Annales Mathematicae et Informaticae
***52** (2020) pp. 117–135*
DOI: https://doi.org/10.33039/ami.2020.10.004
URL: https://ami.uni-eszterhazy.hu

Thickness distribution of Boolean functions in 4 and 5 variables and a comparison with other cryptographic properties

Mathias Hopp[a*], Pål Ellingsen[a], Constanza Riera[a], Pantelimon Stănică[b†]

[a]Department of Computer Science,
Electrical Engineering and Mathematical Sciences,
Western Norway University of Applied Sciences, 5020 Bergen, Norway
mathias.hopp@spv.no,{pel,csr}@hvl.no

[b]Applied Mathematics Department,
Naval Postgraduate School, Monterey, USA
pstanica@nps.edu

Submitted: September 23, 2020
Accepted: October 20, 2020
Published online: October 29, 2020

Abstract

This paper explores the distribution of algebraic thickness of Boolean functions (that is, the minimum number of terms in the ANF of the functions in the orbit of a Boolean function, through all affine transformations), in four and five variables, and the complete distribution is presented. Additionally, a complete analysis of some complexity properties (e.g., nonlinearity, balancedness, etc.) of all relevant orbits of Boolean functions is presented. Some properties of our notion of rigid function (which enabled us to reduce significantly the computation) are shown and some open questions are proposed, providing some further explanation of one of these questions.

Keywords: Boolean function, algebraic normal form, thickness, nonlinearity, affine equivalence

MSC: 06E30, 11T06, 94A60, 94D10.

*Currently with Sparebanken Vest, Bergen, Norway
†Corresponding author

1. Introduction

In this paper, we deal with the concept of algebraic thickness, defined by Carlet in [3, 4] as the minimum number of terms of all Boolean functions in the affine equivalence orbit of a Boolean function – and aim to reveal the distribution of algebraic thickness of all Boolean functions in four and five variables.

As will be discussed in the coming sections, by using an exhaustive search, the calculation of this distribution for $n \leq 4$ variables is at best a straightforward, and at worst, a lengthy – but manageable – endeavor. There are 2^{2^n} Boolean functions in n variables, which, for $n = 4$, equals 65536. Since there are 322560 different affine transformations needed to be checked for *each* Boolean function, the calculation of the algebraic thickness for all Boolean functions in four variables is a time consuming task, albeit doable.

However, in moving from four to five variables, this number grows significantly. The total number of unique Boolean functions is 4 294 967 296, and the number of different affine transformations is 319 979 520. One of the sub-goals of the paper was to find an efficient method able to handle the magnitude of the computation, and another was to effectively handle and analyze the resulting data set for $n = 5$.

Additionally, throughout the paper, when discussing functions $n \leq 5$, we omit the trivial cases $n = 0, 1$, unless specified. We used SageMath [9] for all computations in this paper.

A Boolean function f in n variables, where n is any positive integer, is a function from the vector space $\mathbb{F}_2^n$ to the finite field $\mathbb{F}_2$, i.e. $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$, and the symbol $\oplus$ denotes addition modulo 2, in $\mathbb{F}_2$, $\mathbb{F}_2^n$, and $\mathcal{B}_n$.

Every Boolean function f has a unique representation called its *algebraic normal form* (ANF) as a polynomial over $\mathbb{F}_2$ in n variables:

$$f(\mathbf{x}) = \bigoplus_{\mathbf{u}\in\mathbb{F}_2^n} c_{\mathbf{u}} \left(\prod_{i=1}^{n} x_i^{u_i} \right) = \bigoplus_{\mathbf{u}\in\mathbb{F}_2^n} c_{\mathbf{u}} \mathbf{x}^{\mathbf{u}},$$

where each $c_{\mathbf{u}} \in \mathbb{F}_2$, $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{x} = (x_1, \ldots, x_n)$. The algebraic *degree* of f is the largest weight of $\mathbf{u}$ such that $c_{\mathbf{u}} \neq 0$. A *homogeneous* function is a sum of monomials of the same degree.

An *affine function* $\ell_{\mathbf{u},c}$ is a function with algebraic degree at most 1, which takes the form

$$\ell_{\mathbf{u},c}(\mathbf{x}) = \mathbf{u} \cdot \mathbf{x} \oplus c = u_1 x_1 \oplus \cdots \oplus u_n x_n \oplus c, \tag{1.1}$$

where $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. If $c = 0$, such that $\ell_{\mathbf{u},0}$ only consists of monomials of algebraic degree 1, and no constant, then it is a *linear* function. The *Hamming weight* of a vector $\mathbf{x} \in \mathbb{F}_2^n$ is denoted by $wt(\mathbf{x})$ and is equal to the number of 1's in the vector $\mathbf{x}$. For a Boolean function f on $\mathbb{F}_2^n$, let $\Omega_f = \{\mathbf{x} \in \mathbb{F}_2^n \mid f(\mathbf{x}) = 1\}$ be the *support* of f. The Hamming weight of f is then $|\Omega_f|$, or equivalently, the weight of the vector of its truth table. The *Hamming distance* between two

functions $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$, denoted by $d(f,g)$, is defined as $d(f,g) = wt(f \oplus g)$. A *balanced* function on n variables has weight exactly 2^{n-1}. For $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer-valued function

$$\mathcal{W}_f(\mathbf{u}) = \sum_{x \in \mathbb{F}_2{}^n} (-1)^{f(\mathbf{x})+\mathbf{ux}},\ \mathbf{u} \in \mathbb{F}_2^n.$$

The *nonlinearity* $\mathcal{N}_f$ of a function f is defined as

$$\mathcal{N}_f = \min_{\phi \in \mathcal{A}_n} d(f, \phi)$$

where $\mathcal{A}_n$ is the class of all affine functions on $\mathbb{F}_2^n$. The largest nonlinearity, namely $2^{n-1} - 2^{\frac{n}{2}-1}$ is achieved by *bent* functions (they exist for even dimension n) and they have only two values in their Walsh spectrum (the multiset of Walsh coefficients), namely $\pm 2^{\frac{n}{2}}$. The *semi-bent* functions will have three values in their Walsh spectrum, namely, $\{0, \pm 2^{\frac{n+2}{2}}\}$, $\{0, \pm 2^{\frac{n+1}{2}}\}$, for n even, respectively, odd, and they can be balanced, as opposed to bent functions, whose weight can only be $2^{n-1} \pm 2^{\frac{n}{2}-1}$.

