

СИБИРСКИЕ ЭЛЕКТРОННЫЕ  
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

<http://semr.math.nsc.ru>

---

---

Том 16, стр. 144–150 (2022)  
DOI 10.33048/semi.2022.16.xxx

УДК 512.5  
MSC 13A99

## A QUADRATIC PART OF A BENT FUNCTION CAN BE ANY

N.N. TOKAREVA

**ABSTRACT.** Boolean functions in  $n$  variables that are on the maximal possible Hamming distance from all affine Boolean functions in  $n$  variables are called bent functions ( $n$  is even). They are intensively studied since sixties of XX century in relation to applications in cryptography and discrete mathematics. Often, bent functions are represented in their algebraic normal form (ANF). It is well known that the linear part of ANF of a bent function can be arbitrary. In this note we prove that a quadratic part of a bent function can be arbitrary too.

**Keywords:** Boolean function, bent function, linear function, quadratic function, homogeneous function.

## 1. INTRODUCTION

Recall that Boolean functions in even number of variables that are on the maximal possible Hamming distance from the set of all affine Boolean functions are called bent functions [7]. Bent functions play an important role in constructions of symmetric ciphers since they help to defend ciphers against linear cryptanalysis[4] and have many applications in discrete mathematics and communications, see [8]. It is well known that every Boolean function can be in the unique way represented in its Algebraic Normal Form (ANF). This representation is used very often for property description and realization of a Boolean function. It is known that bent functions are too far from classification. No conditions on ANF of a Boolean function are known in order to say that the function is bent.

In this paper a new problem in bent functions is stated and studied: is it true that an arbitrary homogeneous Boolean function of degree  $k$  in  $n$  variables ( $n$  is

---

TOKAREVA, N.N., A QUADRATIC PART OF A BENT FUNCTION CAN BE ANY.

© 2022 TOKAREVA, N.N..

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2022-281 with the Ministry of Science and Higher Education of the Russian Federation.

*Received March, 1, 2022, published March, 1, 2022.*

even) is a  $k$ -degree part in ANF of some bent function in  $n$  variables? For small  $k$  it can be formulated like this. Is it true that linear (quadratic, cubic, etc.) part of ANF of a bent function can be arbitrary? For sure, this question is interesting not only for bent functions.

It is well known that a linear part in ANF of a bent function can be arbitrary. Moreover, any linear function can be added to a bent function without changing its property to be bent. In this paper we prove that a quadratic part of a bent function can also be arbitrary. Namely, we prove that an arbitrary quadratic homogeneous Boolean function in  $n$  variables is a quadratic part of some bent function in  $n$  variables, where  $n$  is even,  $n \geq 6$ . For cubic parts the question remains open.

## 2. PRELIMINARIES

We use the following standard notation:

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

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

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

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

$a_1x_1 \oplus \dots \oplus a_nx_n \oplus b$  — an *affine function* in variables  $x_1, \dots, x_n$ , where  $a \in \mathbb{F}_2^n$  and  $b \in \mathbb{F}_2$ , sign  $\oplus$  stands for addition modulo 2 (XOR);

*bent function* — a Boolean function in  $n$  variables ( $n$  is even) that is on the maximal possible Hamming distance from the set of all affine functions. It is known [7] that this distance is equal to  $2^{n-1} - 2^{(n/2)-1}$ ;

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

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

Recall that any Boolean function can be uniquely represented in 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  $\mathbb{F}_2$ . 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  $deg(f)$ . A Boolean function is *affine*, *quadratic*, *cubic* and so on if its degree is not more than 1, or equal to 2, 3, etc.

In what follows let  $n$  be an even number.

According to O.Rothaus (1966, 1976) [7] and V. A. Eliseev, O. P. Stepchenkov (1962) [8], 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. For any possible degree from 2 to  $n/2$  it is not difficult to construct a bent function of such degree.

Several restrictions on ANF of bent functions can be naturally considered. A bent function is called *homogeneous* if all monomials of its ANF are of the same degree. C. Qu, J. Seberri and J. Pieprzyk proved [14] that there are 30 homogeneous bent functions of degree 3 in 6 variables. Partial results on classification of cubic homogeneous bent functions in 8 variables were obtained by C.Charnes et al. in [1].

C. Charney, M. Rotteler and T. Beth [2] have proved the following fact that we will use further.

**Proposition 1.** *There exist cubic homogeneous bent functions in each even number of variables  $n$  for  $n \geq 6$ .*

For the homogeneous bent functions of higher degrees it is known only a little.

