S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 13, стр. 888–896 (2016) УДК 519.147
DOI 10.17377/semi.2016.13.071 MSC 05B40

ON PACKINGS OF (n, k)-PRODUCTS

A. V. SAUSKAN, YU. V. TARANNIKOV

Abstract. An (n, k)-product (or simply a product), $n \geq 2k$, is the product of k binomials on the set of n variables; the variables in the product are not repeated. The decomposition of a product is the set of 2^k monomials of length k appearing after expanding the brackets in this product. The sum of some products is called a packing if after the decomposition of all products in this sum every monomial appears at most once. The length of the sum of products is the number of products in this sum. A packing is called perfect if every possible monomial of length k appears exactly once. The problem of packings is motivated by the construction of Boolean functions with cryptographically important properties. In the paper we give recursive constructions of packings of products (including perfect ones) and the corresponding recurrence bounds on their length. We give necessary conditions on the parameters n and k for the existence of a perfect packing of (n, k)-products. We give the complete solution of the problem of the existence of perfect packings of (n, k)-products for $k \leq 3$. We find the exact value for the maximal length of a packing of $(n, 2)$-products for any n.

Keywords: Packings, combinatorial designs, perfect structures, combinatorial constructions, coding theory, Boolean functions, cryptography, nonlinearity, resiliency, maximal possible nonlinearity, bounds.

1. Introduction and preliminaries

The (n, k)-*product* (or simply *the product*) is the product of k binomials on the set of n variables; the variables in the product are not repeated. *The decomposition*

Sauskan, A.V., Tarannikov, Yu. V., On packings of (n, k)-products.
© 2016 Sauskan A.V., Yu.V. Tarannikov.
The work of the second author is supported by RFBR, grant 16–01–00226.
Received August, 22, 2016, published October, 24, 2016.

of a product is the set of 2^k monomials of length k appearing after expanding the brackets in this product. It is assumed that the decomposition of $(n,0)$-product is the monomial of length 0. The sum of some products is called *a packing* if the decompositions of any two products P_i and P_j, $i \neq j$, from the sum do not contain joint monomials. *The length* of the sum of products is the number of products in this sum. The maximal possible length of a packing of (n,k)-products is denoted by $A_{n,k}$. A packing is called *perfect* if every possible monomial of length k appears exactly once.

Remark 1. It is easy to understand that if there exists a perfect packing of (n,k)-products then $A_{n,k} = \frac{\binom{n}{k}}{2^k}$.

Packings of (n,k)-products are used for the construction of cryptographically important Boolean functions (see [5, 7, 8]). More precisely, they are used to construct Boolean functions of n variables that achieve the nonlinearity upper bound $2^{n-1} - 2^{m+1}$ for m-resilient functions.

The following relations on the value $A_{n,k}$ were given in [7]:

Proposition 1. [7] *The following relations hold:*
a) $A_{n,k} \leq \frac{\binom{n}{k}}{2^k}$;
b) $A_{n,k} \leq \binom{n}{2k}$;
c) $A_{n,k} \geq \binom{\lfloor \frac{n}{2} \rfloor}{k}$;
d) $A_{n,k} \geq A_{n-2,k} + A_{n-2,k-1}$ *for* $2 \leq 2k \leq n-2$;
e) $A_{n,0} = 1$;
f) $A_{n,1} = \lfloor \frac{n}{2} \rfloor$;
g) $A_{n,2} = \binom{\frac{n}{2}}{2}$ *for even* n;
h) $A_{n,\lfloor \frac{n}{2} \rfloor} = 1$;
i) $A_{n,\frac{n}{2}-1} = \frac{n}{2}$ *for even* n;
j) $A_{10,3} = 15$.

The following example was given in [5] (in the matrix form) and in [7].

Example 1. Consider the following sum of $(10,3)$-products:

$$(x_1+x_2)(x_3+x_4)(x_5+x_6)+(x_1+x_2)(x_4+x_6)(x_8+x_9)+(x_1+x_2)(x_7+x_9)(x_8+x_{10})+$$
$$(x_1+x_3)(x_2+x_5)(x_7+x_8)+(x_1+x_4)(x_5+x_7)(x_6+x_9)+(x_1+x_5)(x_2+x_3)(x_9+x_{10})+$$
$$(x_1+x_6)(x_3+x_{10})(x_4+x_8)+(x_1+x_7)(x_2+x_{10})(x_5+x_6)+(x_1+x_{10})(x_2+x_7)(x_3+x_4)+$$
$$(x_2+x_8)(x_3+x_7)(x_4+x_9)+(x_2+x_9)(x_5+x_{10})(x_6+x_8)+(x_3+x_5)(x_4+x_9)(x_7+x_{10})+$$
$$(x_3+x_5)(x_6+x_8)(x_7+x_{10})+(x_3+x_8)(x_4+x_6)(x_5+x_9)+(x_4+x_7)(x_6+x_{10})(x_8+x_9).$$

