

# Algebraic normal form of a bent function: what is it?

Natalia Tokareva

Sobolev Institute of Mathematics,  
Novosibirsk State University  
Russia  
tokareva@math.nsc.ru

Maximally nonlinear Boolean functions in  $n$  variables, where  $n$  is even, are called **bent functions**.

There are some ways how to present Boolean functions. One of the oldest and classical one is using **algebraic normal form** (ANF).

## What can we say about ANF of a bent function?

We try to collect here known and new facts related to the ANF of a bent function. We deal with algebraic degrees of bent functions from different classes, classifications of ANFs for small number of variables, particular constructions of bent functions based on ANF's properties. We discuss is it possible to meet in ANF of a bent functions items of special types and other questions.

## Definitions

$\mathbb{F}_2^n$  — the vector space over  $\mathbb{F}_2$ ;

$f, g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  — Boolean functions;

$dist(f, g)$  — Hamming distance between  $f$  and  $g$ , i. e. the number of coordinates in which their vectors of values differ;

$x = (x_1, \dots, x_n)$  — a binary vector;

$\langle x, y \rangle = x_1y_1 + \dots + x_ny_n$  — the standard inner product modulo 2;

$\langle a, x \rangle + b$  is an **affine function** in variables  $x_1, \dots, x_n$ ;

**Bent function** — a Boolean function in  $n$  variables ( $n$  is even) that is on the maximal possible distance from the set of all affine functions. This distance is  $2^{n-1} - 2^{(n/2)-1}$ .

$\mathcal{A}_n$  — the set of all affine functions in  $n$  variables.

$\mathcal{B}_n$  — the set of all bent functions in  $n$  variables.

## Algebraic normal form

Let  $\oplus$  denote the addition modulo 2 (XOR). Any Boolean function can be uniquely represented by its **algebraic normal form** (ANF):

$$f(x_1, \dots, x_n) = \left( \bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \cdot \dots \cdot x_{i_k} \right) \oplus a_0,$$

where for each  $k$  indices  $i_1, \dots, i_k$  are pairwise distinct and sets  $\{i_1, \dots, i_k\}$  are exactly all different nonempty subsets of the set  $\{1, \dots, n\}$ ; coefficients  $a_{i_1, \dots, i_k}, a_0$  take values from  $\mathbb{F}_2$ .

## Algebraic normal form

In Russian math literature it is usually called a **Zhegalkin polynomial** in honor of Ivan Zhegalkin (1869–1947), a mathematician who introduced such a representation in 1927.

For a Boolean function  $f$  the number of variables in the longest item of its ANF is called the **algebraic degree** of a function (or briefly **degree**) and is denoted by  $\text{deg}(f)$ . A Boolean function is **affine**, **quadratic**, **cubic** and so on if its degree is not more than 1, or equal to 2, 3, etc.

## A bit of history

**Oscar Rothaus** (1927-2003) was the recognized authority in this area. Bent functions were introduced by him in 1966 (publ. 1976).

By O. Rothaus the main properties of bent functions were obtained, simple constructions of bent functions were given, and several steps for the classification of bent functions in six variables were made.

# Oscar Rothaus



## A bit of history

In the USSR, bent functions were also studied in the 1960s. It is known that Yu. A. Vasiliev, B.M. Kloss, V.A.Eliseev, and O.P.Stepchenkov studied properties of the Walsh-Hadamard transform of a Boolean function at that time.

The notion of a minimal function (just another name for “bent function”) was introduced in the USSR by **V.A. Eliseev** and **O.P. Stepchenkov** (1962).



V.A.Eliseev



# O.P.Stepchenkov



## Robert McFarland; John Dillon



**J.F. Dillon** (1972) Bent functions in connection to differential sets;  
**R.L. McFarland** (1973) Large class of bent functions.

## Applications of bent functions

Now bent functions are studied very widely since they have numerous applications in computer science.

**Hadamard matrices** (combinatorics);

Classification problems for H. m. and bent functions are equivalent.

