On the weightwise nonlinearity of weightwise perfectly balanced functions

Agnese Gini, Pierrick Méaux

University of Luxembourg, Luxembourg
agnese.gini@uni.lu, pierrick.meaux@uni.lu

Abstract. In this article we perform a general study on the criterion of weightwise nonlinearity for the functions which are weightwise perfectly balanced (WPB). First, we investigate the minimal value this criterion can take over WPB functions, deriving theoretic bounds, and exhibiting the first values. We emphasize the link between this minimum and weightwise affine functions, and we prove that for $n \geq 8$ no n-variable WPB function can have this property. Then, we focus on the distribution and the maximum of this criterion over the set of WPB functions. We provide theoretic bounds on the latter and algorithms to either compute or estimate the former, together with the results of our experimental studies for n up to 8. Finally, we present two new constructions of WPB functions obtained by modifying the support of linear functions for each set of fixed Hamming weight. This provides a large corpus of WPB function with proven weightwise nonlinearity, and we compare the weightwise nonlinearity of these constructions to the average value, and to the parameters of former constructions in 8 and 16 variables.

Keywords: Cryptology, Boolean functions, FLIP cipher, Weightwise perfectly balancedness, Weightwise nonlinearity, Krawtchouk polynomials, Spherically punctured Reed-Muller codes.

1 Introduction.

The stream cipher family FLIP [MJSC16] introduced in the context of hybrid homomorphic encryption deviates from the usual models of stream ciphers and pseudorandom generators used in cryptographic frameworks by applying a Boolean function on input ranging not over the full vector space $\mathbb{F}_2^n$ but only on a subset of this vector space. More precisely, the filtering function is always applied on vectors of Hamming weight $n/2$, which makes the usual cryptographic criteria on Boolean functions not adapted to determine the security in this context. It leads to considering the properties which are cryptographically relevant for a function restricted to a subset of $\mathbb{F}_2^n$, or a partition of this space, and to finding functions that provide secure primitives while their input is restricted to fixed sets. In [CMR17], the main cryptographic criteria of Boolean functions (balancedness, nonlinearity and algebraic immunity) are adapted to restricted sets, with a particular focus on the properties relative to the sets of fixed Hamming weight, also called slices of the Boolean hypercube. Since 2017 the properties of Boolean functions on restricted sets have been studied in different works, various of them focusing on finding functions with good cryptographic properties on all the slices.

The property of balancedness for a Boolean function, *i.e.* to output 0 on exactly half of the inputs and 1 for the other half, is an important cryptographic criterion for Boolean functions often necessary to avoid building primitives with statistical biases. Regarding the sets of fixed Hamming weight it leads to the concept of weightwise perfectly balanced (WPB) functions, which are the Boolean functions which are balanced on each set $\{x \in \mathbb{F}_2^n \,|\, \mathsf{wH}(x) = k\}$ for $1 \leq k \leq n-1$. Having exactly half of the inputs mapping to 0 restricts to consider only slices with even cardinality, hence WPB functions exist only for n a power of 2, and by convention the value in 0_n and 1_n are fixed to 0 and 1 respectively to ensure the global balancedness. Since the introduction of the concept in [CMR17], various constructions have been proposed, trying to find larger families or constructions with other relevant properties such as good weightwise nonlinearity or algebraic immunity. In particular, the weightwise nonlinearity measures how far a function is from the affine functions restricted to a slice. Similarly to the nonlinearity for the full space context, it is used to bound the complexity

of attacks where an adversary uses the best affine approximation to approximate the output of a filtering function. The first construction of WPB function is given in [CMR17], it is a recursive construction giving WPB functions for all powers of 2 and weightwise almost perfectly balanced functions (the generalization for n not a power of 2). The weightwise nonlinearity of this WPB construction has been studied later in [Su21]. A secondary construction from 3 n-variable WPB to one $2n$-variable WPB is also provided in [CMR17]. Then, a construction based on the field representation is presented in [LM19], corresponding to 2-rotation symmetric functions. The construction in [TL19] splits $2n$-length words in 2 as (x, y) and considers sets based on the value of the comparison of $\mathsf{w_H}(x)$ and $\mathsf{w_H}(y)$ to build the support, it provides the first construction of a WPB functions with optimal algebraic immunity. Recently, the modifications of this construction presented in [MSL21] allow one to obtain WPB functions still with optimal algebraic immunity but with higher weightwise nonlinearity. A line of work started in 2020 with [MS21] provide recursive constructions based on the modification of the support of a low degree function over $\mathbb{F}_2^n$; more precisely on linear [MS21], quadratic [MS21,LS20] or quartic functions [ZS21]. Finally, in the recent preprint [MPJ+22] an experimental approach with evolutionary algorithms is considered to find 8-variable WPB with high weightwise nonlinearity.

These works on WPB functions usually focus on a new construction and determine the weightwise nonlinearity for small values of n, or lower bounds for larger values of n. In this article we perform a general study of the weightwise nonlinearity of WPB functions, highlighting its connections with other concepts such as spherically punctured Reed Muller codes, zeroes of Krawtchouk polynomials, and weightwise affine functions. Our study focuses on investigating the minimal and maximal value the weightwise nonlinearity of WPB functions can take, the distribution of these values, and we consider new constructions with a large corpus. More precisely, for the minimum we derive theoretic bounds and exhibit the values for the WPB functions up to 2^{10} variables. We highlight the relation between this minimum and functions affine on each slice, and we show that for $n \geq 8$ no WPB function can have this property. Then, we consider the maximum and the distribution of the weightwise nonlinearity over the WPB functions, we give theoretic bounds on the former and present algorithms to compute or estimate the latter. We provide the results of experimental studies for n up to 8. Finally, we introduce two constructions of WPB functions obtained by modifying a linear function for each slice. It gives a large corpus of WPB function with proven weightwise nonlinearity, and we compare the weightwise nonlinearity of these constructions to the average value, and to the parameters of former ones in 8 and 16 variables.

2 Preliminaries

In addition to classic notations we use $[n]$ to denote the subset of all integers between 1 and n: $\{1, \ldots, n\}$. For readability we use the notation $+$ instead of $\oplus$ to denote the addition in $\mathbb{F}_2$ and $\sum$ instead of $\bigoplus$. For a vector $v \in \mathbb{F}_2^n$ we denote $\mathsf{w_H}(v)$ its Hamming weight $\mathsf{w_H}(v) = |\{i \in [n] \,|\, v_i = 1\}|$. For two vectors v and w of $\mathbb{F}_2^n$ we denote $\mathsf{d_H}(v, w)$ the Hamming distance between v and w, $\mathsf{d_H}(v, w) = \mathsf{w_H}(v + w)$.

2.1 Boolean functions and weightwise considerations

In this part we introduce the main concepts on Boolean functions and their weightwise properties (properties on the slides) we will use in the article. We refer to *e.g.* [Car21] for Boolean functions and cryptographic parameters and to [CMR17] for the weightwise properties, also called properties on the slices. For $k \in [0, n]$ we call slice of the Boolean hypercube (of dimension n) the set $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$. Accordingly the Boolean hypercube is partitioned into $n + 1$ slices where the elements have the same Hamming weight.

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 $\mathcal{B}_n$.*

To denote when a property or a definition is restricted to a slice we will use the subscript k. For example, for a n-variable Boolean function f we denote its support $\mathsf{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ and we refer to $\mathsf{supp}_k(f)$ for its support restricted to a slice, *i.e.* $\mathsf{supp}(f) \cap \mathsf{E}_{k,n}$.

Definition 2 (Balancedness). *A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if $|\mathsf{supp}(f)| = 2^{n-1} = |\mathsf{supp}(f+1)|$.*

For $k \in [0, n]$ the function is balanced on the slice k if $||\mathsf{supp}_k(f)| - |\mathsf{supp}_k(f+1)|| \leq 1$. In particular when $|\mathsf{E}_{k,n}|$ is even $|\mathsf{supp}_k(f)| = |\mathsf{supp}_k(f+1)| = |\mathsf{E}_{k,n}|/2$.

Definition 3 (Weightwise Perfectly Balanced Function (WPB)). *Let $m \in \mathbb{N}^*$ and f be a Boolean function in $n = 2^m$ variables. It will be called weightwise perfectly balanced (WPB) if, for every $k \in [n-1]$, f is balanced on the slice k, that is $\forall k \in [n-1], |\mathsf{supp}_k(f)| = \binom{n}{k}/2$, and:*

$$f(0, \cdots, 0) = 0, \quad \text{and } f(1, \cdots, 1) = 1.$$

The set of WPB functions in 2^m variables is denoted $\mathcal{WPB}_m$.

Definition 4 (Nonlinearity). *The nonlinearity $\mathsf{NL}(f)$ of a Boolean function $f \in \mathcal{B}_n$, where n is a positive integer, is the minimum Hamming distance between f and all the affine functions in $\mathcal{B}_n$:*

$$\mathsf{NL}(f) = \min_{g,\, \mathsf{deg}(g) \leq 1} \{d_H(f, g)\},$$

where $g(x) = a \cdot x + \varepsilon$, $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$ (where $\cdot$ is some inner product in $\mathbb{F}_2^n$; any choice of an inner product will give the same value of $\mathsf{NL}(f)$).

For $k \in [0, n]$ we denote NL_k the nonlinearity on the slice k, the minimum Hamming distance between f restricted to $\mathsf{E}_{k,n}$ and the restrictions to $\mathsf{E}_{k,n}$ of affine functions over $\mathbb{F}_2^n$. Accordingly:

$$\mathsf{NL}_k(f) = \min_{g,\, \mathsf{deg}(g) \leq 1} |\mathsf{supp}_k(f+g)|.$$

We refer to the global weightwise nonlinearity of f as $\mathsf{GWNL}(f) = \sum_{k=0}^{n} \mathsf{NL}_k(f)$.

Another expression of the nonlinearity on the slice is useful to study this criterion, using a variant of the Walsh transform restricted to a subset [CMR17, MMM+18].

Property 1 (Nonlinearity on the slice, adapted from [CMR17], Proposition 6)**.** *Let $n \in \mathbb{N}^*, k \in [0, n]$, for every n-variable Boolean function f over $\mathsf{E}_{k,n}$:*

$$\mathsf{NL}_k(f) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_{k,a}(f)|}{2}, \text{ and } \sum_{a \in \mathbb{F}_2^n} \mathcal{W}_{k,a}^2 = 2^n |\mathsf{E}_{k,n}|,$$

where $\mathcal{W}_{k,a}(f) = \sum_{x \in \mathsf{E}_{k,n}} (-1)^{f(x)+ax}$ is the Walsh transform of f, in a, restricted to the slice k.

An upper bound on the nonlinearity on the slice can be derived from Property 1:

Property 2 (Upper bound on NL_k, adapted from [CMR17] Proposition 7)**.** *Let $n \in \mathbb{N}^*, k \in [0, n]$, for every n-variable Boolean function f over $\mathsf{E}_{k,n}$:*

$$\mathsf{NL}_k(f) \leq \frac{1}{2}\left(\binom{n}{k} - \sqrt{\binom{n}{k}}\right).$$

We introduce the notion of weightwise affine functions, which highlights connections between considerations on the slices and other works on Boolean functions used in cryptography.

Definition 5 (Weightwise affine functions). *Let $n \in \mathbb{N}^*$ and for $k \in [0,n]$ $\varphi_{k,n}$ denotes the indicator function of $\mathsf{E}_{k,n}$. An n-variable Boolean function f, written as $f = \sum_{k=0}^{n} f_k \varphi_{k,n}$, is called weightwise affine if and only if for each $k \in [0,n]$ f_k coincide with an affine function over $\mathsf{E}_{k,n}$. Equivalently, f is weightwise affine if and only if for each $k \in [0,n]$ $\mathsf{NL}_k(f) = 0$.*

The set of weightwise affine functions is noted $\mathcal{WD}_n^1$, and in general for $d \in [0,n]$ the set of weightwise functions of degree lower than or equal to d is noted $\mathcal{WD}_n^d$.

Note that various weightwise affine functions have already been studied for their cryptographic properties without this formalism. The weightwise constant functions ($\mathcal{WD}_n^0$) correspond to the symmetric functions at the center of many works (*e.g.* [Car04,CV05,BP05,SM07,CL11,CM19,Méa19,Méa21,CM21]). The hidden weight bit function introduced in [Bry91] is the weightwise affine function corresponding to the choice $f_0 = 0$ and $f_k = x_k$ for $k \in [n]$, the cryptographic properties of this function have been studied in [WCST14]. In [CMR17], the bent functions evoked in Propositions 1 and 2 are weightwise affine.

2.2 Spherically Punctured Reed-Muller Codes

Reed Muller codes $RM(r,n)$ are binary codes of length 2^n whose codewords are the evaluations of all Boolean functions of algebraic degree at most r in n variables on their 2^n entries. Fixing the Hamming weight to the entries to k gives the spherically punctured Reed-Muller codes studied by Kapralova and Dumer [DK13, DK17]. The properties of these codes are connected to Boolean functions with fixed weight entries. Since we will study the weightwise nonlinearity of some functions we will introduce only the spherically punctured Reed Muller codes of order-1.