### 3. ON THE QUADRATIC PART OF ANF OF A BENT FUNCTION

It is well known that the class of bent functions is closed under addition of affine functions and under affine transformations of variables, see [3]. In other words it holds

**Proposition 2.** *For any bent function  $g$  in  $n$  variables ( $n$  is even,  $n \geq 2$ ) the function  $g'(x) = g(Ax \oplus b) \oplus c_1x_1 \oplus \dots \oplus c_nx_n \oplus d$  is also bent, where  $A$  is a nonsingular matrix,  $b, c$  are arbitrary binary vectors of length  $n$ ,  $d$  is a constant from  $\mathbb{F}_2$ .*

Functions  $g$  and  $g'$  are called *EA-equivalent*.

Note that we can add an arbitrary affine function to a bent function without changing its property to be bent. Recall that it is not possible to find a non affine Boolean function that does the same, since for any non affine Boolean function  $f$  there exists a bent function  $g$  such that  $f \oplus g$  is not bent, see [12], [9]. For instance, it is not possible even to add a quadratic function to all bent functions in order to save their property to be bent. But we want to prove that it is possible to find a bent function with an arbitrary quadratic part of ANF!

In this section we show that an arbitrary quadratic homogeneous Boolean function in  $n$  variables is a quadratic part of some bent function in  $n$  variables, where  $n$  is even,  $n \geq 6$ .

To prove this fact, we need the following statements.

In [6] one can find

**Proposition 3.** *There exist exactly 156 nonisomorphic graphs with 6 vertices.*

In [6] all these graphs can be found. Let us prove first the following result.

**Proposition 4.** *An arbitrary quadratic homogeneous Boolean function in 6 variables is a quadratic part of some bent function in 6 variables.*

*Proof.* Let us put into the correspondence to an arbitrary quadratic homogeneous Boolean function  $f$  in 6 variables a graph  $G_f$  on 6 vertices by the following rule: vertices correspond to variables; there is an edge between two vertices if and only if the product of corresponding variables belongs to ANF of  $f$ .

Consider only those quadratic homogeneous Boolean functions that correspond to nonisomorphic graphs. It is clear that if a quadratic homogeneous function  $f$  is a quadratic part of some bent function then any quadratic homogeneous function  $f'$  with graph  $G_{f'}$  isomorphic to  $G_f$  is also a quadratic part of some bent function. It holds since any permutation on vertices produce an affine transformation of variables and hence by Proposition 2 does not change a property of a function to be bent.

According to Proposition 3 there are exactly 156 nonisomorphic graphs with 6 variables. We prove the statement by listing in the table in Appendix 1 all 156 corresponding (to graphs) homogeneous quadratic Boolean functions and cubic

parts that can be added to them in order to get a bent function in every case. So, the function equal to the sum of the quadratic function from the second column and cubic function from the third column of the table is always bent. Note that we list quadratic parts in the lexicographical order. For every quadratic part we have found a cubic part of the minimal possible length. Sometimes it is of length 0 and we put sign "-" in the table: it means that a quadratic part is already a bent function. Symbol | in both columns should be replaced by  $\oplus$ , and items like 12 and 123 by  $x_1x_2$  and  $x_1x_2x_3$  respectively. We use such short notation in the table for a compactness. Thus, we prove the statement.  $\square$

The following iterative construction was proposed by O. Rothaus (1966, 1976) and J. Dillon (1974), see [8].

**Proposition 5.** *Let  $f'$ ,  $f''$ ,  $f'''$  be bent functions in  $n$  variables such that  $f' \oplus f'' \oplus f'''$  is a bent function too. Then*

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

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

Now let us prove the main result.

**Theorem 1.** *An arbitrary quadratic homogeneous Boolean function in  $n$  variables is a quadratic part of some bent function in  $n$  variables, where  $n$  is even,  $n \geq 6$ .*

*Proof.* Let us prove it by induction. For  $n = 6$  the result follows from Proposition 4. Suppose that it is proven for some  $n$ . Consider the case of  $n + 2$  variables. Let  $x$  be a vector of variables  $(x_1, \dots, x_n)$ . Assume that  $q(x, x_{n+1}, x_{n+2})$  is an arbitrary homogeneous quadratic Boolean function in  $n + 2$  variables. If  $q$  is identically zero, then by Proposition 1 there exists a cubic homogeneous bent function in every number of variables: it will be a bent function with an empty quadratic part.

