t is the dimension of $\mathsf{Span}(s_1, \ldots, s_m)$.

Proof. ψ is balanced, since for $a = 0_n$, using Proposition 1 and the constraints on h, we have:

$$\mathsf{W}_\psi(0_n) = \mathsf{W}_h(0_n) - 2\sum_{u \in S}(-1)^{0_n \cdot u} = 2^{r/2} - 2 \cdot 2^{r/2-1} = 0.$$

The rest of the proof follows similar arguments as the one of Proposition 2.
First, we show that the function ψ has at most $2^{r-t+1} = 2^{n-t}$ Walsh zeroes: using Property 1, Property 2 and Property 3, we get that the values of the Walsh transform of h are $\pm 2^{r/2}$ for $2^n - 2$ elements and $\pm 2^r \pm 2^{r/2}$ for the two elements $(b, 0)$ and $(b, 1)$. Using Proposition 1 on ψ we obtain:

$$\mathsf{W}_\psi(a) = \mathsf{W}_h(a) - 2\sum_{u \in S}(-1)^{h(u)+a \cdot u} = \mathsf{W}_h(a) - 2\sum_{u \in S}(-1)^{a \cdot u}.$$

Since $|S| = 2^{r/2-1}$ and $r > 2$, $\mathsf{W}_\psi(a) = 0$ can only happen if $a \cdot u$ takes the same value for all u in S and $a \notin \{(b, 0), (b, 1)\}$. Since t is the dimension of $\mathsf{Span}(s_1, \ldots, s_m)$, we can build a matrix $\mathbf{U}$ of t rows corresponding to t linearly independent elements of S. Then, the number of elements a of $\mathbb{F}_2^n$ such that $\mathbf{U}a^T = 0_n^T$ is 2^{n-t} (the only difference with Proposition 2 is that the number of elements such that $\mathsf{W}_\psi(a) = 0$ can be strictly less than 2^{n-t}, because of the condition $a \notin \{(b, 0), (b, 1)\}$). The same reasoning applies relatively to 1_n^T, hence there are at most 2^{n-t+1} vectors a such that $|\sum_{u \in S}(-1)^{a \cdot u}| = 2^{r/2-1}$. It allows to conclude $|\mathsf{Wsupp}_\psi| \geq 2^n - 2^{n-t+1}$.
Finally, we have $|\mathsf{Wsupp}_\psi| \leq 2^n - 1$, since ψ is balanced.

□

Proposition 6. *Let r be an even integer, $r \geq 10$, and let $n = r + 1$. There exist functions from Construction 2 such that $|\mathsf{Wsupp}_\psi| = 2^n - 1$.*

Proof. The proof uses arguments similar to those in the proof of Proposition 3, replacing g by ψ, but it is slightly more complex. It uses some intermediate steps from the proof of Proposition 5. First, we show that, for $r \geq 10$, we can choose the elements of S such that $t = r + 1 = n$, which guarantees that $|\mathsf{Wsupp}_\psi| \in [2^n - 2, 2^n - 1]$ by Proposition 5. Then, using the matrix representation $\mathbf{U}$ of S as in the proofs of Proposition 5 we demonstrate that for $r \geq 10$ there is only one a such that $\mathbf{U}a^T = 0_n^T$ and no a such that $\mathbf{U}a^T = 1_n^T$, allowing to conclude that there is only one Walsh zero.
For the first part of the proof, since $r \geq 10$ we get that $|S| \geq r + 1 = n$. Since $\mathsf{W}_h(0_n) = 2^{r/2}$, there are $2^r + 2^{r/2-1}$ elements x of $\mathbb{F}_2^n$ such that $h(x) = 0$. This quantity is greater than $2^r + 1$ so we can take n of them that are linearly independent. Then they span $\mathbb{F}_2^n$. Calling this subset S', we build S such that $S' \subset S$, then $t = n$ and applying Proposition 5 we get $|\mathsf{Wsupp}_\psi| \in [2^n - 2, 2^n - 1]$.
For the other part of the proof, since $r \geq 10$ we get that $|S| > n$. In this case, we can build S' as in the

previous part and add 0_n since $h(0_n) = 0$ from Definition 10. Using the matrix $\mathbf{U}$ given by the elements of S' as in the proof of Proposition 5, we get that $\mathbf{U}a^T = 0_n^T$ admits only $2^{n-r-1} = 1$ solution, the vector 0_n. Then, adding the row 0_n to $\mathbf{U}$, the corresponding matrix $\mathbf{V}$ is such that $\mathbf{V}a^T = 1_{n+1}$ has no solution. In other words, there exists no vector $a \in \mathbb{F}_2^n$ such that $a \cdot u = 1$ for all $u \in S$, which is a necessary condition to obtain the second Walsh zero. □

Similarly to the results of Section 3.2, we can exhibit an example of function with a unique Walsh zero for $n = 9$ using similar ideas as in Proposition 6 and Proposition 4. By taking $f = \sigma_{2,8}$ and $g = \sigma_{1,r} = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8$, the function h satisfies the conditions of Construction 2. Taking the set $S = \{2, 4, 8, 16, 32, 64, 128, 256\}$, the function $\psi = h^S$ has a unique Walsh zero, in 0_9.