**Differential sets** (group theory);

**Orthogonal spreads** (finite geometries);

**Codes of the constant amplitude in CDMA systems** — the 3d generation mobile systems (communication theory);

**Kerdock codes** (coding theory);

**S-boxes** in block and stream ciphers resistant to linear cryptanalyses. E. g. CAST, Grain, etc. (cryptography);

**Authentication schemes, hash functions; pseudo-random generators** (cryptography)

## Well-known open problems in bent functions

**To find asymptotic value for the number of bent functions.**

Now the exact number of bent functions is known only for  $n \leq 8$ .

It is very hard even to find good lower and upper bound for the number of bent functions.

Lower bound:  $2^{2^{(n/2)+\log(n-2)}-1}$  (McFarland construction)

Upper bound:  $2^{2^{n-1} + \frac{1}{2} \binom{n}{n/2}}$  (# of functions of degree  $\leq n/2$ )

**To classify bent functions** with respect to some (affine?) equivalence.

**To find new constructions of bent functions.**

There are known a few constructions that cover only the small part of all bent functions.

**To reach a tradeoff between high nonlinearity and other cryptographic properties of a Boolean function.**



**Degree** of a bent function is between 2 and  $n/2$

## Degree of a bent function

In what follows let  $n$  be an even number. According to O. Rothaus and V. A. Eliseev and O. P. Stepchenkov (1962) it holds

**Theorem.** *Degree  $\deg(f)$  of a bent function  $f$  in  $n \geq 4$  variables is not more than  $n/2$ . If  $n = 2$  a bent function is quadratic.*

One can find a proof of this fact in the book of T. W. Cusick and P. Stanica «Cryptographic Boolean functions and applications» (2009, 2017).

Obviously, a Boolean function of degree less or equal to one can not be bent. It is easy to see that there exist bent functions of all other possible degrees from 2 to  $n/2$  if  $n \geq 4$  (just use the Maiorana — McFarland construction for this). E. g. the quadratic Boolean function  $f(x_1, \dots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{n-1}x_n$  is bent for any even  $n$ .

## Degree of a $p$ -ary bent function

In 2004 X. D. Hou determined the bound for  $p$ -ary bent functions.

**Theorem.** *If  $f$  is a  $p$ -ary bent function ( $p$  is prime) in  $n$  variables,*

$$\deg(f) \leq \frac{(p-1)n}{2} + 1.$$

*If  $f$  is weakly regular, then*

$$\deg(f) \leq \frac{(p-1)n}{2}.$$



## Degree of a dual bent function

Recall that for a bent function  $f$  the *dual function*  $\tilde{f}$  in  $n$  variables is defined by the equality

$$W_f(y) = 2^{n/2}(-1)^{\tilde{f}(y)}.$$

This definition is correct since  $W_f(y) = \pm 2^{n/2}$  for any vector  $y$ .

Recall that  $\tilde{f}$  is bent too. It holds  $\tilde{\tilde{f}} = f$ .

What about the degree of the dual function?

- if  $\deg(f) = n/2$  then  $\deg(\tilde{f}) = n/2$ .

In general, the following fact is well known (see for instance chapters of C. Carlet on Boolean functions, 2008)

**Theorem.** *Let  $f$  be an arbitrary bent function in  $n$  variables. Then*

$$n/2 - \deg(f) \geq \frac{n/2 - \deg(\tilde{f})}{\deg(\tilde{f}) - 1}.$$



In ANF of a bent function we meet...  
**every variable**

## In ANF of a bent function we meet every variable

A Boolean function  $f$  in  $n$  variables *has a degenerate (fictitious) variable*  $x_i$  if for any vector  $b \in \mathbb{F}_2^n$  it holds  $f(b) = f(b \oplus e_i)$ , where  $e_i$  is a vector of weight 1 with  $i$ -th coordinate being nonzero.

In other words, a variable is **fictitious** if and only if it does not occur in ANF of  $f$ . A Boolean function is **nondegenerate** if it has no fictitious variables.

**Theorem.** *A bent function in  $n$  variables is nondegenerate, i. e. all variables are presented in its ANF.*

It is easy to prove this using the definition of bent function as a function being on the max possible distance from all affine functions.