Let us consider a nonzero  $q$ . Since it is nonzero, there exists at least one item in its ANF. W.l.o.g. suppose that ANF of  $q$  contains item  $x_{n+1}x_{n+2}$ . Otherwise by renumbering of variables we turn to this case. So,  $q(x, x_{n+1}, x_{n+2})$  is of the form:  $q(x, x_{n+1}, x_{n+2}) = h(x) \oplus a(x)x_{n+1} \oplus b(x)x_{n+2} \oplus x_{n+1}x_{n+2}$ , where  $h$  is a homogeneous quadratic Boolean function in  $n$  variables,  $a, b$  are some linear functions in  $n$  variables.

Consider the quadratic homogeneous Boolean function  $h(x) \oplus a(x)b(x)$  in  $n$  variables. By induction, there exists a cubic homogeneous Boolean function  $c(x)$  such that  $f'(x) = c(x) \oplus h(x) \oplus a(x)b(x)$  is a bent function in  $n$  variables. Let  $f''(x) = f'(x) \oplus a(x)$  and  $f'''(x) = f'(x) \oplus b(x)$ . According to Proposition 2 functions  $f''$ ,  $f'''$  are bent too. Note that  $f' \oplus f'' \oplus f'''$  is also bent by the same reason.

Then, by Proposition 5 a Boolean function

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

is a bent function in  $n + 2$  variables. We see that

$$g(x, x_{n+1}, x_{n+2}) = f'(x)(f'(x) \oplus a(x)) \oplus f'(x)(f'(x) \oplus b(x)) \oplus (f'(x) \oplus a(x))(f'(x) \oplus b(x)) \\ \oplus x_{n+1}f'(x) \oplus x_{n+1}(f'(x) \oplus a(x)) \oplus x_{n+2}f'(x) \oplus x_{n+2}(f'(x) \oplus b(x)) \oplus x_{n+1}x_{n+2} = \\ f'(x) \oplus a(x)b(x) \oplus a(x)x_{n+1} \oplus b(x)x_{n+2} \oplus x_{n+1}x_{n+2}.$$

Hence, we get a bent function

$$g(x, x_{n+1}, x_{n+2}) = c(x) \oplus h(x) \oplus a(x)x_{n+1} \oplus b(x)x_{n+2} \oplus x_{n+1}x_{n+2} = c(x) \oplus q(x, x_{n+1}, x_{n+2})$$

in  $n + 2$  variables with prescribed quadratic part  $q(x, x_{n+1}, x_{n+2})$ .  $\square$

#### 4. FUTURE REMARKS

Can a  $k$ -degree part of ANF of a bent function be any?

In particular, 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:  $123 \oplus 14 \oplus 25 \oplus 36$ ,  $123 \oplus 245 \oplus 12 \oplus 14 \oplus 26 \oplus 35 \oplus 45$  and  $123 \oplus 245 \oplus 346 \oplus 14 \oplus 26 \oplus 34 \oplus 35 \oplus 36 \oplus 45 \oplus 46$ , but there are five classes of nonequivalent homogeneous cubic Boolean functions in 6 variables. So, we need to have items of the next degree in order to have a possibility to “put” all variants of the cubic part in a bent function. Here in notation we again use 123 for  $x_1x_2x_3$  and so on.

- 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, see [5]) does not include the list of representatives of EA-classes.

We think it is a very interesting open problem to study in the general case.

In 2011 we have formulated the following hypothesis, see [11].

**Hypothesis 1.** *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,  $n \geq 2$ ).*

The problem to prove or disprove this hypothesis is known now as the *Bent sum decomposition problem*. It is closely connected to the problem of asymptotic of the number of all bent functions.

For now the following is known in relation to this hypothesis.

- Hypothesis is confirmed for  $n = 2, 4, 6$  (see [11] and [13]).
- Hypothesis was proved for quadratic Boolean functions, Maiorana–McFarland bent functions, partial spread functions, see [13].
- A weakened variant of the hypothesis was proved: every Boolean function in  $n$  variables of a constant degree  $d$ , where  $d \leq n/2$ ,  $n$  is even, can be represented as the sum of constant number of bent functions in  $n$  variables, see [10].

Hypothesis 1 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.*

Here we just give an idea that follows from Hypothesis 1 (assuming it holds):  *$k$ -degree part of the ANF of a bent function “tends” to be arbitrary.* It is necessary that at least  $\sqrt{2^{\binom{n}{k}}}$  different variants of  $k$ -degree part of ANF should be realized in a bent function. Recall that the total number of all such variants is  $2^{\binom{n}{k}}$ .