For these definitions and to know more on Boolean functions, and their cryptographic properties, the reader can consult [2, 5].

2. Algebraic thickness

Carlet, in [3], defined algebraic thickness, and discussed lower and upper bounds. His paper also includes further discussion on the relation that algebraic thickness has with other complexity criteria (e.g., nonlinearity, algebraic degree, etc.). In [4], Carlet improved some of the prior results, and further expanded on the properties of algebraic thickness.

Definition 2.1 ([4])**.** *The* algebraic thickness $\mathcal{T}(f)$ *of a Boolean function f is the minimum number of monomials with non-zero coefficients in the ANF of the functions $f \circ \mathcal{A}$, where $\mathcal{A} \in \mathrm{GL}(n, \mathbb{F}_2)$ (the general affine group). When we want to emphasize the number of variables, we shall write $\mathcal{T}_n(f)$.*

Surely, the algebraic thickness of affine functions is at most 1 [1, 4]. The quadratic functions are also well understood, due to the well-known Dickson's theorem (see MacWilliams and Sloane [8], or the simpler version below taken from Boyar and Find [1]).

Theorem 2.2 (Dickson's Theorem)**.** *If $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is a quadratic Boolean function, then there exist an invertible $n \times n$ matrix A, $\mathbf{b} \in \mathbb{F}_2^n$, $t \leq \frac{n}{2}$, and $c \in \mathbb{F}_2$ such that for $\mathbf{y} = A\mathbf{x} + \mathbf{b}$ one of the following two equations holds:*

$$f(x) = y_1y_2 + y_3y_4 + \cdots + y_{t-1}y_t + c, \text{ or}$$
$$f(x) = y_1y_2 + y_3y_4 + \cdots + y_{t-1}y_t + y_{t+1}.$$

Furthermore A, $\mathbf{b}$, and c can be found efficiently.

We also mention that we re-computed (see Table 4) the distribution of nonlinearities of all functions in $2 \leq n \leq 5$ variables, confirming known results (see, for instance, the paper by Sertkaya and Doğanaksoy [10]).

For Boolean functions in n variables, it is of interest to determine the maximum value possible for the thickness, namely, $\tau_n = \max_{f \in \mathcal{B}_n}(\mathcal{T}(f))$, and specifically, its growth. Surely, we have the trivial upper bound $\tau_n \leq 2^n$, since the maximum number of terms in the ANF of a function in n variables is $\leq 2^n$.

Regarding the lower bound of the thickness, Carlet showed in [3] that, for every $\lambda < \frac{1}{2}$ and positive integer n, the density in $\mathcal{B}_n$ of the subset

$$\{f \in \mathcal{B}_n \,|\, \mathcal{T}(f) \geq \lambda 2^n\}$$

is greater than $1 - 2^{2^n H_2(\lambda) - 2^n + n^2 + n}$, where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the *entropy function*, and therefore *almost* all Boolean functions have algebraic thickness greater than $\lambda 2^n$. This was improved in [4], showing that *almost* all Boolean functions have algebraic thickness greater than $2^{n-1} - n2^{\frac{n-1}{2}}$. The best upper bound on algebraic thickness is still the one in [3], namely,

$$\mathcal{T}(f) \leq \frac{2}{3}2^n,$$

which is believed to be improvable.

3. Some theoretical results on thickness

Brute force computation is still possible for $n = 4$, but for $n = 5$ we need to find some techniques to reduce the computational time, as it would take thousands of years on a personal computer. The idea is that this new technique may be useful in approaching the thickness distribution computation for $n = 6$ (or at least for some subclass of $\mathcal{B}_6$).

For any Boolean function f, we define its *orbit* or *equivalence class* as the set of functions $\{f \circ \mathcal{A} : \mathcal{A} \in \mathrm{GL}(n, \mathbb{F}_2)\}$.

Given a Boolean function f, if f_{min} is an element (not necessarily unique) of its equivalence class with minimum number of terms, then the algebraic thickness of f_{min} is the number of terms in its ANF.

Definition 3.1 (Rigid Boolean functions)**.** *We call a Boolean function f with $\mathcal{T}(f)$ monomials in its ANF, a* rigid function*. The set of all rigid functions will be denoted by $\mathcal{S}_n$.*

Thus, a rigid Boolean function cannot be mapped to a function with lower monomial count, through any affine transformation. Furthermore, any Boolean function can be mapped to a rigid function. The reason for this should be clear, but for completion, we state it as a lemma.

Proposition 3.2. *Any Boolean function can be mapped to a rigid function, by an affine transformation.*

Proof. Given a Boolean function $f \in \mathcal{B}_n$, let g be a function in the orbit of f (through affine transformations), where the monomial count of g is equal to $\mathcal{T}(f)$. If g is not a rigid function, then g does not have the minimum monomial count in its orbit. Suppose h is in the orbit of g, and has lower monomial count than g. Since f maps to g and g maps to h, then by composition of transformations, f maps to h as well. Thus, we reach a contradiction. □

Experimentally, it was found that $\mathcal{S}_n \subset \mathcal{S}_{n+1}$, for small values of n, suggesting that perhaps this is true in general, and will be shown next.

Theorem 3.3. *All rigid functions in n variables are also rigid functions in $(n+1)$ variables, that is, $\mathcal{S}_n \subset \mathcal{S}_{n+1}$.*

Remark 3.4. As is customary in this area (for easy writing), in the following proof, we disregard the usual linear algebra convention of matrix-vector multiplication and regard $\mathbf{x}$ and $\mathbf{b}$ both as a row- and a column vector, when there is no danger of confusion.