This sum contains 15 products; $2^3 = 8$ monomials appear in the decomposition of each product; all $15 \times 8 = 120$ monomials are different. At the same time there are exactly $\binom{10}{3} = 120$ possible monomials of length 3 of 10 variables. So, we have an example of a perfect packing of $(10,3)$-products.

Corollary 1. *There exists a perfect packing of* $(10,3)$*-products.*

Besides constructions of cryptographically important functions, packings of (n,k)-products have a close connection with other problems of combinatorics and discrete mathematics. So, packings of (n,k)-products can be considered as tiling of Johnson

graph by Boolean cubes. The vertices of the Johnson graph $J(n,k)$ are binary vectors of length n with exactly k ones, two vertices are connected by an edge if and only if corresponding vectors differ in exactly two components. Then it easy to understand that the set of characteristic vectors of all monomials appearing after the decomposition of some (n,k)-product has the structure of k-dimensional Boolean cube in $J(n,k)$. On tiling of graphs see e. g. [1].

Also packings of (n,k)-products relate to the construction of ordered combinatorial designs. Besides classic designs, also different kinds of ordered designs are studied, e. g. Mendelson designs etc. [3, 2]. For example, the case of packings of $(n,3)$-products can be considered as special coverings of the triples by sextuples.

The perfect packings of (n,k)-products have relation to the Hartman halving conjecture [4]. Hartman conjectured that $t-(v,k,\lambda)$-design that contains exactly a half of all possible blocks exists whenever natural conditions of divisibility hold. If in some perfect packings of (n,k)-products we replace all pluses by minuses and after the decomposition of $\sum\prod_{l=1}^{k}(x_{i_l}-x_{j_l})$ take only monomials with pluses (or, contrary, with minuses) then we obtain the $(k-1)-\left(n,k,\frac{n-k+1}{2}\right)$-design. This suggests that the problem of the existence of perfect packings of (n,k)-products is at least not easier than the Hartman halving conjecture for $t=k-1$.

Packings of (n,k)-products can be used also for a compact generation of systems of homogeneous monomials.

The case of perfect packings of $(n,2)$-products was formulated in the terminology of a doubles tennis tournament in a problem at the final stage of the All-Russian Mathematical Olympiad 1993 [6].

2. Results

We denote a packing of (n,k)-products by $P(X,k)$ where X is the set of variables, $|X|=n$. The direct multiplication $P(X,k_1)\times P(Y,k_2)$ of two packings $P(X,k_1)$ and $P(Y,k_2)$, $X\cap Y=\emptyset$ is the collection of (n_1+n_2,k_1+k_2)-products that are all possible multiplications of a product from $P(X,k_1)$ to the product from $P(Y,k_2)$.

In the next proposition we generalize the inequality in Proposition 1, d).

Proposition 2. *The inequality*

$$A_{n_1+n_2,k}\geq\sum_{i=0}^{k}A_{n_1,i}\cdot A_{n_2,k-i}$$

holds.

Proof. Let $|X|=n_1$, $|Y|=n_2$. We form the following union of direct multiplications of products packings:

$$\bigsqcup_{i=0}^{k}U_i,\qquad U_i=P\left(X,i\right)\times P\left(Y,k-i\right)$$

where $P(X,i)$ are the corresponding packings of length $A_{n_1,i}$; $P(Y,k-i)$ are the corresponding packings of length $A_{n_2,k-i}$.

It is easy to check that $\bigsqcup_{i=0}^{k}U_i$ is a packing of length $\sum_{i=0}^{k}A_{n_1,i}\cdot A_{n_2,k-i}$ of (n_1+n_2,k)-products. □

Proposition 3. *The inequality*

$$A_{n-1,k-1} \geq \frac{2k}{n} A_{n,k}$$

holds.