Definition 6 (Spherically punctured Reed Muller codes of order-1). *For all $n \in \mathbb{N}^*$, $k \in [0,n]$, we denote by $\mathsf{P}_{k,n}$ the punctured order-1 Reed Muller code of length $\binom{n}{k}$ obtained by puncturing all entries of Hamming weight different from k.*

Property 3 ($\mathsf{P}_{k,n}$ properties, (adapted from [DK13] Theorem 4)**.** *Let $n \in \mathbb{N}, n \geq 4$ and $k \in [n-1]$, the code $\mathsf{P}_{k,n}$ has length $\binom{n}{k}$, dimension n, and minimal distance:*

$$\mathsf{d}_{k,n} = \begin{cases} 2\binom{n-2}{k} & \text{if } k = \frac{n}{2}, \\ \binom{n-1}{\max(k,n-k)} & \text{if } k \neq \frac{n}{2}. \end{cases}$$

Since $\mathsf{P}_{k,n}$ corresponds to the evaluation of all affine functions in n variables over $\mathsf{E}_{k,n}$, the nonlinearity on the slice k of a Boolean function f corresponds to the distance between f's truth table restricted to this slice and $\mathsf{P}_{k,n}$. It gives an alternative definition of NL_k given by the following property.

Property 4 (Weightwise nonlinearity and $\mathsf{P}_{k,n}$)**.** *Let $f \in \mathcal{B}_n$, $k \in [0,n]$, and $v_f \in \mathbb{F}_2^{\binom{n}{k}}$ be the vector of output of f over $\mathsf{E}_{k,n}$. The following holds:*

$$\mathsf{NL}_k(f) = \min_{c \in \mathsf{P}_{k,n}} \mathsf{d}_{\mathsf{H}}(v_f, c).$$

We recall the concept of covering radius of a code.

Definition 7 (Covering radius). *For a binary linear code $\mathcal{C}$ of length n the covering radius $r \in \mathbb{N}$ is the smallest r such that for all $w \in \mathbb{F}_2^n$ there exist at least an element of the code x such that $\mathsf{d_H}(x, w) \leq r$.*

Being the covering radius the maximal distance between an element of the space and the code, for $\mathsf{P}_{k,n}$ it gives the maximum value that NL_k can take (and is achieved). We denote $\rho_{k,n}$ the covering radius of $\mathsf{P}_{k,n}$, upper bounds on $\rho_{k,n}$ are given in [CMR17] and [MZD19].

2.3 Krawtchouk polynomials and properties on binomial coefficients

For some proofs we will use Krawtchouk polynomials and some of their properties, we give the necessary preliminaries here and refer to *e.g.* [MS78] for more details.

Definition 8 (Krawtchouk Polynomials). *The Krawtchouk polynomial of degree k, with $0 \leq k \leq n$ is given by:* $\mathsf{K}_k(x, n) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j}$.

Property 5 (Krawtchouk polynomials relations)**.** *Let $n \in \mathbb{N}^*$ and $k \in [0, n]$, the following relations hold:*

- $\mathsf{K}_k(n-x, n) = (-1)^k \mathsf{K}_k(x, n)$,
- $\mathsf{K}_{n-k}(x, n) = (-1)^x \mathsf{K}_k(x, n)$,
- *if n is even,* $\mathsf{K}_{n/2}(1, n) = 0$.

Property 6 (Proposition 5 [DMS06])**.** *For n even,*

$$\mathsf{K}_k(n/2, n) = \begin{cases} 0 & \text{if } k \text{ odd}, \\ (-1)^{k/2} \binom{n/2}{k/2} & \text{if } k \text{ even}. \end{cases}$$

We will also use the following properties on binomial coefficients.

Property 7 (Lucas's Theorem, binary case)**.** *Let $n, k \in \mathbb{N}$ and p a prime: $\binom{n}{k} = \prod_{i=0}^{t} \binom{n_i}{k_i} \pmod p$ where $n = n_t p^t + n_{t-1} p^{t-1} + \cdots + n_1 p + n_0$ and $k = k_t p^t + k_{t-1} p^{t-1} + \cdots + k_1 p + k_0$ are the base p expansions of n and k respectively.*

When $p = 2$, $\binom{n}{k}$ is even if and only if there exists $i \in [0, t]$ such that $n_i = 0$ and $k_i = 1$.

Property 8. *Let $m, k \in \mathbb{N}$, and $m \geq 2$, for $k \in [2^m - 1] \setminus \{2^{m-1}\}$ it holds: $\binom{2^m}{k} = 0 \pmod 4$.*

3 Generalities on WPB functions

This section is a mathematical introduction to the quantities we study in this article. First, we give the number of weightwise perfectly balanced functions and the formal definitions of the main quantities we investigate: minimum and maximum weightwise nonlinearity of WPB functions. Then, we provide some general remarks on the symmetry between slices and the behavior of the weightwise nonlinearity relatively to the addition of symmetric or a weightwise affine functions. Finally, we give the article's roadmap.

Rephrasing Definition 3, the WPB functions are the ones which support is half of each slice for k between 1 and $n-1$, and the all-one vector. From this description we can directly derive the number of WPB functions in $n = 2^m$ variables:

$$|\mathcal{WPB}_m| = \prod_{k=1}^{n-1} |\mathsf{E}_{\binom{n}{k}/2, \binom{n}{k}}| = \prod_{k=1}^{n-1} \binom{\binom{n}{k}}{\binom{n}{k}/2}. \tag{1}$$

For different constructions of WPB functions the NL_k has been exhibited for small values of m (typically $2 \leq m \leq 4$), or bounded for greater values. These values are often compared to the upper bound on the maximum NL_k given in [CMR17] and the values obtained by other constructions (as summarized in Table 2 of [MSL21] for example). On one side, the maximum value of $\mathsf{NL}_k(f)$, which corresponds to the covering radius of $\mathsf{P}_{k,n}$ is not known and it might be greater than the NL_k that a WPB function can reach. On the other side, the NL_k of known constructions is sometimes relatively close to 0, which leads to think that such constructions have a bad behavior relatively to the weightwise nonlinearity. In order to understand better the NL_k of WPB functions we introduce some notations relatively to the minimum and maximum value this parameter can take.

Definition 9 (Minimum and maximum weightwise nonlinearity of WPB functions.). *Let $m \in \mathbb{N}^*$ and $n = 2^m$. For $k \in [n-1]$ we define the minimum and maximum weightwise nonlinearity of a WPB function as:*

$$\mu_{k,n} = \min_{f \in \mathcal{WPB}_m} \mathsf{NL}_k(f), \quad \textit{and} \quad \mathsf{M}_{k,n} = \max_{f \in \mathcal{WPB}_m} \mathsf{NL}_k(f).$$

and the global minimum and maximum weightwise nonlinearity of a WPB function as:

$$\mu_n = \sum_{k=1}^{n-1} \mu_{k,n}, \quad \textit{and} \quad \mathsf{M}_n = \sum_{k=1}^{n-1} \mathsf{M}_{k,n}.$$

Remark 1. The codes $\mathsf{P}_{1,n}$ and $\mathsf{P}_{n-1,n}$ have their dimension equal to their length (see Property 3), then any function restricted to $\mathsf{E}_{1,n}$ or to $\mathsf{E}_{n-1,n}$ coincide with an affine function on this sets hence $\mu_{1,n} = \mathsf{M}_{1,n} = 0$ and $\mu_{n-1,n} = \mathsf{M}_{n-1,n} = 0$. Accordingly, the sum to define μ_n and M_n can be restricted to $k \in [2, n-2]$.

Remark 2. Note also that the codes $\mathsf{P}_{k,n}$ and $\mathsf{P}_{n-k,n}$ have the same parameters (length, dimension and minimal distance) from Property 3. In fact, since the affine automorphism of $\mathbb{F}_2^n$ given by $x \mapsto x + 1_n$ maps $\mathsf{E}_{k,n}$ to $\mathsf{E}_{n-k,n}$, the two codes are equivalent, therefore they share the same properties. Accordingly, $\mu_{k,n} = \mu_{n-k,n}$ and $\mathsf{M}_{k,n} = \mathsf{M}_{n-k,n}$, which gives another expression of μ_n and M_n.

By definition of μ_n and M_n the global weightwise nonlinearity of any n-variable WPB function is between these two extremes. In the following we show that there are at least 2^{n-1} WPB functions reaching the same value $\mathsf{GWNL}(f)$.

Proposition 1. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and f an n-variable WPB function, there are at least 2^{n-1} elements g_i in $\mathcal{WPB}_m$ such that $\mathsf{GWNL}(g_i) = \mathsf{GWNL}(f)$.*

Proof. Let h be an n-variable symmetric function such that $h(0_n) = h(1_n) = 0$, we show that $f + g$ is WPB and has the same weightwise nonlinearity as f on all the slices. First, for the balancedness, on each slice $\mathsf{E}_{k,n}$ such that $k \in [n-1]$ the support of $f + h$ is the one of f or $f + 1$, hence of size $\binom{n}{k}/2$ or $\binom{n}{k} - \binom{n}{k}/2 = \binom{n}{k}/2$. Additionally $(f+h)(0_n) = f(0_n) = 0$ and $(f+h)(1_n) = f(1_n) = 1$, therefore $f + h$ is WPB. Then, for the weightwise nonlinearity, since h is constant on each slice, for $k \in [n-1]$:

$$\mathsf{NL}_k(f+h) = \min_{\substack{g \\ \deg(g) \leq 1}} |\mathsf{supp}_k(f+h+g)| = \min_{\substack{g \\ \deg(g) \leq 1}} |\mathsf{supp}_k(f+g+\varepsilon)| = \min_{\substack{g' \\ \deg(g') \leq 1}} |\mathsf{supp}_k(f+g')| = \mathsf{NL}_k(f),$$

where $\varepsilon \in \{0, 1\}$. Thereafter $\mathsf{GWNL}(f + h) = \mathsf{GWNL}(f)$, and h is defined by the values ε_k it takes for each $\mathsf{E}_{k,n}$ for $k \in [n-1]$, therefore there are 2^{n-1} possible choices for h. It concludes the proof.

□

Remark 3. Proposition 1 uses the fact that adding a symmetric function null in 0_n and 1_n does not alter the WPB property, and in general WPB functions could be considered up to the addition of such symmetric functions. Note that the global weightwise nonlinearity of a function is kept invariant by the addition of a weightwise affine function, but adding such functions can change the support size on the slices hence changing the weightwise balancedness.

In the main parts of this article we investigate the quantities $\mu_{k,n}$ and $\mathsf{M}_{k,n}$, giving more insights on the minimal and maximal value the weightwise nonlinearity can take for WPB functions and how this value is distributed among WPB functions. In Section 4 we study the quantities $\mu_{k,n}$ and μ_n. We provide theoretical and experimental bounds, we also show that for $n \geq 8$ no WPB function is weightwise affine. In Section 5 we study the quantities $\mathsf{M}_{k,n}$ and M_n. We explicit theoretic bounds on $\mathsf{M}_{k,n}$ and perform an experimental investigation to determine the small values of $\mathsf{M}_{k,n}$ but also the full distribution of the weightwise nonlinearity of WPB functions in a few variables. In Section 6 we give two constructions of WPB functions with prescribed weightwise nonlinearity. We determine the exact number of WPB functions that are built with one of the constructions and compare the weightwise nonlinearties of these functions to former works. In Section 7 we conclude the paper and discuss open questions.

4 Minimal value

In this part we study the minimum weightwise nonlinearity. First, we investigate the connection between this quantity and the minimum of Krawtchouk polynomials. Then, we focus on the existence of functions which are both WPB and weightwise affine, we show that such functions exist in 2 or 4 variables but not for bigger n. Finally, we derive general bounds on μ_n and determine it experimentally for small values.

4.1 $\mu_{k,n}$ and minimum of Krawtchouk polynomials

The functions with the lowest NL_k are the one such that their truth table restricted to the slice k are the closest to an element of $\mathsf{P}_{k,n}$. To study $\mu_{k,n}$ using the error-correcting code perspective we first determine the Hamming weight of this code's elements.

Proposition 2 (Weight of $\mathsf{P}_{k,n}$ elements). *Let $m \in \mathbb{N}^*$ and $n = 2^m$ and $k \in [1, n-1]$ the Hamming weight of $\mathsf{P}_{k,n}$'s elements are the elements of the set:*

$$\left\{ \frac{\binom{n}{k}}{2} \pm \frac{\mathsf{K}_k(\ell, n)}{2}, \quad \ell \in [0, n] \right\}.$$

Proof. The code $\mathsf{P}_{k,n}$ is the restriction of the order-1 Reed Muller code $RM(1, n)$ to $\mathsf{E}_{k,n}$, hence the code's elements correspond to the affine functions of $\mathbb{F}_2^n$ restricted to $\mathsf{E}_{k,n}$. Therefore, the Hamming weight of $\mathsf{P}_{k,n}$'s elements can be determined by studying the Hamming weight of the affine functions, $a \cdot x + \varepsilon = \sum_{i=1}^{n} a_i x_i + \varepsilon$ where $a \in \mathbb{F}_2^n$ and $\varepsilon \in \mathbb{F}_2$, over $\mathsf{E}_{k,n}$. In the following we denote $\mathsf{w_H}(a \cdot x + \varepsilon)$ the Hamming weight of $a \cdot x + \varepsilon$ over $\mathsf{E}_{k,n}$.