Proof. Let $f \in \mathcal{S}_n$ with $\mathcal{T}(f) = t$. We embed f in $n+1$ variables, and we denote its embedding by $\tilde{f}$, such that $\tilde{f}(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n)$. Let a non-zero affine transformation of the input of $\tilde{f}$ be given by $\mathbf{x} \mapsto \tilde{A}\tilde{\mathbf{x}} + \mathbf{b}$, where $\tilde{A}$ is an $(n+1) \times (n+1)$ matrix and $\mathbf{b} = (b_1 \ldots, b_n)$, and $\tilde{\mathbf{x}} = (x_1, \ldots, x_n, x_{n+1}), \mathbf{x} = (x_1, \ldots, x_n)$. We label the first n rows and n columns in $\tilde{A}$ by A and so,

$$\tilde{A} = \begin{pmatrix} & & a_{1,n+1} \\ & A & \vdots \\ a_{n+1,1} & \cdots & a_{n+1,n+1} \end{pmatrix}.$$

Thus,

$$\tilde{A}\tilde{\mathbf{x}} + \mathbf{b} = \begin{pmatrix} A\mathbf{x} + x_{n+1} \begin{pmatrix} a_{1,n+1} \\ \vdots \\ a_{n,n+1} \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ a_{n+1,1}x_1 + \cdots + a_{n+1,n+1}x_{n+1} + b_{n+1} \end{pmatrix},$$

and so

$$\tilde{f}(\tilde{A}\tilde{\mathbf{x}} + \mathbf{b}) = f\left(A\mathbf{x} + x_{n+1} \begin{pmatrix} a_{1,n+1} \\ \vdots \\ a_{n,n+1} \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \right),$$

from which our claim is inferred. □

In summary, the introduction of x_{n+1} does not induce any further monomial eliminations not already possible in n variables. Therefore, for a rigid function f with monomial count t,

$$\mathcal{T}_n(f) = t = \mathcal{T}_{n+1}(\tilde{f}).$$

Corollary 3.5. *For any Boolean function f in n variables,*

$$\mathcal{T}_n(f) = \mathcal{T}_{n+1}(\tilde{f}),$$

where $\tilde{f}$ is the embedding of f in $\mathcal{B}_{n+1}$, such that

$$\tilde{f}(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n).$$

Proof. Given a rigid Boolean function f in n variables, let $\mathcal{A}_n(f)$ be the orbit of f through all nonzero affine transformations, and let $\mathcal{T}_n(f) = t$. As we know, from the definition of algebraic thickness, any Boolean function $g \in \mathcal{A}_n(f)$ satisfies $\mathcal{T}_n(g) = t$, as well. Since f is rigid, $\mathcal{T}_{n+1}(f) = t$, by Theorem 3.3. Clearly, then, $\mathcal{A}_n(f) \subseteq \mathcal{A}_{n+1}(\tilde{f})$, by the very same affine transformations as in n variables (leaving the new variable x_{n+1} mapped to itself), and therefore all functions in $\mathcal{A}_n(f)$ have thickness t in $n+1$ variables, as well. □

3.1. Multiplication by a new variable may conserve thickness

We showed in Theorem 3.3 that all rigid functions in $\mathcal{B}_n$ are also rigid functions in $\mathcal{B}_{n+1}$. Moreover, $f \in \mathcal{B}_n$, $\mathcal{T}_n(f) = \mathcal{T}_{n+1}(\tilde{f})$, as well. These properties give insight into the distribution of algebraic thickness in $(n+1)$ variables, when the distribution for n variables is known. Surely, we cannot expect an inductive procedure for the computation of thickness, but as observed already in Theorem 3.3, a connection does exist that may decrease the complexity even further.

Proposition 3.6. *Let $f \in \mathcal{B}_n$ be a Boolean function in variables $\mathbf{x} = (x_1, ..., x_n)$ vector, and let x_{n+1} be a new variable. Then*:

$$\mathcal{T}_{n+1}(f(x_1, \ldots, x_n) \cdot x_{n+1}) \leq \mathcal{T}_n(f).$$

Proof. Given a Boolean function $f \in \mathcal{B}_n$, with known algebraic thickness $\mathcal{T}_n(f) = t$, on the variables $(x_1, \ldots, x_n)$, we let $f_{\min} \in \mathcal{B}_n$ be the representative function with monomial count t of the orbit of f, and let π denote the affine transformation such that $\pi(f) = f_{\min}$. As before, x_{n+1} is the new variable introduced in $\mathcal{B}_{n+1}$.

In $\mathcal{B}_{n+1}$, then, $\pi'(f(x_1, \ldots, x_n) \cdot x_{n+1}) = f_{\min}(x_1, \ldots, x_n) \cdot x_{n+1}$, by the transformation $\pi'(x_j) = \pi(x_j)$, for $j < (n+1)$, and $\pi'(x_{n+1}) = x_{n+1}$. Since $f_{\min}$ has monomial count t, $f_{\min}(x_1, \ldots, x_n) \cdot x_{n+1}$ also has monomial count t, and therefore $\mathcal{T}_{n+1}(f(x_1, \ldots, x_n) \cdot x_{n+1}) \leq \mathcal{T}_n(f)$. □

Based upon extensive computations (exhaustive for lower dimensions and random for higher dimensions) and the previous proposition, we propose the following question.

Open question 3.7 (Thickness conservation)**.** *Let $f \in \mathcal{B}_n$ be a Boolean function in variables $\mathbf{x} = (x_1, ..., x_n)$ vector, and let x_{n+1} be a new variable. Is it true that*

$$\mathcal{T}_{n+1}(f(x_1, \ldots, x_n) \cdot x_{n+1}) = \mathcal{T}_n(f)?$$

While this is not necessarily the goal of the paper, and we cannot provide an answer to this question, we attempt to explain it further. Assume that there exists a function f in n variables such that $\mathcal{T}_n(f) > \mathcal{T}_{n+1}(f \cdot x_{n+1}) = t$. Take an affine transformation that brings $f(x_1, \ldots, x_n) \cdot x_{n+1}$ to its minimal thickness form, transformation determined by the vector $\mathbf{b} = (b_1, \ldots, b_{n+1})$, and the matrix $\tilde{A}$ of the form

$$\tilde{A} = \begin{pmatrix} & & a_{1,n+1} \\ & A & \vdots \\ a_{n+1,1} & \cdots & a_{n+1,n+1} \end{pmatrix},$$

where A is an $n \times n$ matrix, and so,

$$\tilde{A}\tilde{\mathbf{x}} + \mathbf{b} = \begin{pmatrix} A\mathbf{x} + x_{n+1} \begin{pmatrix} a_{1,n+1} \\ \vdots \\ a_{n,n+1} \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ a_{n+1,1}x_1 + \cdots + a_{n+1,n+1}x_{n+1} + b_{n+1} \end{pmatrix},$$