Proof. Consider a maximum packing P of length $A_{n,k}$ of (n,k)-products. The total number of variable appearances in P is $2kA_{n,k}$; some variable x_i appears in at least $\frac{2k}{n}A_{n,k}$ products. Cancel all products without x_i; cancel the brackets with x_i in all remaining products. We obtain a packing of $(n-1,k-1)$-products of length at least $\frac{2k}{n}A_{n,k}$. □

Corollary 2. *If there exists a perfect packing of (n,k)-products then there exists a perfect packing of $(n-1,k-1)$-products.*

Proof. If there exists a perfect packing of (n,k)-products then by Remark 1 we have

$$A_{n,k} = \frac{\binom{n}{k}}{2^k}.$$

By Proposition 3 it follows

$$A_{n-1,k-1} \geq \frac{2k}{n} A_{n,k} = \frac{2k}{n} \cdot \frac{\binom{n}{k}}{2^k} = \frac{\binom{n-1}{k-1}}{2^{k-1}}.$$

So, by Remark 1 we obtain a perfect packing of $(n-1,k-1)$-products. □

Example 2. In Example 1 we had a perfect packing of $(10,3)$-products. Take the variable x_1 (for instance). Cancel all products without x_1, cancel the brackets with x_1 in all remaining products. We obtain a packing of $(9,2)$-products of length 9:

$$\begin{gathered}(x_3+x_4)(x_5+x_6)+(x_4+x_6)(x_8+x_9)+(x_7+x_9)(x_8+x_{10})\\ +(x_2+x_5)(x_7+x_8)+(x_5+x_7)(x_6+x_9)+(x_2+x_3)(x_9+x_{10})\\ +(x_3+x_{10})(x_4+x_8)+(x_2+x_{10})(x_5+x_6)+(x_2+x_7)(x_3+x_4).\end{gathered}$$

Corollary 3. *There exists a perfect packing of $(9,2)$-products.*

In Theorem 1, we give a necessary condition for the existence of a perfect packing of (n,k)-products.

Theorem 1. *If there exists a perfect packing of (n,k)-products, $k \geq 1$, then*

$$n \equiv k-1 \pmod{2^{d_k}}$$

where $d_k = \max\{d_{k-1}, k+p(k)\}$, $d_0 = 0$, $p(k)$ is the maximal power of 2 that divides k.

Proof. The proof is by induction on k. For $k=1$ the statement is obvious. Suppose that the statement is true for $k-1$, $k \geq 2$; prove it for k.

By Corollary 2 and the induction assumption we have $n-1 \equiv k-2 \pmod{2^{d_{k-1}}}$. It follows that

$$n \equiv k-1 \pmod{2^{d_{k-1}}}. \tag{1}$$

By Remark 1 the value $\frac{\binom{n}{k}}{2^k}$ is integer; it follows that $n(n-1)\dots(n-k+1)$ is divisible by $k! \cdot 2^k$. By (1) we have $n-k+1 \equiv 0 \pmod{2^{d_{k-1}}}$. By definition of

d_k we have $k-1 \le d_{k-1} < 2^{d_{k-1}}$. Therefore the maximal power of 2 that divides $n-k+1+i$ is the same as for i, $i = 1, \ldots, k-1$. Thus, $n-k+1$ must be divisible by $k \cdot 2^k$. It follows

$$n - k + 1 \equiv 0 \pmod{2^{k+p(k)}}. \tag{2}$$

Combining (1) and (2) we complete an inductive step. □

Some initial values of d_k are given in the following table.

k	d_k	k	d_k
1	1	9	11
2	3	10	11
3	3	11	11
4	6	12	14
5	6	13	14
6	7	14	15
7	7	15	15
8	11	16	20

It easy to see that

$$k \le d_k \le k + \log_2 k. \tag{3}$$

The lower bound in (3) is achieved (at least) when $k = 2^t - 1$; the upper bound in (3) is achieved when $k = 2^t$ where t is integer.

Theorem 2. *Suppose that there exists a perfect packing of (n_1, k)-products and there exists a perfect packing of (n_2, k)-products. Then there exists a perfect packing of $(n_1 + n_2 - k + 1, k)$-products.*

Proof. By Corollary 2 for all $i = 0, 1, \ldots, k$ there exist perfect packings of $(n_1 - i, k - i)$-products and perfect packings of $(n_2 - i, k - i)$-products. Let $|X| = n_1 - k + 1$, $|Y| = n_2 - k + 1$, $Z = \{z_1, z_2, \ldots, z_{k-1}\}$.

We form the following union of products packings:

$$\bigsqcup_{i=0}^{k} U_i, \qquad U_i = P\left(X \sqcup \left\{\bigsqcup_{j=1}^{i-1} z_j\right\}, i\right) \times P\left(Y \sqcup \left\{\bigsqcup_{j=i+1}^{k-1} z_j\right\}, k-i\right), \tag{4}$$

where $P(.\,,.)$ are the corresponding perfect packings.