4 A secondary construction

In this part we give a secondary construction building a function with a single Walsh zero in dimension $n + 2$ from a function with a single Walsh zero in dimension n. This is the first systematic secondary construction known so far.

Theorem 1. *Let n be any positive integer such that there exists an n-variable Boolean function g with exactly one Walsh zero. Let g' be any n-variable Boolean function with an even Hamming weight and no Walsh zero*[5]*. Let h_1 be any n-variable Boolean function with an odd Hamming weight. Then we define the functions $h_2 = h_1 + g + g'$, and*

$$f(x, x_{n+1}, x_{n+2}) = x_{n+1}x_{n+2} + x_{n+1}h_1(x) + x_{n+2}h_2(x) + h_1(x)h_2(x) + g(x).$$

Then $f \in \mathcal{B}_{n+2}$ has exactly one Walsh zero.

Proof. We have:

$$\begin{aligned}\mathsf{W}_f(a, a_{n+1}, a_{n+2}) &= \sum_{\substack{x\in\mathbb{F}_2^n \\ x_{n+1}\in\mathbb{F}_2 \\ x_{n+2}\in\mathbb{F}_2}} (-1)^{f(x,x_{n+1},x_{n+2})+a\cdot x+a_{n+1}x_{n+1}+a_{n+2}x_{n+2}} \\ &= \sum_{x\in\mathbb{F}_2^n} \sum_{\substack{x_{n+1}\in\mathbb{F}_2 \\ x_{n+2}\in\mathbb{F}_2}} (-1)^{(x_{n+1}+h_2(x)+a_{n+2})(x_{n+2}+h_1(x)+a_{n+1})+g(x)+a_{n+1}h_2(x)+a_{n+2}h_1(x)+a\cdot x+a_{n+1}a_{n+2}}.\end{aligned}$$

Applying the changes of variables $x_{n+1} \mapsto x_{n+1} + h_2(x) + a_{n+2}$ and $x_{n+2} \mapsto x_{n+2} + h_1(x) + a_{n+1}$ gives:

$$\begin{aligned}\mathsf{W}_f(a, a_{n+1}, a_{n+2}) &= \sum_{\substack{x\in\mathbb{F}_2^n \\ x_{n+1}\in\mathbb{F}_2 \\ x_{n+2}\in\mathbb{F}_2}} (-1)^{x_{n+1}x_{n+2}+g(x)+a_{n+1}h_2(x)+a_{n+2}h_1(x)+a\cdot x+a_{n+1}a_{n+2}} \\ &= 2\,(-1)^{a_{n+1}a_{n+2}} \sum_{x\in\mathbb{F}_2^n} (-1)^{g(x)+a_{n+1}h_2(x)+a_{n+2}h_1(x)+a\cdot x+a_{n+1}a_{n+2}}.\end{aligned}$$

Hence, the number of Walsh zeros of f is equal to the sum of the Walsh zeros of the four functions $f_{a_{n+1},a_{n+2}}(x)$, defined as:

$$f_{a_{n+1},a_{n+2}}(x) = g(x) + a_{n+1}h_2(x) + a_{n+2}h_1(x),$$

[5] For even n, we can take a bent function; for odd n, we can concatenate a bent function in dimension $n - 1$ with a nonzero linear function.

where $(a_{n+1}, a_{n+2}) \in \mathbb{F}_2^2$.

We have that $f_{0,0} = g$ has one single Walsh zero, $f_{1,0} = g + h_2$ and $f_{0,1} = g + h_1$ have no Walsh zero since they have odd Hamming weight (because g having a Walsh zero has necessarily an even Hamming weight), and $f_{1,1} = g + h_1 + h_2 = g'$ has by hypothesis no Walsh zero. □

5 Impossibility results, for $2 \leq n \leq 6$

It has been checked in [CM04] that there is no n-variable Boolean function f with $n \in [2, 6]$ whose Walsh support $\{u \in \mathbb{F}_2^n; W_f(u) \neq 0\}$ equals the complement of a singleton. For $n = 1$, the identity function has such a Walsh support; the case of $n = 2$ has been proven mathematically in the appendix of [DMR23], the cases of $n \in [2, 3]$ have been both addressed mathematically in [PQ00, Theorem 1] (but this paper is rather difficult to follow). The cases of $n \in [2, 3]$ are also addressed mathematically in [JM25] by showing that the cardinalities 3 and 7 are impossible for any number of variables. In the same paper, the cardinality 15 is also proven impossible (solving the case $n = 4$) combining mathematical proofs and a classification in [CM04]. The cases of $n \in [4, 5]$ have been made with the help of a computer (and of known classification tables). The case of 6-variable functions of algebraic degree at most 4 has been proved mathematically and the case of degree 5 has been made by a computer search. Other works such as [UÇD14] have made searches with computers.
In summary, no mathematical proof is known except for $n = 2, 3$ and for $n = 6$ when the algebraic degree is at most 4. For completeness, in this section, we recall the theoretical proofs available and we give new ones, from diverse approaches (which all have their own interest).