as in Theorem 3.3. We label $r_{i,\tilde{A}}$, $r_{i,A}$, the ith row of $\tilde{A}$, respectively A, and $\tilde{\mathbf{x}} = (x_1, \ldots, x_n, x_{n+1}), \mathbf{x} = (x_1, \ldots, x_n)$. Thus, using "$\cdot$" to denote the usual scalar product,

$$\begin{aligned} &(f(x_1, \ldots, x_n) \cdot x_{n+1}) \circ (\tilde{A}\tilde{\mathbf{x}} + \mathbf{b}) \\ &= f(r_{1,A} \cdot \mathbf{x} + a_{1,n+1}x_{n+1} + b_1, \ldots, r_{n,A} \cdot \mathbf{x} + a_{n,n+1}x_{n+1} + b_n) \\ &\qquad \cdot (a_{n+1,1}x_1 + \cdots + a_{n+1,n+1}x_{n+1} + b_{n+1}). \end{aligned} \tag{3.1}$$

We let $b'_i = b_i + a_{i,n+1}x_{n+1}$, $1 \le i \le n+1$ and $\mathbf{b}' = (b'_1, \ldots, b'_n)$. Since the first factor is simply $f(A\mathbf{x} + \mathbf{b}')$ (we regard its coefficients in $\mathbb{F}_2[x_{n+1}]$, and assume that A is invertible; again, it may happen that it is not), it must have more than $\mathcal{T}_{n+1}(f(x_1, \ldots, x_n) \cdot x_{n+1}) = t$ terms (call them $T_i(x_1, \ldots, x_n)$, of degrees $\deg T_i = d_i$, $1 \le i \le s$, with $d_1 \le d_2 \le \cdots \le d_s$), given our assumption. We thus write its algebraic normal form as

$$\begin{aligned} f(A\mathbf{x} + \mathbf{b}') = (\alpha_1 x_{n+1} + \beta_1)T_1(x_1, \ldots, x_n) + \cdots \\ + (\alpha_s x_{n+1} + \beta_s)T_s(x_1, \ldots, x_n), s > t, \end{aligned}$$

(α_i, β_i are not zero simultaneously, since we need to have $s > t$ terms in $f(A\mathbf{x}+\mathbf{b}')$), and therefore Equation (3.1) becomes (for easy writing, we denote the $(n+1)$st row of $\tilde{A}$ by $(\gamma_1, \ldots, \gamma_{n+1})$ and we will not write the input $(x_1, \ldots, x_n)$ for T_i),

$$\begin{aligned} &\sum_{i=1}^{s} (\alpha_i x_{n+1} + \beta_i) T_i \left(\sum_{j=1}^{n} \gamma_j x_j + \gamma_{n+1}x_{n+1} + b_{n+1} \right) \\ &= \sum_{j=1}^{n} \sum_{i=1}^{s} (\alpha_i x_{n+1} + \beta_i)\gamma_j x_j T_i(x_1, \ldots, x_n) \end{aligned}$$

$$
\begin{aligned}
&+\sum_{i=1}^{s}\gamma_{n+1}(\alpha_i+\beta_i)x_{n+1}T_i+\sum_{i=1}^{s}(\alpha_i x_{n+1}+\beta_i)b_{n+1}T_i\\
&=\sum_{i=1}^{s}x_{n+1}T_i\left(\alpha_i b_{n+1}+\gamma_{n+1}(\alpha_i+\beta_i)+\alpha_i\sum_{j=1}^{n}\gamma_j x_j\right)\\
&\quad+\sum_{j=1}^{n}\sum_{i=1}^{s}\beta_i\gamma_j x_j T_i+\sum_{i=1}^{s}\beta_i b_{n+1}T_i.\\
&=\sum_{i=1}^{s}\left(\alpha_i b_{n+1}+\gamma_{n+1}(\alpha_i+\beta_i)+\alpha_i\sum_{j=1}^{n}\gamma_j x_j\right)x_{n+1}T_i\\
&\quad+\sum_{i=1}^{s}\beta_i\left(b_{n+1}+\sum_{j=1}^{n}\gamma_j x_j\right)T_i.
\end{aligned}
\tag{3.2}
$$

We thus get

$$
\begin{aligned}
&(f(x_1,\dots,x_n)\cdot x_{n+1})\circ(\tilde{A}\tilde{\mathbf{x}}+\mathbf{b})\\
&=x_{n+1}\sum_{i=1}^{s}\left(\alpha_i b_{n+1}+\gamma_{n+1}(\alpha_i+\beta_i)+\alpha_i\sum_{j=1}^{n}\gamma_j x_j\right)T_i\\
&\quad+\sum_{i=1}^{s}\beta_i\left(b_{n+1}+\sum_{j=1}^{n}\gamma_j x_j\right)T_i.
\end{aligned}
$$

For the inequality to hold, we need to have enough cancellations in both sums

$$
\begin{aligned}
S_1&=\sum_{i=1}^{s}\left(\alpha_i b_{n+1}+\gamma_{n+1}(\alpha_i+\beta_i)+\alpha_i\sum_{j=1}^{n}\gamma_j x_j\right)T_i\\
S_2&=\sum_{i=1}^{s}\beta_i\left(b_{n+1}+\sum_{j=1}^{n}\gamma_j x_j\right)T_i,
\end{aligned}
$$

for a total of more than $(s-t)$ terms. We let A_i be the index support for T_i (that is, if $T_i(x_1,\dots,x_n)=x_{i_1}\cdots x_{i_\ell}$, then $A_i=\{i_1,\dots,i_\ell\}$). Therefore, the above sums can be written as (we let $|J|_2=|J| \pmod 2$, where $J=\{j|\gamma_j\neq 0\}$, and $|J_i|_2=|J_i| \pmod 2$, where $J_i=\{j\in A_i|\gamma_j\neq 0\}$),

