FACTA UNIVERSITATIS (NIŠ)
SER.: ELEC. ENERG. vol. 24, no. 3, December 2011, 357-383

Classes of Bent Functions Identified by Specific Normal Forms and Generated Using Boolean Differential Equations

Bernd Steinbach and Christian Posthoff

Abstract: This paper aims at the identification of classes of bent functions in order to allow their construction without searching or sieving.

In order to reach this aim, we studied first the relationship between bent functions and complexity classes defined by the *Specific Normal Forms* of all Boolean functions. As result of this exploration we found classes of bent functions which are embedded in different complexity classes defined by the *Specific Normal Form*.

In the second step to reach our global aim, we utilized the found classes of bent functions in order to express bent functions in terms of derivative operations of the Boolean Differential Calculus.

In detail, we studied bent functions of two and four variables. This exploration leads finally to *Boolean differential equations* that will allow the direct calculation of all bent functions of two and four variables. A given generalization allows to calculate subsets of bent functions for each even number of Boolean variables.

Keywords: Bent function; classification; specific normal form; Boolean differential calculus; Boolean differential equation; XBOOLE.

1 Introduction

Bent functions $f(x_1,\ldots,x_n)$ are special Boolean functions having valuable properties for applications in cryptography.

Manuscript received July 20, 2011. An earlier version of this paper was presented at the Reed Muller 2011 Workshop, May 25-26, 2011, Gustavelund Conference Centre, Tuusula, Finland.

B. Steinbach is with Institute of Computer Science, Freiberg University of Mining and Technology, Bernhard-von-Cotta-Str. 2, D-09596 Freiberg, Germany (e-mail: steinb@informatik.tu-freiberg.de). C. Posthoff is with Department of Computing and Information Technology, The University of the West Indies, Trinidad & Tobago (e-mail: Christian.Posthoff@sta.uwi.edu).)

Digital Object Identifier: 10.2298/FUEE1103357S

A summary of the knowledge about bent functions in the context of Boolean Algebras was published recently by Butler and Sasao [1]. Our paper follows their approach, including the fact that only even values for *n* are considered. This follows from the original definition of [2].

Naturally, the representation of a function does not have an influence on the function itself. It is, however, very common to use for bent functions the representation in the form of Exclusive-Sum-Of-Products (ESOPs).

The research over the last 10 years in the field of minimal ESOPs has lead to the discovery of a new normal form [3] called *Specific Normal Form* (SNF) [4][1]. The SNF is a unique ESOP out of all possible ESOPs of a Boolean function. Due to the property that the number of cubes in the SNF is a very simple possibility to classify Boolean functions with regard to their complexity [5] [6], SNFs will be used for the analysis of bent functions in section 3. Using the SNF, the most complex Boolean functions [7], [8] can be detected and generated. We analyze in this paper how the bent functions are distributed over the classes of SNFs. Especially, we want to check whether the bent functions belong to these most complex Boolean functions.

Boolean Differential Calculus [9], [10], [11], allows to study the change of the behavior of Boolean functions. Changes of function values can transform a linear function into a bent function or vice versa. Hence, we study in this paper how the Boolean Differential Calculus (BDC) can help to classify the bent functions.

The bent functions are a small set of Boolean functions. In concluding remarks of [1], bent functions are characterized as very rare, they are *a vanishingly small fraction of the total number of functions* when the number of variables increases. In the same book chapter, it is stated that *there is no formal method of constructing all bent functions*. These two properties make the bent functions very valuable for cryptography [12]. We will weaken the second of these statements.

It has been shown in the PhD thesis [13] that the solution of a Boolean differential equation is a set of Boolean functions. In this PhD thesis several approaches to solve Boolean differential equations are given. When a Boolean differential equation for the set of bent functions in a selected Boolean space of an even number of variables has been found, a formal method for constructing all bent functions is available. Section 4 explores these issues.

2 Basic Concepts

Bent functions $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ are Boolean functions that have the largest Hamming distance to any linear function $f_L(\mathbf{x})$.

[1] Previous publications used "special" or "specialized".

Definition 1. *The function $f(\mathbf{x})$ is a **linear** function if it can be written as*

$$f(\mathbf{x}) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n \tag{1}$$

with $a_0, a_1, \ldots, a_n \in B$ given constants.

Since there are $n+1$ independent constants, 2^{n+1} linear functions can be found. Furthermore, there are 2^{2^n} Boolean functions altogether. Hence, $2^{2^n} - 2^{n+1}$ functions do not show the property of linearity.[2]

Definition 2. *The Hamming distance $hd(f,g)$ between two functions $f(\mathbf{x})$ and $g(\mathbf{x})$, is the number of positions (argument vectors) with different values.*

Example. The number of positions where the functions f and g differ from each other is equal to the number of values 1 of the function $f \oplus g$ and can be evaluated using Karnaugh maps:

$f = x_1 x_2 \oplus x_3 x_4$ $\qquad$ $g = x_1 x_3 \oplus x_2 x_4$ $\qquad$ $f \oplus g = (x_1 \oplus x_4)(x_2 \oplus x_3)$

$x_3\ x_4$					f
0 0	0	0	1	0	
0 1	0	0	1	0	
1 1	1	1	0	1	
1 0	0	0	1	0	
	0	1	1	0	x_2
	0	0	1	1	x_1

$x_3\ x_4$					g
0 0	0	0	0	0	
0 1	0	1	1	0	
1 1	0	1	0	1	
1 0	0	0	1	1	
	0	1	1	0	x_2
	0	0	1	1	x_1

$x_3\ x_4$					g
0 0	0	0	1	0	
0 1	0	1	0	0	
1 1	1	0	0	0	
1 0	0	0	0	1	
	0	1	1	0	x_2
	0	0	1	1	x_1

or function tables:

x_1	0000	0000	1111	1111
x_2	0000	1111	0000	1111
x_3	0011	0011	0011	0011
x_4	0101	0101	0101	0101
f	0001	0001	0001	1110
g	0000	0101	0011	0110
$f \oplus g$	0001	0100	0010	1000

As result, we get $hd(f,g) = 4$.

Definition 3. *The **nonlinearity** $NL(f)$ of a nonlinear Boolean function $f(\mathbf{x})$ is the minimum of all Hamming distances between this function and all linear functions.*

We also can say that this is equal to the minimum number of truth table entries that must change in order to convert $f(\mathbf{x})$ into a linear function.

This definition implies some *algorithmic* considerations:

[2] Some authors make a difference between $a_0 = 0$ and $a_0 = 1$. Only the functions of the first set are linear functions, the functions of the second set are called *affine* functions.

- We must calculate the Hamming distance of the given function to all linear functions.
- The minimum of the found values is the nonlinearity of the given function.

In order to find the nonlinearity of each nonlinear function, $2^{2^n} - 2^{n+1}$ nonlinear functions must be tested against 2^{n+1} linear functions, i.e. $(2^{2^n} - 2^{n+1}) \cdot 2^{n+1}$ Hamming distances have to be calculated, basically. This huge amount of comparisons can be restricted to one half, i.e. $(2^{2^n} - 2^{n+1}) \cdot 2^n$, where only linear functions $f_i^l(\mathbf{x})$ (1) with $a_0 = 0$ are used for comparisons. Due to the complement caused for $a_0 = 1$, the Hamming distances for the remaining linear functions $\overline{f_i^l(\mathbf{x})}$ can be calculated using a simple difference $hd(f(\mathbf{x}), \overline{f_i^l(\mathbf{x})}) = 2^n - hd(f(\mathbf{x}), f_i^l(\mathbf{x}))$. However, the reduction by a constant factor of 2 does not change the exponential complexity to calculate the nonlinearity of each nonlinear function.

The term *bent function* was introduced in 1976 by Rothaus [2]. However, his considerations have been based on the algebraic structure of *Galois fields*. The set $B = \{0,1\}$ together with $\wedge$ as multiplication and $\oplus$ as addition satisfies the axioms of a Galois field $GF(B)$ as well as B^n with the same operations (indicated by $GF(B^n)$). Functions from $GF(B^n)$ into $GF(B)$ allow the definition of a *Fourier-transformation*, and for bent functions all Fourier-coefficients had to be equal to ± 1. It could be shown that such functions exist only if n is even. In this case the set of bent functions is equal to the set of functions with maximal nonlinearity. Therefore it is common to define bent functions only when n is even. However, the concept of maximal nonlinearity can also be applied when n is odd. This needs further investigations.