In ANF of some special bent functions we meet...  
**every product of variables!!**

## Products of variables in ANF of Kasami functions

In 2013 A. Gorodilova (Frolova) proved a more strong result related to Kasami bent functions. A Boolean function in  $n$  variables we call  **$k$ -nondegenerate** if for each product of any  $k$  pairwise different variables there exists a monomial in ANF of  $f$  that contains this product.

For instance, the product  $x_1x_5x_9$  we find in ANF like this:

$$\dots + \mathbf{x_1x_2x_4x_5x_9} + \dots$$

The maximal such number  $k$  for a Boolean function  $f$  we call its **order of nondegeneracy**. The previous result can be formulated like this: for any bent function this order is at least 1.

A.Gorodilova proved

**Theorem.** *The order of nondegeneracy of an arbitrary Kasami Boolean function of degree  $d$  equals  $d - 3$  or  $d - 2$ .*

Frolova A.A. The essential dependence of Kasami bent functions on the products of variables / J. of Appl. and Industr. Math. 2013. V. 7, N 2, 166–176.



Can ANF of a bent function be **homogeneous**?

## Homogeneous bent functions

This subclass of bent functions was introduced by C. Qu, J. Seberri and J. Pieprzyk in 2000 as consisting of the functions with relatively simple ANFs.

A bent function is called **homogeneous** if all monomials of its ANF are of the same degree.

- There are 30 homogeneous bent functions of degree 3 in 6 variables (C. Qu, J. Seberri and J. Pieprzyk, 2000).
- There are some partial results on cubic homogeneous bent functions in 8 variables (C.Charnes, U.Dempwolff, J.Pieprzyk, 2008)
- It was proven that there exist cubic homogeneous bent functions in each number of variables  $n > 2$  (C. Charnes, M. Rotteler, T. Beth, 2002).

What about the homogeneous bent functions of higher degree?

- It was obtained that for  $n > 3$ , there are no homogeneous bent functions in  $n$  variables of the maximal possible degree  $n/2$  (T. Xia, J. Seberry, J. Pieprzyk, and C. Charnes, 2004).
- In 2007 Q. Meng, H. Zhang, M. C. Yang, and J. Cui generalized some previous results and proved

**Theorem.** *For any nonnegative integer  $k$ , there exists a positive integer  $N$  such that for  $n \geq 2N$  there exist no  $n$ -variable homogeneous bent functions having degree  $(n/2) - k$  or more, where  $N$  is the least integer satisfying*

$$2^{N-1} > \binom{N+1}{0} + \binom{N+1}{1} + \dots + \binom{N+1}{k+1}.$$



But what is the tight upper bound on the degree of a homogeneous bent function?

For now there is no answer to this question. There is only

**Conjecture (Q. Meng, et al. 2007).** *For every  $k > 1$ , there is  $N \geq 2$  such that homogeneous bent functions of degree  $k$  of  $n$  variables exist for every even  $n > N$ .*

In 2010 Q. Meng, L. Chen and F.-W. Fu presented partial results towards the conjectured nonexistence of homogeneous rotation symmetric bent functions having degree more than 2.

## Homogeneous bent functions & talk of Pante Stanica on BFA-2017

Do you remember an excellent talk of P.Stanica «(Generalized) Boolean functions: invariance under some groups of transformations and differential properties» on BFA-2017?

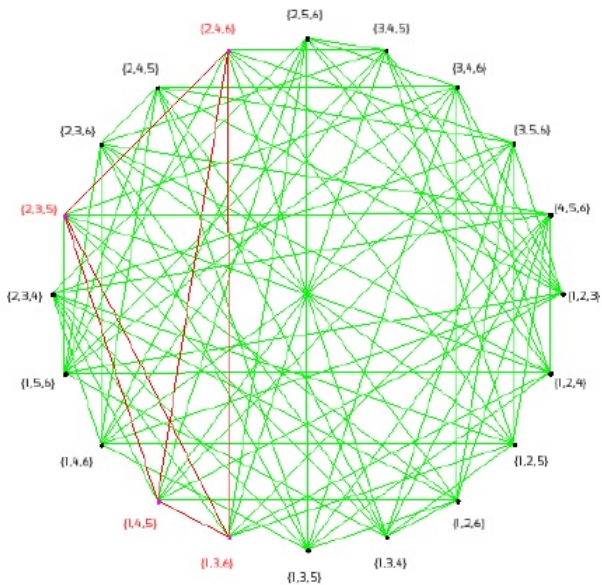
There were ideas on visualization of Boolean functions...