$$
\begin{aligned}
S_1&=\sum_{i=1}^{s}(\alpha_i b_{n+1}+\gamma_{n+1}(\alpha_i+\beta_i))T_i+\sum_{i=1}^{s}\alpha_i\left(|J_i|_2+\sum_{j\in J\setminus J_i}x_j\right)T_i\\
&=\sum_{i=1}^{s}\left(\alpha_i b_{n+1}+\gamma_{n+1}(\alpha_i+\beta_i)+\alpha_i|J_i|_2\right)T_i+\sum_{i=1}^{s}\alpha_i T_i\sum_{j\in J\setminus J_i}x_j
\end{aligned}
$$

$$= \sum_{i=1}^{s} \alpha_i \left(b_{n+1} + |J_i|_2\right) T_i + \sum_{i=1}^{s} \alpha_i T_i \sum_{j \in J \setminus J_i} x_j + \gamma_{n+1} \sum_{i=1}^{s} (\alpha_i + \beta_i) T_i,$$

$$S_2 = \sum_{i=1}^{s} \beta_i b_{n+1} T_i + \sum_{i=1}^{s} \beta_i \left(\sum_{j \in A_i} \gamma_j + \sum_{j \notin A_i} \gamma_j x_j \right) T_i$$

$$= \sum_{i=1}^{s} \beta_i \left(b_{n+1} + |J_i|_2\right) T_i + \sum_{i=1}^{s} \beta_i T_i \sum_{j \in J \setminus J_i} x_j.$$

If $\gamma_{n+1} = 0$ then, for i such that $b_{n+1} + |J_i|_2 \neq 0$, then either $\alpha_i \left(b_{n+1} + |J_i|_2\right) T_i$, or $\beta_i \left(b_{n+1} + |J_i|_2\right) T_i$ survives. Similarly, assuming that for an i, $J \setminus J_i \neq \emptyset$, then either $\alpha_i T_i \sum_{j \in J \setminus J_i} x_j$, or $\beta_i T_i \sum_{j \in J \setminus J_i} x_j$ survives. If it were true that for all i, $J \setminus J_i \neq \emptyset$, then the inequality would be false and the conjecture would "hold" in this case. However, at least $J \setminus J_s = \emptyset$, since otherwise our affinely equivalent function would have degree higher than $d_s + 2$ (recall that S_1 is multiplied by x_{n+1}), and that is impossible. If one would attempt to find a counterexample for a negative answer to our open question, then one could take a matrix $\tilde{A}$ where the last row is rather very sparse, along with b such that $A\mathbf{x} + b'$ has most of the $\beta_i = 0$. Can that be achieved? We do not know the answer to this question.

3.2. Gaps in thickness distribution

Noting the algebraic thickness distributions listed in Table 3, it is easy to see that, for $n \leq 5$ and $m > 0$, if there exists a representative with $\mathcal{T}_n = m$, then there exists a representative with $\mathcal{T}_n = m - 1$, and conversely: if there are no representatives with $\mathcal{T}_n = m - 1$, then there are no representatives with $\mathcal{T}_n = m$. The following conjecture is an extension of Lemma 3.9.

Conjecture 3.8. *For any n, in any given monomial count $m \leq 2^n$, if there are no rigid functions with m monomials, then for any $f \in \mathcal{B}_n$,*

$$\mathcal{T}_n(f) < m.$$

The idea here is that if there are no rigid functions in a set monomial count m, then there are no rigid functions in any monomial count M, where $M > m$. Proving this would have implications for further attempts at determining maximum algebraic thickness (and the following thickness distribution) using the methods described in this paper, as finding no rigid functions in n variables with monomial count (e.g.) 2^{n-1} would imply there are no rigid functions with monomial count greater than 2^{n-1}, thus eliminating half of the set of functions to search through.

The definition for rigid functions is closely related to Carlet's definition for algebraic thickness. We record that below.

Proposition 3.9. *Given all Boolean functions in n variables with monomial count k in their ANF, if there are no rigid functions with k monomials, then there are no functions f in n variables with $\mathcal{T}_n(f) = k$.*

This simple proposition was the inception of the program described later to find the thickness distribution.

n	Number of rigid functions
0	2
1	3
2	6
3	28
4	588
5	211 259

Table 1: Number of rigid functions in $n \leq 5$ variables

The distribution of the number of rigid functions in $n \leq 5$ variables is listed in Table 1, where: for $n \leq 4$ variables, these numbers were collected from analysis of the data sets calculated by brute-force, and for $n = 5$, the number was (along with double-checking values for $n < 5$) collected from analysis of the data sets calculated by the program described later.

We hope that our methods will prove useful for $n > 5$, as well, since an iterative approach is impossible by modern computing standards for these dimensions. Searching for rigid functions and – most importantly – disregarding non-rigid functions, should improve the efficiency of any program (at the very least, it improves the program given later).

Determining which functions are rigid functions in n variables yields information regarding the thickness distribution in $n + 1$ variables as well, by Theorem 3.3. Furthermore, by Corollary 3.5, unveiling the distribution of all functions in $\mathcal{B}_n$ immediately gives the distribution of 2^{2^n} functions in $\mathcal{B}_{n+1}$ – which may be a small portion compared to $2^{2^{n+1}}$, but is nonetheless a start.

The functions in $\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2$ (i.e., the rigid functions in $n = 0, 1, 2$ variables) are listed below:

$$\begin{aligned}
\mathcal{S}_0 &= \{0,\, 1\} \\
\mathcal{S}_1 &= \{0,\, 1,\, x_1\} \\
\mathcal{S}_2 &= \{0,\, 1,\, x_1,\, x_2,\, x_1x_2,\, x_1x_2 + 1\}
\end{aligned}$$

Since the sets $\mathcal{S}_3, \mathcal{S}_4$ are of rather large sizes (28 and 588, respectively), they will not be listed here (but the data can be found in [7]).

4. Representatives

By uncovering one function ϕ for each of these orbits, every function in n variables can be generated from a corresponding ϕ, by iteration through all affine transformations for each one. Calculating the algebraic thickness of each ϕ yields the thickness distribution for all functions in $\mathcal{B}_n$, as $\mathcal{T}$ is (trivially) an affine invariant. Since these ϕ would be representing their orbits, the name representative function

n	Number of equivalence classes
1	3
2	5
3	10
4	32
5	382
6	15 768 919

Table 2: Number of affine equivalence classes of Boolean functions [6]

was chosen. As the rigid functions are the functions with the minimum number of monomials in their ANF, these representative functions were chosen to be the *smallest* rigid functions in their orbit (we call smallest, a function with a minimal sum of the degrees of each monomial in its ANF, with lowest indexed variables, in lexicographical order, in descending order by degree of monomials).