Definition 4. *Let $f(\mathbf{x})$ be a Boolean function of n variables, where n is even. $f(\mathbf{x})$ is a **bent function** if its nonlinearity is as large as possible.*

This means that after the calculation of the nonlinearity of each nonlinear function the maximum of all these values has to be found, and all nonlinear functions with this maximum nonlinearity are the bent functions $f_b(x_1, \ldots, x_n)$.

The simplest bent functions exist for $n = 2$.

Here we have eight linear functions

$$f(x_1, x_2) = a_0 \oplus a_1 x_1 \oplus a_2 x_2,$$

according to the three constants $a_0, a_1, a_2 \in B$.

$a_0a_1a_2$	000	001	010	011	100	101	110	111
f	0	x_2	x_1	$x_1 \oplus x_2$	1	$1 \oplus x_2$	$1 \oplus x_1$	$1 \oplus x_1 \oplus x_2$

There is only one nonlinear term x_1x_2, all nonlinear functions can be built by adding one linear function to this nonlinear term, and we get

$$\begin{array}{llll} x_1x_2 \oplus 0, & x_1x_2 \oplus x_2, & x_1x_2 \oplus x_1, & x_1x_2 \oplus x_1 \oplus x_2, \\ x_1x_2 \oplus 1, & x_1x_2 \oplus x_2 \oplus 1, & x_1x_2 \oplus x_1 \oplus 1, & x_1x_2 \oplus x_1 \oplus x_2 \oplus 1. \end{array}$$

For all the nonlinear functions the nonlinearity is equal to 1, therefore all of them are bent functions because this is the maximum value.

In order to evaluate the bent functions in the context of the *Specific Normal Form* (SNF), we introduce the basic concepts of the SNF, too. An algebraic property of the exclusive-or operation and the Boolean variable x can be seen in the following formulas:

$$x = \overline{x} \oplus 1 \ , \tag{2}$$

$$\overline{x} = 1 \oplus x \ , \tag{3}$$

$$1 = x \oplus \overline{x} \ . \tag{4}$$

These three formulas show that each element of the set $\{x, \overline{x}, 1\}$ can be expressed by the two other elements. The application of these formulas from the left to the right doubles the number of cubes and is called expansion. For each variable of a given ESOP the applicable formula (2), (3), or (4) is executed from the left to the right in the algorithm **Exp(f)** which was defined in [4].

A second important property of the exclusive-or operation for a Boolean function f and a cube C is shown by the following formulas:

$$\begin{aligned} f &= f \oplus 0 \ , \\ 0 &= C \oplus C \ , \\ f &= f \oplus C \oplus C \ . \end{aligned}$$

¿From these formulas follows that two identical cubes can be added to or removed from any ESOP without changing the represented function. Utilizing these formulas, all pairs of identical cubes are removed from a given ESOP of f by the algorithm **R(f)** which was defined in [4], too.

Using the algorithms Exp(f) and R(f), it is possible to create a specific ESOP with a number of remarkable properties which are specified and proven in [4]. Please notice that we have changed the term ”specialized”, used in [4], into the better understandable term ”specific” for the definition of the SNF.

Definition 5. *Take any ESOP of a Boolean function f. The ESOP resulting from*

$$SNF(f) = R(Exp(f))$$

*is called the **Specific Normal Form (SNF)** of the function f.*

3 Basic Results

3.1 Distribution of Bent functions into SNF classes

The number of cubes of $SNF(f)$ is a simple measure of the complexity of a Boolean function $f(\mathbf{x})$. In the first experiment we study the distribution of bent functions over $SNF(f)$-classes.

Tab. 1. Distribution of 8 Bent Functions over $SNF(f)$-Classes for all 16 Boolean Functions of 2 Variables.

Cubes in the		Number of	
SNF	Minimal ESOP	all Functions	Bent Functions
0	0	1	0
4	1	9	4
6	2	6	4

Table 1 shows first that there are bent functions of different complexities. Additionally it can be seen that the SNF - classes consist of bent functions together with functions that are not bent functions. There are 4 bent functions of two variables which belong to the class of the most complex Boolean functions in B^2.

Table 2 shows again that bent function of four variables are distributed over several SNF - classes. Consequently, the bent functions in the Boolean space B^4 have again different complexities. Contrary to the Boolean space B^2 no bent function of four variables belongs to the class of the most complex Boolean functions over B^4. An interesting observation of this first experiment is that for all bent functions f_b of four variables, the number of cubes in the $SNF(f_b)$ modulo 4 is equal to 2. A more detailed analysis is necessary to detect further properties of bent functions.

3.2 Identification of classes of Bent functions

Meier and Staffelbach have found in [14] that the weight of bent functions of n variables is equal to

$$2^{n-1} \pm 2^{\frac{n}{2}-1} \quad .$$

Therefore we study the SNF of such functions more in detail. Especially, we distinguish for bent functions of four variables between the allowed weights of $2^3 - 2^1 = 6$ and $2^3 + 2^1 = 10$. Table 3 reveals that for each bent function of the weight 6 exists an associated bent function of the weight 10. These pairs of bent functions are complements of each other. The complement of a bent function of the

Tab. 2. Distribution of 896 Bent Functions into Classes of $SNF(f)$ for all 65536 Boolean Functions of 4 Variables.

Cubes in the		Number of	
SNF	Minimal ESOP	all Functions	Bent Functions
0	0	1	0
16	1	81	0
24	2	324	0
28	2	1296	0
30	2	648	48
32	3	648	0
34	3	3888	240
36	3	6624	0
36	4	108	0
38	3	7776	384
40	3	2592	0
40	4	6642	0
42	3	216	0
42	4	14256	192
44	4	12636	0
46	4	3888	0
46	5	1296	16
48	5	1944	0
50	5	648	16
54	6	24	0

weight 6 requires an EXOR-operation with a constant 1 which leads to four additional cubes in the SNF of the bent function of weight 10. It should be mentioned that in some cases the minimal ESOPs of a bent function f_b and their complement $\overline{f}_b$ contain the same number of cubes.

Within the set of bent functions of each SNF - class and each weight we identified classes of $2^4 = 16$ bent functions characterized by the following property. If $f(x_1, x_2, x_3, x_4)$ is a bent function then

$$f(x_1 \oplus c_1, x_2 \oplus c_2, x_3 \oplus c_3, x_4 \oplus c_4) \tag{5}$$

is a bent function too, where $c_i \in \{0, 1\}$.

Please notice, in general such a class is not a known affine class which is created by an EXOR of a selected Boolean function and all linear functions of the Boolean space.

For a later evaluation we enumerate the classes of bent functions of four variables having a weight of six. As representative bent functions, we select from each class that function which can be expressed by an ESOP of positive literals.

Tab. 3. Distribution of 896 Bent Functions over $SNF(f)$-Classes for B^4 distinguished between the Weights 6 and 10.

Cubes in the		Number of Bent Functions	
SNF	Minimal ESOP	of Weight 6	of Weight 10
30	2	48	0
34	3	192	48
38	3	192	192
42	4	0	192
46	5	16	0
50	5	0	16

Additionally we give a minimal ESOP and the Karnaugh-map of the selected representative bent functions.

This detailed analysis is summarized in the appendix of this paper and shows that each bent function of four variables can be expressed by an ESOP that consists of conjunctions of two variables. This verifies the general proposition of Rothaus [2] about the degree of Reed-Muller forms of bent functions for the Boolean space B^4.