5.1 Proof from Parseval's identity

Let us first briefly recall the proof in the case $n \in \{2, 3\}$.
For $n = 2$ it is a direct consequence of Parseval's relation and the well-known result that the sum of four squares equals 4^r for some r if and only if one of these squares equals 4^r and the others are zero (which would give three zeroes of the Walsh transform and does not fit), or all these squares equal 4^{r-1} (which would give no zero at all and does not fit either). This result on the sum of squares is proved in [CCCF02] (and can be proved by an induction).
For $n = 3$, a clearer proof than in [PQ00] is given in [JM25].
We now recall and complete the presentation of the proof from [CM04] for $n = 6$, and we extend it. Recall from [CS02, Theorem 4.1] that the Walsh transform values of a balanced Boolean function f on n variables and of algebraic degree d are divisible by $2^{2+\lfloor \frac{n-2}{d} \rfloor}$. Note that d cannot equal n, because the Hamming weight of a balanced function is even. For $d = n - 1$, this divisibility bound only says that the Walsh transform values are multiples of 4 which is known for every even weight Boolean function. For $d \leq n - 2$, the Walsh spectrum of f is of the form $\pm 8k$. Let n_k be the number of vectors $\omega \in \mathbb{F}_2^n$ such that $W_f(\omega) = \pm 8k$. We want that $n_0 = 1$. Parseval's relation requires that $(\star)$ $\sum_{k \geq 1} k^2 n_k = 2^{2n-6}$. Moreover the condition $S_f = \mathbb{F}_2^n \setminus \{0\}$ implies that $(\star\star)$ $\sum_{k \geq 1} n_k = 2^n - 1$. One can check that for $n \leq 6$, there is no solution for the diophantine system formed with $(\star)$ and $(\star\star)$. This shows that d must be equal to $n - 1$.

Now, we prove, using Parseval's identity, that there exists no function with a unique Walsh zero coefficient when $n = 4$ (our proof works also for $n = 2$).

Proposition 7. *Let $n \in \mathbb{N}, n \geq 3$. Let $f \in \mathcal{B}_n$ such that $|\mathsf{Wsupp}_f| = 2^n - 1$, then the following holds:*

$$\forall a \in \mathbb{F}_2^n, \mathsf{W}_f(a) \in 4\mathbb{Z}, \quad \textit{and} \quad \exists b \in \mathbb{F}_2^n \mid |\mathsf{W}_f(b)| \geq 8.$$

Proof. First, it is obvious that $\mathsf{W}_f(a) \in 4\mathbb{Z}$, since if a Boolean function f has a Walsh zero, say $\mathsf{W}_f(c) = 0$, then it has an even weight because $f(x) + c \cdot x$ has an even weight, and every Boolean function with an

even weight has a Walsh transform valued in $4\mathbb{Z}$, because we have then that $\widehat{f}(a) = \sum_{x \in supp(f)} (-1)^{a \cdot x}$ is even and then that for $a \neq 0$, $\mathsf{W}_f(a) = -2\widehat{f}(a)$ belongs to $4\mathbb{Z}$.

Then, we prove the existence of b by contradiction. Assume that all non-zero Walsh coefficients have absolute value 4. Using Equation 1, we obtain:

$$\sum_{a \in \mathbb{F}_2^n} \mathsf{W}_f(a)^2 = 0^2 + 4^2(2^n - 1) = 2^{2n}.$$

Let $y = 2^n$. The equation holds if and only if $y^2 - 16y + 16 = 0$. The two roots of this quadratic equation are $y = 8 \pm 4\sqrt{3}$, which are not powers of 2, leading to a contradiction. Accordingly, there exists at least one element $b \in \mathbb{F}_2^n$ such that $|\mathsf{W}_f(b)| > 4$, and since $\mathsf{W}_f(b)$ is a multiple of 4, we conclude that $|\mathsf{W}_f(b)| \geq 8$.

□

We show that at least one other Walsh coefficient must have absolute value at least 8, which implies that $|\mathsf{Wsupp}_f| = 2^n - 1$ is impossible for $2 \leq n \leq 4$.

Proposition 8. *Let $f \in \mathcal{B}_n$ such that $|\mathsf{Wsupp}_f| = 2^n - 1$, then $n \geq 5$.*

Proof. From Proposition 7, we know that there exists at least one element b such that $|\mathsf{W}_f(b)| \geq 8$. We first show that having only one such element is impossible. We proceed by contradiction. Using Equation 1, we have:

$$\sum_{a \in \mathbb{F}_2^n} \mathsf{W}_f(a)^2 = 0^2 + 4^2(2^n - 2) + \mathsf{W}_f(b)^2 = 2^{2n}.$$

Accordingly, $\mathsf{W}_f(b)$ must be a square root of $2^{2n} - 16(2^n - 2)$. Let $y = 2^n$; then we consider the equation:

$$y^2 - 16(y - 2) = x^2.$$

Solving for $y = \pm\sqrt{x^2 + 32} + 8$, and then solving $x^2 + 32 = z^2$ using Fermat's factorization, we find that the only integer solutions are:

$$(x, y) \in \{(\pm 7, -1), (\pm 7, 17), (\pm 2, 2), (\pm 2, 14)\}.$$

However, 2^n can never be -1, 17, or 14, and for $n \geq 2$, it is not equal to 2, leading to a contradiction.

