



Problem 10. «Bent decompositions»

Problem for a special prize!

Boolean bent functions are studied since 60-s of XX century in connection to cryptographic applications of them and their generalizations, [1].

We invite you to study the following open problem: is it true that an arbitrary Boolean function in n variables (n is even, $n \geq 2$) of degree not more than $n/2$ can be represented as the sum of two bent functions in n variables?

This question was raised in 2011 in close connection with the problem of the asymptotic value of the number of all bent functions in n variables. There is a hypothesis that the answer is «yes». For now all known facts confirm the hypothesis. The hypothesis was checked for $n = 2, 4, 6$ and for some special classes of Boolean functions.

Could you obtain new results in connection to this hypothesis?

More details. A Boolean function $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ in an even number of variables n is called a *bent function* if it is at the maximum Hamming distance from the set of all affine Boolean functions in n variables. Equivalently, the Walsh–Hadamard transform of f ,

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}, \quad y \in \mathbb{Z}_2^n,$$

takes only the values $\pm 2^{n/2}$. The set of all bent functions in n variables is denoted by $\mathcal{B}_n$.

Hypothesis. Let n be an even positive integer. Then every Boolean function in n variables of degree at most $n/2$ can be represented as the sum of two bent functions in n variables. In other words, for every Boolean function f in n variables with $\deg f \leq n/2$, there exist bent functions $g, h \in \mathcal{B}_n$ such that $f = g \oplus h$.

The hypothesis was stated in [2] and verified by computer for $n \leq 6$ in [2; 3].

Known results.

- It is proved in [4] that every Boolean function in n variables of degree d , where $d \leq n/2$ and n is even, can be represented as the sum of a constant number of bent functions in n variables. The constant depends on d and n .
- Every cubic Boolean function in 8 variables is the sum of not more than 4 bent functions in 8 variables, see [4].
- A bent function is decomposable into the sum of two bent functions if and only if its dual bent function is also decomposable, see [5].
- It is proved in [6] that the hypothesis holds for $n \leq 6$; every quadratic Boolean function in n variables is the sum of two bent functions. It is shown that every Maiorana–MacFarland bent function and every partial spread function for an arbitrary n are also decomposable.

• It is proved in [7] that every bent function in 8 variables of degree at most 3 can be represented as the sum of two bent functions in 8 variables; every quadratic Boolean function in an even number of variables $n \geq 4$ can be represented as the sum of two bent functions of a special form.

The problem. Please, try to prove or disprove the hypothesis. You can consider some partial subclasses of Boolean functions for the investigation. Here are variations of classes:

- All Boolean functions of degree 4 in 8 variables.
- All cubic Boolean functions for all even n .
- All Boolean functions of degree $\leq n/2$ that depend essentially on at most $n/2 + c$ variables, where $c \geq 2$.
- Decomposition to sum of a constant number of bent functions, where the constant does not depend on n .

References

- [1] O. S. Rothaus. On bent functions // J. Combin. Theory Ser. A, 1976. V. 20. N 3 P. 300–305.
- [2] N. Tokareva. On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances in Mathematics of Communications, 2011, V 5. N 4. P. 609–621.
- [3] Qu L. and Li C. New results on the Boolean functions that can be expressed as the sum of two bent functions // IEICE Trans. Fund. Elect. Commun. Comput. Sci. 2016. V. 99-A. N 8. P. 1584–1590.
- [4] N. N. Tokareva. On decomposition of a Boolean function into sum of bent functions // Siberian Electronic Mathematical Reports, 2014. V 11. P. 745–751.
- [5] N. Tokareva. Bent functions: results and applications to cryptography // Acad. Press. Elsevier, 2015. 220 pages.
- [6] L. Qu, S. Fu, Q. Dai, C. Li. When a Boolean Function can be Expressed as the Sum of two Bent Functions // IACR Cryptology ePrint Archive, Report 2014/048, 2014.
- [7] A. S. Shaporenko. Derivatives of bent functions in connection with the bent sum decomposition problem. Designs, Codes and Cryptography, 2023. V. 91. N 5. P. 1607–1625.