We will demonstrate that any monomial of length k at the set $X \sqcup Y \sqcup Z$ appears exactly once after expanding the brackets in products from (4). Suppose that a monomial M contains exactly s_x variables from X, exactly s_y variables from Y (and exactly $k - s_x - s_y$ variables from Z). Denote by $s'_{z,i}$ the number of variables from $\{z_1, z_2, \ldots, z_{i-1}\}$ in the monomial M, and by $s''_{z,i}$, the number of variables from $\{z_{i+1}, z_{i+2}, \ldots, z_{k-1}\}$ in M. If $s_x = 0$ then the monomial M can appear only in U_0, and it really appears there. If $s_y = 0$ then the monomial M can appear only in U_k, and it really appears there. Let $s_x > 0$, $s_y > 0$. Then the monomial M can appear after expanding the brackets only in such direct multiplications U_i of packings, $1 \le i \le k-1$, that the two equalities

$$S'_i = s_x + s'_{z,i} - i = 0; \tag{5}$$

and

$$S''_i = s_y + s''_{z,i} - k + i = 0. \tag{6}$$

hold simultaneously. On the other hand, if conditions (5) and (6) hold simultaneously, it provides the appearance of the monomial M. For $i = 0$ we have $S'_0 > 0$, whereas for $i = k$, obviously, it holds $S'_k \le 0$. Beginning with $i = 0$, we start to increase i by 1. When we go from i to $i+1$, the value S'_i

$$\begin{cases} \text{decreases by 1,} & \text{if the variable } z_i \text{ is not contained in the monomial } M, \\ \text{does not change} & \text{if the variable } z_i \text{ is contained in the monomial } M \end{cases} \tag{7}$$

whereas the value S''_i

$$\begin{cases} \text{increases by 1,} & \text{if the variable } z_{i+1} \text{ is not contained in the monomial } M, \\ \text{does not change} & \text{if the variable } z_{i+1} \text{ is contained in the monomial } M. \end{cases} \tag{8}$$

Therefore for some $i = i_0 > 0$ the value S'_i will be equal to 0 for the first time, i. e., $S'_{i_0-1} > 0$, $S'_{i_0} = 0$.

Summarizing the equations (5) and (6) for $i = i_0$, we have $S''_{i_0} = S'_{i_0} + S''_{i_0} = s_x + s_y + s'_{z,i_0} + s''_{z.i_0} - k$, which implies that

$$S''_{i_0} = \begin{cases} 0, & \text{if the variable } z_{i_0} \text{ is not contained in the monomial } M, \\ -1, & \text{if the variable } z_{i_0} \text{ is contained in the monomial } M. \end{cases} \tag{9}$$

If the case $S''_{i_0} = 0$ takes place then both (5) and (6) are satisfied, and the monomial M appears in the direct multiplication U_{i_0} (we will check the uniqueness a bit later). Suppose that the case $S''_{i_0} = -1$ takes place. Then by (9) the variable z_{i_0} is contained in the monomial M, which together with (7) yields $S'_{i_0+1} = 0$. Let l be the smallest number greater than i_0 such that the variable z_l is not contained in the monomial M (this number exists since $S''_k \ge 0$). Then by (7) and (8) we have $S'_l = S''_l = 0$, i. e. the monomial M appears in the direct multiplication U_l.

Now we demonstrate that the monomial M appears in a unique U_i. Let l be the smallest number such that $S'_l = S''_l = 0$. Then by (8) and (9) the variable z_l is not contained in M, which together with (7) yields $S'_{l+1} < 0$. Thus, the uniqueness is proved, which completes the proof of the theorem. □

Corollary 4. *For $n \equiv 2 \pmod 8$, $n \ge 6$, there exists a perfect packing of $(n,3)$-products.*

Proof. The statement follows from the existence of a perfect packing of $(10,3)$-products (see Example 1) and Theorem 2. □

Theorem 3. *A perfect packing of $(n,3)$-products, $n \ge 6$, exists if and only if $n \equiv 2 \pmod 8$.*

Proof. The statement follows from Theorem 1 and Corollary 4. □

Corollary 5. *For $n \equiv 1 \pmod 8$, $n \ge 4$, there exists a perfect packing of $(n,2)$-products.*

Proof. The statement follows from Corollary 4 and Corollary 2. □

Corollary 6. *A perfect packing of $(n,2)$-products, $n \ge 4$, exists if and only if $n \equiv 1 \pmod 8$.*

Proof. The statement follows from Theorem 1 and Corollary 5. □

Corollary 6 was given in another terminology as a problem at the final stage of the All-Russian Mathematical Olympiad 1993; the author of the problem is Sergey I. Tokarev [6].