#### 5. CONCLUSION

It is very interesting to study if it is possible to define a bent function through the conditions on ANF. Of course, these questions are interesting in respect to an arbitrary class of cryptographic Boolean functions, not only to bent functions. The author is very grateful to E. Ponomareva for valuable contribution in proving of

Theorem 1, to V. Idrisova for kind help and remarks, and to the reviewer of this paper for the careful reading of the work and comments.

#### REFERENCES

- [1] C. Charney, U. Dempwolff and J. Pieprzyk, *The eight variable homogeneous degree three bent functions*, Journal of Discrete Algorithms, **6**:1 (2008), 66–72.
- [2] C. Charney, M. Rotteler, T. Beth, *Homogeneous bent functions, invariants, and designs*, Designs, Codes and Cryptography, **26**:1–3 (2002), 139–154.
- [3] T. Cusick, P. Stanica, *Cryptographic Boolean Functions and Applications*, Elsevier (2009), ISBN: 9780123748904, 248 pages.
- [4] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, In: Hellesteth T. (eds) Advances in Cryptology EUROCRYPT '93. Lecture Notes in Computer Science, **765** (1994), 386–397.
- [5] P. Langevin, G. Leander, *Counting all bent functions in dimension eight* 99270589265934370305785861242880, Designs, Codes and Cryptography, **59** (2011), 193–205.
- [6] *List of all 156 nonisomorphic graphs on 6 vertices*, <https://users.cecs.anu.edu.au/bdm/data/graphs.html>.
- [7] O. Rothaus, *On bent functions*, Journal of Combinatorial Theory Series A, **20**:3 (1976), 300–305.
- [8] N. Tokareva, *Bent functions: results and applications to cryptography*, Elsevier (2015), ISBN-10: 012802318X. ISBN-13: 978-0128023181, 220 pages.
- [9] N. N. Tokareva, *Duality between bent functions and affine functions*, Discrete Mathematics, **312**:3 (2012), 666–670.
- [10] N. N. Tokareva, *On decomposition of a Boolean function into sum of bent functions*, Siberian Electronic Mathematical Reports, **11** (2014), 745–751.
- [11] N. N. Tokareva, *On the number of bent functions from iterative constructions: lower bounds and hypotheses*, Advances in Mathematics of Communications, **5**:4 (2011), 609–621.
- [12] N. N. Tokareva, *The group of automorphisms of the set of bent functions*, Discrete Mathematics and Applications, **20**:5–6 (2010), 655–664.
- [13] L. Qu, S. Fu, Q. Dai, C. Li, *When a Boolean Function can be Expressed as the Sum of two Bent Functions*, Cryptology ePrint Archive, Report 2014/048, available on <http://eprint.iacr.org/>.
- [14] C. Qu, J. Seberry, J. Pieprzyk, *Homogeneous bent functions*, Discrete Applied Mathematics, **102**:1–2 (2000), 133–139