First, note that $\mathsf{w_H}(a \cdot x + 1) = \binom{n}{k} - \mathsf{w_H}(a \cdot x)$ since the constant function 1 corresponds to the all-1 vector (of length $\binom{n}{k}$). Then, denoting $\ell = \mathsf{w_H}(a)$, we get $a \cdot x = 1$ if and only if an odd number of the ℓ

elements indexed by a are equal to 1. Therefore on the set $\mathsf{E}_{k,n}$, for $\ell \in [0,n]$, it gives:

$$\begin{aligned}
\mathsf{w_H}(a\cdot x) &= \sum_{\substack{i=1\\ i \text{ odd}}}^{\ell} \binom{\ell}{i}\binom{n-\ell}{k-i},\\
&= \frac{1}{2}\left(\sum_{\substack{i=1\\ i \text{ odd}}}^{\ell} \binom{\ell}{i}\binom{n-\ell}{k-i} + \sum_{\substack{i=0\\ i \text{ even}}}^{\ell} \binom{\ell}{i}\binom{n-\ell}{k-i} + \sum_{\substack{i=1\\ i \text{ odd}}}^{\ell} \binom{\ell}{i}\binom{n-\ell}{k-i} - \sum_{\substack{i=1\\ i \text{ even}}}^{\ell} \binom{\ell}{i}\binom{n-\ell}{k-i}\right),\\
&= \frac{1}{2}\left(\sum_{i=0}^{n} \binom{\ell}{i}\binom{n-\ell}{k-i} - \sum_{i=0}^{n}(-1)^i\binom{\ell}{i}\binom{n-\ell}{k-i}\right),\\
&= \frac{1}{2}\left(\binom{n}{k} - \mathsf{K}_k(\ell,n)\right).
\end{aligned}$$

The last equality is obtained by using Vandermonde convolution and the expression of Krawtchouk polynomial (Definition 8). Finally, since the Hamming weight of a belongs to $[0,n]$ it allows to conclude, the code's elements have Hamming weight in the set $\{(\binom{n}{k} \pm \mathsf{K}_k(\ell,n))/2, \quad \ell \in [0,n]\}$.

□

Using Proposition 2 we show how the quantity $\mu_{k,n}$ is linked to the minimal absolute value of the degree-k Krawtchouk polynomial in n variables.

Theorem 1 **($\mu_{k,n}$ and minimum of Krawtchouk polynomial).** *Let $m \in \mathbb{N}^*$, $n = 2^m$ and $k \in [1, n-1]$ the following holds on $\mu_{k,n}$:*

$$\mu_{k,n} = \min_{\ell\in[1,n/2]} \frac{1}{2}|\mathsf{K}_k(\ell,n)|.$$

Proof. By definition $\mu_{k,n} = \min_{f\in\mathcal{WPB}_m} \mathsf{NL}_k$ and therefore considering the code perspective $\mu_{k,n}$ is the minimum distance between an element of $\mathsf{E}_{\binom{n}{k}/2,\binom{n}{k}}$ (support of a WPB on the slice with cardinal $\binom{n}{k}$) and the $\mathsf{P}_{k,n}$. For readability we use ν to denote $\binom{n}{k}$ in the following. Thereafter:

$$\begin{aligned}
\mu_{k,n} &= \min_{w\in\mathsf{E}_{\nu/2,\nu}} \mathsf{d_H}(w,\mathsf{P}_{k,n}) = \min_{w\in\mathsf{E}_{\nu/2,\nu}} (\min_{c\in\mathsf{P}_{k,n}} \mathsf{d_H}(w,c)),\\
&= \min_{c\in\mathsf{P}_{k,n}} \min_{w\in\mathsf{E}_{\nu/2,\nu}} (w+c) = \min_{c\in\mathsf{P}_{k,n}} |\mathsf{w_H}(c) - \nu/2|.
\end{aligned}$$

Then, using Proposition 2:

$$\begin{aligned}
\mu_{k,n} &= \min_{\ell\in[0,n]} \left\{\frac{1}{2}\left(\nu \pm \mathsf{K}_k(\ell,n) - \nu\right)\right\} = \min_{\ell\in[0,n]} \frac{1}{2}|\mathsf{K}_k(\ell,n)|,\\
&= \min_{\ell\in[1,n/2]} \frac{1}{2}|\mathsf{K}_k(\ell,n)|.
\end{aligned}$$

The last equality is obtained using the properties on Krawtchouk polynomials, $\mathsf{K}_k(0,n) = \binom{n}{k}$ and $\mathsf{K}_k(\ell,n) = (-1)^k\mathsf{K}_k(n-\ell,n)$.

□

Theorem 1 relates $\mu_{k,n}$ and the minimum (absolute value) of Krawtchouk polynomials. In the following part we consider the particular cases given by the zeros of Krawtchouk polynomials.

4.2 (In)existence of WPB weightwise affine functions

When the Krawtchouk polynomial of degree k in n variables admits an integer zero, Theorem 1 gives that $\mu_{k,n}$ is null, which means that a WPB function is affine on the corresponding slice. Then, it leads to consider the existence of functions with extreme properties; being at the same time WPB and weightwise affine functions. Such functions are the one such that $\mu_n = 0$ and they would lead to very efficient attacks if they were used in the context of filter permutators.

Determining the integer zeros of Krawtchouk polynomials has been the focus of various works such as [KL96, SW99, Ale12]. Some of these zeros are called trivial zeros, for example for all n even and k odd $\mathsf{K}_k(\ell, n)$ admits a zero in $n/2$, and for n even $\mathsf{K}_{n/2}(1, n) = 0$. These zeroes are sufficient to prove the existence of WPB weightwise linear functions in 2 and 4 variables:

Proposition 3 (Existence of weightwise affine WPB functions). *Let $m \in [1, 2]$ and $n = 2^m$, then $\mathcal{WPB}_m \cap \mathcal{WD}_n^1 \neq \emptyset$.*

Proof. For $m = 1$, the only weight in $[n-1]$ is $k = 1$ and $\mathsf{K}_1(1, 2) = 0$, hence using Theorem 1 $\mu_{1,2} = 0$, then $\mu_2 = 0$ therefore some functions in $\mathcal{WPB}_1$ are weightwise affine.

For $m = 2$, the weights in $[n-1]$ are $k = 1, 2$ and 3. For 1 and 3 n is even and k odd hence the corresponding Krawtchouk polynomials admit an integer 0 in $n/2$ by Proposition 6. Since $2 = n/2$, by Property 5 $\mathsf{K}_2(1, 4) = 0$. Following the same reasoning as in the former case we can conclude $\mathcal{WPB}_2 \cap \mathcal{WD}_4^1 \neq \emptyset$.

□

Remark 4. Using the indicator functions $\varphi_{k,n}$ of the slices we can give an expression of some of the weightwise affine WPB functions. For $m = 1$ these functions can be written as: $0\varphi_{0,2} + x_i\varphi_{1,2} + 1\varphi_{2,2}$ for $i \in [2]$. It gives the functions x_1, and x_2 which are the two only WPB functions in 2 variables.

For $m = 2$, the weightwise affine WPB functions considered in the proof can be written as:

$$(x_i + x_j)\varphi_{1,4} + (x_k)\varphi_{2,4} + (x'_i + x'_j)\varphi_{3,4} + \varphi_{4,4}, \quad \text{where } i, j, k, i', j' \in [4], i \neq j, i' \neq j'.$$

This expression gives $6 * 4 * 6 = 144$ weightwise affine WPB functions. Contrarily to the case $m = 1$ the set of WPB functions and weightwise affine functions are different. Since $\mathsf{K}_2(2, 4) = -2$ the linear functions $x_i + x_j$ ($i \neq j$) have Hamming weight 4 on $\mathsf{E}_{2,4}$ hence $\mathcal{WD}_4^1 \not\subset \mathcal{WPB}_2$. Then, taking the vector of $\mathbb{F}_2^6$ representing such linear function $(x_i + x_j)$ over $\mathsf{E}_{2,4}$, any vector v obtained by removing one element from its support has Hamming weight 3 and therefore corresponds to a function balanced on $\mathsf{E}_{2,4}$. Since $\mathsf{P}_{2,4}$ has parameters $[6, 4, 2]$ by Property 3, v does not belong to the code hence $\mathcal{WPB}_2 \not\subset \mathcal{WD}_4^1$.

In the following we will see that weightwise affine WPB functions exist only for these two values of m. First, we summarize in the following property results on the limited number of non-trivial zeros of Krawtchouk polynomials taken from [KL96] and [SW99].

Property 9. *Let $n \in \mathbb{N}^*$, the following holds for the nontrivial zeros of Krawtchouk polynomials $\mathsf{K}_k(x, n)$:*

- *for $k = 2$ and $n > 4$, $\mathsf{K}_2(x, n)$ admits zeros if and only if n is a square,*
- *for $k = 4$ and $n > 8$, $\mathsf{K}_4(x, n)$ admits zeros for finitely many n and none of them is a power of 2,*
- *for $k = 6$ and $n > 12$, $\mathsf{K}_6(x, n)$ admits zeros for finitely many n and none of them is a power of 2,*
- *for k even greater than 6 and $n > 2k$, $\mathsf{K}_k(x, n)$ admits zeros for finitely many n.*

Then we can conclude on the nonexistence of weightwise affine WPB in more than 4 variables:

Proposition 4 (Non existence of weightwise affine WPB functions for $m > 2$). *Let $m > 2$ and $n = 2^m$, then $\mathcal{WPB}_m \cap \mathcal{WD}_n^1 = \emptyset$.*

Proof. Using Property 9, for $n = 8$ (*i.e.* $m = 3$) $\mathsf{K}_2(x, 8)$ does not admit a zero then $\mu_{2,8} > 0$ using Theorem 1 and therefore no 8-variable WPB is weightwise affine. For $m > 3$, the second or third item of the property are sufficient to conclude, using the second one for all $m > 3$ it implies $\mu_{4,2^m} > 0$ therefore $\mathcal{WPB}_m \cap \mathcal{WD}_n^1 = \emptyset$. □

Weightwise affine WPB functions exists if and only if μ_m equals 0, since Proposition 4 proves this quantity cannot be null for $m > 2$ we study the general bounds applying to this quantity in the following part.

4.3 General bounds on μ_n

Using Theorem 1 the value of μ_n (for n a power of 2) can be expressed as the sum of absolute minimum of Krawtchouk polynomials. In this part, first we give this expression using the simplification given by the trivial zeros of Krawtchouk polynomials. Then, we derive a lower and an upper bound on μ_{2^m}. Finally, we experimentally determine the values of μ_{2^m} for the first values of m.

Proposition 5 (μ_n expression). *Let $m \in \mathbb{N}^*$ and $n = 2^m$, the global minimum weightwise nonlinearity of $\mathcal{WPB}_m$ has the following expression:*

$$\mu_n = \begin{cases} 0 & \text{if } m \in [2], \\ \displaystyle\sum_{t=1}^{n/4-1} \min_{\ell \in [n/2]} |\mathsf{K}_{2t}(\ell, n)| & \text{if } m > 2. \end{cases}$$

Proof. First, the cases $m = 1$ and $m = 2$ are proven by Proposition 3. Then, for $m > 2$, since $\mu_n = \sum_{k=2}^{n-2} \mu_{k,2}$ by Remark 1, Theorem 1 gives the following expression:

$$\mu_n = \frac{1}{2} \sum_{k=2}^{n-2} \min_{\ell \in [n/2]} |\mathsf{K}_k(\ell, n)|.$$

Due to the trivial zeroes of Krawtchouk polynomials, the values with k odd and $n/2$ are not intervening in the sum. Finally, using Property 5, the relation on $\mathsf{K}_{n-k}(\ell, n)$ allows to consider only the terms for $k < n/2$, giving:

$$\mu_n = \sum_{\substack{k=2 \\ k \text{ even}}}^{n/2-2} \min_{\ell \in [n/2]} |\mathsf{K}_k(\ell, n)| = \sum_{t=1}^{n/4-1} \min_{\ell \in [n/2]} |\mathsf{K}_{2t}(\ell, n)|.$$

□

Proposition 4 and Property 9 allow to derive a lower bound on μ_n:

Proposition 6 (Lower bound on μ_n). *Let $m \in \mathbb{N}^*$, $m > 2$, and $n = 2^m$, the following holds on μ_n:*

$$\mu_n \geq \begin{cases} 2 & \text{if } m = 3, \\ 4 & \text{if } m > 3, m \text{ even}, \\ 6 & \text{if } m > 3, m \text{ odd}. \end{cases}$$

Proof. Using Proposition 4, for $m > 2$ we know that $\mu_n > 0$. Then, counting 1 for each value of k (and $n-k$ using Property 5) for which Property 9 gives that $\mathsf{K}_k(x,n)$ cannot be zero, gives the final result.

□

Upper bounds can be obtained by considering particular linear functions over the slices. We give the following one based on linear functions with one monomial.

