Kutsenko, A. V.; **Tokareva, N. N.**

Metrical properties of the set of bent functions in view of duality. (English) Zbl 07312022

Prikl. Diskretn. Mat. 2020, No. 49, 18-34 (2020).

Summary: In the paper, we give a review of metrical properties of the entire set of bent functions and its significant subclasses of self-dual and anti-self-dual bent functions. We present results for iterative construction of bent functions in $n + 2$ variables based on the concatenation of four bent functions and consider related open problem proposed by one of the authors. Criterion of self-duality of such functions is discussed. It is explored that the pair of sets of bent functions and affine functions as well as a pair of sets of self-dual and anti-self-dual bent functions in $n \geq 4$ variables is a pair of mutually maximally distant sets that implies metrical duality. Groups of automorphisms of the sets of bent functions and (anti-)self-dual bent functions are discussed. The solution to the problem of preserving bentness and the Hamming distance between bent function and its dual within automorphisms of the set of all Boolean functions in n variables is considered.

MSC:

94D10 Boolean functions

Keywords:

Boolean bent function; self-dual bent function; Hamming distance; metrical regularity; automorphism group; iterative construction

Full Text: DOI MNR

References:

[1] Rothaus O. S., "On bent functions", J. Combin. Theory. Ser. A, 20:3 (1976), 300-305 · Zbl 0336.12012

[2] Tokareva N., Bent Functions: Results and Applications to Cryptography, Acad. Press, Elsevier, 2015, 230 pp. · Zbl 1372.94002

[3] Carlet C., Mesnager S., "Four decades of research on bent functions", Des. Codes Cryptogr., 78:1 (2016), 5-50 · Zbl 1378.94028

[4] Mesnager S., Bent Functions: Fundamentals and Results, Springer, Berlin, 2016, 544 pp. · Zbl 1364.94008

[5] Kolomeec N., "The graph of minimal distances of bent functions and its properties", Des. Codes Cryptogr., 85:3 (2017), 1-16 · Zbl 1417.94138

[6] Janusz G. J., "Parametrization of self-dual codes by orthogonal matrices", Finite Fields Appl., 13:3 (2007), 450-491 · Zbl 1138.94389

[7] Dillon J., Elementary Hadamard Difference Sets, PhD. dissertation, Univ. Maryland, College Park, 1974

[8] Carlet C., "Boolean functions for cryptography and error correcting codes", Boolean Models and Methods in Mathematics, Computer Science, and Engineering, eds. Y. Crama, P. L. Hammer, Cambridge University Press, Cambridge, 2010, 257-397 · Zbl 1209.94035

[9] Hou X.-D., "New constructions of bent functions", J. Combin. Inform. System Sci., 25:1-4, Proc. Intern. Conf. Combinatorics, Inform. Theory and Statistics (2000), 173-189 · Zbl 1219.94079

[10] Cusick T. W., Stănică P., Cryptographic Boolean Functions and Applications, Acad. Press, London, 2017, 288 pp. · Zbl 1359.94001

[11] Tokareva N. N., "On the number of bent functions from iterative constructions: lower bounds", Adv. Math. Commun., 5:4 (2011), 609-621 · Zbl 1238.94032

[12] Tokareva N. N., "On decomposition of a Boolean function into sum of bent functions", Siberian Electronic Math. Reports, 11 (2014), 745-751 · Zbl 1325.94143

[13] Tokareva N. N., "On decomposition of a dual bent function into sum of two bent functions", Prikladnaya Diskretnaya Matematika, 2014, no. 4(26), 59-61 (in Russian)

[14] Kutsenko A., "The group of automorphisms of the set of self-dual bent functions", Cryptogr. Commun., 12:5 (2020), 881-898

[15] Hou X.-D., "Classification of self dual quadratic bent functions", Des. Codes Cryptogr., 63:2 (2012), 183-198 · Zbl 1264.06021

[16] Carlet C., Danielson L. E., Parker M. G., Solé P., "Self-dual bent functions", Int. J. Inform. Coding Theory, 1 (2010), 384-399 · Zbl 1204.94118

[17] Feulner T., Sok L., Solé P., Wassermann A., "Towards the classification of self-dual bent functions in eight variables", Des.

