

УДК 519.7

EVERY CUBIC BOOLEAN FUNCTION IN 8 VARIABLES IS THE SUM OF NOT MORE THAN 4 BENT FUNCTIONS¹

N. N. Tokareva

It is shown that any cubic Boolean function in 8 variables is the sum of not more than 4 bent functions in 8 variables.

Keywords: *bent function, cubic Boolean function, affine classification.*

Boolean functions with extremal nonlinear properties are called *bent functions*. They are exactly those functions that have the maximal possible Hamming distance to the class of all affine Boolean functions in n variables. Note that degree of a bent function is not more than $n/2$. One of the most important problem in bent functions is to find the number of them. In [1] we introduced a new approach to this problem and formulated the following hypothesis: *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, $n \geq 2$).* In general, it is interesting to obtain decompositions in *constant* number of bent functions.

In this paper we study bent decompositions for Boolean functions in 8 variables. Recall that Boolean functions f and g in n variables are *affine equivalent*, if there exist nonsingular binary $n \times n$ matrix A , vectors u, v of length n and constant $\lambda \in \mathbb{Z}_2$, such that $g(x) = f(Ax + u) + \langle v, x \rangle + \lambda$, where $\langle v, x \rangle = x_1v_1 + \dots + x_nv_n$ is the *inner product*. We study bent decompositions only for affine nonequivalent Boolean functions due to the following facts:

- A Boolean function affine equivalent to a bent function is bent too.
- Let a Boolean function f in n variables be represented as the sum of k bent functions.

Then every Boolean function affine equivalent to f also can be represented as the sum of k bent functions.

In [2] it is proven that every quadratic Boolean function in n variables (n is even) is the sum of two bent functions in n variables. The proof of this fact was based on the known affine classification of all quadratic Boolean functions in n variables (due to the Dickson's theorem). Thus, let us consider Boolean functions of degree 3.

Theorem 1. Every cubic Boolean function in 8 variables is the sum of not more than 4 bent functions.

Recall that if all items of algebraic normal form of a Boolean function contain exactly k variables then such a function is called *homogeneous of degree k* . In the table bellow we list all affine nonequivalent homogeneous Boolean functions of degree 3 according to classification from [3]. To be short we write monomial $x_1x_2x_3$ as 123 and so on. Let $f(x) = f_3(x) + f_2(x)$ be an arbitrary cubic Boolean function in 8 variables, where $f_3(x)$ is a homogeneous part of degree 3 and $f_2(x)$ has degree ≤ 2 . W.l.o.g. assume that f_3 is from the table bellow (otherwise consider a function affine equivalent to f).

It is not hard to get decompositions of the Boolean function f up to the quadratic part. It is enough to use only following nonequivalent bent functions:

$$\begin{aligned} a &= 123 + 14 + 25 + 36 + 78; \\ b &= 123 + 145 + 34 + 16 + 27 + 58; \\ c &= 123 + 145 + 346 + 35 + 16 + 15 + 27 + 48; \\ d &= 123 + 347 + 356 + 14 + 76 + 25 + 45 + 38; \\ e &= 123 + 145 + 247 + 346 + 35 + 17 + 25 + 26 + 48. \end{aligned}$$

¹Work is supported by RFBR No. 14-01-00507.

We give the required decomposition in the form $f(x) = g(\pi(x)) + h(\sigma(x)) + q(x)$, where g and h are bent functions from the set $\{a, b, c, d, e\}$, substitutions π, σ are nonsingular affine transformations of variables (permutations in most cases), function q is a certain Boolean function of degree ≤ 2 (we do not concretize it). According to [2] any quadratic function q is the sum of two bent functions. Thus, f can be represented as the sum of not more than 4 bent functions in 8 variables.

For example, function $f(x) = x_1x_2x_3 + x_2x_4x_6 + x_3x_5x_7 + x_1x_2x_8 + x_1x_3x_8$ (number 15 in the table) is the sum $b(x_2 + x_3, x_1, x_8, x_4, x_6, x_3, x_5, x_7) + d(x_1 + x_2, x_2, x_3, x_4, x_5, x_7, x_6, x_8) + q(x)$, where q is a quadratic function.