We give an example below.

Example 4.1. For $n = 3, \mathcal{T}_3 = 3$, and there is a single orbit with maximum thickness, containing 9 rigid functions, namely: $x_1x_2x_3 + x_3 + 1$, $x_1x_2x_3 + x_2 + 1$, $x_1x_2x_3 + x_1 + 1$, $x_1x_2x_3 + x_2 + x_3$, $x_1x_2x_3 + x_1 + x_3$, $x_1x_2x_3 + x_1 + x_2$, $x_1x_2x_3 + x_2x_3 + x_1$, $x_1x_2x_3 + x_1x_3 + x_2$, $x_1x_2x_3 + x_1x_2 + x_3$. In the first three functions, the sum of the monomial degrees for each function is 4, the next three functions have this sum 5, and the last three, 6. We therefore, look at the first three functions, and going through from the highest to the lowest degree monomials in the three functions, and observing that x_1 is smaller (lexicographically), we therefore choose $x_1x_2x_3 + x_1 + 1$ as a representative.

It is clear that the choice of a representative in any orbit is purely implementation specific and will not affect any properties related to algebraic thickness. As with rigid functions, the set of all representative functions will be denoted as $\mathcal{R}_n \subseteq \mathcal{S}_n$ for representatives in n variables.

The number of Boolean functions in n variables that have exactly m monomials in their ANF is $\binom{2^n}{m}$, and so, the number of Boolean functions with at least m monomials is the sum of the binomial coefficients $\binom{2^n}{i}$, where $i \geq m$, that is, $\sum_{i=m}^{2^n} \binom{2^n}{i}$.

Using Carlet's upper-bound for algebraic thickness in n variables, $\mathcal{T} \leq \left\lfloor \frac{2}{3}2^n \right\rfloor$, it follows that no rigid function will have more than $\left\lfloor \frac{2}{3}2^5 \right\rfloor = 21$ monomials in its ANF. We checked and ultimately, the first monomial count where a rigid function could be found, was $m = 8$ (i.e., first, in descending order). Thus, the maximum thickness of $n = 5$ is 8, by Proposition 3.9.

Our code takes advantage of various "quality-of-life" method calls for printing out current positions – and saving the positions of the iterations, in case of power failure. Surely, the "bottleneck" of finding representatives of functions in five variables is the number of affine transformations to go through for each function – but also the fact that the number of affine transformations is much larger than the number of functions in any orbit (by the pigeonhole principle). This means

that there are several affine transformations that, for each f, maps f to the same function. However, since there is no way of predicting, as far as we know, *which* transformations will do this, it cannot be avoided. The final program used for finding all 382 representatives in $n = 5$ variables (and lower dimensions) can be found in [7], which also includes a listing of these.

5. Distribution of thickness

The full distribution of algebraic thickness of the representative functions in $n \leq 5$ variables is given in Table 3, summarizing the results of the data collection conducted by our program. The distribution for number of functions within each thickness value is further detailed and described later.

$\mathcal{T}$	$n=0$	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$
0	1	1	1	1	1	1
1	1	2	3	4	5	6
2	-	-	1	4	10	19
3	-	-	-	1	10	46
4	-	-	-	-	5	81
5	-	-	-	-	1	111
6	-	-	-	-	-	81
7	-	-	-	-	-	33
8	-	-	-	-	-	4
Sum	2	3	5	10	32	382
$\max(\mathcal{T}_n)$	1	1	2	3	5	8

Table 3: Distribution of representatives within each thickness value

While this is known, we re-checked the distribution of functions with a specific nonlinearity $\mathcal{N}$ for $n \leq 5$, confirming the results listed in [10]. Columns for $n = 2, 3$ are not strictly relevant to the following property analysis, but are included for completeness.

$\mathcal{N}$	$n=2$	$n=3$	$n=4$	$n=5$
0	8	16	32	64
1	8	128	512	2048
2	-	112	3840	31 744
3	-	-	17 920	317 440
4	-	-	28 000	2 301 440
5	-	-	14 336	12 888 064
6	-	-	896	57 996 288
7	-	-	-	215 414 784
8	-	-	-	647 666 880
9	-	-	-	1 362 452 480
10	-	-	-	1 412 100 096
11	-	-	-	556 408 832
12	-	-	-	27 387 136
$\max(\mathcal{N})$	1	2	6	12

Table 4: Distribution of number of $f \in \mathcal{B}_n$ with given $\mathcal{N}$-value, $n \leq 5$

Furthermore, the distribution of the number of orbits within each possible $\mathcal{N}$-

value (i.e., the distribution of nonlinearity of the representatives) is shown in Table 5 – recall that nonlinearity is an affine invariant. Note that there are 16 representatives (and therefore orbits) in $n = 5$ variables where $\mathcal{N} = 5$. Further, we can see that there are two orbits with maximum nonlinearity in $n = 4$ (and therefore two orbits that contain all bent functions in $n = 4$), and 14 orbits with maximum nonlinearity in $n = 5$ ($\mathcal{N} = 6$ and $\mathcal{N} = 12$, respectively; recall that the maximum nonlinearity for $n = 5$ is $2^{n-1} - 2^{\frac{n-1}{2}} = 12$, the well known bent concatenation bound).

$\mathcal{N}$	$n = 2$	$n = 3$	$n = 4$	$n = 5$
0	3	3	3	3
1	2	4	4	4
2	-	3	5	5
3	-	-	6	6
4	-	-	8	12
5	-	-	4	16
6	-	-	2	31
7	-	-	-	46
8	-	-	-	68
9	-	-	-	72
10	-	-	-	73
11	-	-	-	32
12	-	-	-	14

Table 5: Distribution of number of orbits with given $\mathcal{N}$-value, $n \leq 5$

6. Conclusions

Table 3 summarizes the outcome of our computation to find the number of orbits in each thickness class, for $n \leq 5$ variables, with the number of orbits and maximum thickness listed. As a double check, the number of equivalence classes (orbits) in $\mathcal{B}_n$ matches the one of Harrison [6].