Then, since at least two elements b and c correspond to Walsh coefficients of absolute value at least 8, we additionally use the fact that at least one coefficient must have absolute value at least $2^{n/2}$—otherwise, the sum of squares cannot reach 2^{2n}. With this additional constraint, Equation 1 yields the following inequality:

$$(2^{n/2})^2 + 16(2^n - 3) + 64 \leq 2^{2n}.$$

Setting $y = 2^n$, the inequality becomes the quadratic inequality $0 \leq y^2 - 17y - 16$ whose solution set is:

$$\left\{ y \in \mathbb{R},\ y \leq \frac{17 - \sqrt{353}}{2} \text{ or } y \geq \frac{17 + \sqrt{353}}{2} \right\} \approx \{ y \in \mathbb{R},\ y \leq -0.89 \text{ or } y \geq 17.89 \}.$$

Since $y = 2^n$ and $n \geq 2$, it allows to conclude $n \geq 5$ (so that $2^n = y \geq 17$).

□

5.2 Proof using the Walsh transform modulo 2^t

We begin by introducing a new result on the numerical degree of the Walsh transform modulo a power of two.

Theorem 2. *Let $n \geq 2$ be a natural number and $f \in \mathcal{B}_n$. The function $\mathsf{W}_f(a)$ modulo 2^t has numerical degree at most $t-2$ for $2 \leq t \leq n$.*

Proof. Let f be given by its NNF: $f(x) = \sum_{I \subseteq [1,n]} \lambda_I \, x^I$. We know (see *e.g.* [Car21][Relation (2.61)]) that:

$$\begin{aligned}
\forall u \neq 0_n, \mathsf{W}_f(u) &= (-1)^{\mathsf{w_H}(u)+1} \sum_{I \subseteq \{1,\ldots,n\};\ supp(u) \subseteq I} 2^{n-|I|+1} \lambda_I \\
&\equiv (-1)^{\mathsf{w_H}(u)+1} \sum_{\substack{I \subseteq \{1,\ldots,n\};\ \bar{I} \subseteq supp(\bar{u}) \\ n-|I|+1 \leq t-1}} 2^{n-|I|+1} \lambda_I \pmod{2^t} \\
&\equiv (-1)^{\mathsf{w_H}(u)+1} \sum_{\substack{J \subseteq \{1,\ldots,n\};\ J \subseteq supp(\bar{u}) \\ |J|+1 \leq t-1}} 2^{|J|+1} \lambda_{\bar{J}} \pmod{2^t} \\
&\equiv (-1)^{w_H(u)+1} \sum_{\substack{J \subseteq \{1,\ldots,n\} \\ |J| \leq t-2}} \bar{u}^J 2^{|J|+1} \lambda_{\bar{J}} \pmod{2^t}, \qquad (3)
\end{aligned}$$

where we have denoted $J = \bar{I} = \{1, \ldots, n\} \setminus I$ and where $\bar{u}$ is the complement $(1, \ldots, 1) - u$ of u, and $\bar{u}^J = \prod_{i \in J}(1 - u_i)$.

We have $(-1)^{w_H(u)+1} = -\prod_{k=1}^n (-1)^{u_k} = -\prod_{k=1}^n (1 - 2u_k)$, which is congruent with $\sum_{\substack{K \subseteq \{1,\ldots,n\} \\ |K| \leq t-|J|-2}} (-1)^{|K|+1} 2^{|K|} \prod_{k \in K} u_k$ modulo $2^{t-|J|-1}$, which has degree $t-2-|J|$. The expression in Relation (3) has then degree at most $t-2$. We have also $W_f(0) = 2^n - \sum_{I \subseteq \{1,\ldots,n\}} 2^{n-|I|+1} \lambda_I$ and since $n \geq t$, the term in 2^n cancels modulo 2^t and the expression in (3) is then also valid for $u = 0_n$, which completes the proof. □

Using this theorem, we can show that no Boolean function in fewer than 6 variables can have a unique Walsh zero.

Proposition 9. *Let $f \in \mathcal{B}_n$ such that $|\mathsf{Wsupp}_f| = 2^n - 1$, then $n \geq 6$.*

Proof. Let $f \in \mathcal{B}_n$ be a Boolean function with a single Walsh zero, where $n \geq 2$. We show that $n \geq 6$.