Proposition 7 (Upper bound on μ_n). *Let $m \in \mathbb{N}^*$, $m > 2$, and $n = 2^m$, the following holds on μ_n:*

$$\mu_n \leq \binom{n-1}{n/2-2} - n + 1.$$

Proof. We begin with the expression of μ_n from Proposition 5:

$$\mu_n = \sum_{t=1}^{n/4-1} \min_{\ell \in [n/2]} |\mathsf{K}_{2t}(\ell, n)| \leq \sum_{t=1}^{n/4-1} |\mathsf{K}_{2t}(1,n)| = \sum_{t=1}^{n/4-1} \mathsf{K}_{2t}(1,n) \leq \sum_{k=2}^{n/2-2} \mathsf{K}_k(1,n),$$

where the equality and last inequality come from the the property that $\mathsf{K}_k(1,n) = \binom{n-1}{k} - \binom{n-1}{k-1}$ is positive for $k \in [n/2-1]$. Then:

$$\sum_{k=2}^{n/2-2} \mathsf{K}_k(1,n) = \sum_{k=2}^{n/2-2} \binom{n-1}{k} - \binom{n-1}{k-1} = \sum_{k=2}^{n/2-2} \binom{n-1}{k} - \sum_{k=1}^{n/2-3} \binom{n-1}{k} = \binom{n-1}{n/2-2} - \binom{n-1}{1},$$

which gives the final result.

□

To conclude this part, we give the global minimum weightwise nonlinearity of WPB functions for small values of m, determined experimentally in Table 1.

m	μ_n	lower bound	upper bound	$\mu_{2t,n}, t \in [1, n/4]$
3	2	2	14	[1, 0]
4	14	4	4990	[0, 7, 0, 0]
5	4750	6	265182494	[1, 4, 84, 455, 248, 868, 715, 0]

Table 1. Value of μ_n for $n = 2^m$, $m \in [3,5]$. μ_n is the real value, obtained by computation, the lower bound comes from Proposition 6 and the upper bound from Proposition 7.

m	$\lfloor \log_2(\mu_n) \rfloor$	lower bound	$\lfloor \log_2(\text{upper bound}) \rfloor$
6	27	4	59
7	59	6	123
8	122	4	250
9	250	6	506
10	505	4	1017

Table 2. Value of μ_n for $n = 2^m$, $m \in [6,10]$. μ_n is the real value, obtained by computation, the lower bound comes from Proposition 6 and the upper bound from Proposition 7.

5 Maximal value and weightwise nonlinearity distribution

In this part we study the (global) maximum weightwise nonlinearity of WPB functions $\mathsf{M}_{k,n}$ (and M_n). First, in Section 5.1 we provide theoretic lower and upper bounds on $\mathsf{M}_{k,n}$. Then, in the journey to experimentally determine $\mathsf{M}_{k,n}$ for small values of n we found out that light modifications of the algorithms we use to compute the maximum are sufficient to study the whole distribution of NL_k of WPB functions. It has the advantage to give a more informative experimental part, for example as we will see in Section 6 it shows that most known constructions in 8 variables have NL_k lower than average. Accordingly, in Section 5.2 we introduce the weightwise nonlinearity distribution and the formalism necessary for the correctness of our (deterministic and undeterministic) algorithms. In Section 5.3 we present the results of the experimental determination of the distributions and provide the technical algorithmic aspects. In order to give more insights on the NL_k distributions, the study is performed on $n \in [4, 8]$ rather than on powers of 2 only.

5.1 $\mathsf{M}_{k,n}$ theoretic bounds

To get a lower bound on $\mathsf{M}_{k,n}$ we can use the standard argument to bound from below the covering radius of a code, taking in consideration here that the set of points we consider is not the entire space but the elements of Hamming weight half the length.

Proposition 8 (Lower bound on $\mathsf{M}_{k,n}$). *Let $m \in \mathbb{N}^*$, $n = 2^m$, and $k \in [2, n-2]$. Let r' be the smallest integer such that:*

$$2^n \sum_{i=0}^{r'} \binom{\binom{n}{k}}{r'} \geq \binom{\binom{n}{k}}{\binom{n}{k}/2},$$

then $r' \leq \mathsf{M}_{k,n}$.

Proof. Using Property 3, $\mathsf{P}_{k,n}$ has dimension n, hence the union of balls centered in these 2^n elements with a radius of r (in Hamming distance) recover at most $2^n \sum_{i=0}^{r} \binom{\binom{n}{k}}{r}$ elements. While this quantity is smaller than $|\mathsf{E}_{\binom{n}{k},\binom{n}{k}/2}|$ there exists at least one element of $\mathsf{E}_{\binom{n}{k},\binom{n}{k}/2}$ at distance greater than r from $\mathsf{P}_{k,n}$. Accordingly, denoting r' the smallest integer such that:

$$2^n \sum_{i=0}^{r'} \binom{\binom{n}{k}}{r'} \geq \binom{\binom{n}{k}}{\binom{n}{k}/2},$$

we get $r' \leq \mathsf{M}_{k,n}$.

□

In the following we give a simpler expression of the NL_k for WPB functions and an upper bound on $\mathsf{M}_{k,n}$ using the connection between NL_k and Walsh transform restricted to a slice.

Proposition 9 (Upper bound on $\mathsf{M}_{k,n}$). *Let $m \in \mathbb{N}^*$, $n = 2^m$, and $f \in \mathcal{WPB}_m$, then for $k \in [2, n-2]$:*

$$\mathsf{NL}_k(f) = \frac{\binom{n}{k}}{2} - \max_{a \in \mathbb{F}_2^n \setminus \{0_n, 1_n\}} \Big| \sum_{\substack{x \in \mathsf{E}_{k,n} \\ ax=1}} (-1)^{f(x)} \Big|,$$

and $\mathsf{M}_{k,n} \leq \frac{1}{2}\left(\binom{n}{k} - \sqrt{\frac{2^n}{2^n-2}\binom{n}{k}}\right)$.

Proof. First we use the expression of the weightwise nonlinearity from Property 1:

$$\mathsf{NL}_k(f) = \frac{1}{2}\left(\binom{n}{k} - \max_{a\in\mathbb{F}_2^n} |\mathcal{W}_{k,a}(f)|\right), \text{where } \mathcal{W}_{k,a}(f) = \sum_{x\in\mathsf{E}_{k,n}} (-1)^{f(x)+ax}.$$

Since f is WPB, f is perfectly balanced on each slice $k \in [n-1]$ therefore $\mathcal{W}_{k,0_n}(f) = 0$. Moreover, at least one other value of the Walsh spectrum restricted on a slice is zero for a WPB function:

$$\mathcal{W}_{k,1_n}(f) = \sum_{x\in\mathsf{E}_{k,n}} (-1)^{f(x)+\sum_{i=1}^n x_i} = (-1)^k \sum_{x\in\mathsf{E}_{k,n}} (-1)^{f(x)} = (-1)^k \mathcal{W}_{k,0_n}(f) = 0.$$

It allows to derive the upper bound for $\mathsf{M}_{k,n}$, using the second part of Property 1:

$$\sum_{a\in\mathbb{F}_2^n} \mathcal{W}_{k,a}(f)^2 = \sum_{a\in\mathbb{F}_2^n\setminus\{0_n,1_n\}} \mathcal{W}_{k,a}(f)^2 = 2^n\binom{n}{k},$$

hence the average of the $\mathcal{W}_{k,a}(f)$ for $a \in \mathbb{F}_2^n \setminus \{0_n, 1_n\}$ is $\sqrt{\frac{2^n}{2^n-2}\binom{n}{k}}$. The maximum being at least equal to the average, the expression from Property 1 gives the upper bound on $\mathsf{M}_{k,n}$.

Then we prove the alternative expression of NL_k for WPB functions. We rewrite $\mathcal{W}_{k,a}(f)$, for $a \in \mathbb{F}_2^n$:

$$\begin{aligned}
\mathcal{W}_{k,a}(f) &= \sum_{x\in\mathsf{E}_{k,n}} (-1)^{f(x)+ax} = \sum_{\substack{x\in\mathsf{E}_{k,n}\\ ax=0}} (-1)^{f(x)} - \sum_{\substack{x\in\mathsf{E}_{k,n}\\ ax=1}} (-1)^{f(x)},\\
&= \sum_{x\in\mathsf{E}_{k,n}} (-1)^{f(x)} - 2\sum_{\substack{x\in\mathsf{E}_{k,n}\\ ax=1}} (-1)^{f(x)} = \mathcal{W}_{k,0_n}(f) - 2\sum_{\substack{x\in\mathsf{E}_{k,n}\\ ax=1}} (-1)^{f(x)},\\
&= -2\sum_{\substack{x\in\mathsf{E}_{k,n}\\ ax=1}} (-1)^{f(x)}.
\end{aligned}$$

Replacing $\mathcal{W}_{k,a}(f)$ by $-2\sum_{\substack{x\in\mathsf{E}_{k,n}\\ ax=1}} (-1)^{f(x)}$ in the expression from Property 1 gives the final expression.

□

5.2 Weightwise nonlinearity distribution

In this part we introduce the notion of distribution of the NL_k of WPB functions which provides us a more global overview over the quantities $\mu_{k,n}$ and $\mathsf{M}_{k,n}$ and the background for the algorithms we use in the following experimental part.

Definition 10 (Nonlinearity on the slice distribution). *Let $m \in \mathbb{N}^*$, $n = 2^m$ and $k \in [1, n-1]$. The weightwise nonlinearity distribution $\mathfrak{W}_{k,n}$ is a discrete probability distribution describing the probability of getting a certain nonlinearity on the slice $\mathsf{E}_{k,n}$ by taking a random WPB function, namely for any $x \in \mathbb{N}$*

$$p_{\mathfrak{W}_{k,n}}(x) = \frac{|\{f \in \mathcal{WPB}_m \colon \mathsf{NL}_k(f) = x\}|}{|\mathcal{WPB}_m|}.$$

Definition 11 (Global weightwise nonlinearity distribution). *Let $m \in \mathbb{N}^*$, $n = 2^m$. The global weightwise nonlinearity distribution $\mathfrak{W}_n$ is a discrete probability distribution describing the probability of getting a certain value of* GWNL *by taking a random WPB function, namely for any $x \in \mathbb{N}$*

$$p_{\mathfrak{W}_n}(x) = \frac{|\{f \in \mathcal{WPB}_m \colon \mathsf{GWNL}(f) = x\}|}{|\mathcal{WPB}_m|}.$$

Therefore, we naturally obtain alternative definitions of minimum and maximum weightwise nonlinearity of WPB functions:

$$\mu_{k,n} = \min_{a \in \mathbb{N}}[p_{\mathfrak{W}_{k,n}}(a) \neq 0], \quad \text{and} \quad \mathsf{M}_{k,n} = \max_{a \in \mathbb{N}}[p_{\mathfrak{W}_{k,n}}(a) \neq 0],$$

and

$$\mu_n = \min_{a \in \mathbb{N}}[p_{\mathfrak{W}_n}(a) \neq 0], \quad \text{and} \quad \mathsf{M}_n = \max_{a \in \mathbb{N}}[p_{\mathfrak{W}_n}(a) \neq 0].$$

This implies that investigating the distribution provides information also on the minimum and maximum weightwise nonlinearity.

In this part we discuss the experimental computation of the distribution via exploiting its alternative definition as minimal distance of the evaluation vector from a spherically punctured Reed Muller code. Namely, for the purpose of studying $\mathfrak{W}_{k,n}$ experimentally Definition 10 is not very convenient, we define therefore a further family of distributions $\mathfrak{D}_{k,n}$ and we prove that we can investigate them instead of $\mathfrak{W}_{k,n}$.

Definition 12 (Distance distribution). *Let $n \in \mathbb{N}^*$ and $k \in [n-1]$. Let $\mathsf{P}_{k,n}$ the spherically punctured Reed Muller code of order 1 of length $\nu = \binom{n}{k}$. The $\mathfrak{D}_{k,n}$ is a discrete probability distribution describing the the distance between $\mathsf{P}_{k,n}$ and $\mathsf{E}_{\lfloor \nu/2 \rfloor, \nu}$, namely for any $x \in \mathbb{N}$*

$$p_{\mathfrak{D}_{k,n}}(x) = \frac{|\left\{v \in \mathsf{E}_{\lfloor \nu/2 \rfloor, \nu} \colon \min_{c \in \mathsf{P}_{k,n}} \mathsf{d_H}(v,c) = x\right\}|}{|\mathsf{E}_{\lfloor \nu/2 \rfloor, \nu}|}.$$

Proposition 10. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and $k \in [n-1]$. Then $\mathfrak{D}_{k,n} = \mathfrak{W}_{k,n}$.*

Proof. By Property 4 given any WPB function f we can compute $\mathsf{NL}_k(f)$ by retrieving the minimal Hamming distance of v_f, *i.e.* the vector of evaluations of f over the slice $\mathsf{E}_{k,n}$, from the spherically punctured Reed Muller code $\mathsf{P}_{k,n}$. In addition, $\{\mathsf{supp}_k(f) \colon f \in \mathcal{WPB}_m\}$ coincides with the family of vectors of length ν and hamming weight $\lfloor \nu/2 \rfloor$. □

To retrieve $\mathfrak{W}_{k,n}$ we should iterate over functions, instead for computing $\mathfrak{D}_{k,n}$ we can directly iterate over the possible supports, *i.e.* over $\mathsf{E}_{\lfloor \nu/2 \rfloor, \nu}$. The latter is more convenient from an algorithmic point of view and Proposition 10 implies that this is equivalent when $n = 2^m$. This implies that in such case Algorithm 1 returns $\mathfrak{W}_{k,n}$.

Algorithm 1

Input: Let $n \in \mathbb{N}$, $0 < k < n$.