For each bent function f_b of class $C_i, i = 1,\ldots,28$, exists a complementary bent function $\overline{f}_b$. In the Karnaugh-maps of the representative bent function of the complementary classes $CC_i, i = 1,\ldots,28$, the values zero and one are exchanged in comparison to the 28 classes C_i. The representative bent function $\overline{f}_{bri}$ of the complementary classes CC_i can be built by an EXOR - operation with the constant 1:

$$\overline{f}_{bri} = f_{bri} \oplus 1 \qquad i = 1,\ldots,27 \ ,$$

and

$$\overline{f}_{br28} = x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \ .$$

There is no ESOP expression of representative bent functions $\overline{f}_{bri}, i = 1,\ldots,3$ for B^4 having less products than the positive polarity expression given in the appendix. To complete this analysis, we give the minimal ESOPs of representative bent functions $\overline{f}_{bri_{min}}, i = 4,\ldots,28$ for B^4 which need fewer cubes than the expression where the complement is realized by an EXOR operation with the constant 1.

$$\overline{f}_{br4_{min}} = x_1\overline{x}_2 \oplus x_3\overline{x}_4 \oplus \overline{x}_1\overline{x}_3 \qquad \overline{f}_{br5_{min}} = x_1\overline{x}_2 \oplus \overline{x}_3x_4 \oplus \overline{x}_1\overline{x}_4$$
$$\overline{f}_{br6_{min}} = \overline{x}_1x_2 \oplus x_3\overline{x}_4 \oplus \overline{x}_2\overline{x}_3 \qquad \overline{f}_{br7_{min}} = \overline{x}_1x_2 \oplus \overline{x}_3x_4 \oplus \overline{x}_2\overline{x}_4$$

$$\overline{f}_{br8_{min}} = x_1\overline{x}_3 \oplus x_2\overline{x}_4 \oplus \overline{x}_1\overline{x}_2 \qquad \overline{f}_{br9_{min}} = x_1\overline{x}_3 \oplus \overline{x}_2 x_4 \oplus \overline{x}_1\overline{x}_4$$
$$\overline{f}_{br10_{min}} = \overline{x}_1 x_3 \oplus x_2\overline{x}_4 \oplus \overline{x}_2\overline{x}_3 \qquad \overline{f}_{br11_{min}} = \overline{x}_1 x_3 \oplus \overline{x}_2 x_4 \oplus \overline{x}_3\overline{x}_4$$

$$\overline{f}_{br12_{min}} = x_1\overline{x}_4 \oplus x_2\overline{x}_3 \oplus \overline{x}_1\overline{x}_2 \qquad \overline{f}_{br13_{min}} = x_1\overline{x}_4 \oplus \overline{x}_2 x_3 \oplus \overline{x}_1\overline{x}_3$$
$$\overline{f}_{br14_{min}} = \overline{x}_1 x_4 \oplus x_2\overline{x}_3 \oplus \overline{x}_2\overline{x}_4 \qquad \overline{f}_{br15_{min}} = \overline{x}_1 x_4 \oplus \overline{x}_2 x_3 \oplus \overline{x}_3\overline{x}_4$$

$$\overline{f}_{br16_{min}} = \overline{x}_1 x_3 \oplus \overline{x}_1 x_4 \oplus x_1 x_2 \oplus \overline{x}_3\overline{x}_4$$
$$\overline{f}_{br17_{min}} = \overline{x}_2 x_3 \oplus \overline{x}_2 x_4 \oplus x_1 x_2 \oplus \overline{x}_3\overline{x}_4$$
$$\overline{f}_{br18_{min}} = \overline{x}_1 x_2 \oplus \overline{x}_1 x_3 \oplus x_3 x_4 \oplus \overline{x}_2\overline{x}_3$$
$$\overline{f}_{br19_{min}} = \overline{x}_1 x_2 \oplus \overline{x}_1 x_4 \oplus x_3 x_4 \oplus \overline{x}_2\overline{x}_4$$

$$\overline{f}_{br20_{min}} = \overline{x}_1 x_2 \oplus \overline{x}_1 x_4 \oplus x_1 x_3 \oplus \overline{x}_2\overline{x}_4$$
$$\overline{f}_{br21_{min}} = \overline{x}_2 x_3 \oplus \overline{x}_2 x_4 \oplus x_1 x_3 \oplus \overline{x}_3\overline{x}_4$$
$$\overline{f}_{br22_{min}} = \overline{x}_1 x_2 \oplus \overline{x}_1 x_3 \oplus x_2 x_4 \oplus \overline{x}_2\overline{x}_3$$
$$\overline{f}_{br23_{min}} = \overline{x}_1 x_3 \oplus \overline{x}_1 x_4 \oplus x_2 x_4 \oplus \overline{x}_3\overline{x}_4$$

$$\overline{f}_{br24_{min}} = \overline{x}_1 x_2 \oplus \overline{x}_1 x_3 \oplus x_1 x_4 \oplus \overline{x}_2\overline{x}_3$$
$$\overline{f}_{br25_{min}} = \overline{x}_2 x_3 \oplus \overline{x}_2 x_4 \oplus x_1 x_4 \oplus \overline{x}_3\overline{x}_4$$
$$\overline{f}_{br26_{min}} = \overline{x}_1 x_2 \oplus \overline{x}_1 x_4 \oplus x_2 x_3 \oplus \overline{x}_2\overline{x}_4$$
$$\overline{f}_{br27_{min}} = \overline{x}_1 x_3 \oplus \overline{x}_1 x_4 \oplus x_2 x_3 \oplus \overline{x}_3\overline{x}_4$$

$$\overline{f}_{br28_{min}} = \overline{x}_1 x_2 x_4 \oplus x_1\overline{x}_2\overline{x}_4 \oplus x_1\overline{x}_3 \oplus x_2 x_3 \oplus x_3 x_4$$

This detailed analysis shows that for each bent function of four variables there exists an ESOP consisting of pairs of variables. All representative bent functions of four variables include non-negated variables only. From this property and (5) follows that for each bent function of four variables exists an ESOP of pairs of variables where each variable appears in a single polarity. The number of such pairs k, the weight w of the bent function and the number of variables n in the Boolean space B^n determine directly the number of cubes $\left|C_{f_b}^{SNF}(n,k,w)\right|$ of a bent function in their SNF:

$$\left|C_{f_b}^{SNF}(n=4,k,w)\right| = 2^n + 2^{n-2} * k + w \ .$$

4 Boolean Differential Equations of Bent Functions

4.1 Boolean differential calculus

The Boolean Differential Calculus (BDC) is a comprehensive and powerful theory. Some introduction into the BDC including selected applications are given in [9] and [10]. A comprehensive description of the BDC in connection with a large number of applications has been published in [11]. Here we repeat a small set of definitions which are required to express the bent functions.

Definition 6. *Let* $f(\mathbf{x}) = f(x_i, \mathbf{x}_1)$ *be a Boolean function of n variables with* $\mathbf{x}_1 = (x_1, \ldots x_{i-1}, x_{i+1}, \ldots, x_n)$. *Then*

$$\frac{\partial f(\mathbf{x})}{\partial x_i} = f(x_i = 0, \mathbf{x}_1) \oplus f(x_i = 1, \mathbf{x}_1) \tag{6}$$

is the (simple) derivative with regard to x_i.

The result of a simple derivative operation is a new Boolean function g which does not depend on the variable x_i anymore (x_i has been set to 0 and to 1). The *derivative* is equal to 1 iff the change of the variable x_i changes the function value for constant values of the remaining variables $\mathbf{x}_1$ (since $0 \oplus 1 = 1 \oplus 0 = 1$); otherwise it is equal to 0.

The simple derivative operation of the Boolean Differential Calculus allows to verify whether a given function is linear. From both Definition 1 and Definition 6 follows directly that

$$\frac{\partial f(\mathbf{x})}{\partial x_i} = a_i \quad .$$

Hence, any linear function $f(\mathbf{x})$ must satisfy either

$$\frac{\partial f(\mathbf{x})}{\partial x_i} = 0 \tag{7}$$

or

$$\frac{\partial f(\mathbf{x})}{\partial x_i} = 1 \tag{8}$$

for each variable x_i.

Due to (7) the constant functions $f = 0$ and $f = 1$ are linear functions. All the other linear functions can be built by extending these constant linear functions by variables x_i (which are added by $\oplus$).

Definition 7. *Let* $f(\mathbf{x}) = f(\mathbf{x}_0, \mathbf{x}_1)$ *be a Boolean function of n variables, where* $\mathbf{x}_0 = (x_1, \ldots, x_k)$, $\mathbf{x}_1 = (x_{k+1}, \ldots, x_n)$, *and* $\overline{\mathbf{x}}_1 = (\overline{x}_{k+1}, \ldots, \overline{x}_n)$. *Then*

$$\frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0} = f(\mathbf{x}_0, \mathbf{x}_1) \oplus f(\overline{\mathbf{x}}_0, \mathbf{x}_1) \tag{9}$$

is the vectorial derivative with regard to $\mathbf{x}_0$.