We define the set A_4 as $A_4 = \{a \mid \mathsf{W}_f(a) \equiv 4 \mod 8\}$. Using Theorem 2, the function $\mathsf{W}_f(a) \mod 2^3$ has numerical degree at most 1. We define the function $g \in \mathcal{B}_n$ as:

$$g(x) = \frac{\mathsf{W}_f(a) \mod 8}{4} \mod 2.$$

The function g is Boolean, since $\mathsf{W}_f(a) \mod 8$ belongs to the set $\{0, 4\}$, by Proposition 7. Since the numerical degree is no greater than the algebraic degree, g has degree at most 1. Hence,

$$|A_4| = |\{x \mid g(x) = 1\}|$$

takes a value in $\{0, 2^{n-1}, 2^n\}$. However, since f admits a Walsh zero, the case $|A_4| = 2^n$ cannot occur. Therefore, only two cases remain:

- Case $|A_4| = 0$. If $|A_4| = 0$, then all $2^n - 1$ nonzero Walsh coefficients have absolute value at least 8. Using Parseval's identity (Equation 1), we obtain $64(2^n - 1) \leq 2^{2n}$. Setting $y = 2^n$, we get the quadratic inequality:
$$0 \leq y^2 - 64y + 64.$$

This inequality holds approximately for $y \geq 62.9839$ or $y \leq 1.01613$. Therefore, the only valid case for integer powers of two is $y \geq 64$, which implies $n \geq 6$.

– Case $|A_4| = 2^{n-1}$. In this case exactly $2^{n-1} - 1$ Walsh coefficients have absolute value at least 8, and 2^{n-1} have absolute value at least 4. Therefore, we obtain the following inequality $64(2^{n-1} - 1) + 16 \cdot 2^{n-1} \leq 2^{2n}$. Setting $y = 2^n$, we get:

$$0 \leq y^2 - 40y + 64.$$

This inequality holds approximately for $y \geq 38.3303$ or $y \leq 1.6697$, which implies again that $y \geq 64$, and thus $n \geq 6$.

□

5.3 Proof from linear codes

In this part we give another proof of Proposition 8 using results on linear codes. We start by formalizing the existence of a function with a unique Walsh zero as the existence of a specific code.

Theorem 3. *For a given $n \geq 2$, there is a $[2^{n-1}, n]_2$ linear code C with unique columns which contains no elements of weight 2^{n-2} if and only if there is a balanced Boolean function with Walsh support $\mathbb{F}_2^n \setminus \{0_n\}$.*

Proof. Let $\mathsf{supp}(f) = \{x_1, \ldots, x_{2^{n-1}}\}$ and f be balanced. We further assume that $\mathsf{supp}(f)$ spans the whole space, otherwise the underlying function is affine (hence with more than one Walsh zero for $n \geq 2$). Then, f has a second Walsh zero if and only if there exists $a \in \mathbb{F}_2^n \setminus \{0_n\}$ such that:

$$\begin{aligned}
\mathsf{W}_f(a) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} = \sum_{x \in \mathsf{supp}(f)} (-1)^{a\cdot x} - \sum_{x \notin \mathsf{supp}(f)} (-1)^{a\cdot x} \\
&= \sum_{x \in \mathbb{F}_2^n} (-1)^{a\cdot x} + 2 \sum_{x \in \mathsf{supp}(f)} (-1)^{ax} \\
&= 0 + 2 \sum_{x \in \mathsf{supp}(f)} (-1)^{a\cdot x} = 0.
\end{aligned}$$

The condition $2\sum_{x \in \mathsf{supp}(f)} (-1)^{a\cdot x} = 0$ is satisfied only when:

$$|\{x \in \mathsf{supp}(f) \mid a \cdot x = 0\}| = |\{x \in \mathsf{supp}(f) \mid a \cdot x = 1\}| = |\mathsf{supp}(f)|/2 = 2^{n-2}.$$

By $v_1, \ldots, v_n$ we denote a basis of $\mathbb{F}_2^n$. We define the following generator matrix of a $[2^{n-1}, n]_2$ linear code C_f:

$$\mathbf{G} = \begin{bmatrix} v_1 \cdot x_1 & v_1 \cdot x_2 & v_1 \cdot x_3 & \cdots & v_1 \cdot x_{2^{n-1}} \\ v_2 \cdot x_1 & v_2 \cdot x_2 & v_2 \cdot x_3 & \cdots & v_2 \cdot x_{2^{n-1}} \\ v_3 \cdot x_1 & v_3 \cdot x_2 & v_3 \cdot x_3 & \cdots & v_3 \cdot x_{2^{n-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_n \cdot x_1 & v_n \cdot x_2 & v_n \cdot x_3 & \cdots & v_n \cdot x_{2^{n-1}} \end{bmatrix} \in \mathrm{Mat}\left(\mathbb{F}_2, n, 2^{n-1}\right). \tag{4}$$

Accordingly, f admits another Walsh zero if and only if $A_{2^{n-2}}(C_f) > 0$, that is if C_f admits codewords of Hamming weight 2^{n-2}.