Output: $\mathfrak{D}_{k,n}$

1: generate $\mathsf{P}_{k,n}$ the spherically punctured Reed Muller code of order 1 of length $\nu = \binom{n}{k}$
2: compute the distribution $\mathfrak{D}_{k,n}$ of the distance between $\mathsf{P}_{k,n}$ and $\mathsf{E}_{\lfloor \nu/2 \rfloor, \nu}$
3: **return** $\mathfrak{D}_{k,n}$

5.3 Experimental determination of $\mathfrak{D}_{k,n}$ for n up to 8

Although for small values of n an exhaustive search over $\mathsf{E}_{\lfloor \nu/2 \rfloor,\nu}$ is feasible, for larger values a complete examination of the set would require considerable computational power. Therefore, in the following we provide first a description of an exhaustive strategy and subsequently a variant for performing a randomized search. Those algorithms provide us both an intuition and an approximation of the distribution $\mathfrak{D}_{k,n}$, hence of $\mathfrak{W}_{k,n}$ when $n = 2^m$.

We recall that $\{\mathsf{supp}_k(f) \colon f \in \mathcal{WPB}_m\}$ coincides with the family of vectors of length ν and Hamming weight $\lfloor \nu/2 \rfloor$. Notice that a precise convention has to be establish *a priori* if any function has to be retrieved.

For practical reason we will often identify $\mathfrak{D}_{k,n}$ with the vector u whose x-th component is $u_{k,n}(x) = |\left\{v \in \mathsf{E}_{\lfloor \nu/2 \rfloor,\nu} \colon \min_{c \in \mathsf{P}_{k,n}} \mathsf{d}_{\mathsf{H}}(v,c) = x\right\}|$. Moreover, using the upper bound on the maximal weightwise nonlinearity (Proposition 9) we can get a finite length representation of such vector. The technical aspects regarding the actual implementation of Algorithm 1 (deterministic and undeterministic) will be discuss in a devoted paragraph at the end of the section. Instead, we discuss here some results on the distributions. When $\binom{\nu}{\lfloor \nu/2 \rfloor}$ is too large, the distribution of the distance can be estimated performing the second step as a random sampling, since for a sufficiently large sample a good approximation can be expected. However, this does not guarantee to retrieve the exact distribution neither the actual value of $\mathsf{M}_{k,n}$, but a lower bound on this quantity. Indeed, running the algorithm for various n we observed that the distribution has a specific trend, according to whom the probability of randomly hitting a function with weightwise nonlinearity $\mathsf{M}_{k,n}$ is actually very low.

The distributions computed are displayed by Figures 1, 2, 3 for $n \in [4,7]$, and 4,5, 6 for $n = 8$. The figures in orange correspond to an exhaustive determination (Algorithm 2) and the blue ones to a random determination (Algorithm 3). Only the distributions for $n = 4$ and $n = 8$ correspond to WPB functions, the others allow to illustrate the trend of these distributions when n increases.

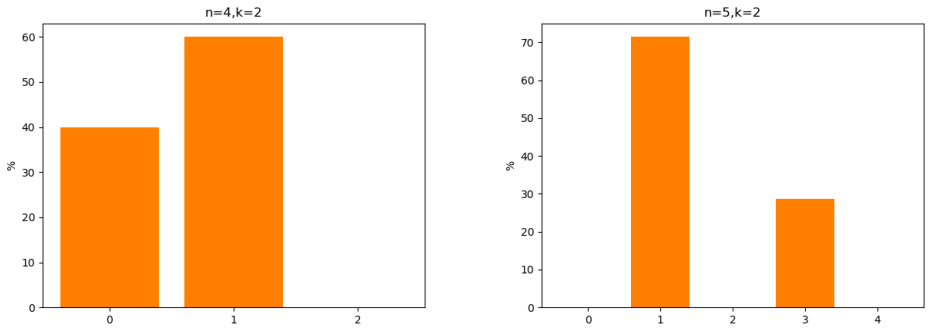


Fig. 1. From left to right: $\mathfrak{D}_{2,4}$ and $\mathfrak{D}_{2,5}$

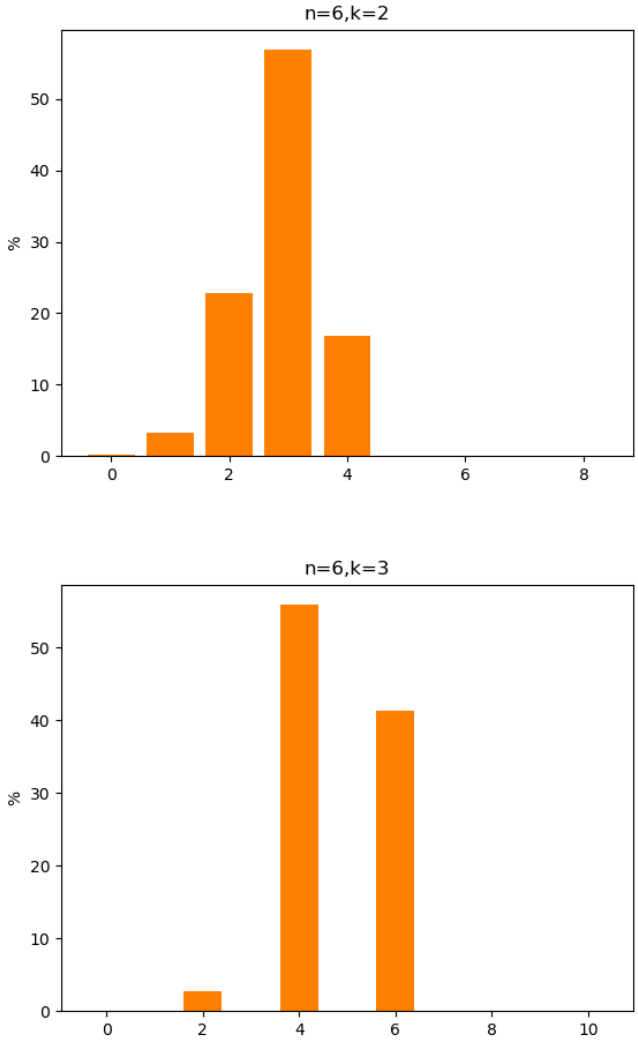


Fig. 2. From top to bottom: $\mathfrak{D}_{2,6}$ and $\mathfrak{D}_{3,6}$

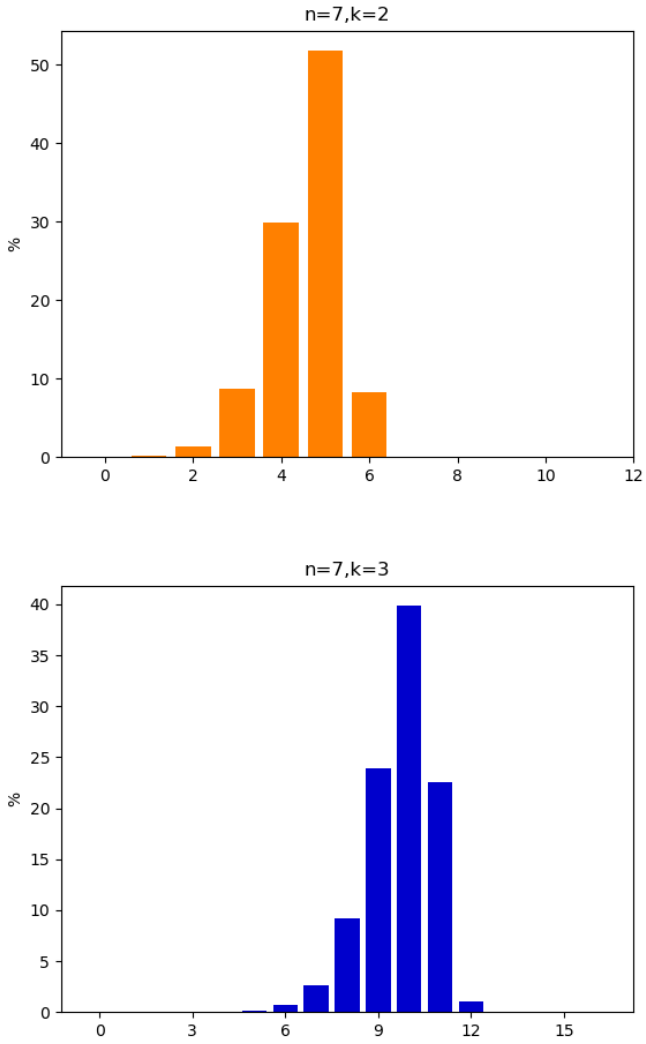
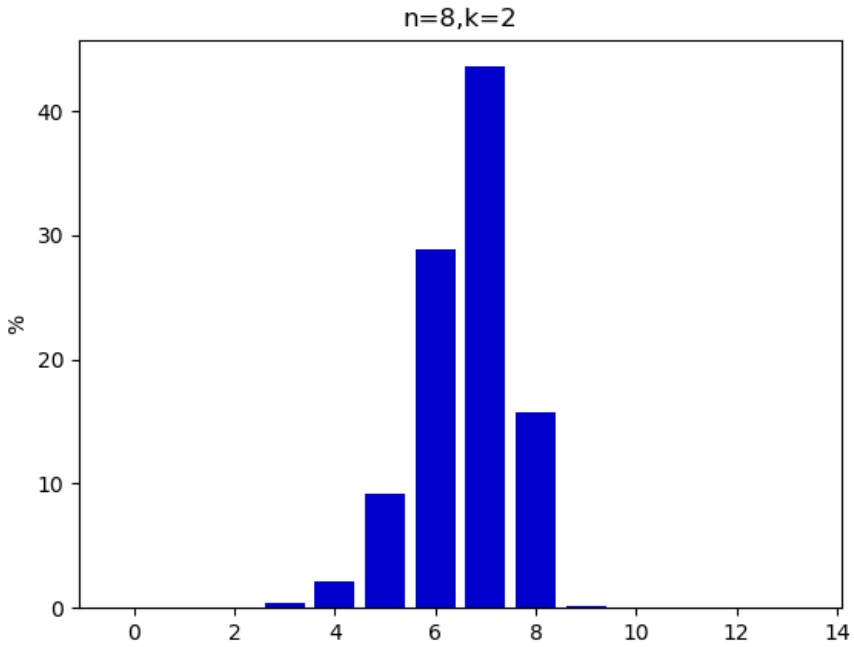
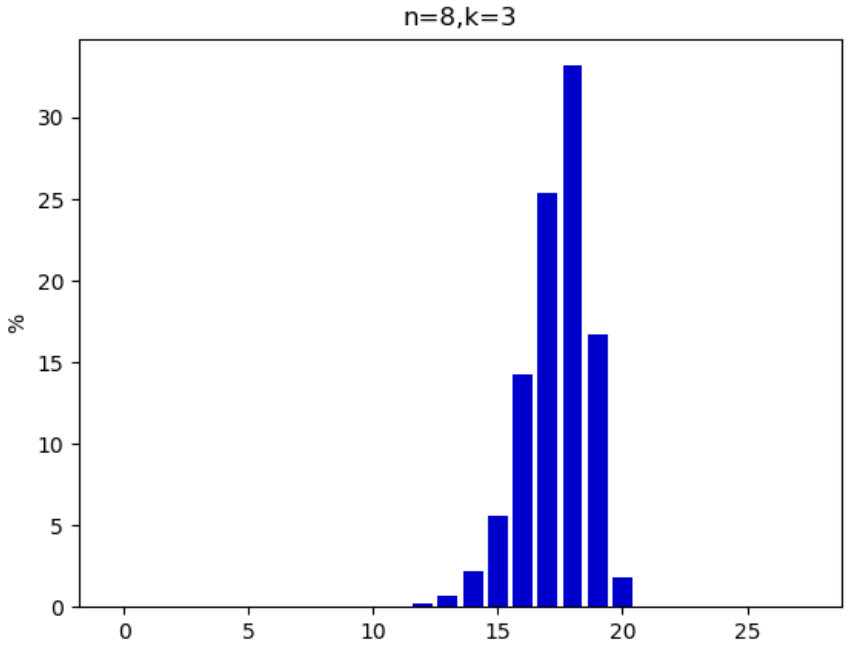


Fig. 3. From top to bottom: $\mathfrak{D}_{2,7}$ and approximation of $\mathfrak{D}_{3,7}$ via random sampling, sample size $1048576 = 2^{20}$, $|\mathsf{E}_{\lfloor \nu/2 \rfloor,\nu}| \approx 2^{32}$.