In 2002 C. Charnes, M. Rotteler and T. Beth proposed a simple method to get all 30 homogeneous bent functions of degree 3 in 6 variables.

**Nagy graphs** (or **intersection graphs**)  $\Gamma_{(n,k)}$  can be defined like this:

- its vertices are all unordered  $k$ -element subsets of  $\{1, 2, \dots, n\}$ ;
- an edge connects vertices when corresponding subsets have exactly one common element.

# Graph $\Gamma_{6,3}$



- Find a maximal clique in  $\Gamma_{(6,3)}$ ;
- Take the complement to it in the graph;
- For every vertex  $\{i, j, k\}$  of the complement take an item  $x_i x_j x_k$  to the ANF;
- Get a homogeneous Boolean function of degree 3. It is bent!

What about generalizations of this method for other  $\Gamma_{(n,k)}$ ?

P.Stanica (2017) proposed to look at the complements of the maximal cliques of the graphs

- $\Gamma_{(10,4)}$ ,  $\Gamma_{(12,4)}$  (do they produce homogeneous quartic functions?)
- $\Gamma_{(12,5)}$ ,  $\Gamma_{14,5}$  (what about quintic functions?)

A. Shaporenko (2018) has studied this question.

First, what are the maximal cliques in  $\Gamma_{(k,n)}$ ?

- A. Shaporenko proved that the clique of size  $k + 1$  not necessarily exists in every  $\Gamma_{(n,k)}$ . And if it exists it is not necessary maximal.

For instance in  $\Gamma_{(8,3)}$  the maximal clique is of size 7.

- it was proven that if  $n = k(k + 1)/2$  then the clique of size  $k + 1$  is maximal in graph  $\Gamma_{(n,k)}$ .
- it is obtained that homogeneous Boolean functions obtained from  $\Gamma_{(10,4)}$  and  $\Gamma_{(28,7)}$  by the mentioned method are not bent.

So, till now there are **no** other examples of homogeneous bent functions obtained in such way.



Can ANF of a bent function be **symmetric**?

## Bent functions with symmetric ANF

A Boolean function  $f$  in  $n$  variables is called **symmetric** if for any permutation  $\pi$  on its coordinates it holds  $f(x) = f(\pi(x))$ . It is the strongest symmetric property for a Boolean function. One can easily obtain that there are exactly  $2^{n+1}$  symmetric Boolean functions since the value  $f(x)$  depends only on the Hamming weight of  $x$ . In 1994 P. Savicky classified all symmetric bent functions.

**Theorem.** *There are only four symmetric bent functions in  $n$  variables:  $f(x)$ ,  $f(x) \oplus 1$ ,  $f(x) \oplus \sum_{i=1}^n x_i$  and  $f(x) \oplus \sum_{i=1}^n x_i \oplus 1$ , where*

$$f(x) = \bigoplus_{i=1}^n \bigoplus_{j=i+1}^n x_i x_j,$$

In 2006 Y. Zhao and H. Li discussed a kind of bent functions that have symmetric properties with respect to some variables.



When ANF of a bent function is **rotation symmetric**?



## When ANF of a bent function is rotation symmetric?

In 1999 J. P. Pieprzyk and C. X. Qu introduced a new concept of the rotation symmetric Boolean function and have applied it in studying of hash functions. There were other related papers (E. Filiol, C. Fountain, 1998), J. P. Pieprzyk (1994).