In the other direction, given a $[2^{n-1}, n]_2$ code C with generator matrix without repetition of columns, by identifying a basis $v_1, \ldots, v_n$ of $\mathbb{F}_n^n$, one can construct a balanced Boolean function by setting $f(x) = 1\,[\,x \textit{ defines a column of } C\,]$, which has support $\mathbb{F}_2^n \setminus \{0_n\}$ if and only if $A_{2^{n-2}}(C) > 0$ (by the same argument as before). The resulting function is balanced because each column is unique, which ensures $|\mathsf{supp}(f)| = 2^{n-1}$. □

Note that row transformations of $\mathbf{G}$ do not change the code C_f and that column transpositions do not change f. We can thus assume that $\mathbf{G}$ is in standard form:

$$\mathbf{G} = \begin{bmatrix} \mathbf{I}_n & \mathbf{A} \end{bmatrix}$$

with $\mathbf{A} \in \mathrm{Mat}\left(\mathbb{F}_2, n, 2^{n-1} - n\right)$.

From this representation we can derive another proof for the non existence of function with a unique Walsh zero for the cases $n \in \{2, 3, 4\}$ (giving an alternative proof for Proposition 8).

Proof. We consider the three values of $n \in \{2, 3, 4\}$ separately.

- case $n = 2$: $2^{n-1} - n = 0$, but $\mathbf{G} = \mathbf{I}_2$ has balanced codewords (Note that the case $n = 2$ is also simple since a balanced f must be affine).
- case $n = 3$: $2^{n-1} - n = 1$ and

  $$\mathbf{G} = \begin{bmatrix} 1\,0\,0\,a_0 \\ 0\,1\,0\,a_1 \\ 0\,0\,1\,a_2 \end{bmatrix}.$$

  Each row has weight $1 + a_i$. Therefore, the only possibility for C_f to not contain codewords of weight 2^{n-2} is when all the a_i are equal to 0. In this case, the sum of two rows of $\mathbf{G}$ is a vector of C_f of weight $2 = 2^{n-2}$. It allows us to conclude that no $[4, 3]$ linear code can satisfy the constraint of Theorem 3, hence there is no 3-variable Boolean function with a unique Walsh zero.
- case $n = 4$: $2^{n-1} - n = 4$, $\mathbf{A}$ is a 4×4 matrix. First, we note no row of $\mathbf{A}$ may contain a weight 3 vector, and we perform a disjunction of cases on the existence of rows of vector of weight 2 to show that no code can satisfy the constraints of Theorem 3.
  - We assume $\mathbf{A}$ has a row of weight 2, that we denote by u. In this case, there are is no row of $\mathbf{A}$ of weight 0 or 4, otherwise the sum of two rows of $\mathbf{G}$ give a vector of weight 4. If a row of $\mathbf{A}$ has weight 1, it is unique, otherwise the sum of two rows of $\mathbf{G}$ gives a vector of weight 4. Furthermore, this vector cannot have its 1 on a column where u has a 1, otherwise the sum of two rows of $\mathbf{G}$ gives a vector of weight 4.
    Accordingly, the presence of u in the rows of $\mathbf{A}$ force the other rows to be zero or one row with weight 1 and rows of weight 2. If there is another vector of weight 2, it cannot have only one 1 in common with u, otherwise the sum of two rows of $\mathbf{G}$ gives a vector of weight 4. Accordingly, the two only possibilities are the following. If there is a vector of weight 1, the two last rows are copies of u. If there is no vector of weight 1, the rows are copies of u or its complementary. For the two cases, two columns of $\mathbf{A}$ are identical, hence this case does not lead to a code satisfying the constraints of Theorem 3.
  - We assume $\mathbf{A}$ has no row of Hamming weight 2. In this case $\mathbf{A}$ has at most one row of weight 0, one of weight 4 and also at most one row of weight 1 otherwise the sum of two rows of $\mathbf{G}$ gives a vector of weight 4. We cannot find 4 vectors to build $\mathbf{A}$ with these constraints.

□

6 Experimental results: functions with a unique Walsh zero in 7, 8 and 9 variables.

In this section, we describe our methodology for experimentally finding Boolean functions with a unique Walsh zero. To this end, we use the Walsh–Fourier transform of a Boolean function f:

Definition 11 (Walsh-Fourier transform). *Let $f \in \mathcal{B}_n$ be a Boolean function, its Walsh-Fourier transform $\widehat{f}$ at $a \in \mathbb{F}_2^n$ is defined as:*

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x}.$$

We characterize the property of a balanced Boolean function having a unique Walsh zero in terms of its Walsh–Fourier transform.