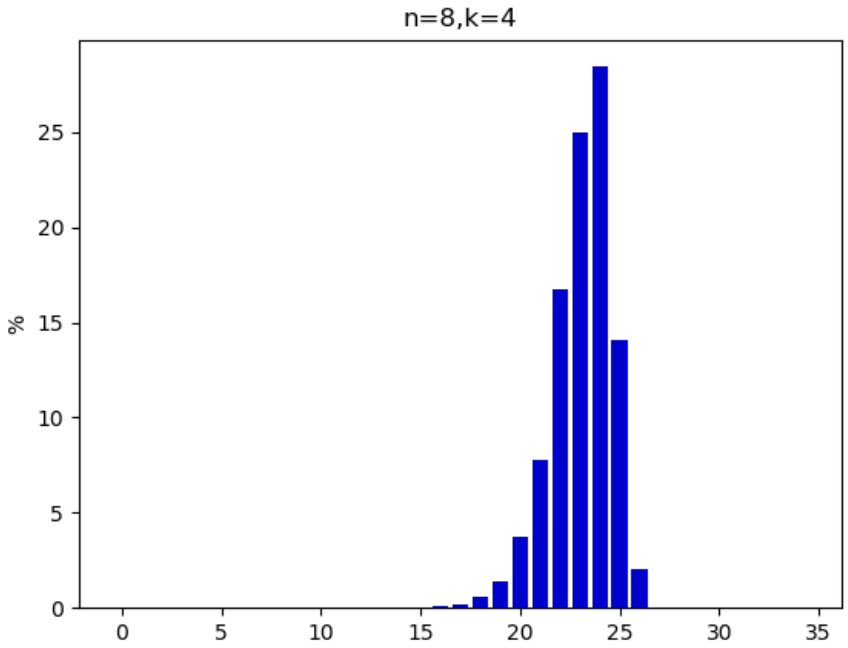
x	1	2	3	4	5	6	7	8	9
$u_{2,8}(x)$	3	40	477	2627	11257	35304	53323	19220	149
$p_{\mathfrak{D}'_{2,8}}(x)$	0.002%	0.033%	0.390%	2.146%	9.197%	28.843%	43.565%	15.703%	0.122%

Fig. 4. Approximation of $\mathfrak{D}_{2,8}$ via random sampling. We denote $u_{2,8}(x) = |\{v\colon \min_{c\in \mathsf{P}_{2,8}} \mathsf{d}_{\mathsf{H}}(v,c) = x\}|$, and the sample size is $\sum_{x\in\mathbb{N}} u(x) = 122400 \approx 2^{17}$, $|\mathsf{E}_{\nu/2,\nu}| \approx 2^{25}$.



x	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$u_{3,8}(x)$	6	12	62	194	913	2684	9051	22907	58206	103799	135783	68319	7240	24
$p_{\mathfrak{D}'_{3,8}}(x)$	0.001%	0.003%	0.015%	0.047%	0.223%	0.656%	2.212%	5.598%	14.224%	25.366%	33.183%	16.696%	1.769%	0.006%

Fig. 5. Approximation of $\mathfrak{D}_{3,8}$ via random sampling. We denote $u_{3,8}(x) = |\{v\colon \min_{c\in \mathsf{P}_{3,8}} \mathsf{d}_{\mathsf{H}}(v,c) = x\}|$, and the sample size is $\sum_{x\in\mathbb{N}} u(x) = 409200 \approx 2^{19}$, $|\mathsf{E}_{\lfloor \nu/2 \rfloor,\nu}| \approx 2^{53}$.



x	8	9	10	11	12	13	14	15	16	17
$u_{4,8}(x)$	1	0	0	2	10	35	180	554	2202	5714
$p_{\mathfrak{D}'_{4,8}}(x)$	0.000%	0.000%	0.000%	0.000%	0.000%	0.001%	0.005%	0.016%	0.063%	0.164%

x	18	19	20	21	22	23	24	25	26	27
$u_{4,8}(x)$	19455	47168	130439	270098	582065	868341	988400	488180	71482	778
$p_{\mathfrak{D}'_{4,8}}(x)$	0.560%	1.357%	3.754%	7.772%	16.750%	24.987%	28.442%	14.048%	2.057%	0.022%

Fig. 6. Approximation of $\mathfrak{D}_{4,8}$ via random sampling. We denote $u_{4,8}(x) = |\{v\colon \min_{c\in\mathsf{P}_{4,8}} \mathsf{d}_{\mathsf{H}}(v,c) = x\}|$, and the sample size is $\sum_{x\in\mathbb{N}} u(x) = 3475104 \approx 2^{22}$, $|\mathsf{E}_{\lfloor \nu/2 \rfloor,\nu}| \approx 2^{67}$.

We list the values and bounds on $\mathsf{M}_{k,n}$ we obtained with the experiments in Table 3. More precisely, when n is not a power of 2 we denote $\mathsf{M}_{k,n} = \max_{a\in\mathbb{N}}[p_{\mathfrak{D}_{k,n}}(a) \neq 0]$, and we denote $\mathsf{M}^*_{k,n}$ the maximal value obtained with a non-deterministic algorithm (since $\mathsf{M}^*_{k,n} \leq \mathsf{M}_{k,n}$ and the WPB functions reaching the highest NL_k could be too scarce to appear in the search). The lower bounds on $\mathsf{M}_{k,n}$ come from Proposition 8. When n is not a power of two some slices have odd cardinality, then a function is considered balanced on a slice of odd cardinality if and only if its weight is $(\nu \pm 1)/2$. The arguments leading to the upper bound given in Proposition 8 also apply in this case, the only difference is that $\nu/2$ on the right size becomes $\lfloor \nu/2 \rfloor$. The upper bound $\mathsf{M}_{k,n}$ comes from Proposition 9 when n is a power of 2 and from Property 2 otherwise. These experiments tend to show that the value of $\mathsf{M}_{k,n}$ is closer to the upper bound than the lower bound, but not reaching it. The pictures displayed in this section illustrate how scarce the WPB functions with low or high NL_k are. For example, for $n = 8$ and $k = 3$ no functions will null NL_3 are found experimentally (their existence is proven in Section 4), neither a function with $\mathsf{NL}_3 = 22$ as built in [LM19].

n	k	$\mathsf{M}_{k,n}$	lower bound	upper bound	Step 2
4	2	1	1	1	exhaustive
5	2, 3	3	1	3	exhaustive
6	2, 4	4	2	5	exhaustive
6	3	6	4	7	exhaustive
7	2, 5	6	4	8	exhaustive
n	k	$\mathsf{M}^*_{k,n}$	lower bound	upper bound	Step 2
7	3, 4	13*	9	14	random
8	2, 6	9*	6	11	random
8	3, 5	21*	16	24	random
8	4	27*	21	30	random

Table 3. Values and bounds on $\mathsf{M}_{k,n}$ for $n \in [4, 8]$ given by the experiment. $\mathsf{M}_{k,n}$ refers to the exact quantity whereas $\mathsf{M}^*_{k,n}$ refers to the maximum value obtained by a non-deterministic process.

Technical algorithmic aspects The source code of our experiments is available at `https://github.com/agnesegini/NL-WPB`. This has been produced by using `sagemath` [The17] in association with some `python`'s modules, later specified.

While generating $\mathsf{P}_{k,n}$ is quite efficient for the considered value of n, we observed that the bottleneck of Algorithm 1 resides in the second step. Indeed, a naive implementation faces time and memory barriers even for small n. Nevertheless, the integrated usage of tools such as *data parallelism*, *iterators* and *randomization*, allowed us to analyses larger sets. Specifically, python's iterators are objects implementing a prescribed iterator protocol and they are highly convenient in this context because the do not allocate in memory the full list of objects. For instance, since $\mathsf{E}_{\lfloor \nu/2 \rfloor, \nu}$ quickly becomes very large increasing n and k, we encoded this set as iterator. For this we used the `itertool` package. Moreover, an iterator can be used also for getting a compact representation of $\mathsf{P}_{k,n}$: given any generator matrix $\mathbf{M}$ the full code can be produce as the set of $\mathbf{v} \cdot \mathbf{M}$, iterating over $\mathbf{v}$. Iterators are also parallelism-friendly. Namely, the execution of a function over multiple input values can be distributed across processes, by using tools such as the `map` method of a `Pool`

object from the multiprocessing module `multiprocessing`; and this input data can be given via an iterator. This implies we can compute the distance between several vectors concurrently, scaling the running time of Step 2. Therefore, by using these two ingredients we were able to compute exhaustively $\mathfrak{D}_{k,n}$ for $n \leq 7$. We summarized our exhaustive method in Algorithm 2, denoting in pseudo-code by `it-get` the operation of getting an iterator of the input set and by par-for the fact that the loop is performed in parallel.

Algorithm 2 Exhaustive search distribution

Input: $\mathsf{P}_{k,n}$.
Output: $\mathfrak{D}_{k,n}$.
1: $\mathfrak{D}_{k,n} = \mathbf{0} \in \mathbb{N}^u$, where u is an upper bound for $\mathsf{M}_{k,n}$.
2: $it_\nu = \texttt{it-get}(\mathsf{E}_{\lfloor \nu/2 \rfloor, \nu})$
3: **par-for** $r \leftarrow it_\nu$ **do**
4: $\quad h \leftarrow \min_{c \in \mathsf{P}_{k,n}} \mathsf{d}_{\mathsf{H}}(r, c)$ ▷ We can use an iterator here.
5: $\quad \mathfrak{D}_{k,n}[h] = \mathfrak{D}_{k,n}[h] + 1$
6: **end for**
7: **return** $\mathfrak{D}_{k,n}$

The forementioned optimizations are not sufficient however to determine the distribution for $n = 8$. Thus, in order to estimate $\mathfrak{D}_{k,n}$ we modified the algorithm by substituting $\mathsf{E}_{\lfloor \nu/2 \rfloor, \nu}$ with a uniform randomized sample. This is displayed by Algorithm 3, where $\texttt{gen}_\pi(a, b)$ is a function that returns a random element of $\mathsf{E}_{a,b}$. Notice that, when using random generation in parallel within a `Pool`, it is important to control the source of randomness used for being sure that all processes are independent. The output of this algorithm is a distribution $\mathfrak{D}'_{k,n}$ that is an approximation of $\mathfrak{D}_{k,n}$.

Algorithm 3 Randomized search distribution

Input: $\mathsf{P}_{k,n}$, s sample size.
Output: $\mathfrak{D}'_{k,n}$.
1: $\mathfrak{D}'_{k,n} = \mathbf{0} \in \mathbb{N}^u$, where u is an upper bound for $\mathsf{M}_{k,n}$.
2: **par-for** $i \in \{1, \ldots, s\}$ **do**
3: $\quad r \leftarrow \texttt{gen}_{\pi_i}(\lfloor \nu/2 \rfloor, \nu)$
4: $\quad h \leftarrow \min_{c \in \mathsf{P}_{k,n}} \mathsf{d}_{\mathsf{H}}(r, c)$ ▷ We can use an iterator here.
5: $\quad \mathfrak{D}'_{k,n}[h] = \mathfrak{D}'_{k,n}[h] + 1$
6: **end for**
7: **return** $\mathfrak{D}'_{k,n}$

6 Constructions with prescribed weightwise nonlinearities

In this section we study a general construction of WPB functions for all $n \geq 8$ with non null weightwise nonlinearity. The main idea is to build functions by modifying the support of linear functions on each slice. First, modifying enough the weightwise support guarantees the balancedness on each slice. Second, the modification is light enough to ensure that the initial linear function is still the closest one, which directly

gives the weightwise nonlinearity of the built functions. This strategy allows to build a relatively large corpus of WPB function with the same NL_k and GWNL.

First we give a general construction of WPB functions with bounded NL_k (Construction 1). Then, we highlight a sub-part of the functions given by this construction, determining the exact weightwise nonlinearities of these functions and the size of their corpus, it corresponds to Construction 2. Finally, we summarize the NL_k values of these functions and compare it to the other known constructions in tables for $n = 8$ and 16.

Construction 1

Input: Let $m \in \mathbb{N}$, $m \geq 3$ and $n = 2^m$.

Output: f an n-variable Boolean function.

1: Initiate the support of f to $\{1_n\}$.
2: **for** $k \leftarrow 1$ to $n-1$ **do**
3: choose ℓ in $[n-1]$ such that $|\mathsf{K}_k(\ell,n)| \leq \mathsf{d}_{k,n}$ where $\mathsf{d}_{k,n}$ is the minimal distance of $\mathsf{P}_{k,n}$
4: choose an homogeneous linear function g with ℓ monomials in its ANF
5: $t = \lfloor \frac{\mathsf{d}_{k,n} - |\mathsf{K}_k(\ell,n)|}{4} \rfloor$
6: **if** $\mathsf{K}_k(\ell,n) \geq 0$ **then**
7: add $\mathsf{supp}_k(g)$ minus t elements to $\mathsf{supp}(f)$ and $\mathsf{K}_k(\ell,n)/2 + t$ elements from $\mathsf{supp}_k(g+1)$,
8: **else**
9: add $\mathsf{supp}_k(g+1)$ minus t elements to $\mathsf{supp}(f)$ and $-(\mathsf{K}_k(\ell,n))/2 + t$ elements from $\mathsf{supp}_k(g)$.
10: **end if**
11: **end for**
12: **return** f

Theorem 2 (Weightwise perfectly balancedness and NL_k of Construction 1). *Let $m \in \mathbb{N}$, $m \geq 3$ and $n = 2^m$. Any function given by Construction 1 is weightwise perfectly balanced, and with weightwise nonlinearity $\mathsf{NL}_k \geq \frac{\mathsf{d}_{k,n}-3}{2}$ for $k \in [n-1]$.*

Proof. First, we prove that such functions are WPB. We show that for all $k \in [n-1]$ f is balanced on the corresponding slice. Using Proposition 2, the Hamming weight of the selected function g is $(\binom{n}{k} - \mathsf{K}_k(\ell,n))/2$ on $\mathsf{E}_{k,n}$, hence $|\mathsf{K}_k(\ell,n)/2|$ elements from this slice need to be added to reach the balancedness if $\mathsf{K}_k(\ell,n) \geq 0$ (and withdrawn if $\mathsf{K}_k(\ell,n)$ is negative). We focus on the case $\mathsf{K}_k(\ell,n) \geq 0$ (the other one follows with similar arguments), $\mathsf{supp}_k(f)$ is formed with $|\mathsf{supp}_k(g)| - t$ elements from $\mathsf{supp}_k(g)$ and $\mathsf{K}_k(\ell,n)/2 + t$ from $\mathsf{supp}_k(g+1)$. We verify that both $|\mathsf{supp}_k(g)| - t$ and $|\mathsf{supp}_k(g+1)| - \mathsf{K}_k(\ell,n)/2 - t$ are positive integers:

$$|\mathsf{supp}_k(g)| - t = \frac{\binom{n}{k} - \mathsf{K}_k(\ell,n)}{2} - \lfloor \frac{\mathsf{d}_{k,n} - |\mathsf{K}_k(\ell,n)|}{4} \rfloor \geq \frac{2\binom{n}{k} - \mathsf{K}_k(\ell,n) - \mathsf{d}_{k,n}}{4}, \text{and}$$

$$|\mathsf{supp}_k(g+1)| - \frac{\mathsf{K}_k(\ell,n)}{2} - t = \frac{\binom{n}{k} + \mathsf{K}_k(\ell,n)}{2} - \frac{\mathsf{K}_k(\ell,n)}{2} - \lfloor \frac{\mathsf{d}_{k,n} - |\mathsf{K}_k(\ell,n)|}{4} \rfloor \geq \frac{2\binom{n}{k} - \mathsf{d}_{k,n} - \mathsf{K}_k(\ell,n)}{4},$$

and since by definition both $\mathsf{K}_k(\ell,n)$ and $\mathsf{d}_{k,n}$ are not greater than $\binom{n}{k}$ both quantities are positive.