## APPENDIX 1N

N	homogeneous quadratic function	homogeneous cubic function
1	—	123 125 126 134 136 145 146 156 234 235 245 246 256 345 346 356
2	12	134 136 145 156 235 236 245 246 345 346 356 456
3	12 13	126 136 146 156 234 235 236 245 256 345 346 456
4	12 13 14	234 235 236 246 256 345 356 456
5	12 13 14 15	123 124 126 146 234 236 245 246 256 345 346 356
6	12 13 14 15 16	123 125 134 145 234 235 245 246 256 345 346 356
7	12 13 14 15 16 23	146 156 245 256 345 346 456
8	12 13 14 15 16 23 24	125 134 135 345 356 456
9	12 13 14 15 16 23 24 25	124 125 134 145 345 346 356
10	12 13 14 15 16 23 24 25 26	123 125 135 136 146 234 245 345 346 356
11	12 13 14 15 16 23 24 25 26 34	125 135 156 256 356
12	12 13 14 15 16 23 24 25 26 34 35	124 134 146 246 346
13	12 13 14 15 16 23 24 25 26 34 35 36	124 125 135 145 234 245 345
14	12 13 14 15 16 23 24 25 26 34 35 36 45	—
15	12 13 14 15 16 23 24 25 26 34 35 36 45 46	145 156 235 256 345
16	12 13 14 15 16 23 24 25 26 34 35 36 45 46 56	—
17	12 13 14 15 16 23 24 25 26 34 35 45	123 125 134 136 146
18	12 13 14 15 16 23 24 25 26 34 36 45	—
19	12 13 14 15 16 23 24 25 26 35 36 45 46	134 145 156 234 235 256 345
20	12 13 14 15 16 23 24 25 26 35 46	—
21	12 13 14 15 16 23 24 25 34	—
22	12 13 14 15 16 23 24 25 34 35	124 145 234 246 346
23	12 13 14 15 16 23 24 25 34 35 45	—
24	12 13 14 15 16 23 24 25 34 35 46 56	124 134 135 145 245
25	12 13 14 15 16 23 24 25 34 36	—
26	12 13 14 15 16 23 24 25 35 46	123 126 136
27	12 13 14 15 16 23 24 26 34 35 45	—
28	12 13 14 15 16 23 24 34	125 145 235 256 356
29	12 13 14 15 16 23 24 34 56	—
30	12 13 14 15 16 23 25 26 34	125 135 235
31	12 13 14 15 16 23 25 26 34 35 46	123 124 134
32	12 13 14 15 16 23 25 34	—
33	12 13 14 15 16 24 25 26 34 35	124 145 245
34	12 13 14 15 16 24 25 26 34 35 36	123 125 134 145 235 246 345
35	12 13 14 15 16 24 25 34 35	123 124 145 245 246 256
36	12 13 14 15 16 24 25 34 36	—
37	12 13 14 15 16 24 25 35 36 46	—
38	12 13 14 15 16 24 25 36	124 134 234
39	12 13 14 15 16 24 35	—
40	12 13 14 15 23	126 136 245 256 345 346 456
41	12 13 14 15 23 24	126 134 136 346 356 456
42	12 13 14 15 23 24 25	124 125 126 135 136 145 146 246 345 346 356
43	12 13 14 15 23 24 25 34	126 136 156 256 356
44	12 13 14 15 23 24 25 34 35	124 126 136 146 234 246 346
45	12 13 14 15 23 24 25 34 35 45	146 156 236 256 346
46	12 13 14 15 23 24 25 34 36 46 56	—
47	12 13 14 15 23 24 25 35 46	—
48	12 13 14 15 23 24 25 36	123 145 156 234 456
49	12 13 14 15 23 24 25 36 46	123 135 136 235 356
50	12 13 14 15 23 24 25 36 46 56	134 145 234 235 345
51	12 13 14 15 23 24 26	123 345 346 356
52	12 13 14 15 23 24 26 34	—
53	12 13 14 15 23 24 26 34 35	123 145 146 156
54	12 13 14 15 23 24 26 34 35 45	—
55	12 13 14 15 23 24 26 34 36 45	123 125 126 136 156
56	12 13 14 15 23 24 26 34 36 46 56	124 125 126 136 145
57	12 13 14 15 23 24 26 34 56	123 125 135
58	12 13 14 15 23 24 26 35 36	124 134 234
59	12 13 14 15 23 24 26 35 36 46	123 124 234
60	12 13 14 15 23 24 26 36	—