Proposition 10. *Let $f \in \mathcal{B}_n$ be a balanced Boolean function, then:*

$$|\mathsf{Wsupp}_f| = 2^n - 1 \Leftrightarrow \forall a \in \mathbb{F}_2^n \setminus \{0_n\},\ \widehat{f}(a) \neq 0.$$

Proof. If f is balanced and $|\mathsf{Wsupp}_f| = 2^n - 1$, then $\mathsf{W}_f(a) \neq 0$ for all $a \in \mathbb{F}_2^n \setminus \{0_n\}$. Hence:

$$\begin{aligned}
-\widehat{f}(a) &= -\sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x} = -\sum_{x \in \mathsf{supp}(f)} (-1)^{a \cdot x} = -\sum_{x \in \mathsf{supp}(f)} (-1)^{a \cdot x} + \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} \\
&= \sum_{x \in \mathsf{supp}(f)} (-1)^{f(x)+a \cdot x} + \frac{1}{2} \left(\sum_{x \in \mathsf{supp}(f)} (-1)^{a \cdot x} + \sum_{x \in \mathbb{F}_2^n \setminus \mathsf{supp}(f)} (-1)^{a \cdot x} \right) \\
&= \sum_{x \in \mathsf{supp}(f)} (-1)^{f(x)+a \cdot x} + \frac{1}{2} \left(-\sum_{x \in \mathsf{supp}(f)} (-1)^{f(x)+a \cdot x} + \sum_{x \in \mathbb{F}_2^n \setminus \mathsf{supp}(f)} (-1)^{f(x)+a \cdot x} \right) \\
&= \frac{1}{2} \left(\sum_{x \in \mathsf{supp}(f)} (-1)^{f(x)+a \cdot x} + \sum_{x \in \mathbb{F}_2^n \setminus \mathsf{supp}(f)} (-1)^{f(x)+a \cdot x} \right) = \frac{1}{2} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a \cdot x} \\
&= \frac{\mathsf{W}_f(a)}{2} \neq 0.
\end{aligned}$$

In the first line we used that $\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x}$ equals 0 when a is not the null vector.

For the reverse implication, suppose that f is balanced and that $\widehat{f}(a) \neq 0$ for all $a \in \mathbb{F}_2^n \setminus \{0_n\}$. Since f is balanced, we have $\mathsf{W}_f(0) = 0$, and thus $|\mathsf{Wsupp}_f| \leq 2^n - 1$. From the equality established above, we know that for all $a \neq 0$, $\mathsf{W}_f(a) = -2\widehat{f}(a)$. Since $\widehat{f}(a) \neq 0$ for all $a \neq 0_n$, it follows that $\mathsf{W}_f(a) \neq 0$ for all $a \neq 0_n$, and hence $|\mathsf{Wsupp}_f| \geq 2^n - 1$. Combining both bounds, we conclude that $|\mathsf{Wsupp}_f| = 2^n - 1$.

□

To find a function with a reduced number of Walsh zeroes, we start from a balanced Boolean function and iteratively modify it so that its Walsh–Fourier transform becomes zero at as many nonzero points as possible. In particular, to obtain a balanced function with a unique Walsh zero, and following Proposition 10, we stop once we reach a function whose transform is nonzero at all elements of $\mathbb{F}_2^n \setminus \{0\}$. To develop the corresponding algorithm, we first analyze how the Walsh–Fourier spectrum evolves when the function is modified at two points, in a manner similar to Proposition 1.

Proposition 11. *Let $f \in \mathcal{B}_n$ be a balanced Boolean function, with $y \in \mathsf{supp}(f)$ and $z \in \mathbb{F}_2^n \setminus \mathsf{supp}(f)$ then the following holds, $\forall a \in \mathbb{F}_2^n$:*

$$\widehat{g}(a) = \widehat{f^{\{y,z\}}}(a) = \widehat{f}(a) - (-1)^{ay} + (-1)^{az}.$$

Proof.

$$\begin{aligned}\widehat{g}(a) = \widehat{f^{\{y,z\}}}(a) &= \sum_{x \in \mathsf{supp}(g)} (-1)^{a \cdot x} = \sum_{x \in (\mathsf{supp}(f) \setminus \{y\}) \cup \{z\}} (-1)^{a \cdot x} \\ &= \sum_{x \in \mathsf{supp}(f)} (-1)^{a \cdot x} - (-1)^{a \cdot y} + (-1)^{a \cdot z} \\ &= \widehat{f}(a) - (-1)^{a \cdot y} + (-1)^{a \cdot z}.\end{aligned}$$

□

Thus, a single pass over the table T representing $\widehat{f}$ is sufficient to update it into the table representing $\widehat{g}$. The algorithm we use to find examples in dimensions 7, 8, and 9 follows a shotgun hill-climbing strategy: we draw a balanced Boolean function at random, attempt to improve it via pairwise swaps, and restart the process whenever no further improvement is possible. Identifying which pair (y, z) can improve the table T requires an additional pass. In practice, the implementation considers all pairs such that $f(y) = 1$ and $f(z) = 0$.

Algorithm 1: Finding f balanced with Walsh support $\mathbb{F}_2^n \setminus \{0\}$

repeat
  Draw a balanced f at random;
  Compute $T[a]$; $\widehat{f}(a)$ for each $a \in \mathbb{F}_2^n \setminus \{0_n\}$;
  while *T can be improved for some choice of y, z* **do**
    Swap y and z in $\mathsf{supp}(f)$;
    Update T;
until *T has no zeros*;
return f;

We provide truth tables of functions for each $n \in \{7, 8, 9\}$ in Appendix 7.