Let  $\rho$  be a cyclic permutation on coordinates  $x_1 \dots x_n$  defined as

$$\rho(x_1, \dots, x_{n-1}, x_n) = (x_n, x_1, \dots, x_{n-1}) \text{ for all } x.$$

A Boolean function  $f$  in  $n$  variables is **rotation symmetric** if

$$f(x) = f(\rho(x)) \text{ for all } x \in \mathbb{F}_2^n.$$

There are several useful techniques for working with rotation symmetric Boolean functions, like the **short ANF** or **SANF**. To get ANF from SANF just take all cyclic shifts of it.

Let us briefly discuss results on rotation symmetric bent functions.

Classification of rotation symmetric bent functions for small  $n$  was done by P. Stanica and S. Maitra in 2003, 2008.

- If  $n = 4$  there are eight rotation symmetric bent functions in 4 variables. Their SANFs (up to a linear part) are 13,  $12 + 13$ .
- If  $n = 6$  there are 48 rotation symmetric bent functions. All of them can be presented by the following 12 functions (free of linear terms): 14,  $12 + 13 + 14$ ,  $134 + 13 + 14$ ,  $124 + 13 + 14$ ,  $124 + 12 + 14$ ,  $134 + 12 + 14$ ,  $123 + 135 + 14$ ,  $123 + 135 + 12 + 13 + 14$ ,  $123 + 134 + 135 + 13 + 14$ ,  $123 + 134 + 135 + 12 + 14$ ,  $123 + 124 + 135 + 12 + 14$ ,  $123 + 124 + 135 + 13 + 14$ . We list them here in SANF. Then to get 48 rotation symmetric functions in 6 variables we add a rotation symmetric affine part of 4 types: zero, one,  $x_1 \oplus \dots \oplus x_n$  or  $x_1 \oplus \dots \oplus x_n \oplus 1$ .

- If  $n = 8$ . P. Stanica and S. Maitra found among the  $2^{21}$  rotation symmetric Boolean functions in 8 variables that exactly 15 104 of them are bent functions.

There are exactly 8 homogeneous rotation symmetric bent functions in 8 variables:  $15$ ,  $15 + 12$ ,  $15 + 13$ ,  $15 + 14$ ,  $15 + 12 + 13$ ,  $15 + 12 + 14$ ,  $15 + 13 + 14$ ,  $15 + 12 + 13 + 14$ . Let us note that it is easy to see some *group structure* in this construction. Indeed, let us take some basis of an Abelian group  $G$  isomorphic to  $\mathbb{Z}_2^3$ ; denote basic vectors by formal symbols “12”, “13”, “14”. Then SANFs of all homogeneous bent functions in 8 variables are exactly elements of the set “15” +  $G$ .

- If  $n = 10$ . P. Stanica and S. Maitra (2008) studied this case. But to classify all rotation symmetric bent functions in 10 variables is still difficult. It was obtained that there are 12 homogeneous rotation symmetric bent functions in 10 variables of degree 2. All of them are here:  $16$ ,  $16 + 12$ ,  $16 + 13$ ,  $16 + 14$ ,  $16 + 15$ ,  $16 + 12 + 15$ ,  $16 + 13 + 14$ ,  $16 + 12 + 13 + 14$ ,  $16 + 12 + 13 + 15$ ,  $16 + 12 + 14 + 15$ ,  $16 + 13 + 14 + 15$ ,  $16 + 12 + 13 + 14 + 15$ . They have not found homogeneous rotation symmetric bent functions of the greater degree. Then, they proposed a conjecture:

**Conjecture.** *There are no homogeneous rotation symmetric bent functions of degree 3 or more.*

There is a some progress in proving of this conjecture in works of P. Stanica.

For a homogeneous degree  $d$  rotation symmetric Boolean function  $f$  with its SANF given by  $\bigoplus_{i=1}^s \beta_i$ , where  $\beta_i = x_{k_1^{(i)}} x_{k_2^{(i)}} \cdots x_{k_d^{(i)}}$  (assume that  $k_1^{(i)} = 1$  for all  $i$ ), we define a sequence  $d_j^{(i)}$ ,  $j = 1, 2, \dots, k_{i-1}^{(i)}$ , by  $d_j^{(i)} = k_{j+1}^{(i)} - k_j^{(i)}$ . Let  $d_f = \max_{i,j} \{d_j^{(i)}\}$ , that is, the largest distance between two consecutive indices in all monomials of  $f$ . The next theorem was proved by P. Stanica in 2008.