N	homogeneous quadratic function	homogeneous cubic function
61	12 13 14 15 23 24 26 36 45	—
62	12 13 14 15 23 24 26 36 46 56	123 126 135 136 235 356
63	12 13 14 15 23 24 26 56	123 135 235
64	12 13 14 15 23 24 34	126 146 236 256 356
65	12 13 14 15 23 24 34 56	—
66	12 13 14 15 23 24 36	—
67	12 13 14 15 23 24 36 46	134 235 236 356
68	12 13 14 15 23 24 36 46 56	134 135 345
69	12 13 14 15 23 24 56	123 136 236
70	12 13 14 15 23 25 26 34 35 46	—
71	12 13 14 15 23 25 26 34 36 46 56	123 126 136
72	12 13 14 15 23 25 34	126 136 236
73	12 13 14 15 23 25 36 46	—
74	12 13 14 15 23 26	124 345 346 456
75	12 13 14 15 23 26 36	126 134 245 246 456
76	12 13 14 15 23 26 36 45	124 126 246
77	12 13 14 15 23 26 36 46	—
78	12 13 14 15 23 26 36 46 56	126 135 136 145 246 345
79	12 13 14 15 23 26 46	—
80	12 13 14 15 23 26 46 56	124 145 245
81	12 13 14 15 24 25 26 34 35	124 145 146 156 245
82	12 13 14 15 24 25 26 34 35 36 46 56	124 126 135 136 145 235 236 245 246 345
83	12 13 14 15 24 25 26 34 36	—
84	12 13 14 15 24 25 26 35 36 46	—
85	12 13 14 15 24 25 34 35	123 124 136 146 234 256 346
86	12 13 14 15 24 25 35 36 46	123 124 134
87	12 13 14 15 24 26 34 35	145 146 156
88	12 13 14 15 24 26 35	—
89	12 13 14 15 24 26 35 36	145 146 156
90	12 13 14 15 24 26 35 36 46	—
91	12 13 14 15 24 26 35 36 46 56	123 126 136
92	12 13 14 15 24 35	126 136 236
93	12 13 14 15 24 36	—
94	12 13 14 15 25 36 46	123 136 236
95	12 13 14 15 26	124 125 234 245 345 346 356
96	12 13 14 15 26 36	123 124 126 136 146 234 245 345
97	12 13 14 15 26 36 46	123 134 234 235 245
98	12 13 14 15 26 36 46 56	123 126 135 145 146 234 235 236 246 345
99	12 13 14 23	136 235 246 256 345 356 456
100	12 13 14 23 24	134 135 136 146 156 345 356 456
101	12 13 14 23 24 34	125 126 136 156 235 256 356
102	12 13 14 23 24 34 56	—
103	12 13 14 23 24 35 46	—
104	12 13 14 23 24 56	134 135 136 146 345
105	12 13 14 23 25	126 346 356 456
106	12 13 14 23 25 34 56	124 126 146
107	12 13 14 23 25 35	125 136 246 256 456
108	12 13 14 23 25 35 45	123 124 136 146 256 346
109	12 13 14 23 25 35 46 56	—
110	12 13 14 23 25 36	—
111	12 13 14 23 25 36 45	124 126 146
112	12 13 14 23 25 36 45 56	—
113	12 13 14 23 25 45 56	—
114	12 13 14 23 25 56	—
115	12 13 14 23 26 45 56	134 136 146
116	12 13 14 23 56	—
117	12 13 14 24 25 35	126 136 236
118	12 13 14 24 25 35 36 45	125 126 156
119	12 13 14 24 26 35 36 45 56	125 126 156
120	12 13 14 24 35	126 156 256

N	homogeneous quadratic function	homogeneous cubic function
121	12 13 14 24 35 56	—
122	12 13 14 25	126 234 236 346 356 456
123	12 13 14 25 26	123 135 156 345 346 356
124	12 13 14 25 26 34 35 56	124 125 145
125	12 13 14 25 26 34 56	—
126	12 13 14 25 26 35	—
127	12 13 14 25 26 35 36 45	123 124 126 136 146 234
128	12 13 14 25 26 35 36 45 46	124 135 146 236 256 345
129	12 13 14 25 26 35 45	123 125 134 136 146 234
130	12 13 14 25 26 35 46	—
131	12 13 14 25 26 56	234 235 345
132	12 13 14 25 35	234 236 246 256 356 456
133	12 13 14 25 35 45	123 126 134 136 146 234 236 246
134	12 13 14 25 35 46	125 126 256
135	12 13 14 25 35 46 56	123 126 236
136	12 13 14 25 35 56	234 236 246
137	12 13 14 25 36	—
138	12 13 14 25 56	234 236 346
139	12 13 14 26 35 56	—
140	12 13 14 56	234 235 236 246 345
141	12 13 23	125 126 134 146 156 234 245 256 345 346 456
142	12 13 23 45	126 134 146 156 234 256 346
143	12 13 23 45 46	125 134 145 156 234 256 345
144	12 13 23 45 46 56	124 126 134 135 145 146 156
145	12 13 24	136 145 146 156 235 236 345 356 456
146	12 13 24 34	123 124 126 134 135 145 146 156 235 236 256 356
147	12 13 24 34 56	124 135 136 145 156 245 246
148	12 13 24 45	236 256 356
149	12 13 25 34 45	126 146 246
150	12 13 25 36 45 46	123 124 134
151	12 13 25 45 46	—
152	12 13 25 46	—
153	12 13 45	125 134 156 235 236 246 256 346
154	12 13 45 46	124 125 145 146 156 235 236 256
155	12 34	125 126 135 146 156 236 245 256 356 456
156	12 34 56	—

NATALIA NIKOLAEVNA TOKAREVA

SOBOLEV INSTITUTE OF MATHEMATICS, PR. KOPTYUGA, 4, 630090, NOVOSIBIRSK, RUSSIA

NOVOSIBIRSK STATE UNIVERSITY, PR. PYROGOVA, 2, 630090, NOVOSIBIRSK, RUSSIA

*Email address:* tokareva@math.nsc.ru