The vectorial derivative results in a Boolean function that depends in general on both the variables of $\mathbf{x}_0$ (which have been included in the derivative operation) and the remaining variables of $\mathbf{x}_1$. There are certain functions $f(\mathbf{x}_0, \mathbf{x}_1)$ where the result of a vectorial derivative operation does not depend on some of these variables.

The vectorial derivative is equal to 1 if the simultaneous change of the variables of $\mathbf{x}_0$ changes the function value for fixed values of the remaining variables of $\mathbf{x}_1$. This is caused by the EXOR-operation in (9) that is equal to 1 if different pairs of function values (e.g. '01' or '10') occur.

The vectorial derivative operation of the Boolean Differential Calculus allows to verify whether a given function is linear, too. From both Definition 1 and Definition 7 follows that any linear function $f(\mathbf{x}) = f(\mathbf{x}_0, \mathbf{x}_1)$ must satisfy either

$$\frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0} = 0 \tag{10}$$

or

$$\frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0} = 1 \tag{11}$$

for each not empty set of variables $\mathbf{x}_0$ because:

1. variables x_i with $a_i = 0$ in (1) do not appear in the expression (9),
2. remaining variables x_i assigned to $\mathbf{x}_1$ appear twice in the expression (9) and can be combined to the constant value 0,
3. remaining variables x_i assigned to $\mathbf{x}_0$ appear as pairs in both non-negated and negated form in the expression (9); each of these pair can be combined to the constant value 1 ($x_i \oplus \overline{x}_i = 1$),
4. the expression evaluates to the constant value 0 (10) for an even number of remaining values 1, and it evaluates to the constant value 1 (11) in case of an odd number of 1 values.

The simple derivatives in (7) and (8) are special cases of the vectorial derivatives in (10) and (11).

Definition 8. *Let* $f(\mathbf{x}) = f(\mathbf{x}_0, \mathbf{x}_1)$ *be a Boolean function of n variables, and let* $\mathbf{x}_0 = (x_1, x_2, \ldots, x_m)$, *and* $\mathbf{x}_1 = (x_{m+1}, \ldots, x_n)$. *Then*

$$\frac{\partial^m f(\mathbf{x}_0, \mathbf{x}_1)}{\partial x_1 \partial x_2 \ldots \partial x_m} = \frac{\partial}{\partial x_m}(\ldots(\frac{\partial}{\partial x_2}(\frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial x_1}))\ldots)$$

is the m-fold derivative with regard to $\mathbf{x}_0$.

In contrast to the vectorial derivative where pairs of function values decide about the result, the results are now determined by all 2^m function values of a subspace $\mathbf{x}_1 = const$. Due to the Definitions 6 and 8, the result of the *m*-fold derivative operation with regard to $\mathbf{x}_0$ does not depend on the variables of $\mathbf{x}_0$. The variables of the vector $\mathbf{x}_0$ can be used in any order. The result of any *m*-fold derivative operation will always be the same, since the respective operations are commutative.

The *m*-fold derivative of a function $f(\mathbf{x}_0, \mathbf{x}_1)$ with regard to $\mathbf{x}_0$ is equal to 1 for such subspaces $\mathbf{x}_1 = const$ that include an odd number of function values 1.

One of the theorems of the BDC allows to express a 2-fold derivative using simple and vectorial derivatives only. In the following subsections Theorem 1 will be used to simplify Boolean differential equations which express certain classes of bent functions. The proof of Theorem 1 is straightforward based on the definitions of involved derivatives and the Shannon decomposition.

Theorem 1. *Let* $f(\mathbf{x}) = f(\mathbf{x}_0, \mathbf{x}_1)$ *be a Boolean function of n variables, and let* $\mathbf{x}_0 = (x_1, x_2)$. *Then it holds that*

$$\frac{\partial^2 f(\mathbf{x}_0, \mathbf{x}_1)}{\partial x_1 \partial x_2} = \frac{\partial f(\mathbf{x})}{\partial x_1} \oplus \frac{\partial f(\mathbf{x})}{\partial x_2} \oplus \frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0} \quad . \tag{12}$$

4.2 Boolean differential equations

A *Boolean Differential Equation* (BDE) is an equation in which Boolean variables, Boolean functions, and derivatives of Boolean functions are connected by Boolean operations in expressions on both sides. It is a result of [13] that

1. the solution of a Boolean differential equation is a set of Boolean functions, and
2. each set of Boolean functions can be expressed by a Boolean differential equation.

There is a special type of Boolean differential equations in which Boolean variables do not appear explicitly.

The solution of such Boolean differential equation are classes of Boolean functions as specified in (5). Because each bent function is a member of such a class, we restrict ourselves here to this special type of Boolean differential equations.

In [13] two approaches for the solution of Boolean differential equations for classes are given.

The first allows the iterative generation of the function classes. The second is called *Separation of Function Classes* and creates all solution classes at the same time. This approach is explained in [9] and [15] too. The calculation steps to solve a Boolean differential equation are very simple and fast. All Boolean differential equations for bent functions given in the next subsections were solved within fractions of a second.

4.3 Bent functions of two variables

It is the main issue to find a Boolean differential equation for a known set of Boolean functions.

Sometimes such equations are rather complicated.

For example, the class of bent functions

$$\{x_1 \wedge x_2, \overline{x}_1 \wedge x_2, x_1 \wedge \overline{x}_2, \overline{x}_1 \wedge \overline{x}_2\} \tag{13}$$

is the solution of the Boolean differential equation (14):

$$\begin{aligned} &f(\mathbf{x}) \cdot \frac{\partial f(\mathbf{x})}{\partial x_1} \cdot \frac{\partial f(\mathbf{x})}{\partial x_2} \cdot \frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)} \vee \overline{f(\mathbf{x})} \cdot \frac{\partial f(\mathbf{x})}{\partial x_1} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_2}} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)}} \vee \\ &\overline{f(\mathbf{x})} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_1}} \cdot \frac{\partial f(\mathbf{x})}{\partial x_2} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)}} \vee \overline{f(\mathbf{x})} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_1}} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_2}} \cdot \frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)} = 1 \ . \end{aligned} \tag{14}$$

There are only $2^{2^2} = 16$ functions in the Boolean space B^2. The substitution of all of them into (14) proves that this equation holds exactly for the functions of the set (13).

The complemented set of bent functions

$$\{x_1 \vee x_2, \overline{x}_1 \vee x_2, x_1 \vee \overline{x}_2, \overline{x}_1 \vee \overline{x}_2\} \tag{15}$$

is the solution of the Boolean differential equation (16):

$$\begin{aligned} &\overline{f(\mathbf{x})} \cdot \frac{\partial f(\mathbf{x})}{\partial x_1} \cdot \frac{\partial f(\mathbf{x})}{\partial x_2} \cdot \frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)} \vee f(\mathbf{x}) \cdot \frac{\partial f(\mathbf{x})}{\partial x_1} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_2}} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)}} \vee \\ &f(\mathbf{x}) \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_1}} \cdot \frac{\partial f(\mathbf{x})}{\partial x_2} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)}} \vee f(\mathbf{x}) \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_1}} \cdot \overline{\frac{\partial f(\mathbf{x})}{\partial x_2}} \cdot \frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)} = 1 \ . \end{aligned} \tag{16}$$

This Boolean differential equation can be confirmed in the same way.

A Boolean differential equation that describes both classes of bent functions together must combine the left-hand sides of (14) and (16) using an OR-operation. Obviously, the terms $(f(\mathbf{x}) \vee \overline{f(\mathbf{x})})$ can be separated in the combined left-hand side using the distributive law. These terms can be replaced by a constant 1 and finally removed. The remaining expression can be further simplified:

$$\frac{\partial f(\mathbf{x})}{\partial x_1} \oplus \frac{\partial f(\mathbf{x})}{\partial x_2} \oplus \frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)} = 1 \ . \tag{17}$$

Using (12) we get from (17) the simple Boolean differential equation:

$$\frac{\partial^2 f(x_1, x_2)}{\partial x_1 \partial x_2} = 1 \tag{18}$$

which describes all bent functions of two variables. This Boolean differential equation can be found directly. It is known that the 2-fold derivative is equal to 1 for all functions $f(x_1, x_2)$ which have an odd number of functions values 1. For B^2 all functions with an odd number of functions values 1 are bent functions.