**Theorem.** *The following hold for a homogeneous rotation symmetric Boolean function  $f$  of degree  $\geq 3$  in  $n \geq 6$  variables:*

- (i) *if the SANF of  $f$  is  $x_1 \cdots x_d$ , then  $f$  is not a bent function;*
- (ii) *if the SANF of  $f$  is  $x_1 x_2 \cdots x_{d-1} x_d \oplus x_1 x_2 \cdots x_{d-1} x_{d+1}$ , then  $f$  is not bent, assuming:  $(n-2)/4 > \lfloor n/d \rfloor$ , if  $n \not\equiv 1 \pmod{d}$ ;  $n/4 > \lfloor n/d \rfloor$ , if  $n \equiv 1 \pmod{d}$ ;*
- (iii) *in general, if  $d_f < (n/2 - 1)/\lfloor n/d \rfloor$ , then  $f$  is not bent.*

In 2009 D. K. Dalai, S. Maitra and S. Sarkar have analyzed combinatorial properties related to the Walsh — Hadamard spectra of rotation symmetric Boolean functions in even number of variables. These results were then applied in studying of rotation symmetric bent functions.

Constructions of quadratic and cubic rotation symmetric bent functions can be found in the paper of G. Gao, X. Zhang, W. Liu and C. Carlet (2012). For example, they construct the first infinite class of **cubic** rotation symmetric bent functions.

In 2014 new constructions of rotation symmetric bent functions via idempotents were proposed by C. Carlet, G. Gao and W. Liu. Namely, they found the first infinite class of such functions of degree **more than 3**.



A **linear part** of ANF of a bent function can be any!

## A linear part of ANF of a bent function can be any!

It is well known that the class of bent functions is closed under addition of affine functions and under affine transformations of variables, i. e. for any bent function  $g$  the function

$$g'(x) = g(Ax + b) + c_1x_1 + \dots + c_nx_n + d$$

is bent again. The functions  $g$  and  $g'$  are called **EA-equivalent**.

Recall that (2010) we can not «add» to a bent function something else to preserve the property to be bent, since for any non affine Boolean function  $f$  there exists a bent function  $g$  such that  $f + g$  is not bent.





A **quadratic part** of ANF of a bent function  
can be any!!!

## A quadratic part of ANF of a bent function can be any!

In 2018 E. Ponomareva proved the following fact.

**Theorem.** *An arbitrary quadratic Boolean function in 6 variables is a quadratic part of some bent function in 6 variables.*

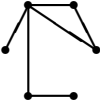
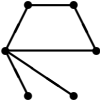

She considered the set of all quadratic Boolean functions in 6 variables — all of them can be described with 156 nonisomorphic graphs.

A **right sequence** is a decreasing sequence of nonnegative integers  $(d_1, d_2, \dots, d_n)$  such that  $\sum_{i=1}^n d_i$  is an even number.

**Theorem (Erdős — Galai, 1960).** *A right sequence  $(d_1, d_2, \dots, d_n)$  is a sequence of graph degrees if and only if for every  $k$ ,  $1 \leq k \leq n - 1$ , it holds*

$$\sum_{i=1}^k d_i \leq k(k-1) + \sum_{i=k+1}^n \min\{k, d_i\}.$$

# The case of 6 variables (part of the table)

40	422211		Bent
			$123 \oplus 124 \oplus 126 \oplus 135 \oplus 145 \oplus 235 \oplus 245 \oplus$ $246 \oplus 256 \oplus 356 \oplus 12 \oplus 14 \oplus 15 \oplus 16 \oplus 23 \oplus 34$
41	422220		$136 \oplus 146 \oplus 346 \oplus 12 \oplus 13 \oplus 23 \oplus 34 \oplus 35 \oplus 45$

## A quadratic part of ANF of a bent function can be any!

Then she turned her attention to the following iterative construction of O. Rothaus (1966, 1976) and J. Dillon (1974).