No	Affine nonequivalent homogeneous Boolean functions of degree 3	g	h	π	σ
1	123	a	b	[1, 4, 5, 2, 3, 6, 7, 8]	id
2	123 + 145	a	a	id	[1, 4, 5, 2, 3, 6, 7, 8]
3	123 + 456	a	a	id	[4, 5, 6, 1, 2, 3, 7, 8]
4	123 + 135 + 236	a	b	id	[3, 1, 5, 2, 6, 4, 7, 8]
5	123 + 124 + 135 + 236 + 456	c	c	[1 + 6, 2, 3, 4, 5, 6, 7, 8]	[3 + 4, 5, 1, 4, 6, 2, 7, 8]
6	123 + 145 + 167	a	b	id	[1, 4, 5, 6, 7, 2, 3, 8]
7	123 + 246 + 357	b	d	[4, 2, 6, 3, 8, 1, 7, 5]	[1, 2, 3, 4, 5, 7, 8, 6]
8	123 + 145 + 167 + 246	a	c	id	[1, 5, 4, 6, 7, 2, 3, 8]
9	123 + 145 + 246 + 357	d	d	[1, 2, 3, 4, 5, 7, 8, 6]	[1, 5, 4, 2, 3, 8, 6, 7]
10	123 + 124 + 135 + 236 + 456 + 167	b	d	[1 + 6, 2, 3, 4, 5, 6, 7, 8]	[2 + 5, 4, 1, 3, 6, 7, 5, 8]
11	123 + 145 + 167 + 246 + 357	b	c	[6, 1, 7, 2, 4, 3, 5, 8]	[1, 2, 3, 5, 4, 7, 6, 8]
12	123 + 478 + 568	a	b	id	[8, 4, 7, 5, 6, 1, 2, 3]
13	123 + 145 + 167 + 568	a	c	id	[1, 4, 5, 6, 7, 8, 2, 3]
14	123 + 246 + 357 + 568	c	d	[4, 2, 6, 8, 3, 5, 1, 7]	[1, 2, 3, 4, 5, 7, 8, 6]
15	123 + 246 + 357 + 128 + 138	b	d	[2 + 3, 1, 8, 4, 6, 3, 5, 7]	[1 + 2, 2, 3, 4, 5, 7, 6, 8]
16	123 + 145 + 167 + 357 + 568	a	e	id	[1, 6, 7, 5, 4, 3, 8, 2]
17	123 + 145 + 478 + 568	a	c	id	[4, 1, 5, 8, 7, 6, 2, 3]
18	123 + 124 + 135 + 236 + 456 + 167 + 258	e	e	[1, 2 + 5, 3, 5, 4, 6, 8, 7]	[1, 2 + 5, 4, 6, 7, 5, 3, 8]
19	123 + 124 + 135 + 236 + 456 + 178	b	d	[1 + 6, 2, 3, 4, 5, 6, 7, 8]	[2 + 5, 4, 1, 3, 7, 8, 5, 6]
20	123 + 145 + 246 + 357 + 568	d	e	[1, 2, 3, 4, 5, 7, 8, 6]	[5, 6, 8, 4, 1, 3, 2, 7]
21	123 + 145 + 246 + 467 + 578	c	e	[4, 3, 8, 7, 6, 5, 1, 2]	[1, 2, 3, 4, 5, 8, 6, 7]
22	123 + 145 + 357 + 478 + 568	a	e	id	[4, 7, 8, 5, 1, 6, 3, 2]
23	123 + 246 + 357 + 478 + 568	c	e	[1, 2, 3, 5, 4, 7, 6, 8]	[5, 6, 8, 4, 1, 7, 2, 3]
24	123 + 246 + 357 + 148 + 178 + 258	c	c	[1, 2, 3, 7, 8, 5, 4, 6]	[2, 5, 8, 4, 6, 1, 3, 7]
25	123 + 145 + 167 + 246 + 357 + 568	c	d	[1, 2, 3, 5, 4, 7, 6, 8]	[1, 7, 6, 2, 5, 8, 4, 3]
26	123 + 145 + 167 + 246 + 238 + 258 + 348	c	e	[1, 7 + 8, 6, 4, 5, 2, 3, 8]	[2, 1 + 8, 3, 8, 5, 4, 6, 7]
27	123 + 145 + 167 + 258 + 268 + 378 + 468	c	e	[1, 3 + 8, 2, 5, 4, 8, 6, 7]	[6, 1 + 6, 7, 8, 4, 3, 2, 5]
28	123 + 145 + 246 + 357 + 238 + 678	c	c	[1, 2, 3, 5, 4, 7, 6, 8]	[2, 3, 8, 6, 4, 7, 1, 5]
29	123 + 145 + 246 + 357 + 478 + 568	c	c	[1, 2, 3, 5, 4, 7, 6, 8]	[4, 2, 6, 8, 7, 5, 1, 3]
30	123 + 124 + 135 + 236 + 456 + 167 + 258 + 378	c	e	[1, 2, 3 + 4, 6, 7, 5, 4, 8]	[5, 8, 2 + 5, 3, 1, 6, 7, 4]
31	123 + 156 + 246 + 256 + 147 + 157 + 357 + 348 + 258 + 458	c	e	[5, 2 + 4, 8, 3, 7, 4, 1, 6]	[2, 4 + 5, 6, 1, 3, 5, 7, 8]

BIBLIOGRAPHY

1. Tokareva N. N. On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances Math. Comm. (AMC). 2011. V. 5. Iss. 4. P. 609–621.
2. Qu L. and Li C. When a Boolean function can be expressed as the sum of two bent functions // Cryptology ePrint Archive. 2014/048.
3. Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., and Yashenko V. V. Boolean functions in coding theory and cryptology. Moscow center for the uninter. math. education, 2012. 584 p. (in Russian)