Codes Cryptogr., 68:1 (2013), 395-406 · Zbl 1280.94053

[18] Hyun J. Y., Lee H., Lee Y., "MacWilliams duality and Gleason-type theorem on self-dual bent functions", Des. Codes Cryptogr., 63:3 (2012), 295-304 · Zbl 1259.94071

[19] Mesnager S., "Several new infinite families of bent functions and their duals", IEEE Trans. Inf. Theory, 60:7 (2014), 4397-4407 · Zbl 1360.94480

[20] Rifà J., Zinoviev V. A., On binary quadratic symmetric bent and almost bent functions, 2019, arXiv:

[21] Mesnager S., "On constructions of bent functions from involutions", Proc. ISIT, 2016, 110-114

[22] Coulter R., Mesnager S., "Bent functions from involutions over \(\mathbb{F}_{2^n} \)", IEEE Trans. Inf. Theory, 64:4 (2018), 2979-2986 · Zbl 1392.94966

[23] Luo G., Cao X., Mesnager S., "Several new classes of self-dual bent functions derived from involutions", Cryptogr. Commun., 11:6 (2019), 1261-1273 · Zbl 1460.11147

[24] Sok L., Shi M., Solé. P., "Classification and construction of quaternary self-dual bent functions", Cryptogr. Commun., 10:2 (2018), 277-289 · Zbl 1412.94257

[25] Kutsenko A., "Metrical properties of self-dual bent functions", Des. Codes Cryptogr., 88:1 (2020), 201-222 · Zbl 07149379

[26] Kutsenko A. V., "The Hamming distance spectrum between self-dual Maiorana-McFarland bent functions", J. Appl. Industr. Math., 12:1 (2018), 112-125 · Zbl 1413.94045

[27] McFarland R. L., "A family of difference sets in non-cyclic groups", J. Combin. Theory. Ser. A, 15:1 (1973), 1-10 · Zbl 0268.05011

[28] MacWilliams F. J., Sloane N. J. A., The Theory of Error-Correcting Codes, North-Holland, Amsterdam-New York-Oxford, 1983, 782 pp. · Zbl 0369.94008

[29] Canteaut A., Charpin P., "Decomposing bent functions", IEEE Trans. Inform. Theory, 49:8 (2003), 2004-2019 · Zbl 1184.94230

[30] Preneel B., Van Leekwijck W., Van Linden L., et al., "Propagation characteristics of Boolean functions", Advances in Cryptology-EUROCRYPT, LNCS, 473, 1990, 161-173 · Zbl 0764.94024

[31] Climent J.-J., Garcia F. J., and Requena V., "A construction of bent functions of \(n+2\) variables from a bent function of \(n\) variables and its cyclic shifts", Algebra, 2014 (2017), 701298, 11 pp. · Zbl 1327.94038

[32] Canteaut A., Daum M., Dobertin H., Leander G., "Finding nonnormal bent functions", Discrete Appl. Math., 154:2 (2006), 202-218 · Zbl 1091.94021

[33] Stănică P., Sasao T., Butler J. T., "Distance duality on some classes of Boolean functions", J. Combin. Math. Combin. Computing, 107 (2018), 181-198 · Zbl 1432.94228

[34] Oblaukhov A., "A lower bound on the size of the largest metrically regular subset of the Boolean cube", Cryptogr. Commun., 11:4 (2019), 777-791 · Zbl 1456.94102

[35] Tokareva N., "Duality between bent functions and affine functions", Discrete Math., 312:3 (2012), 666-670 · Zbl 1234.94068

[36] Markov A. A., "On transformations without error propagation", Selected Works, v. II, Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Informatics and Related Topics, MTsNMO Publ., M., 2003, 70-93 (in Russian)

[37] Dempwolff U., "Automorphisms and equivalence of bent functions and of difference sets in elementary Abelian 2-groups", Commun. Algebra, 34:3 (2006), 1077-1131 · Zbl 1085.05019

[38] Tokareva N. N., "The group of automorphisms of the set of bent functions", Discrete Math. Appl., 20:5-6 (2010), 655-664 · Zbl 1211.94057

[39] Danielsen L. E., Parker M. G., Solé P., "The Rayleigh quotient of bent functions", LNCS, 5921, 2009, 418-432 · Zbl 1234.06010