Since both quantities are positive it allows to build $\mathsf{supp}_k(f)$, with Hamming weight:

$$\frac{\binom{n}{k} - \mathsf{K}_k(\ell,n)}{2} - t + \frac{\mathsf{K}_k(\ell,n)}{2} + t = \frac{\binom{n}{k}}{2} = \frac{|\mathsf{E}_{k,n}|}{2}.$$

It concludes on the balancedness on all slices with $k \in [n-1]$, and since $1_n \in \mathsf{supp}(f)$ and $0_n \notin \mathsf{supp}(f)$, f is a WPB function.

We finish the proof with the statement on the weightwise nonlinearity. By construction, on the slice k f is at distance $2t+|\mathsf{K}_k(\ell,n)|/2$ from g (if $\mathsf{K}_k(\ell,n)$ is positive) or from $g+1$. Since $t = \lfloor(\mathsf{d}_{k,n}-|\mathsf{K}_k(\ell,n)|)/4\rfloor$:

$$2t + \frac{|\mathsf{K}_k(\ell,n)|}{2} \leq 2\left(\frac{\mathsf{d}_{k,n} - |\mathsf{K}_k(\ell,n)|}{4}\right) + \frac{|\mathsf{K}_k(\ell,n)|}{2} \leq \frac{\mathsf{d}_{k,n}}{2},$$

f cannot be closer to another affine function restricted to $\mathsf{E}_{k,n}$ hence $\mathsf{NL}_k(f)$ is given by this distance. Finally, since

$$2t + \frac{|\mathsf{K}_k(\ell,n)|}{2} \geq 2\left(\frac{\mathsf{d}_{k,n} - |\mathsf{K}_k(\ell,n)|}{4} - \frac{3}{4}\right) + \frac{|\mathsf{K}_k(\ell,n)|}{2} \geq \frac{\mathsf{d}_{k,n} - 3}{2},$$

we can conclude $\mathsf{NL}_k(f) \geq (\mathsf{d}_{k,n} - 3)/2$.

□

To highlight the existence of such WPB functions with prescribed weightwise nonlinearity, we give the following construction, which is a particular sub-case.

Construction 2

Input: Let $m \in \mathbb{N}$, $m \geq 3$ and $n = 2^m$.

Output: f an n-variable Boolean function.

1: Initiate the support of f to $\{1_n\}$.
2: **for** $k \leftarrow 1$ to $n-1$ **do**
3: **if** $k \neq n/2$ **then**
4: $\ell = n/2$
5: **else**
6: $\ell = 1$
7: **end if**
8: choose an homogeneous linear function g with ℓ monomials in its ANF
9: $t = \lfloor \frac{\mathsf{d}_{k,n} - |\mathsf{K}_k(\ell,n)|}{4} \rfloor$ where $\mathsf{d}_{k,n}$ is the minimal distance of $\mathsf{P}_{k,n}$,
10: **if** $\mathsf{K}_k(\ell,n) \geq 0$ **then**
11: add $\mathsf{supp}_k(g)$ minus t elements to $\mathsf{supp}(f)$ and $\mathsf{K}_k(\ell,n)/2 + t$ elements from $\mathsf{supp}_k(g+1)$,
12: **else**
13: add $\mathsf{supp}_k(g+1)$ minus t elements to $\mathsf{supp}(f)$ and $-(\mathsf{K}_k(\ell,n))/2 + t$ elements from $\mathsf{supp}_k(g)$.
14: **end if**
15: **end for**
16: **return** f

Corollary 1 (Weightwise perfectly balancedness and NL_k of Construction 2). *Let $m \in \mathbb{N}$, $m \geq 3$ and $n = 2^m$. Any function given by Construction 2 is weightwise perfectly balanced, and with weightwise*

nonlinearity for $k \in [n/2]$:

$$\mathsf{NL}_k = \mathsf{NL}_{n-k} = \begin{cases} \frac{\binom{n-1}{k-1}-1}{2} & \text{if } k \text{ is odd,} \\ \frac{\binom{n-1}{k-1}-3}{2} & \text{if } k \text{ is even, } k \neq n/2, \\ \binom{n-2}{n/2} - 1 & \text{if } k = n/2. \end{cases}$$

Proof. First, we recall that $|\mathsf{K}_k(\ell, n)| = |\mathsf{K}_{n-k}(\ell, n)|$ (Property 5) and $\mathsf{P}_{k,n}$ and $\mathsf{P}_{n-k,n}$ have the same parameters (Property 3), hence we can restrict our study to the case $k \in [n/2]$. Then, we show that this construction gives WPB functions since it is a sub-case of Construction 1 which gives only WPB functions from Theorem 2. The only difference with Construction 1 is the particular choices of ℓ, accordingly it is sufficient to prove that for each k the chosen ℓ (denoted ℓ_k) verifies $|\mathsf{K}_k(\ell_k, n)| \leq \mathsf{d}_{k,n}$. Using Property 5 and 6 on one side and Property 3 on the other side, for $k \in [n/2]$ we obtain:

$$|\mathsf{K}_k(\ell_k, n)| = \begin{cases} \mathsf{K}_k(n/2, n) = 0 & \text{if } k \text{ is odd,} \\ |\mathsf{K}_k(n/2, n)| = \binom{n/2}{k/2} & \text{if } k \text{ is even, } k < \frac{n}{2}, \\ \mathsf{K}_{n/2}(1, n) = 0 & \text{if } k = n/2, \end{cases} \text{ and } \mathsf{d}_{k,n} = \begin{cases} \binom{n-1}{k-1} & \text{if } k \text{ is odd,} \\ \binom{n-1}{k-1} & \text{if } k \text{ is even, } k < \frac{n}{2}, \\ 2\binom{n-2}{n/2} & \text{if } k = n/2. \end{cases}$$

Since for k even $k < n/2$, we have $n/2 < n-1$, $k/2 < k-1$ and $k-1-k/2 < n-1-n/2$ Pascal's formula guaranties $\binom{n/2}{k/2} \leq \binom{n-1}{k-1}$. Therefore, for all cases $|\mathsf{K}_k(\ell_k, n)| \leq \mathsf{d}_{k,n}$, hence Theorem 2 applies and the constructed functions are WPB.

By construction, the NL_k of the functions is given by $2t + |\mathsf{K}_k(\ell_k, n)|/2$ on each slice, where $t = \lfloor (\mathsf{d}_{k,n} - |\mathsf{K}_k(\ell_k, n)|)/4 \rfloor$. In order to give the exact value we study the congruence modulus 4 or 2 of the binomial coefficients appearing in the expression of the different t. Concretely we use that for $n = 2^m$ and $k \in [n/2]$:

$$\binom{n-1}{k-1} = 1 \pmod 4 \quad \text{for } k \text{ odd, and} \quad \binom{n-1}{k-1} = 3 \pmod 4 \quad \text{for } k \text{ even,} \tag{2}$$

$$\binom{n/2}{k/2} = 0 \pmod 4 \quad \text{for } k \text{ even } k < n/2, \tag{3}$$

$$\binom{n-2}{n/2} = 1 \pmod 2. \tag{4}$$

Equation 3 comes from Property 8 since n is a power of 2 greater than 4. Then, since $\binom{2^m}{k} = 0 \pmod 4$ for $k \in [2^{m-1}]$ by Property 8 and $\binom{2^m-1}{0} = 1 = 1 \pmod 4$ using Pascal's formula repetitively gives $\binom{2^m-1}{2k'} = 1 \pmod 4$ and $\binom{2^m-1}{2k'+1} = 3 \pmod 4$ for $k' \in [0, n/4-1]$, it proves Equation 2. Equation 4 is a consequence of Lucas's theorem (Property 7), writing $n-2$ and $n/2$ in binary only the coefficient for the power $m-1$ is equal to 1 in the expansion of $n/2 = 2^{m-1}$ and the same coefficient for $n-2$ is also equal to 1 (since $n-2 = 2^m - 2 = \sum_{i \in [m-1]} 2^i$). Therefore Property 7 allows to conclude that the binomial coefficient is odd.

It allows to conclude on the exact value of NL_k for the three different cases:

– For k odd,

$$2t + \frac{|\mathsf{K}_k(n/2, n)|}{2} = 2t = 2\lfloor \frac{\binom{n-1}{k-1}}{4} \rfloor = \frac{\binom{n-1}{k-1} - 1}{2}.$$

– for k even $k < n/2$,

$$2t+\frac{|\mathsf{K}_k(n/2,n)|}{2} = 2t+\frac{\binom{n/2}{k/2}}{2} = 2\lfloor\frac{\binom{n-1}{k-1}-\binom{n/2}{k/2}}{4}\rfloor+\frac{\binom{n/2}{k/2}}{2} = \frac{\binom{n-1}{k-1}-\binom{n/2}{k/2}-3}{2}+\frac{\binom{n/2}{k/2}}{2} = \frac{\binom{n-1}{k-1}-3}{2}.$$

– for $k = n/2$,

$$2t + \frac{|\mathsf{K}_k(1,n)|}{2} = 2t = 2\lfloor\frac{2\binom{n-2}{n/2}}{4}\rfloor = 2\frac{\binom{n-2}{n/2}-1}{2} = \binom{n-2}{n/2} - 1.$$

□

In the following we show how many different functions can be built from Construction 2. It shows that this construction provides a large corpus of WPB functions.

Proposition 11 (Number of different functions given by Construction 2). *Let $m \in \mathbb{N}$, $m \geq 3$ and $n = 2^m$. Construction 2 produces C_n different WPB functions, where*

$$\mathsf{C}_n = n\binom{\binom{n}{n/2}/2}{(\binom{n-2}{n/2}-1)/2}^2 \prod_{\substack{k\in[n/2-1]\\ k\ odd}} \binom{n}{n/2}^2 \mathsf{A}_{k,n} \prod_{\substack{k\in[n/2-1]\\ k\ even}} \frac{\binom{n}{n/2}^2}{4}\mathsf{B}_{k,n},$$

where

$$\mathsf{A}_{k,n} = \binom{\binom{n}{k}/2}{(\binom{n-1}{k-1}-1)/4}^4, \text{ and } \mathsf{B}_{k,n} = \binom{(\binom{n}{k}-\binom{n/2}{k/2})/2}{(\binom{n-1}{k-1}-\binom{n/2}{k/2}-3)/4}^2 \binom{(\binom{n}{k}+\binom{n/2}{k/2})/2}{(\binom{n-1}{k-1}+\binom{n/2}{k/2}-3)/4}^2.$$

Proof. The number of different WPB functions given by Construction 2 is the product $\prod_{k=1}^{n-1} N_k$ of the number of different balanced sub-parts N_k obtainable for each slice $\mathsf{E}_{k,n}$. As recalled in Corollary 1's proof the codes $\mathsf{P}_{k,n}$ and $\mathsf{P}_{n-k,n}$ have the same properties and $|\mathsf{K}_k(x,n)| = |\mathsf{K}_{n-k}(x,n)|$, therefore by construction $N_{n-k} = N_k$, and in the following we focus only on the cases $k \in [n/2]$.

For the slice k, when a linear function g of ℓ_k terms is chosen, by construction $(\binom{n}{k} - |\mathsf{K}_k(\ell_k,n)|)/2 - t$ elements over $(\binom{n}{k} - |\mathsf{K}_k(\ell_k,n)|)/2$ are chosen from the support and $(|\mathsf{K}_k(\ell_k,n)|)/2 + t$ elements over $(\binom{n}{k} + |\mathsf{K}_k(\ell_k,n)|)/2$ from the co-support of the affine function g or $g+1$ to build this sub-part. Using Corollary 1 and Property 3 each choice gives a function (on $\mathsf{E}_{k,n}$) at distance strictly lower than $\mathsf{d}_{k,n}/2$ therefore they cannot be built from another linear function distinct over $\mathsf{E}_{k,n}$.