Theorems 1, 3 and Corollary 6 state that the smallest open case for the existence of a perfect packing of (n, k)-products is $n = 67$, $k = 4$.

The construction in Theorem 2 works not only for perfect packings.

Proposition 4. *The following recurrent inequality takes place*

$$A_{n_1+n_2-k+1,k} \geq \sum_{i=0}^{k} A_{n_1-k+i,i} \cdot A_{n_2-i,k-i}.$$

Proof. We use the same construction (4) as in the proof of Theorem 2; it is sufficient to be restricted by considerations that any monomial appears in at most one direct multiplication of packings. Naturally, by the fact that the corresponding packings are not necessarily perfect, after expanding the brackets some monomials of length k can be absent. □

Theorem 4. *The value $A_{n,2}$ is expressed by the following formulas*

$$A_{n,2} = \begin{cases} \frac{n(n-2)}{8} & \text{if } n \text{ is even,} \\ \frac{n(n-1)}{8} & \text{if } n \equiv 1 \pmod 8, \\ \frac{(n+2)(n-3)}{8} & \text{if } n \equiv 3 \pmod 8, \\ \frac{(n+3)(n-4)}{8} & \text{if } n \equiv 5 \pmod 8, \\ \frac{(n+1)(n-2)}{8} - 1 & \text{if } n \equiv 7 \pmod 8. \end{cases}$$

Proof. The case $n \equiv 1 \pmod 8$ follows from Corollary 5 and Remark 1. The formula for the case of even n was already given in Proposition 1, g), but we prove it for completeness.

Suppose that n is even. Then for any variable x_i the number $n-1$ of another variables is odd. Any $(n, 2)$-product gives in the decomposition two monomials that contain x_i. So, each variable can appear in at most $(n-2)/2$ products. Summarizing over all variables, we obtain that the total number of products in the packing does not exceed $n(n-2)/8$. At the same time it is possible to form such number of products if we join variables into pairs and multiply the sum of any pair to the sum of any other pair.

Now suppose that $n \equiv 3, 5, 7 \pmod 8$. Represent n as $n = n_1 + n_2 - 1$, $n_1 \equiv 1 \pmod 8$, $n_2 \in \{3, 5, 7\}$. Apply the construction (4) where $k = 2$, $|X| = n_1 - 1$, $|Y| = n_2 - 1$, $Z = \{z_1\}$. In this particular case the construction has the form

$$\bigsqcup_{i=0}^{k} U_i,$$
$$U_0 = P\left(Y \bigsqcup \{z_1\}, 2\right),$$
$$U_1 = P(X, 1) \times P(Y, 1),$$
$$U_2 = P\left(X \bigsqcup \{z_1\}, 2\right)$$

where $P(X \bigsqcup \{z_1\}, 2)$ is a perfect packing of $(n_1, 2)$-products, $P(X, 1) \times P(Y, 1)$ is the direct multiplication of a perfect packing of $(n_1 - 1, 1)$-products to a perfect packing of $(n_2 - 1, 1)$-products.

The decomposition of all products from U_2 contains $\frac{n_1(n_1-1)}{2}$ monomials. The decomposition of all products from U_1 contains $(n_1-1)(n_2-1)$ monomials.

Take as U_0 the following set of products:

$$U_0 = \begin{cases} \emptyset & \text{if } n_2 = 3, \\ \{(x_1+x_2)(x_3+x_4)\} & \text{if } n_2 = 5, \\ \{(x_1+x_2)(x_3+x_4),(x_2+x_4)(x_6+x_7), \\ (x_1+x_3)(x_5+x_6),(x_1+x_5)(x_2+x_7)\} & \text{if } n_2 = 7. \end{cases}$$

So, the total number of monomials in the decompositions of all products from $U_0 \bigsqcup U_1 \bigsqcup U_2$ is

$$N = \begin{cases} (n_1-1)\left(\frac{n_1}{2}+2\right) & \text{if } n_2 = 3, \\ (n_1-1)\left(\frac{n_1}{2}+4\right)+4 & \text{if } n_2 = 5, \\ (n_1-1)\left(\frac{n_1}{2}+6\right)+16 & \text{if } n_2 = 7. \end{cases}$$