4.4 Solving a Boolean differential equation using XBOOLE

A BDE like (18) can be solved easily using XBOOLE [16], [17]. The needed theory is described in [9]. Using this theory, a simple PROBLEM PROGRAM (PRP) for the XBOOLE-Monitor allows to solve the BDE (18) in split second. Hints for download and using the XBOOLE-Monitor for free are given in [9], too.

The main steps to solve the BDE (18) are:

1. convert the BDE (18) into the BDE (17),
2. substitute $u_1 = \frac{\partial f(\mathbf{x})}{\partial x_1}$, $u_2 = \frac{\partial f(\mathbf{x})}{\partial x_2}$, and $u_3 = \frac{\partial f(\mathbf{x})}{\partial (x_1, x_2)}$,
3. solve the associated Boolean equation $u_1 \oplus u_2 \oplus u_3 = 1$ of (17) (executed by the operation `sbe`),
4. transform from the space of changes $\mathbf{u}$ into the space of values $\mathbf{v}$ using $v_0 = u_0$, $v_1 = u_0 \oplus u_1$, $v_2 = u_0 \oplus u_2$, $v_3 = u_0 \oplus u_3$ (executed by the operations `sbe`, `isc`, and `_maxk`),
5. restrict local solutions to allowed global one in two iterations by exchange of columns first $(v_0, v_2) \leftrightarrow (v_1, v_3)$ and second $(v_0, v_1) \leftrightarrow (v_2, v_3)$ (executed by the operation `cco`) and calculation of required intersections (executed by the operation `isc`).

```
space 32 1
avar 1
u0 u1 u2 u3
v0 v1 v2 v3.
sbe 1 1
u1#u2#u3=1.
sbe 1 2
v0=u0,
v1=u0#u1,
v2=u0#u2,
v3=u0#u3.
isc 1 2 3
_maxk 3 <u0 u1 u2 u3> 4
```

a)

```
vtin 1 10
v0 v2.
vtin 1 11
v1 v3.
cco 4 10 11 12
isc 4 12 13
vtin 1 20
v0 v1.
vtin 1 21
v2 v3.
cco 13 20 21 22
isc 13 22 23
sts bent2
```

b)

	v0	v1	v2	v3
1:	0	1	1	1
2:	1	0	0	0
3:	1	0	1	1
4:	0	1	0	0
5:	0	0	0	1
6:	1	1	1	0
7:	1	1	0	1
8:	0	0	1	0

Fig. 1. Solving the BDE for bent functions of two variables using the XBOOLE-Monitor: a) PRP b) solution TVL.

In order to solve the BDE (18), the PRP of Figure 1 a) must be executed in the XBOOLE-Monitor. The solution TVL 23 is shown in Figure 1 b). Each row represent a solution function defined by

$$f(x_1,x_2) = v_0 \wedge \overline{x}_1\overline{x}_2 \vee v_1 \wedge x_1\overline{x}_2 \vee v_2 \wedge \overline{x}_1 x_2 \vee v_3 \wedge x_1 x_2 \quad .$$

Figure 1 b) describes the 8 functions of the function sets (13) and (15).

4.5 Bent functions of four variables

The knowledge of the Boolean differential equations for bent functions of 2 variables helps to find the appropriate Boolean differential equations for bent functions of 4 variables. As seen for B^2, simpler Boolean differential equations exist for pairs of classes which include functions complementary to the functions of the other class.

Definition 9. *A **pair of complementary classes** PCC_i of Boolean functions covers the given class C_i and the class of their complementary functions CC_i.*

As enumerated in the subsection 3.2, there are 28 PCC_i of 4 four variables. For each $PCC_i, i = 1,\ldots,28$ a Boolean differential equation can be given. In order to save space, we focus on the minimal and maximal bent functions of 4 variables.

Definition 10. *A bent function is*

- ***minimal*** *when its fixed polarity ESOP includes the smallest possible number of conjunctions consisting of two variables each, or*
- ***maximal*** *when its fixed polarity ESOP includes the largest possible number of conjunctions consisting of two variables each.*

The detailed analysis of bent functions of 4 variables in Subsection 3.2 identified the minimal PCC_i for i=1, 2 and 3. There is only the single maximal PCC_{28}.

There are six pairs of variables in B^4. The 2-fold derivatives of given functions with regard to these pairs of variables determine whether a given function is a bent function.

The Boolean differential equations for pairs of classes of minimal bent functions in B^4 are:

for PCC_1

$$\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_3}} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_4}} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3}} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4}} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4} = 1 \ , \tag{19}$$

for PCC_2

$$\overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2}} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_3} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_4}} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3}} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4}} = 1 \ ,$$

for PCC_3

$$\overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2}} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_3}} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4}} \cdot \overline{\frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4}} = 1 \ .$$

The Boolean differential equation for the pair of classes PCC_{28} of maximal bent functions in B^4 is:

$$\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_3} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4} = 1 \ .$$

The Boolean differential equations for the other dedicated pairs of classes of bent functions have a similar structure. The correctness of all Boolean differential equations for classes of bent functions has been verified by solving the differential equation using the XBOOLE monitor [17] and checking the solution set.

Theorem 2. *The solution of the Boolean differential equation* (20)

$$\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_3} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} = 1 \ . \tag{20}$$

is a set four variable functions. This set includes exactly 896 functions. All of them are bent functions of four variables. There exist no further bent function of four variables.

Proof. There are exactly 65536 Boolean functions of the four variables x_1, x_2, x_3, and x_4. All of them can be substituted into the Boolean differential equation (20). All such functions, which satisfy (20), are elements of the set $S_{bde-bf4}$. The set $S_{bde-bf4}$ includes exactly 896 Boolean functions of four variables. Applying Definition 4 to all Boolean functions of four variables finds the set $S_{def-bf4}$ of all bent functions. A comparison shows that these finite sets include exactly the same functions so that $S_{bde-bf4} = S_{def-bf4}$. □

It should be mentioned that it is not necessary to check each Boolean function of four variables whether it is a solution of the Boolean differential equation (20). An algorithm that allows to solve a Boolean differential equation is given in [9]. The execution of this algorithm creates the set of exactly all Boolean functions which solve the given Boolean differential equation. The execution of this algorithm for the Boolean differential equation (20) creates exactly the set of all 896 bent functions of four variables.

4.6 Bent functions of more than four variables

In the following, the relative weight of Boolean function will be used for some conditions.

Definition 11. *The **relative weight** $\rho(f(\mathbf{x}))$ of Boolean function f(**x**) of n variables is the number of 1's in the truth table of f(**x**) divided by all 2^n entries.*

Using Definition 4 of a bent function of n variables, it is necessary to compare the given function with 2^{n+1} linear functions in order to decide whether it is a bent function or not. Due to (10) and (11), all $2^n - 1$ vectorial derivatives of a linear function with regard to each set of variables $\mathbf{x}_0$ is one of the constant functions $f = 0$ or $f = 1$. Hence, for a maximal distance to each linear function $f(\mathbf{x}) = f(\mathbf{x}_0, \mathbf{x}_1)$ the relative weight of all vectorial derivatives of a bent function with regard to each set of variable $\mathbf{x}_0$ must be equal to 0.5:

$$\rho\left(\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}_0}\right) = 0.5 \ . \tag{21}$$

Using (21) for all $2^n - 1$ not empty set of variables $\mathbf{x}_0$ reduces the check for a bent function from 2^{n+1} to $2^n - 1$ comparisons. The condition (21) is known from Theorem 5.12 in [18].

The Boolean differential equations in the previous section use 2-fold derivatives in order to identify the bent property. Each variable appears in a 2-fold derivative of the Boolean differential equation of a certain class of bent functions. This raises the question about the relationship between a 2-fold derivative and the condition (21).

Theorem 3. *For each Boolean function of 2 variables* $f(x_1,x_2)$ *the Boolean differential equation* (18) *is necessary and sufficient to satisfy the condition* (21).