Acknowledgement Pierrick Méaux was funded by the European Research Council (ERC) under the Advanced Grant program (reference number: 787390).

References

AL16. Benny Applebaum and Shachar Lovett. Algebraic attacks against random local functions and their countermeasures. In *STOC*, pages 1087–1100. ACM, 2016.

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

CCCF02. Anne Canteaut, Claude Carlet, Pascale Charpin, and Caroline Fontaine. On cryptographic properties of the cosets of r (1, m). *IEEE Transactions on Information Theory*, 47(4):1494–1513, 2002.

CDM+18. Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, and Yann Rotella. On the concrete security of goldreich's pseudorandom generator. In *ASIACRYPT 2018*, volume 11273, pages 96–124. Springer, 2018.

CM04. Claude Carlet and Sihem Mesnager. On the supports of the Walsh transforms of Boolean functions. Proceedings of BFCA (First Workshop on Boolean Functions : Cryptography and Applications), Rouen, Mars 2005, Publications des Universités de Rouen et du Havre, pp. 65-82, 2005 and Cryptology ePrint Archive, Report 2004/256, 2004.

CS02. Claude Carlet and Palash Sarkar. Spectral domain analysis of correlation immune and resilient Boolean functions. *Finite Fields and Their Applications*, 8(1):120–130, 2002.

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.

Dob95. Hans Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In Bart Preneel, editor, *Fast Software Encryption*, pages 61–74, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

Gol00. Oded Goldreich. Candidate one-way functions based on expander graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 7(90), 2000.

HHP21. Samir Hodžić, Peter Horak, and Enes Pasalic. Characterization of basic 5-value spectrum functions through walsh-hadamard transform. *IEEE Transactions on Information Theory*, 67(2):1038–1053, 2021.

HPWZ19. Samir Hodžić, Enes Pasalic, Yongzhuang Wei, and Fengrong Zhang. Designing plateaued boolean functions in spectral domain and their classification. *IEEE Trans. Inf. Theory*, 65(9):5865–5879, 2019.

JLS21. Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from well-founded assumptions. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC*, pages 60–73. ACM, 2021.

JM25. Maxence Jauberty and Pierrick Méaux. On the cardinality of the walsh support of a boolean function. *IACR Cryptol. ePrint Arch.*, page 1651, 2025.

LW24. Yueying Lou and Qichun Wang. An answer to an open problem on balanced boolean functions with the maximum possible walsh supports. In *2024 IEEE International Symposium on Information Theory (ISIT)*, pages 1608–1612. IEEE, 2024.

Mes16. Sihem Mesnager. *Bent functions*, volume 1. Springer, 2016.

PQ00. Dingyi Pei and Wenliang Qin. The correlation of a boolean function with its variables. In *International Conference on Cryptology in India*, pages 1–8. Springer, 2000.

Rot76. Oscar S Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.

Tok15. Natalia Tokareva. *Bent functions: results and applications to cryptography*. Academic Press, 2015.

UÇD14. Erdener Uyan, Çagdas Çalik, and Ali Doganaksoy. Counting Boolean functions with specified values in their Walsh spectrum. *J. Comput. Appl. Math.*, 259:522–528, 2014.

Üna23. Akin Ünal. Worst-case subexponential attacks on prgs of constant degree or constant locality. In *EUROCRYPT 2023*, volume 14004, pages 25–54. Springer, 2023.

WF22. Jiaxin Wang and Fang-Wei Fu. Three new constructions of 5-valued spectrum functions with totally disjoint spectra duals. In *ISIT*, pages 1743–1748, 2022.

YGJL22. Jing Yang, Qian Guo, Thomas Johansson, and Michael Lentmaier. Revisiting the concrete security of goldreich's pseudorandom generator. *IEEE Trans. Inf. Theory*, 68(2):1329–1354, 2022.

7 Truth Tables of Functions with $\mathsf{Wsupp}_f = \mathbb{F}_2^n \setminus \{0\}$

We provide the truth table of examples of function with an unique Walsh zero we found with the algorithm described in Section 6.

$n = 7$

```
[1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1,
0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0,
1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0,
1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0,
1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1,
1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0,
1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1]
```

$n = 8$

```
[1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0,
0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1,
0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1,
0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1,
1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0,
1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1,
1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0,
0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0,
1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0,
0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1,
1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0,
1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1,
1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0,
1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0,
1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1]
```

$n = 9$

```
[0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0,
1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1,
1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1,
0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0,
0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0,
1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0,
0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1,
1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1,
0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1,
1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0,
0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1,
1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1,
0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1,
0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1,
1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1,
0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0,
0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1,
```

0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0,
0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1,
0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1,
1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1,
0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0,
0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1,
1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0,
1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1,
1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0,
0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1,
1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1,
0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1,
0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1,
0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1]