**Theorem.** *Let  $f'$ ,  $f''$ ,  $f'''$  be bent functions in  $n$  variables such that  $f' + f'' + f'''$  is a bent function too. Then*

$$g(x, x_{n+1}, x_{n+2}) = f'(x)f''(x) + f'(x)f'''(x) + f''(x)f'''(x)$$

$$+ x_{n+1}f'(x) + x_{n+1}f''(x) + x_{n+2}f'(x) + x_{n+2}f'''(x) + x_{n+1}x_{n+2}$$

*is a bent function in  $n + 2$  variables.*

Using the last two theorems E. Ponomareva has got (2018)

**Theorem.** *Any quadratic Boolean function in  $n$  variables is a quadratic part of some bent function in  $n$  variables, where  $n$  is even,  $n \geq 6$ .*



A  **$k$ -degree part** of ANF of a bent function  
can be...???

## A $k$ -degree part of ANF of a bent function can be...?

What about the next case?

Is it true that the cubic part of a bent function can be arbitrary?

- in case  $n = 6$  the answer is **no**, since there exists only three classes of nonequivalent cubic bent functions:

$$123 + 14 + 25 + 36$$

$$123 + 245 + 12 + 14 + 26 + 35 + 45$$

$$123 + 245 + 346 + 14 + 26 + 34 + 35 + 36 + 45 + 46$$

but there are five classes of nonequivalent homogeneous cubic Boolean functions in 6 variables.

We need to have items of the next degree in order to «have a space» to put all variants of the cubic part.

- case  $n = 8$  is still open. The problem is that the existing classification of quartic bent functions in 8 variables (obtained by P. Langevin and G. Leander in 2011) does not include the list of representatives of EA-classes...

Note that thanks to X. D. Hou (1998) we have a classification of cubic bent functions in eight variables:

$N$	Nonequivalent bent functions of degree $\leq 3$
1	$12 + 34 + 56 + 78$
2	$123 + 14 + 25 + 36 + 78$
3	$123 + 245 + 34 + 26 + 17 + 58$
4	$123 + 245 + 13 + 15 + 26 + 34 + 78$
5	$123 + 245 + 346 + 35 + 26 + 25 + 17 + 48$
6	$123 + 245 + 346 + 35 + 13 + 14 + 27 + 68$
7	$123 + 245 + 346 + 35 + 26 + 25 + 12 + 13 + 14 + 78$
8	$123 + 245 + 346 + 35 + 16 + 27 + 48$
9	$127 + 347 + 567 + 14 + 36 + 25 + 45 + 78$
10	$123 + 245 + 346 + 147 + 35 + 27 + 15 + 16 + 48$



Bent decomposition problem in terms of ANF



## Bent decomposition problem in terms of ANF

**Hypothesis 1** (2011). *Any Boolean function in  $n$  variables of degree not more than  $n/2$  can be represented as the sum of two bent functions in  $n$  variables ( $n$  is even,  $n \geq 2$ ).*

**Bent sum decomposition problem:** to prove or disprove the Hypothesis. It is closely connected to the problem of asymptotic of the number of all bent functions.

This question appeared in 2011 while iterative bent functions were studied.

- Hypothesis is confirmed for  $n = 2, 4, 6$  (2011, and Qu, Li, 2014).
- It was proved for quadratic Boolean functions, Maiorana—McFarland bent functions, partial spread functions.
- A weakened variant of the hypothesis was proved: any Boolean function of degree  $\leq n/2$  can be represented as the sum of **constant** number of bent functions (2014).