The remaining point is to determine the number of linear functions of ℓ_k monomials distinct over $\mathsf{E}_{k,n}$. Note that there are 2^{n+1} affine functions in n variables but $\mathsf{P}_{k,n}$ has dimension n only, then different affine functions over $\mathbb{F}_2^n$ have the same restriction over $\mathsf{E}_{k,n}$. On $\mathsf{E}_{k,n}$ the sum $\sum_{i=1}^n x_i$ equals 1 for k odd and 0 for k even, hence the affine functions $\sum_{i\in I} x_i$ and $\sum_{i\in[n]\setminus I} x_i + k \mod 2$ have the same truth table on $\mathsf{E}_{k,n}$. We do a disjunction of cases for the number of distinct linear functions depending on the slices.

– For k odd, $\ell_k = n/2$, in this case for each set I' of $n/2$ variables, $\sum_{i\in I'} x_i$ coincide with $1+\sum_{i\in[n]\setminus I'} x_i$ hence the $\binom{n}{n/2}$ choices for the linear function g are different.
– For k even, $k \neq n/2$, $\ell_k = n/2$ and in this case for I' a set of $n/2$ variables $\sum_{i\in I'} x_i$ coincide with $\sum_{i\in[n]\setminus I'} x_i$ and since $|[n]\setminus I'| = n/2$, only $\binom{n}{n/2}/2$ choices of linear functions are distinct on this slice.
– For $k = n/2$, $\ell_k = 1$, in this case x_j coincides with $\sum_{i\in[n]\setminus j} x_i$ hence the n choices lead to distinct functions on the slice.

Doing the product for $k \in [n-1]$ combining the number of linear functions distinct on each slice and the number of functions reachable from each one gives the final result.

□

Construction 2 allows to build a large family of WPB functions with non-trivial nonlinearity on the slices. We illustrate it by displaying the NL_k and GWNL of these functions and the ones of constructions from other works in Table 4 for 8 variables and Table 5 for 16 variables. The values for the minima come from Table 1 in Section 4, the (observed) averages and modes for $n = 8$ come from the distributions observed in the experiment of Section 5.3, and the upper bounds come from Proposition 9 in Section 5.1. The weightwise nonlinearities for Construction 2 are given by Corollary 1, and the values for the other constructions come from the article introducing them, and [Su21] for the WPB function presented in [CMR17]. The corpus size is rarely determined for the different constructions, we list the few ones for which it is determined. For Construction 2 the corpus size is given by Proposition 11, it corresponds to $(2^m)!$ for f_m in [MS21] and $2^{\psi_n - 2}$ for the first construction in [LM19] where ψ_n is the number of different orbits in $\mathbb{F}_2^n$. Most of the known constructions correspond to small corpus sizes or sporadic cases, even considering that each built function can correspond to up to 2^{n-1} different WPB functions by adding symmetric functions (see Proposition 1).

The two tables illustrate that the known constructions are far from optimal in term of weightwise nonlinearity, and in the case $n = 8$ even far from the parameters of a WPB function randomly chosen. Construction 2 allows to generate functions with guaranteed nontrivial nonlinearity on each slide and it gives a corpus of WPB function way larger than former approaches.

Construction	NL_2	NL_3	NL_4	GWNL	Corpus
Minimum	1	0	0	2	
f_m [MS21]	2	0	3	7	40320
f_m [MSL21]	2	8	8	28	
Construction 2	2	10	14	38	$\approx 2^{163}$
[CMR17, Su21]	2	12	19	47	
[LS20]	2	12	19	47	
g_m [MS21]	2	14	19	51	
g_m [MSL21]	6	8	26	54	
[LM19]	$\{6, 9\}$	$\{0, 8, 14, 16, 18, 20, 21, 22\}$	$\{19, [22, 27]\}$	$[31, 89]$	2^{32}
Average*	6.61	17.36	23.09	71.02	
Mode*	7	18	24	72	
Upper Bound	11	24	30	100	

Table 4. Weightwise nonlinearities of 8-variable WPB constructions.

Construction	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8	GWNL	Corpus
Minimum	0	0	7	0	0	0	0	14	
Cons-1 [LM19]	≥ 5	≥ 144	≥ 472	≥ 1056	≥ 2184	≥ 1296	≥ 2184	≥ 12498	
Construction 2	6	52	226	682	1500	2502	3002	12938	$\approx 2^{32319}$
[CMR17, Su21]	4	56	350	1288	3108	4774	5539	25763	
Upper Bound	54	268	888	2150	3959	5666	6378	32348	

Table 5. Weightwise nonlinearities of 16-variable WPB constructions.

7 Conclusion and open problems

In this article we presented a general study on the weightwise nonlinearity of WPB functions. First, we studied the $\mu_{k,n}$ and μ_n; we provided a lower and an upper theoretic bounds and we determined the values for small values of m, up to 10. We also considered the relation between weightwise affine functions and WPB functions, showing that all for $n = 2$ all WPB functions are weightwise affine, for $n = 4$ some WPB functions are weightwise affine but no set is included in the other one, and for $n \geq 8$ no WPB function is weightwise affine. Then, we considered the $\mathsf{M}_{k,n}$, M_n and the distribution of the NL_k. We presented theoretic bounds on $\mathsf{M}_{k,n}$ and provided algorithms to compute or estimate the distribution of the weightwise nonlinearity of WPB functions. Using these algorithms, we provided the weightwise nonlinearity distribution of functions balanced on the slices for $n \in [4, 8]$. Finally, we gave two constructions of WPB functions obtained by modifying linear functions on each slice. We proved their WPB property and for one of the family we determined exactly the NL_k for each slice, and the corpus of this large family. We also compared the NL_k and GWNL of these functions to the ones of former constructions and to the average behavior, in 8 and 16 variables.

From this general study we can conclude that most of the known WPB constructions are far from the upper bounds on the $\mathsf{M}_{k,n}$ and M_n, and for small n where we can observe the distribution the NL_k of these construction it is actually low compared to the average. Accordingly, the next step in order to build WPB functions with good cryptographic parameters would be to determine larger corpora of WPB functions, with GWNL higher than the average value. We highlight further open problems that arise from the results of this study.

- **Upper bound on** μ_n. In Section 4 we derive an upper bound on μ_n in Proposition 7 that has the same order as μ_n^2 for the first values of m based on Table 2. Since this bound is obtained by considering particular linear functions over the slices (the ones with only one monomial in their ANF), it would be interesting to consider different linear functions to obtain a better bound with a simple expression.
- **Bounds on** $\mathsf{M}_{k,n}$ **and** $\rho_{k,n}$. In Section 5.1 we derive bounds on $\mathsf{M}_{k,n}$ by adapting the standard techniques to bound the covering radius of a code. We recall that $\mathsf{M}_{k,n} \leq \rho_{k,n}$, but the exact relation between these two quantities is not known. Proving the equality or difference between these quantities could be a step towards better bounds, since the covering radius of punctured Reed-Muller codes is unknown in general.
- **Determining the WPB functions with low** GWNL. In Section 6 the exhibited constructions are built by perturbing linear functions over each slice such that the perturbation is a the limit of the error correction capacity of each code $\mathsf{P}_{k,n}$. Generalizing this approach by considering all affine functions (Construction 1 and using Proposition 1) and all integers p such that $0 \leq p \leq t$ for each slice gives all WPB functions with low GWNL. More precisely, it would provide all WPB functions with GWNL between μ_n and $\sum_{k=1}^{n-1} \lfloor \mathsf{d}_{k,n}/2 \rfloor$. Finding other characterizations of this family and determining its

cardinal could be used to built new constructions with better weightwise nonlinearities or to determine which known constructions are already part of this family. For example, the quantities displayed in Table 4 show that in 8 variables the constructions f_m from [MS21] and from [MSL21] belong to this family.

– **Relations between $\mathcal{WPB}_m$ and $\mathcal{WD}_n^d$.** Last but not least, we find the concept of weightwise degree-d functions appealing, and an interesting corpus to look for Boolean functions with good cryptographic properties. Since the degree of a WPB is not a relevant quantity (adding symmetric functions null in 0 and 1 changes the degree but not the WPB property neither the weightwise nonlinearity) the notion of weightwise degree would be more relevant to study the properties of WPB functions. In Section 4.2, we show that there are no WPB functions in $\mathcal{WD}_n^1$ for $n \geq 8$, it leads to the problem of determining for all m the smallest d such that $\mathcal{WD}_{2^m}^d \cap \mathcal{WPB}_m \neq \emptyset$, or in other words, to determine the smallest weightwise degree allowing to have WPB functions.

8 Acknowledgments

The two authors were supported by the ERC Advanced Grant no. 787390.

References

Ale12. Ahmad M Alenezi. *Integral zeroes of Krawtchouk polynomials*. PhD thesis, Brunel University, School of Information Systems, Computing and Mathematics, 2012.

BP05. An Braeken and Bart Preneel. On the algebraic immunity of symmetric boolean functions. In *Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005, Proceedings*, pages 35–48, 2005.

Bry91. Randal E. Bryant. On the complexity of VLSI implementations and graph representations of boolean functions with application to integer multiplication. *IEEE Trans. Computers*, 40(2):205–213, 1991.

Car04. Claude Carlet. On the degree, nonlinearity, algebraic thickness, and nonnormality of boolean functions, with developments on symmetric functions. *IEEE Trans. Information Theory*, pages 2178–2185, 2004.

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

CL11. Y. Chen and P. Lu. Two classes of symmetric boolean functions with optimum algebraic immunity: Construction and analysis. *IEEE Transactions on Information Theory*, 57(4):2522–2538, April 2011.

CM19. Claude Carlet and Pierrick Méaux. Boolean functions for homomorphic-friendly stream ciphers. *Algebra, Codes and Cryptology*, pages 166–182, 11 2019.

CM21. Claude Carlet and Pierrick Méaux. A complete study of two classes of boolean functions: direct sums of monomials and threshold functions. *IEEE Transactions on Information Theory*, pages 1–1, 2021.

CMR17. Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.*, 2017(3), 2017.

CV05. Anne Canteaut and Marion Videau. Symmetric boolean functions. *IEEE Trans. Information Theory*, pages 2791–2811, 2005.

DK13. Ilya Dumer and Olga Kapralova. Spherically punctured biorthogonal codes. *IEEE Trans. Information Theory*, 59(9):6010–6017, 2013.

DK17. Ilya Dumer and Olga Kapralova. Spherically punctured reed-muller codes. *IEEE Trans. Information Theory*, 63(5):2773–2780, 2017.

DMS06. Deepak Kumar Dalai, Subhamoy Maitra, and Sumanta Sarkar. Basic theory in construction of boolean functions with maximum possible annihilator immunity. *Designs, Codes and Cryptography*, 2006.

KL96. Ilia Krasikov and Simon Litsyn. On integral zeros of krawtchouk polynomials. *J. Comb. Theory, Ser. A*, 74(1):71–99, 1996.

LM19. Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Des. Codes Cryptogr.*, 87(8):1797–1813, 2019.

LS20. Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. *Discret. Appl. Math.*, 279:218–227, 2020.

Méa19. Pierrick Méaux. On the fast algebraic immunity of majority functions. In Peter Schwabe and Nicolas Thériault, editors, *Progress in Cryptology - LATINCRYPT*, volume 11774 of *LNCS*, pages 86–105. Springer, 2019.

Méa21. Pierrick Méaux. On the fast algebraic immunity of threshold functions. *Cryptography and Commununications*, 13(5):741–762, 2021.

MJSC16. Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 311–343. Springer, Heidelberg, May 2016.

MMM+18. Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy, and Pantelimon Stanica. Tools in analyzing linear approximation for boolean functions related to FLIP. In *Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in India, New Delhi, India, December 9-12, 2018, Proceedings*, pages 282–303, 2018.

MPJ+22. Luca Mario, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced boolean functions. 2022.

MS78. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.

MS21. Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 2021.

MSL21. Sihem Mesnager, Sihong Su, and Jingjing Li. On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. *Boolean Functions and Applications*, 2021.

MZD19. Sihem Mesnager, Zhengchun Zhou, and Cunsheng Ding. On the nonlinearity of boolean functions with restricted input. *Cryptogr. Commun.*, 11(1):63–76, 2019.

SM07. Palash Sarkar and Subhamoy Maitra. Balancedness and correlation immunity of symmetric boolean functions. *Discrete Mathematics*, pages 2351 – 2358, 2007.

Su21. Sihong Su. The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 297:60–70, 2021.

SW99. Roel J. Stroeker and De Weger. On integral zeroes of binary krawtchouk polynomials. 1999.

The17. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.1)*, 2017. `https://www.sagemath.org`.

TL19. Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptogr. Commun.*, 11(6):1185–1197, 2019.

WCST14. Qichun Wang, Claude Carlet, Pantelimon Stanica, and Chik How Tan. Cryptographic properties of the hidden weighted bit function. *Discret. Appl. Math.*, 174:1–10, 2014.

ZS21. Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced boolean functions. *Advances in Mathematics of Communications*, 0:–, 2021.