Proof. At all, there are $2^{2^2} = 16$ Boolean functions in the Boolean space B^2. All of them are enumerated in Table 4 together with the relative weights of all $2^2 - 1 = 3$ vectorial derivatives and the calculated result of the 2-fold derivative with regard to both variables x_1 and x_2. This complete evaluation shows both in all case of relative weights of 0.5 for all vectorial derivatives the 2-fold derivative is equal to the constant value 1 and in all cases with a constant value 1 for the 2-fold derivative the relative weights of all vectorial derivatives are equal to 0.5. Hence, we have a complete proof of Theorem 3. □

Tab. 4. Evaluation of all Boolean Functions $f(x_1,x_2)$ of 2 Variables

$f(\mathbf{x})$	$\rho\left(\frac{\partial f\mathbf{x})}{\partial x_1}\right)$	$\rho\left(\frac{\partial f\mathbf{x})}{\partial x_2}\right)$	$\rho\left(\frac{\partial f\mathbf{x})}{\partial(x_1,x_2)}\right)$	$\frac{\partial^2 f\mathbf{x})}{\partial x_1 \partial x_2}$
0	0	0	0	0
$x_1 \wedge x_2$	0.5	0.5	0.5	1
$\overline{x}_1 \wedge x_2$	0.5	0.5	0.5	1
$x_1 \wedge \overline{x}_2$	0.5	0.5	0.5	1
$\overline{x}_1 \wedge \overline{x}_2$	0.5	0.5	0.5	1
x_1	1	0	1	0
$\overline{x}_1$	1	0	1	0
x_2	0	1	1	0
$\overline{x}_2$	0	1	1	0
$x_1 \oplus x_2$	1	1	0	0
$\overline{x}_1 \oplus x_2$	1	1	0	0
$x_1 \vee x_2$	0.5	0.5	0.5	1
$\overline{x}_1 \vee x_2$	0.5	0.5	0.5	1
$x_1 \vee \overline{x}_2$	0.5	0.5	0.5	1
$\overline{x}_1 \vee \overline{x}_2$	0.5	0.5	0.5	1
1	0	0	0	0

Theorem 4. *For Boolean functions of more than two variables* $f(\mathbf{x}) = f(x_1,x_2,\mathbf{x}_1)$ *the Boolean differential equation*

$$\frac{\partial^2 f(x_1,x_2,\mathbf{x}_1)}{\partial x_1 \partial x_2} = 1 \tag{22}$$

is sufficient but not necessary to satisfy the condition (21). *In* $f(\mathbf{x})$ *each pair of variables can be assigned to the used variables* x_1 *and* x_2.

Proof. For bent functions of more than two variables the set $\mathbf{x}_1$ includes $k \geq 2$ variables. The result of the 2-fold derivative (22) can be split into 2^k subfunctions for the Boolean subspaces defined by $\mathbf{x}_1 = \mathbf{c}$.

The equation (22) is equivalent to 2^k equations (18) created for the 2^k Boolean subspaces defined by $\mathbf{x}_1 = \mathbf{c}$. Due to Theorem 3, it follows form (22) that

$\rho\left(\frac{\partial f\mathbf{x})}{\partial x_1}\right) = 0.5,$

$\rho\left(\frac{\partial f\mathbf{x})}{\partial x_2}\right) = 0.5,$ and

$\rho\left(\frac{\partial f\mathbf{x})}{\partial (x_1,x_2)}\right) = 0.5$

for each subspace and consequently for the whole Boolean space. Because each pair of variables can be assigned to the specified variables x_1 and x_2 and vectorial derivatives with regard to a larger number of variables can be composed by vectorial derivatives with regard fitting subsets of variables, it is shown that (22) is sufficient for the condition (21).

In order to show that (22) is not necessary to satisfy the condition (21), we assume that (22) holds in $2^k - 4$ subspaces. To the remaining 4 subspaces we assign each of the functions $f_1(x_1,x_2) = 0$, $f_2(x_1,x_2) = x_1$, $f_3(x_1,x_2) = x_2$, and $f_4(x_1,x_2) = x_1 \oplus x_2$ exactly once. The 2-fold derivatives with regard to x_1 and x_2 are equal to 0 for these four subspaces. Hence, the equation (22) does not hold. However, from Table 4 follows that all three relative weights $\rho\left(\frac{\partial f\mathbf{x})}{\partial x_1}\right)$, $\rho\left(\frac{\partial f\mathbf{x})}{\partial x_2}\right)$, and $\rho\left(\frac{\partial f\mathbf{x})}{\partial (x_1,x_2)}\right)$ are equal to 1 in two of these subspaces and are equal to 0 in the other two of these subspaces. Hence, all three relative weights in the four subspaces are equal to 0.5. Together with the relative weights of 0.5 in the remaining subspaces caused value 1 of the 2-fold derivative, all three relative weights are equal to 0.5. This example proves that the Boolean differential equation (22) is not necessary to satisfy the condition (21); in this way we have a complete proof of Theorem 4. □

As example for Theorem 4 we can take the representative bent function of class 1: $f_{br1} = x_1 x_2 \oplus x_3 x_4$. As shown in (19) we have for this function $\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2} = 1$, $\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_3} = 0$, $\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_4} = 0$, $\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} = 0$, $\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4} = 0$, and $\frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4} = 1$.

Based on Theorem 4, we can construct recursively a Boolean differential equation that describes a subset of all bent functions for any Boolean space of an even number n of variables.

We enumerate the n variables by $\mathbf{x} = (x_1, \ldots, x_n)$.

1. If $n = 2$, the Boolean differential equation is (18).
2. If $n > 2$, create $n-1$ segmentations of $\mathbf{x}$ into two subsets $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1)$. $\mathbf{x}_0$ includes the first variable of $\mathbf{x}$ and for each segmentation one of the remaining variables of $\mathbf{x}$. $\mathbf{x}_1$ includes the variables not selected for $\mathbf{x}_0$. Build 2-fold

derivatives with regard to the variables of $\mathbf{x}_0$ and connect each of them recursively by the left-hand side of a Boolean differential equation created for the associated set of variables $\mathbf{x}_1$. Use the conjunction between the 2-fold derivatives and the recursively build sub-expression and connect these terms by EXOR to the left-hand side of the Boolean differential equation which is equal to 1.

The Boolean differential equation for all bent function of 4 variables (20) is an example of the application of this recursive construction. Due to Theorem 2 the Boolean differential equation (20) is a necessary and sufficient condition for all bent function of 4 variables.

A corollary of Theorem 4 is the fact that Boolean differential equations of 2-fold derivatives allow to describe subsets of bent functions for a given number of variables. This shows, similarly to the distribution of the bent functions to different function classes which are characterized by their *SNF*, that the bent functions of a fixed number of variables can be classified furthermore.

A sufficient Boolean differential equation (23) for bent functions of 6 variables consists of 15 conjunctions of three 2-fold derivatives each. These terms are connected by EXOR-operations and put into a Boolean differential equation which is equal to 1. All six variables appear in the 2-fold derivatives of each term.

$$\begin{aligned}
&\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2} \cdot \left(\frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_5 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_5} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_4 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_6} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_4 \partial x_5} \right) \oplus \\
&\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_3} \cdot \left(\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_5 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_5} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_4 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_6} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_4 \partial x_5} \right) \oplus \\
&\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_4} \cdot \left(\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_5 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_5} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_6} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_5} \right) \oplus \\
&\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_5} \cdot \left(\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_4 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_6} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_6} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4} \right) \oplus \\
&\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_6} \cdot \left(\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_4 \partial x_5} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_4} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_5} \oplus \frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_5} \cdot \frac{\partial^2 f(\mathbf{x})}{\partial x_3 \partial x_4} \right) = 1.
\end{aligned} \tag{23}$$

It will be a future task to find Boolean differential equations for each Boolean space of an even number of variables which describe all bent functions in a necessary and sufficient manner.

5 Conclusion

We explored in this paper bent functions in the context of the specific normal form (SNF) and the Boolean differential calculus (BDC). In detail we classified the bent functions of two and four variables.