The main hypothesis can be reformulated like this:

*An arbitrary ANF of degree not more than  $n/2$  can be divided into two parts — every part gives the ANF of a bent function.*

Some ideas that follows from the hypothesis (assuming it holds):

- $k$ -degree part of the ANF of a bent function «tends» to be arbitrary. It is necessary that at least

$$\sqrt{2 \binom{n}{n/2}}$$

different variants of  $k$ -degree part of ANF should be realized in bent functions. Recall that the total number of all such variants is

$$2 \binom{n}{n/2}$$

- we see that in cases  $k = 1, 2$  these ideas are confirmed in maximal possible form.



Open problems related to ANF

## Open problems related to ANF

What are relations between ANF and polynomial representation of a bent function?

Can we define a bent function through the conditions on ANF?

# NSUCRYPTO-2018: welcome!



October 14–21, 2018.

# NSUCRYPTO-2018: October 14, 2018. Welcome!

International Students' Olympiad in Cryptography. It is organized by



Novosibirsk State University



Sobolev Institute of Mathematics (Novosibirsk)



University of Leuven (KU Leuven, Belgium)



Belarusian State University



Tomsk State University

**NSUCRYPTO** is the unique cryptographic Olympiad containing **scientific mathematical problems** for senior pupils, students and professionals from any country. The concept of the Olympiad is not to focus on solving only olympic tasks but on including hard and unsolved research problems at the intersection of mathematics and cryptography. It holds in two rounds via Internet. Welcome to participate!

[www.nsucrypto.nsu.ru](http://www.nsucrypto.nsu.ru)

# Master in Crypto — 2018: welcome!

## Master in Cryptography

Novosibirsk State University  
Department of Mechanics and Mathematics

September 2018 - June 2020 Full-time study, 2 years

Master in Cryptography from NSU is an innovative programme designed to involve young researchers in the field of modern cryptography and bring them onto a high professional level in this area. The programme covers all basic aspects of cryptography and cryptanalysis and provides deep theoretical and practical background in this field. Professionals in cryptography will be invited to deliver lectures.

Bart Preneel (Belgium), Lars Knudsen (Denmark), Lilita Budaghyan (Norway), Gregor Leander (Germany), Sijean Peick (Netherlands), Sugata Gangopadhyay (India), Nicky Mouhe (USA) and other specialists are invited

**Courses included into the program:**

- Algebra and finite fields: special aspects
- Discrete mathematics
- Theory of probability and mathematical statistics
- Numerical methods in cryptography
- Information theory and cryptography. Introduction
- Foundations of symmetric cryptography
- Cryptographic Boolean functions
- Cipher design
- Cryptanalysis of symmetric systems
- Asymmetric cryptography and cryptanalysis
- Blockchain: math, problems and applications
- Quantum and postquantum cryptography
- Practical applications of cryptography
- Historical and legal aspects of cryptography
- etc.

Studying in NSU provides you with...

- \* a high-level education
- \* scientific research and perspectives
- \* unique atmosphere and nature of Akademgorodok - the world-famous scientific center located in the beautiful forest near the Ob sea.
- \* modern and compact campus: everything is within walking distance
- \* cultural benefits as visiting the Opera and Ballet Theatre, the largest theatre in Russia with the world-famous artists.

facebook.com/NSUCryptomaster  
twitter.com/NSUCryptomaster  
vk.com/nsucryptomast

You know, we organize the International Students Olympiad in Cryptography - NSUCRYPTO. Now we are waiting you to join our Master Programme. Welcome!

Please send your applications to E-mail: [crypto-master@nsu.ru](mailto:crypto-master@nsu.ru)  
More detail and actual information on [www.crypto-master.nsu.ru](http://www.crypto-master.nsu.ru)

Novosibirsk State University  
THE REAL SCIENCE



# Master in Crypto — 2018: welcome!

It is the first English-taught Master programme in Cryptography in Russia. Well-known specialists in cryptography and discrete mathematics from different parts of the world will deliver lectures.

Bart Preneel, Lars Knudsen, Lilya Budaghyan, Gregor Leander, Stjepan Picek, Sugata Gangopadhyay, Nicky Mouha are invited. We are happy to meet them in Novosibirsk!

We kindly invite your students to join this programme!

**[www.crypto-master.nsu.ru](http://www.crypto-master.nsu.ru)**

Thank you for the attention!