By using the concepts of rigid and representative functions defined in Sections 3 and 4, the thickness distribution of $n \leq 5$ can be calculated in significantly less time than the time estimation of a brute-force application, by (roughly) $2 \cdot 10^6$ years. The case of $n = 4$ took little time compared to $n = 5$ (we display in Table 6 the time our computation took; iterations stand for the number of parallel sessions we ran).

Mon. count	Functions/Iterations	Min. time	Max. time	Total time (add.)
2	28 / 3	4h	4h	12h
3	134 / 4	6h	12h	1d 12h
4	625 / 4	1d 3h	1d 7h	4d 21h
5	2674 / 8	4d 10h	5d 5h	38d 14h
6	10 195 / 14	1d 14h	3d 19h	39d 17h
7	34 230 / 15	1d 4h	3d 15h	36d 16h
8	100 577 / 20	24s	5d 1h	11d 20h
Total			19d 15h	131d 16h

Table 6: Execution time of the iterations completed by our program

We display in Appendices A and B, the distribution of various cryptographic properties (bentness and semi-bentness, balancedness, etc.) as they relate to thickness, for $n = 4$, respectively, $n = 5$. Three physical computers were used for these computations (which took about 35 days): 1) a dedicated Windows server with Intel(R) Xeon(R) E5-2690 v2 3.00 GHz CPU, 20 cores, and 128 GiB RAM, responsible for the bulk of the calculations, 2) a desktop running Ubuntu with Intel(R) Core(TM) i7-6800K 3.40 GHz CPU, 8 cores, and 32 GiB RAM, and finally 3) a desktop running Windows 10 with Intel(R) Core(TM) i5-4460 3.20 GHz CPU, 4 cores, and 16 GiB RAM. The program iterations referenced in Table 6 were run simultaneously and each program was continually updated whenever new representatives were found.

Acknowledgements. The authors would like to thank the referee for the comments and the editors for the prompt handling of our paper.

References

[1] J. Boyar, M. G. Find: *Constructive Relationships Between Algebraic Thickness and Normality*, in: In Fundamentals of Computation Theory, LNCS 9210, Springer, Cham, 2015, pp. 106–117,
doi: https://doi.org/10.1007/978-3-319-22177-9_9.

[2] C. Carlet: *Boolean Functions*, in: van Tilborg H, ed. by J. S. C. A., Springer, Boston, MA: Encyclopedia of Cryptography and Security, 2011, pp. 162–164,
doi: https://doi.org/10.1007/978-1-4419-5906-5_336.

[3] C. Carlet: *On Cryptographic Complexity of Boolean Functions*, in: Proc. 6th Conf. Finite Fields With Applications to Coding Theory, Springer, 2002, pp. 53–69,
doi: https://doi.org/10.1007/978-3-642-59435-9_4.

[4] C. Carlet: *On the Degree, Nonlinearity, Algebraic Thickness, and Nonnormality of Boolean Functions, With Developments on Symmetric Functions*, IEEE Trans. Inf. Theory 50.9 (2004), pp. 2178–2185,
doi: https://doi.org/10.1109/TIT.2004.833361.

[5] T. W. Cusick, P. Stănică: *Cryptographic Boolean Functions and Applications (2nd ed.)* Elsevier-Academic Press, 2017,
doi: https://doi.org/10.1016/C2016-0-00852-5.

[6] M. A. Harrison: *On the classification of Boolean functions by the general linear and affine groups*, Journal of the Society for Industrial and Applied Mathematics 12.2 (1964), pp. 285–299,
doi: https://doi.org/10.1137/0112026.

[7] M. Hopp: *Thickness Distribution of Boolean Functions in* 4 *and* 5 *Variables*, Master Thesis, Department of Computing, Mathematics and Physics, Western Norway University of Applied Sciences (2020).

[8] F. J. MacWilliams, N. J. A. Sloane: *The theory of error correcting codes*, Amsterdam: North-Holland, 1977.

[9] SageMath: *Open-Source Mathematical Software System*, Last Accessed: 2020-09-10,
url: http://www.sagemath.org.

[10] I. Sertkaya, A. Doğanaksoy: *On the Affine Equivalence and Nonlinearity Preserving Bijective Mappings of* $\mathbb{F}_2$, International Workshop on the Arithmetic of Finite Fields, WAIFI Arithmetic of Finite Fields, (2014), pp. 121–136,
doi: https://doi.org/10.1007/978-3-319-16277-57.

Appendix A: Property distribution in $n = 4$, sorted by thickness

We include here the comparison between various cryptographic properties (homogeneous, rigid, balanced, bentness, nonlinearity, degree) of Boolean functions as related to thickness for $n = 4$ variables. Table 7 is a summary of all the property distributions of Tables 8–12 (independent on algebraic thickness).

Properties	Total number
Number of functions	65536
Homogeneous functions	96
Rigid functions	588
Balanced functions	12 870
Bent functions	896
Orbits	32
Bent orbits	2
Balanced orbits	4

Table 7: Summary of the property distribution of $n = 4$

Properties		Nonlinearity		Degrees	
Number of functions	307	0	31	0	1
Homogeneous functions	52	1	16	1	30
Rigid functions	16	2	120	2	140
Balanced functions	30	3	0	3	120
Bent functions	0	4	140	4	16
Orbits	5	5	0		
Bent orbits	0	6	0		
Balanced orbits	1				

Table 8: Property distribution of functions in $\mathcal{B}_4$ with $\mathcal{T}_4 = 1$

Properties		Nonlinearity		Degrees	
Number of functions	6804	0	0	0	0
Homogeneous functions	42	1	256	1	0
Rigid functions	64	2	2880	2	1428
Balanced functions	2760	3	560	3	4560
Bent functions	448	4	2660	4	816
Orbits	10	5	0		
Bent orbits	1	6	448		
Balanced orbits	2				

Table 9: Property distribution of functions in $\mathcal{B}_4$ with $\mathcal{T}_4 = 2$

Properties		Nonlinearity		Degrees	
Number of functions	33 448	0	0	0	0
Homogeneous functions	1	1	240	1	0
Rigid functions	188	2	840	2	448
Balanced functions	10 080	3	8960	3	19 320
Bent functions	448	4	18 480	4	13 680
Orbits	10	5	4480		
Bent orbits	1	6	448		
Balanced orbits	1				