We found that for these Boolean spaces each bent function can be represented by a fixed polarity ESOP with conjunctions of two variables and of an optional complement (additionally a constant 1). For cases where the bent function of a class can be expressed by an ESOP with fewer conjunctions we listed these minimal ESOPs for the representative ESOP of such classes. Commonly, the number of cubes in the SNF and the weight of a bent function indicate the number of cubes in its fixed-polarity ESOP.

The BDC is a convenient theory to describe both linear functions and bent functions. Boolean differential equations (BDE) allow both the specification of classes or pairs of complemented classes and the set of all bent functions. Solving the BDE of a certain set of bent functions generates directly this function set without searching over the huge set of all 2^{2^n} Boolean functions of n variables. The simpleness of the algorithm to solve a BDE for a bent function was shown by a PRP for the XBOOLE-Monitor. Necessary and sufficient BDEs are given for bent functions of B^2 and B^4. A given algorithm allows to create recursively BDEs which describe certain subsets of bent functions for each Boolean space of an even number of variables.

References

[1] J. T. Butler and T. Sasao, *Progress in Applications of Boolean Functions*. Morgan & Claypool Publishers, San Rafael, CA - USA, 2010, ch. Boolean Functions for Cryptography, pp. 33–54.

[2] O. S. Rothaus, "On "bent" functions," *J. Combinatorial Theory*, vol. 20, pp. 300–305, 1976.

[3] B. Steinbach and C. Posthoff, "Extended Theory of Boolean Normal Forms," in *Proceedings of the 6th Annual Hawaii International Conference on Statistics*, Honolulu, Hawaii, 2007, pp. 1124–1139.

[4] B. Steinbach and A. Mishchenko, "SNF: A Special Normal Form for ESOPs," in *Proceedings of the 5th International Workshop on Application of the Reed-Muller Expansion in Circuit Design (RM 2001)*, Mississippi State University, Starkville (Mississippi) USA, Aug. 10–11, 2001, pp. 66–81.

[5] B. Steinbach, V. Yanchurkin, and M. Lukac, "On SNF Optimization: a Functional Comparison of Methods," in *Proceedings of the 6th International Symposium on Representations and Methodology of Future Computing Technology (RM 2003)*, University of Trier, Germany, 2003, pp. 11–18.

[6] B. Steinbach and A. D. Vos, "The Shape of the SNF as a Source of Information," in *Boolean Problems, Proceedings of the 8th International Workshops on Boolean Problems*, Freiberg University of Mining and Technology, Freiberg, Germany, 2008, pp. 127–136.

[7] B. Steinbach, "Most Complex Boolean Functions," in *Proceedings Reed-Muller 2007*, University of Oslo, Norway, 2007, pp. 13–23.

[8] ——, "Most complex boolean functions detected by the specialized normal form," *FACTA UNIVERSITATIS, Ser.: Elec and Energ.*, vol. 20, no. 3, pp. 259–279, Dec. 2007. [Online]. Available: http://factaee.elfak.ni.ac.rs/fu2k73/1steinbach.pdf

[9] C. Posthoff and B. Steinbach, *Logic Functions and Equations - Binary Models for Computer Science*. Dordrecht, The Netherlands: Springer, 2004.

[10] B. Steinbach and C. Posthoff, *Progress in Applications of Boolean Functions*. Morgan & Claypool Publishers, San Rafael, CA - USA, 2010, ch. Boolean Differential Calculus, pp. 55–78.

[11] ——, "Boolean differential calculus - theory and applications," *Journal of Computational and Theoretical Nanoscience*, vol. 7, no. 6, pp. 933–981, 2010.

[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[13] B. Steinbach, "Lösung binärer Differentialgleichungen und ihre Anwendung auf binäre Systeme," Ph.D. dissertation, TH Karl-Marx-Stadt (Chemnitz), Germany, 1981.

[14] W. Meier and O. Staffelbach, *Advances in Cryptology - EUROCRYPT '89*, ser. Lecturer Notes in Computer Science. Springer, 1989, vol. 434, ch. Nonlinearity Criteria for Cryptographic Functions, pp. 549–562.

[15] B. Steinbach and C. Posthoff, "Boolean differential equations," in *Proceedings of the 20th International Workshops on Post-Binary ULSI Systems*, Tuusula, Finnland, 2011, pp. 46–53.

[16] B. Steinbach, "XBOOLE - a toolbox for modelling, simulation, and analysis of large digital systems," *System Analysis and Modeling Simulation*, vol. 9, no. 4, pp. 297–312, 1992.

[17] B. Steinbach and C. Posthoff, *Logic Functions and Equations - Examples and Exercises*. Springer Science + Bussiness Media B.V., 2009, iSBN=9781402095948.

[18] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. Academic Press, 2009.

6 Appendix: Representative Bent Functions of 4 Variables

Representative bent function of class 1: Cubes in SNF = 30

x_3	x_4					f
0	0	0	0	1	0	
0	1	0	0	1	0	
1	1	1	1	0	1	
1	0	0	0	1	0	
		0	1	1	0	x_2
		0	0	1	1	x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br1} = x_1 x_2 \oplus x_3 x_4$$

Representative bent function of class 2: Cubes in SNF = 30

x_3 x_4					f
0 0	0	0	0	0	
0 1	0	1	1	0	
1 1	0	1	0	1	
1 0	0	0	1	1	
	0	1	1	0	x_2
	0	0	1	1	x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br2} = x_1 x_3 \oplus x_2 x_4$$

Representative bent function of class 3: Cubes in SNF = 30

x_3 x_4					f
0 0	0	0	0	0	
0 1	0	0	1	1	
1 1	0	1	0	1	
1 0	0	1	1	0	
	0	1	1	0	x_2
	0	0	1	1	x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br3} = x_1 x_4 \oplus x_2 x_3$$

Representative bent function of class 4: Cubes in SNF = 34

x_3 x_4					f
0 0	0	0	1	0	
0 1	0	0	1	0	
1 1	1	1	1	0	
1 0	0	0	0	1	
	0	1	1	0	x_2
	0	0	1	1	x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br4} = x_1 x_2 \oplus x_3 x_4 \oplus x_1 x_3$$

Representative bent function of class 5: Cubes in SNF = 34

x_3 x_4					f
0 0	0	0	1	0	
0 1	0	0	0	1	
1 1	1	1	1	0	
1 0	0	0	1	0	
	0	1	1	0	x_2
	0	0	1	1	x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br5} = x_1 x_2 \oplus x_3 x_4 \oplus x_1 x_4$$

Representative bent function of class 6: Cubes in SNF = 34

x_3 x_4					f
0 0	0	0	1	0	
0 1	0	0	1	0	
1 1	1	0	1	1	
1 0	0	1	0	0	
	0	1	1	0	x_2
	0	0	1	1	x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br6} = x_1 x_2 \oplus x_3 x_4 \oplus x_2 x_3$$

Representative bent function of class 7: Cubes in SNF = 34

x_3 x_4					f
0 0	0	0	1	0	
0 1	0	1	0	0	
1 1	1	0	1	1	
1 0	0	0	1	0	
	0	1	1	0	x_2
	0	0	1	1	x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br7} = x_1 x_2 \oplus x_3 x_4 \oplus x_2 x_4$$

Representative bent function of class 8: Cubes in SNF = 34

x_3	x_4				f
0	0	0	0	1	0
0	1	0	1	0	0
1	1	0	1	1	1
1	0	0	0	0	1
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br8} = x_1x_3 \oplus x_2x_4 \oplus x_1x_2$$

Representative bent function of class 9: Cubes in SNF = 34

x_3	x_4				f
0	0	0	0	0	0
0	1	0	1	0	1
1	1	0	1	1	0
1	0	0	0	1	1
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br9} = x_1x_3 \oplus x_2x_4 \oplus x_1x_4$$

Representative bent function of class 10: Cubes in SNF = 34

x_3	x_4				f
0	0	0	0	0	0
0	1	0	1	1	0
1	1	0	0	1	1
1	0	0	1	0	1
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br10} = x_1x_3 \oplus x_2x_4 \oplus x_2x_3$$

Representative bent function of class 11: Cubes in SNF = 34

x_3	x_4				f
0	0	0	0	0	0
0	1	0	1	1	0
1	1	1	0	1	0
1	0	0	0	1	1
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br11} = x_1x_3 \oplus x_2x_4 \oplus x_3x_4$$