Thus, the total number of monomials that do not appear in the decompositions of products from $U_0 \bigsqcup U_1 \bigsqcup U_2$ is

$$\frac{n(n-1)}{2} - N = \begin{cases} 3 & \text{if } n_2 = 3, \\ 6 & \text{if } n_2 = 5, \\ 5 & \text{if } n_2 = 7. \end{cases}$$

Any additional $(n,2)$-product gives 4 monomials. Therefore, the constructed packing $U_0 \bigsqcup U_1 \bigsqcup U_2$ is maximum for $n_2 = 3$. In the cases $n_2 = 5$ and $n_2 = 7$ if the constructed packing $U_0 \bigsqcup U_1 \bigsqcup U_2$ is not maximum then the maximum packing does not contain exactly $6-4=2$ and $5-4=1$ monomials, respectively. At the same time, for odd n the value $N^-(P)$ of monomials that do not appear in the decompositions of products from any packing P of $(n,2)$-products cannot be equal 1 or 2. Indeed, if some monomial x_ix_j does not belong to the decompositions of products then there exist at least one such monomial $x_ix_{j'}$, $j' \neq i,j$, and at least one such monomial $x_{i'}x_j$, $i' \neq i,j$, since n is odd. Therefore, if $N^-(P) > 0$ then $N^-(P) \geq 3$. By this reason the constructed packing $U_0 \bigsqcup U_1 \bigsqcup U_2$ is maximum in all cases under consideration. This completes the proof of theorem. □

3. Acknowledgements

The authors are grateful to Prof. Denis S. Krotov and the anonymous referee for valuable remarks that improved the presentation of this paper. The authors are grateful to Prof. Ilya I. Bogdanov and Evgeniy V. Khinko for pointing out on the Problem 447 in [6, pp. 58, 276–277].

References

[1] Avgustinovich S. V., *Multidimensional permanents in enumeration problems*, Journal of Applied and Industrial Mathematics, **4**:1 (2010), 19–20.

[2] Cameron P. J., *A generalisation of t-designs*, Discrete Math., **309**:14 (2009), 4835–4842. Zbl 1186.05024

[3] Colbourn C. J., Dinitz J. H., *The CRC handbook of Combinatorial Designs*, (2nd ed.), (2007), Boca Raton: Chapman & Hall/ CRC, ISBN 1–58488–506–8. Zbl 1101.05001

[4] Hartman A., *Halving the complete design*, Ann. Discrete Math., **34** (1987), 207–224. Zbl 0643.05013

[5] Tarannikov Y. V., *Generalized proper matrices and constructing of m-resilient Boolean functions with maximal nonlinearity for expanded range of parameters*, Siberian Electronic Mathematical Reports, **11** (2014) 229–245 (http://semr.math.nsc.ru/v11/p229-245.pdf). Zbl 06510889

[6] Agahanov N. H., Bogdanov I. I., Kozhevnikov P. A., Podlipskij O. K., Tereshin D. A., *Vserossijskie olimpiady shkol'nikov po matematike 1993–2006: Okruzhnoj i final'nyj jetapy*, Pod red. N. H. Agahanova, M.: MCNMO, 2007, Problem 447, pp. 58, 276–277 (in Russian).

[7] Tarannikov Yu. V., *Nesokratimye razlozhenija odnorodnyh proizvedenij dvuchlenov dlja postroenija m-ustojchivyh funkcij s maksimal'no vozmozhnoj nelinejnost'ju*, Problemy teoreticheskoj kibernetiki. Materialy XII mezhdunarodnoj konferencii (Kazan, 16–20 June 2014), Kazan': Otechestvo, (2014), 271–272 (in Russian).

[8] Tarannikov Yu. V., *O vozmozhnosti postroenija m-ustojchivyh funkcij s optimal'noj nelinejnost'ju v ramkah odnogo metoda*, Materialy XII Mezhdunarodnogo seminara «Diskretnaja matematika i ee prilozhenija» imeni akademika O. B. Lupanova (Moscow, MSU, 20–25 June 2016.), M.: Izd-vo mehaniko-matematicheskogo fakul'teta MSU, (2016), 394–397 (in Russian).

Andrey Vladimirovich Sauskan
nab. Admirala Tributsa, 37–20,
236006, Kaliningrad, Russia
E-mail address: super.irinka55555@yandex.ru

Yuriy Valer'evich Tarannikov
Mech. & Math. Department,
Lomonosov Moscow State University,
119992, Moscow, Russia
E-mail address: yutarann@gmail.com