Table 10: Property distribution of functions in $\mathcal{B}_4$ with $\mathcal{T}_4 = 3$

Properties		Nonlinearity		Degrees	
Number of functions	22 288	0	0	0	0
Homogeneous functions	0	1	0	1	0
Rigid functions	271	2	0	2	0
Balanced functions	0	3	8400	3	6720
Bent functions	0	4	6720	4	15 568
Orbits	5	5	7168		
Bent orbits	0	6	0		
Balanced orbits	0				

Table 11: Property distribution of functions in $\mathcal{B}_4$ with $\mathcal{T}_4 = 4$

Properties		Nonlinearity		Degrees	
Number of functions	2688	0	0	0	0
Homogeneous functions	0	1	0	1	0
Rigid functions	48	2	0	2	0
Balanced functions	0	3	0	3	0
Bent functions	0	4	0	4	2688
Orbits	1	5	2688		
Bent orbits	0	6	0		
Balanced orbits	0				

Table 12: Property distribution of functions in $\mathcal{B}_4$ with $\mathcal{T}_4 = 5$

Appendix B: Property distribution in $n = 5$, sorted by thickness

The cryptographic properties dealt with and the goals of the comparison for $n = 5$ are the same as for $n = 4$.

Properties	Total amount
Number of functions	4 294 967 296
Homogeneous functions	2111
Rigid functions	211 259
Balanced functions	601 080 390
Semi-Bent functions	14 054 656
Number of orbits	382
Semi-Bent orbits	9
Balanced orbits	38

Table 13: Summary of the property distribution of $n = 5$

Properties		Nonlinearity		Degrees	
Number of f	2451	0	63	0	1
Homogeneous f	203	1	32	1	62
Rigid f	32	2	496	2	620
Balanced f	62	3	0	3	1240
Semi-Bent f	0	4	1240	4	496
Orbits	6	5	0	5	32
Semi-Bent orbits	0	6	0		
Balanced orbits	1	7	0		
		8	620		
		9	0		
		10	0		
		11	0		
		12	0		

Table 14: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 1$

Properties		Nonlinearity		Degrees	
Number of f	695 796	0	0	0	0
Homogeneous f	987	1	1024	1	0
Rigid f	336	2	23 808	2	23 188
Balanced f	84 072	3	4960	3	466 736
Semi-Bent f	13 888	4	104 160	4	194 928
Orbits	19	5	0	5	10 944
Semi-Bent orbits	1	6	45 136		
Balanced orbits	3	7	4960		
		8	180 420		
		9	0		
		10	317 440		
		11	0		
		12	13 888		

Table 15: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 2$

Properties		Nonlinearity		Degrees	
Number of f	31 424 328	0	0	0	0
Homogeneous f	859	1	992	1	0
Rigid f	2480	2	7440	2	41 664
Balanced f	4 228 896	3	158 720	3	7620792
Semi-Bent f	874 944	4	1 536 360	4	22 119 120
Orbits	46	5	34 720	5	1 642 752
Semi-Bent orbits	3	6	2 138 752		
Balanced orbits	6	7	853 120		
		8	15 323 920		
		9	317 440		
		10	9 900 160		
		11	277 760		
		12	874 944		

Table 16: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 3$

Properties		Nonlinearity		Degrees	
Number of f	240 101 200	0	0	0	0
Homogeneous f	61	1	0	1	0
Rigid f	11 520	2	0	2	0
Balanced f	15 582 336	3	153 760	3	23 290 176
Semi-Bent f	2 499 840	4	659 680	4	168 597 840
Orbits	81	5	1 416 576	5	48 213 184
Semi-Bent orbits	2	6	10 731 952		
Balanced orbits	6	7	17 541 536		
		8	112 334 080		
		9	18 213 120		
		10	63 162 624		
		11	10 888 192		
		12	4 999 680		

Table 17: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 4$

Properties		Nonlinearity		Degrees	
Number of f	1 086 598 112	0	0	0	0
Homogeneous f	0	1	0	1	0
Rigid f	47 220	2	0	2	0
Balanced f	187 210 240	3	0	3	27 664 896
Semi-Bent f	2 666 496	4	0	4	763 701 120
Orbits	111	5	7 936 992	5	295 232 096
Semi-Bent orbits	1	6	42 413 952		
Balanced orbits	11	7	53 524 352		
		8	364 837 760		
		9	193 162 240		
		10	375 614 848		
		11	40 608 512		
		12	8 499 456		

Table 18: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 5$

Properties		Nonlinearity		Degrees	
Number of f	1 842 215 424	0	0	0	0
Homogeneous f	0	1	0	1	0
Rigid f	59 760	2	0	2	0
Balanced f	308 646 912	3	0	3	7 999 488
Semi-Bent f	7 999 488	4	0	4	951 105 792
Orbits	81	5	3 499 776	5	883 110 144
Semi-Bent orbits	2	6	2 666 496		
Balanced orbits	9	7	96 827 136		
		8	154 990 080		
		9	694 122 240		
		10	788 449 536		
		11	88 660 992		
		12	12 999 168		

Table 19: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 6$

Properties		Nonlinearity		Degrees	
Number of f	935 273 472	0	0	0	0
Homogeneous f	0	1	0	1	0
Rigid f	64 470	2	0	2	0
Balanced f	85 327 872	3	0	3	0
Semi-Bent f	0	4	0	4	174 655 488
Orbits	33	5	0	5	760 617 984
Semi-Bent orbits	0	6	0		
Balanced orbits	2	7	46 663 680		
		8	0		
		9	436 638 720		
		10	174 655 488		
		11	277 315 584		
		12	0		

Table 20: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 7$

Properties		Nonlinearity		Degrees	
Number of f	158 656 512	0	0	0	0
Homogeneous f	0	1	0	1	0
Rigid f	25 440	2	0	2	0
Balanced f	0	3	0	3	0
Semi-Bent f	0	4	0	4	0
Orbits	4	5	0	5	158 656 512
Semi-Bent orbits	0	6	0		
Balanced orbits	0	7	0		
		8	0		
		9	19 998 720		
		10	0		
		11	138 657 792		
		12	0		

Table 21: Property distribution of functions in $\mathcal{B}_5$ with $\mathcal{T}_5 = 8$