Representative bent function of class 12: Cubes in SNF = 34

x_3	x_4				f
0	0	0	0	1	0
0	1	0	0	0	1
1	1	0	1	1	1
1	0	0	1	0	0
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br12} = x_1x_4 \oplus x_2x_3 \oplus x_1x_2$$

Representative bent function of class 13: Cubes in SNF = 34

x_3	x_4				f
0	0	0	0	0	0
0	1	0	0	1	1
1	1	0	1	1	0
1	0	0	1	0	1
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br13} = x_1x_4 \oplus x_2x_3 \oplus x_1x_3$$

Representative bent function of class 14: Cubes in SNF = 34

x_3 x_4					f
0	0	0	0	0	0
0	1	0	1	0	1
1	1	0	0	1	1
1	0	0	1	1	0
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br14} = x_1x_4 \oplus x_2x_3 \oplus x_2x_4$$

Representative bent function of class 15: Cubes in SNF = 34

x_3 x_4					f
0	0	0	0	0	0
0	1	0	0	1	1
1	1	1	0	1	0
1	0	0	1	1	0
		0	1	1	0 x_2
		0	0	1	1 x_1

The positive polarity ESOP is the minimal ESOP:

$$f_{br15} = x_1x_4 \oplus x_2x_3 \oplus x_3x_4$$

Representative bent function of class 16: Cubes in SNF = 38

x_3 x_4					f
0	0	0	0	1	0
0	1	0	0	0	1
1	1	1	1	0	1
1	0	0	0	0	1
		0	1	1	0 x_2
		0	0	1	1 x_1

Positive polarity ESOP:

$$f_{br16} = x_1x_2 \oplus x_3x_4 \oplus x_1x_3 \oplus x_1x_4$$

Minimal ESOP in terms of products:

$$f_{br16_{min}} = x_1\overline{x}_2 \oplus \overline{x}_1x_3x_4 \oplus x_1\overline{x}_3\overline{x}_4$$

Representative bent function of class 17: Cubes in SNF = 38

x_3 x_4					f
0	0	0	0	1	0
0	1	0	1	0	0
1	1	1	1	0	1
1	0	0	1	0	0
		0	1	1	0 x_2
		0	0	1	1 x_1

Positive polarity ESOP:

$$f_{br17} = x_1x_2 \oplus x_3x_4 \oplus x_2x_3 \oplus x_2x_4$$

Minimal ESOP in terms of products:

$$f_{br17_{min}} = \overline{x}_1x_2 \oplus \overline{x}_2x_3x_4 \oplus x_2\overline{x}_3\overline{x}_4$$

Representative bent function of class 18: Cubes in SNF = 38

x_3 x_4					f
0	0	0	0	1	0
0	1	0	0	1	0
1	1	1	0	0	0
1	0	0	1	1	1
		0	1	1	0 x_2
		0	0	1	1 x_1

Positive polarity ESOP:

$$f_{br18} = x_1x_2 \oplus x_3x_4 \oplus x_1x_3 \oplus x_2x_3$$

Minimal ESOP in terms of products:

$$f_{br18_{min}} = x_3\overline{x}_4 \oplus x_1x_2\overline{x}_3 \oplus \overline{x}_1\overline{x}_2x_3$$

Representative bent function of class 19: Cubes in SNF = 38

x_3 x_4					f
0	0	0	0	1	0
0	1	0	1	1	1
1	1	1	0	0	0
1	0	0	0	1	0
		0	1	1	0 x_2
		0	0	1	1 x_1

Positive polarity ESOP:

$$f_{br19} = x_1x_2 \oplus x_3x_4 \oplus x_1x_4 \oplus x_2x_4$$

Minimal ESOP in terms of products:

$$f_{br19_{min}} = \overline{x}_3x_4 \oplus x_1x_2\overline{x}_4 \oplus \overline{x}_1\overline{x}_2x_4$$

Representative bent function of class 20: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	1	0	
0	1	0	1	1	1	
1	1	0	1	0	0	
1	0	0	0	0	1	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br20} = x_1x_3 \oplus x_2x_4 \oplus x_1x_2 \oplus x_1x_4$$

Minimal ESOP in terms of products:

$$f_{br20_{min}} = x_1\overline{x}_3 \oplus \overline{x}_1x_2x_4 \oplus x_1\overline{x}_2\overline{x}_4$$

Representative bent function of class 21: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	0	0	
0	1	0	1	1	0	
1	1	1	1	0	0	
1	0	0	1	0	1	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br21} = x_1x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_3x_4$$

Minimal ESOP in terms of products:

$$f_{br21_{min}} = \overline{x}_1x_3 \oplus x_2\overline{x}_3x_4 \oplus \overline{x}_2x_3\overline{x}_4$$

Representative bent function of class 22: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	1	0	
0	1	0	1	0	0	
1	1	0	0	0	1	
1	0	0	1	1	1	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br22} = x_1x_3 \oplus x_2x_4 \oplus x_1x_2 \oplus x_2x_3$$

Minimal ESOP in terms of products:

$$f_{br22_{min}} = x_2\overline{x}_4 \oplus x_1\overline{x}_2x_3 \oplus \overline{x}_1x_2\overline{x}_3$$

Representative bent function of class 23: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	0	0	
0	1	0	1	0	1	
1	1	1	0	0	1	
1	0	0	0	1	1	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br23} = x_1x_3 \oplus x_2x_4 \oplus x_1x_4 \oplus x_3x_4$$

Minimal ESOP in terms of products:

$$f_{br23_{min}} = \overline{x}_2x_4 \oplus x_1x_3\overline{x}_4 \oplus \overline{x}_1\overline{x}_3x_4$$

Representative bent function of class 24: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	1	0	
0	1	0	0	0	1	
1	1	0	1	0	0	
1	0	0	1	1	1	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br24} = x_1x_4 \oplus x_2x_3 \oplus x_1x_2 \oplus x_1x_3$$

Minimal ESOP in terms of products:

$$f_{br24_{min}} = x_1\overline{x}_4 \oplus \overline{x}_1x_2x_3 \oplus x_1\overline{x}_2\overline{x}_3$$

Representative bent function of class 25: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	0	0	
0	1	0	1	0	1	
1	1	1	1	0	0	
1	0	0	1	1	0	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br25} = x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4$$

Minimal ESOP in terms of products:

$$f_{br25_{min}} = \overline{x}_1x_4 \oplus x_2x_3\overline{x}_4 \oplus \overline{x}_2\overline{x}_3x_4$$

Representative bent function of class 26: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	1	0	
0	1	0	1	1	1	
1	1	0	0	0	1	
1	0	0	1	0	0	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br26} = x_1x_4 \oplus x_2x_3 \oplus x_1x_2 \oplus x_2x_4$$

Minimal ESOP in terms of products:

$$f_{br26_{min}} = x_2\overline{x}_3 \oplus x_1\overline{x}_2x_4 \oplus \overline{x}_1x_2\overline{x}_4$$

Representative bent function of class 27: Cubes in SNF = 38

x_3	x_4					f
0	0	0	0	0	0	
0	1	0	0	1	1	
1	1	1	0	0	1	
1	0	0	1	0	1	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br27} = x_1x_4 \oplus x_2x_3 \oplus x_1x_3 \oplus x_3x_4$$

Minimal ESOP in terms of products:

$$f_{br27_{min}} = \overline{x}_2x_3 \oplus x_1\overline{x}_3x_4 \oplus \overline{x}_1x_3\overline{x}_4$$

Representative bent function of class 28: Cubes in SNF = 46

x_3	x_4					f
0	0	1	1	0	1	
0	1	1	0	0	0	
1	1	0	0	1	0	
1	0	1	0	0	0	
		0	1	1	0	x_2
		0	0	1	1	x_1

Positive polarity ESOP:

$$f_{br28} = x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus 1$$

Minimal ESOP in terms of products:

$$f_{br28_{min}} = \overline{x}_2\overline{x}_3\overline{x}_4 \oplus \overline{x}_1\overline{x}_2x_3 \oplus \overline{x}_1\overline{x}_2x_4 \oplus \overline{x}_1x_2\overline{x}_3\overline{x}_4 \oplus x_1x_2x_3x_4$$